KASPERSKY lab

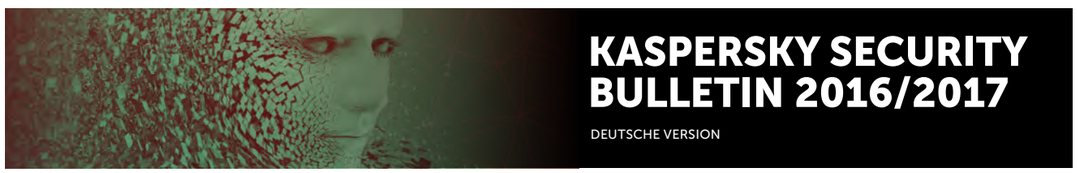
Kaspersky Lab Global Research and Analysis Team (GReAT)

KASPERSKY SECURITY BULLETIN 2016/2017

DEUTSCHE VERSION

GREAT

INHALT



KASPERSKY SECURITY BULLETIN 2016/2017

Stefan Rojacher
Corporate Communications Manager DACH
Kaspersky Lab

Autor: Stefan Rojacher

JAHRESANALYSE VON KASPERSKY LAB FÜR 2016 UND 2017

Cybersicherheitsthemen hielten uns 2016 in Atem. Das Jahr begann mit einem Cybersabotageangriff auf das ukrainische Stromnetz. Locky, TeslaCrypt und andere Ransomware-Erpresser verschlüsselten unsere Daten und forderten Lösegeld. Angriffe auf beliebte Handy-Apps wie Pokemon Go oder Apps von Banken zielten direkt auf unsere Geldbörse. Cyberbankräuber erbeuteten über einen Angriff auf das SWIFT-System von der Zentralbank in Bangladesch über 100 Millionen US-Dollar.

Spektakulär auch eine Attacke aus dem Internet der Dinge auf die Deutsche Telekom – 900.000 Betroffene in Deutschland. Noch im Dezember wurden wir Zeuge von einem Datenleck bei Yahoo – über 1 Milliarde Nutzerkonten fielen in die Hände Cyberkrimineller.

Mit dem Kaspersky Security Bulletin 2016/2017 veröffentlicht Kaspersky Lab seine Analyse der Cybergefahren und deren Entwicklungen für das vergangene Jahr sowie eine Prognose für zukünftige Internetgefahren und Angriffsszenarien. Neben den wichtigsten Ereignissen und Statistiken liefert der Jahresbericht auch Tipps zur Cybersicherheit.

> From threats to protection technologies

Was erwartet uns im nächsten Jahr?

Ransomware wird leider ein Thema bleiben. Geldautomaten rücken zunehmend ins Visier Cyberkrimineller. Und im Vorfeld der Bundestagswahl im September kann es zu einem Informationskrieg im Internet kommen. Die Hintermänner der Cyberangriffe bleiben im Dunkeln und finden immer neue Wege, sich zu tarnen.

Aber die Cybersicherheitsindustrie hat Lösungen parat. Insbesondere so genannte Security Intelligence und Technologien, die mit künstlicher Intelligenz arbeiten, sorgen für ein hohes Schutzniveau in Unternehmen und bei Privatanwendern.

Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexer und aufkommender Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter **http://www.kaspersky.com/de/**. Kurzinformationen erhalten Sie zudem über **www.twitter.com/Kaspersky_DACH** und **www.facebook.com/Kaspersky.Lab.DACH**. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter **www.viruslist.de** und auf dem **Kaspersky-Blog auf http://blog.kaspersky.de/** abrufbar.

KASPERSKY SECURITY BULLETIN 2016/2017. STATISTIK FÜR 2016

Autor(en): Maria Garnaeva, Fedor Sinitsyn, Yury Namestnikov, Denis Makrushin, Alexander Liskin

QUICK INFO

DAS JAHR IN ZAHLEN

VON CYBERKRIMINELLEN AUSGENUTZTE ANGREIFBARE ANWENDUNGEN

SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)

- Top 10 der Länder, auf deren Ressourcen Schadprogramme untergebracht sind
- Top 20 der Schadprogamme im Internet
- Verschlüsselungsprogramme
  - Zahl der neuen Verschlüsselungsprogramme der Klasse Trojan-Ransom
  - Zahl der von Verschlüsselungsprogrammen angegriffenen Nutzer
  - Geografie der Attacken
  - Top 10 der am weitesten verbreiteten Familien von Verschlüsselungstrojanern
  - Verschlüsselungs-Ransomware und der Unternehmenssektor
- Online-Bedrohungen im Bankensektor
  - Geografie der Attacken
  - Top 10 der Banken-Schädlinge
- Länder, in denen Computer dem größten Risiko einer Infektion über das Internet ausgesetzt sind

LOKALE BEDROHUNGEN

- Top 20 der auf den Computern der Anwender entdeckten schädlichen Objekte
- Länder, in denen die Computer dem höchsten Risiko einer lokalen Infektion ausgesetzt waren

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
STATISTIK FÜR 2016

Die unten stehenden Statistiken beruhen auf den Daten, die von verschiedenen Komponenten der Produkte von Kaspersky Lab gesammelt wurden. Alle im Bericht verwendeten statistischen Daten wurden mit Hilfe des verteilten Antiviren-Netzwerks Kaspersky Security Network (KSN) zusammengetragen und ausgewertet. Die Daten stammen von den KSN-Anwendern, die ihre Zustimmung zur Übertragung der Informationen gegeben haben. An dem globalen Informationsaustausch über die Virenaktivität nehmen Millionen von Anwender von Kaspersky-Produkten aus 213 Ländern der Welt teil.

DAS JAHR IN ZAHLEN

- Im Laufe des Jahres waren **31,9** Prozent der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt.
- Die Lösungen von Kaspersky Lab wehrten **758.044.650** Attacken ab, die von Internet-Ressourcen aus verschiedenen Ländern der Welt durchgeführt wurden.
- Die Komponenten von Kaspersky Anti-Virus erkannten **261.774.932** individuelle, schädliche URLs.
- **29,1** Prozent der von Kaspersky-Produkten blockierten Webattacken wurden unter Verwendung schädlicher Webressourcen durchgeführt, die sich in den USA befinden.
- Im Laufe des gesamten Jahres erkannte Kaspersky Anti-Virus **69.277.289** individuelle schädliche Objekte.
- **1.445.434** Computer von individuellen Nutzern wurden von Verschlüsselungs-Malware angegriffen.
- Die Produkte von Kaspersky Lab wehrten auf den Geräten von **2.871.965** Anwendern Versuche ab, schädliche Software zu starten, die auf den Diebstahl von Geld via Online-Zugriff auf Bankkonten spezialisiert ist.
- Kaspersky Anti-Virus erkannte **4.071.588** schädliche und potenziell unerwünschte Programme auf den Computern der Anwender.

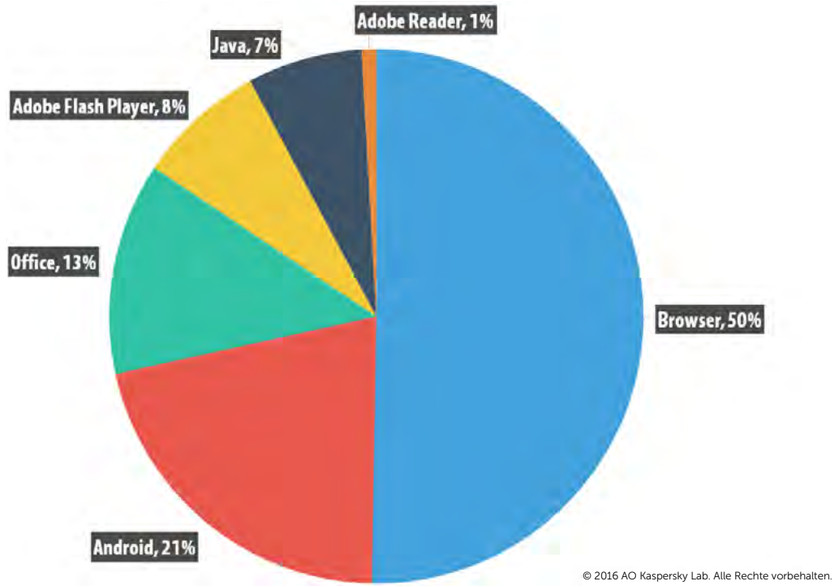
VON CYBERKRIMINELLEN AUSGENUTZTE ANGREIFBARE ANWENDUNGEN

Im Jahr 2016 haben viele wichtige Player den Exploit-Kit-Markt verlassen. Im zweiten Quartal des Jahres verschwanden die Giganten Angler und Nuclear von der Bildfläche, nachdem sie jahrelang den Markt dominiert hatten. Das bedeutete für die Online-Verbrecher, dass sie nun auf andere Exploit-Kits umsteigen mussten, und daher fiel der furiose Aufstieg von Neutrino ebenfalls in dieses Quartal. Doch die Prominenz währte nicht lange, denn auch dieses Exploit-Kit verließ kurz darauf, im dritten Quartal, wieder den Markt. Zum Ende des Jahres 2016 werden die Exploit-Kits Rig und Magnitude weiterhin aktiv genutzt; Rig hat die Lücke ausgefüllt, die Neutrino hinterlassen hatte, und wir beobachten, dass es immer weitere Verbreitung findet.

Wie bereits im Vorjahr erfreuten sich auch im Laufe des Jahres 2016 Exploits für den Adobe Flash Player einer großen Nachfrage. Vier der entsprechenden Sicherheitslücken schafften es in die Liste der am häufigsten von Cyberkriminellen ausgenutzten Sicherheitslücken:

- CVE-2015-8651 (Adobe Flash)
- CVE-2016-1001 (Adobe Flash)
- CVE-2016-0034 (Microsoft Silverlight)
- CVE-2015-2419 (Internet Explorer)
- CVE-2016-4117 (Adobe Flash)
- CVE-2016-4171 (Adobe Flash)

Da der Markt von Exploit-Kits dominiert wurde, die typischerweise Sicherheitslücken im Adobe Flash Player angreifen, hat der Anteil von Flash gegenüber dem Vorjahr deutlich zugenommen, und zwar von drei auf acht Prozent.



Verteilung der von Cyberkriminellen in ihren Attacken verwendeten Exploits nach Typen der angreifbaren Anwendungen, 2016

Das Rating der angreifbaren Anwendungen basiert auf Daten über die von unseren Produkten blockierten Exploits, die von Cyberkriminellen sowohl in Attacken über das Internet als auch bei Angriffen auf lokale Anwendungen verwendet werden, unter anderem auch auf die mobilen Geräte der Anwender.

Im Jahr 2016 ist auch der Anteil von Exploits für Sicherheitslücken in Microsoft-Office-Programmen gestiegen – von vier Prozent im letzten Jahr auf 13 Prozent in diesem Jahr. Der Grund dafür war eine Schadspam-Flut, die Exploits für Microsoft Office enthielt. Doch zum Ende des Jahres nahm diese Art von Spam wieder ab.

Der Anteil von Exploits, die sich gegen das mobile Betriebssystem Android richten, beträgt 21 Prozent, ein Zuwachs von sieben Prozentpunkten. Dieser Anstieg ist in erster Linie der zunehmenden Zahl aufkommender Exploits geschuldet, die eine Erweiterung der Privilegien auf Rootrechte auf einem mobilen Gerät ermöglichen.

Insgesamt konnten wir feststellen, dass sich ein langfristiger Trend auch im Jahr 2016 fortgesetzt hat: Exploits für Sicherheitslücken im Adobe Flash Player, in Microsoft Office und im Internet Explorer erfreuen sich unter Cyberkriminellen nach wie vor der größten Beliebtheit. Im oben abgebildeten Tortendiagramm werden die Exploits für den Internet Explorer als Browser-Exploits klassifiziert (50 % aller Exploits), wie auch die Detektionen von Landingpages, über die die Exploits in Umlauf gebracht werden.

SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)

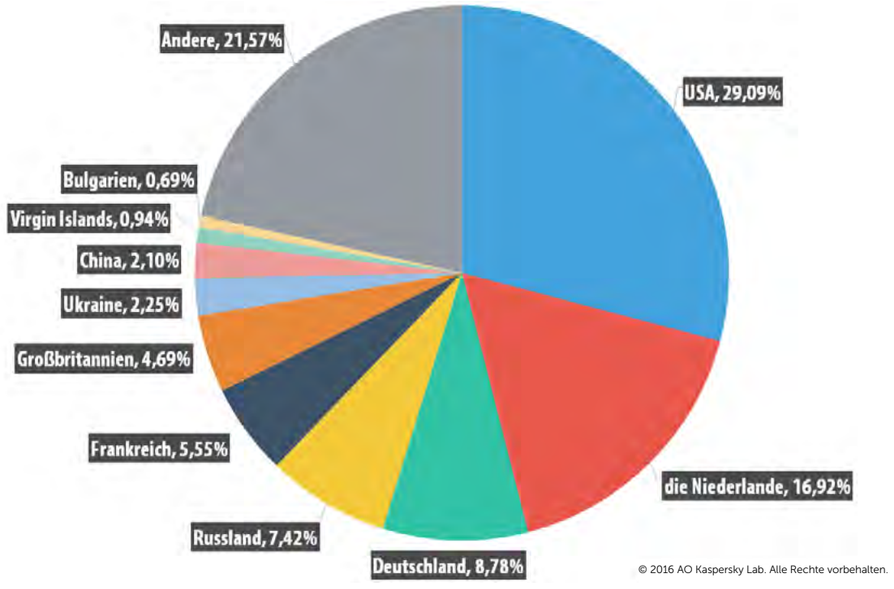
Die statistischen Daten in diesem Abschnitt basieren auf dem Modul Kaspersky Anti-Virus, das die Nutzer in dem Moment schützt, in dem Schadcode von einer schädlichen oder infizierten Webseite geladen wird. Schädliche Webseiten werden von Cyberkriminellen speziell zu diesem Zweck erstellt. Infiziert sein können Webressourcen, deren Inhalt von den Nutzern selbst generiert wird (zum Beispiel Foren) und gehackte legitime Ressourcen.

Im Laufe des gesamten Jahres 2016 erkannte Kaspersky Anti-Virus **69.277.2889** individuelle schädliche Objekte (zum Beispiel Skripte, Exploits und ausführbare Dateien) und stufte **261.774.932** individuelle URLs als schädlich ein. Die Lösungen von Kaspersky Lab wehrten **758.044.650** Attacken ab, die von Internet-Ressourcen aus 212 verschiedenen Ländern der Welt durchgeführt wurden.

Top 10 der Länder, auf deren Ressourcen Schadprogramme untergebracht sind

Diese Statistik zeigt die Verteilung der Quellen der von Kaspersky Anti-Virus blockierten Webattacken auf die Computer der KSN-Teilnehmer nach Ländern (zum Beispiel Webseiten mit Redirects auf Exploits, Webseiten mit Exploits und anderen Schadprogrammen sowie Steuerungszentren von Botnetzen). Jeder individuelle Host kann der Ursprung einer oder mehrerer Webattacken sein. In dieser Statistik wurden die Verbreitungsquellen von Adware sowie Hosts, die mit der Tätigkeit von Werbeprogrammen in Verbindung stehen, nicht berücksichtigt.
Zur Bestimmung der geografischen Ursprünge der Attacken werden der Domain-Name und die reale IP-Adresse gegenübergestellt, auf der die entsprechende Domain untergebracht ist. Zudem bestimmen die Kaspersky-Experten die geografische Herkunft der jeweiligen IP-Adresse (GEOIP).

Zur Durchführung der **758.044.650** Attacken über das Internet, die die Lösungen von Kaspersky Lab im Jahr 2016 blockierten, verwendeten die Cyberkriminellen 3.014.685 individuelle Hosts.
Insgesamt 78 Prozent der Benachrichtigungen über die Blockierung von Attacken entfielen auf Angriffe von Webressourcen, die sich in insgesamt zehn Ländern der Welt befinden.



Verteilung der Quellen von Webattacken nach Ländern
(November 2015 bis Oktober 2016)

↺ ZURÜCK ZUM INHALT

Die ersten neun Positionen in der Liste der Länder, auf deren Ressourcen Malware untergebracht ist, blieben gegenüber dem vorangegangenen Jahr unverändert. Die Niederlande und Deutschland haben die Plätze getauscht, ebenso China und die Jungferninseln. Schweden ist nicht mehr unter den ersten Zehn und wurde von Bulgarien (Platz zehn) ersetzt.

Top 20 der Schadprogramme im Internet

Im Laufe des gesamten Jahres 2016 erkannte Kaspersky Anti-Virus **69.277.289** individuelle schädliche Objekte (Samples, die einen eindeutigen Hash-Wert haben, zum Beispiel Skripte, Exploits und ausführbare Dateien). Im Laufe des Jahres wurden auf 15,6 Prozent aller Computer, auf denen Kaspersky Anti-Virus Alarm geschlagen hat, Werbeprogramme und deren Komponenten registriert. Von allen Schadprogrammen, die im Jahr 2016 an Internet-Attacken beteiligt waren, hat das Kaspersky-Team nachfolgend die 20 aktivsten aufgeführt.

Auf diese 20 Programme entfielen 96,6 Prozent aller Internet-Attacken.

	NAME*	PROZENTUALER ANTEIL AN ALLEN ATTACKEN**
1	Malicious URL	77.26
2	Trojan-Clicker.HTML.Iframe.dg	8.15
3	Trojan.Script.Generic	6.74
4	Trojan.Script.Iframer	3.14
5	Trojan-Downloader.Script.Generic	0.35
6	Exploit.Script.Generic	0.20
7	Packed.Multi.MultiPacked.gen	0.15
8	Trojan.JS.FBook.bh	0.13
9	Exploit.Script.Blocker	0.11
10	Trojan-Downloader.JS.Iframe.div	0.11
11	Trojan.JS.Redirector.ns	0.09
12	Trojan-Dropper.VBS.Agent.bp	0.08
13	Trojan-Downloader.JS.Agent.hjc	0.08
14	Trojan.JS.Iframe.ako	0.07
15	Trojan.Win32.Generic	0.06
16	Trojan.Win32.Generic	0.06
17	Trojan.JS.Agent.ckf	0.05
18	Trojan-Spy.HTML.Fraud.gen	0.05
19	Trojan.Win32.Invader	0.04
20	Exploit.SWF.Agent.gen	0.04

* Von Kaspersky Anti-Virus erkannte Objekte. Die Informationen stammen von KSN-Teilnehmern, die der Übermittlung von statistischen Daten zugestimmt haben.

** Anteil an allen Web-Attacken der Malware, die auf den Computern einzelner KSN-Teilnehmer registriert wurden.

Wie so oft setzen sich auch diese Top 20 in erster Linie aus Objekten zusammen, die bei Drive-by-Attacken eingesetzt werden. Sie werden mit heuristischen Methoden als Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic, etc. detektiert.

Auf Platz eins befinden sich Malicious URL. Darunter fallen Links aus unserer Schwarzen Liste (Links auf Webseiten mit Redirects auf Exploits, Webseiten mit Exploits und anderen Schadprogrammen, Steuerungsserver von Botnetzen, Erpresser-Webseiten und so weiter).

Das Skript Trojan.JS.FBook.bh erhält einen Link von einer bestimmten C&C-Adresse, um den Status des Nutzers auf Facebook zu aktualisieren, dem Status einen Link hinzuzufügen und alle Freunde des Nutzers zu markieren. Ein Klick auf den Link führt zu der Installation einer Browser-Erweiterung, die sich Zugriff auf den Facebook-Account des Nutzers verschafft, und das bedeutet, dass sie dann verschiedenste Aktionen im Namen des Nutzers durchführen kann. Unter anderem ist sie auch in der Lage, ein Verbreitungsschema zu etablieren.

Trojan-Downloader.JS.Agent.hjc ist ein „dynamischer" Klicker, der auf einen C&C-Server zugreift, um die Konfigurationsdatei zu lesen; diese Datei enthält einen Link, der in ein iframe integriert und besucht wird, wenn der User auf die Webseite klickt.

Als Trojan-Spy.HTML.Fraud.gen werden HTML-Phishing-Seiten detektiert, die sich als Internetshop ausgeben oder als Webseite einer Bank, und die in einer Phishing-Webmail enthalten sind.

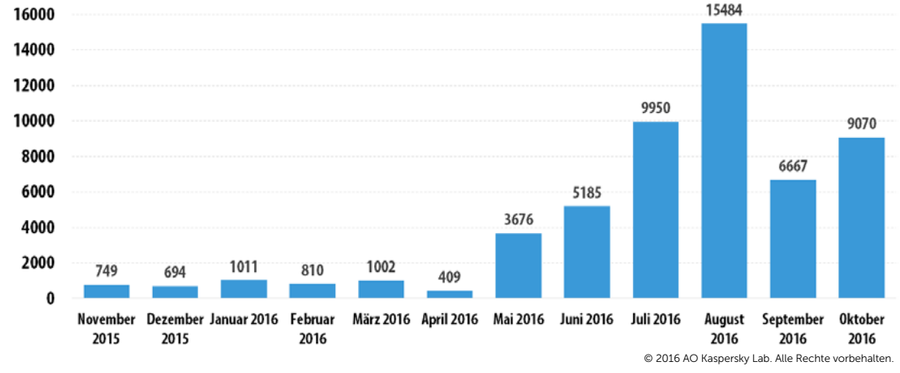
Verschlüsselungsprogramme

Die Bedrohung durch erpresserische Verschlüsselungsprogramme nimmt immer weiter zu. Sowohl die Zahl der neuen Familien als auch die Zahl der neuen Modifikationen ist in der zweiten Jahreshälfte gestiegen. Mit erschreckender Regelmäßigkeit erscheinen immer wieder neue Trojaner, von denen sich die meisten als halbherzig ausgeführte und weitgehend wirkungslose Experimente unqualifizierter Entwickler erweisen. Doch einige unter ihnen, wie Locky, Cerber und CryptXXX, haben sich zu den wichtigsten neuen Bedrohungen sowohl für individuelle Nutzer als auch für Unternehmen entwickelt. Unterdessen haben auch ältere Trojaner wie CTB-Locker, CryptoWall und TorrentLocker den Betrieb nicht eingestellt, und die Kriminellen hinter diesen Schädlingen sind nicht scharf darauf, dass ihre Kampagnen stillgelegt werden – so wie im Fall von TeslaCrypt.

↺ ZURÜCK ZUM INHALT

Zahl der neuen Verschlüsselungsprogramme der Klasse Trojan-Ransom

Im Laufe des Jahres detektierten wir über **54.000 Modifikationen** von Verschlüsselungs-Ransomware und entdeckten **62 neue Familien**.

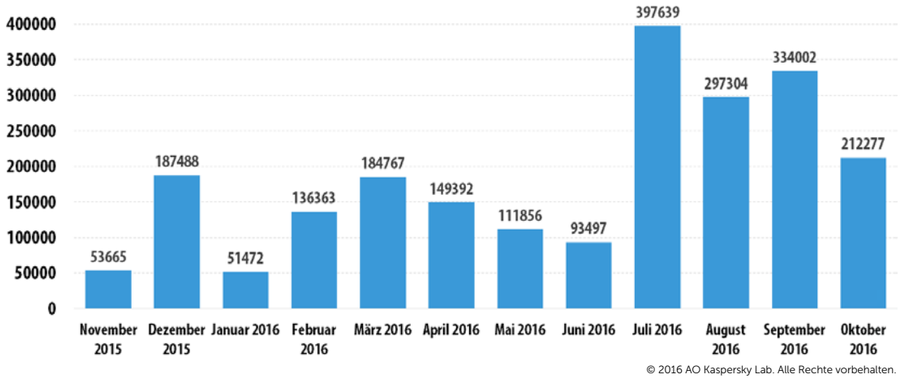


Zahl der neuen Modifikationen von Verschlüsselungsprogrammen der Klasse Trojan-Ransom (November 2015 bis Oktober 2016)

Die Gesamtzahl der Modifikationen von Verschlüsselungsprogrammen in unserer Virenkollektion beträgt aktuell mindestens **65.000**.

Zahl der von Verschlüsselungsprogrammen angegriffenen Nutzer

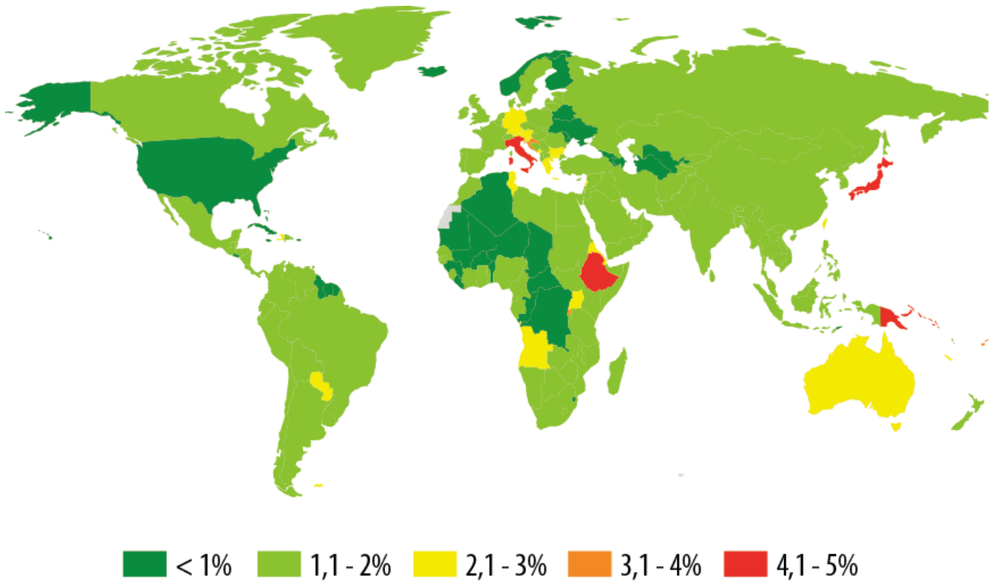
Im Jahr 2016 wurden **1.445.434 individuelle KSN-Nutzer** von Verschlüsselungsschädlingen angegriffen.



Zahl der von Verschlüsselungs-Malware der Klasse Trojan-Ransom angegriffenen Nutzer (November 2015 bis Oktober 2016)

Man sollte unbedingt bedenken, dass die tatsächliche Anzahl von Vorfällen um ein Vielfaches höher ist. Diese Statistik bezieht nur die Resultate der Signatur-basierten und der heuristischen Erkennung ein, doch die Produkte von Kaspersky Lab detektieren Verschlüsselungstrojaner in den meisten Fällen auch mit Hilfe von verhaltensbasierten Methoden.

Geografie der Attacken



Geografie der Angriffe von Verschlüsselungs-Malware der Klasse Trojan-Ransom im Jahr 2016 (prozentualer Anteil der angegriffenen Nutzer)

Top 10 der von Verschlüsselungsschädlingen angegriffenen Länder

	LAND*	PROZENTUALER ANTEIL DER VON VERSCHLÜSSELUNGS-MALWARE ANGEGRIFFENEN NUTZER**
1	Japan	4.46
2	Italien	4.17
3	Kroatien	3.23
4	Luxemburg	3.15
5	Bulgarien	2.86
6	Uganda	2.55
7	Tunesien	2.54
8	Österreich	2.45
9	Hong Kong	2.43
10	Libanon	2.39

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 50.000 liegt.

** Prozentualer Anteil der individuellen Nutzer, deren Computer von Verschlüsselungsprogrammen der Klasse Trojan-Ransom angegriffen wurden, an allen individuellen Nutzern von Kaspersky-Lab-Produkten in diesem Land.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
STATISTIK FÜR 2016

Top 10 der am weitesten verbreiteten Familien von Verschlüsselungstrojanern

	NAME	DETEKTIERT ALS*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

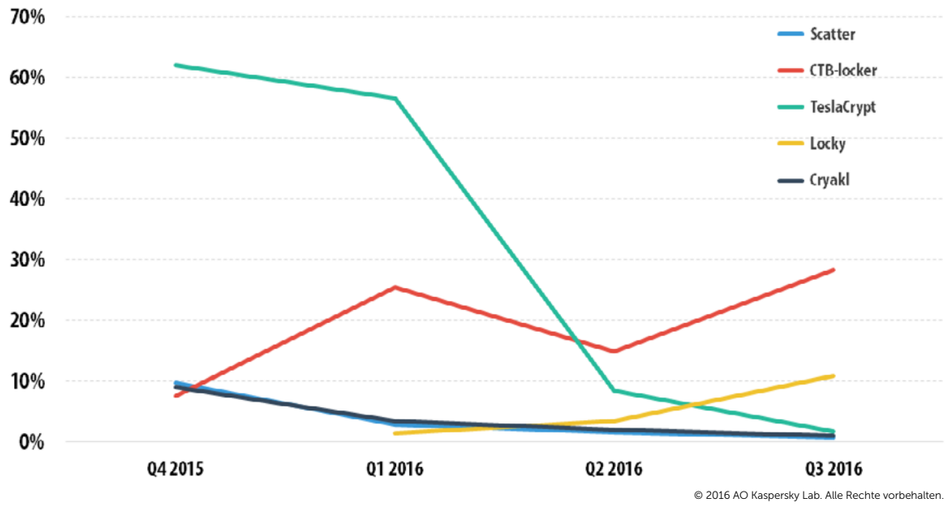
* Die Statistik basiert auf Daten der Produkte von Kaspersky Lab, deren Anwender der Übermittlung statistischer Informationen zugestimmt haben.

** Prozentualer Anteil der von einer bestimmten Trojan-Ransom-Familie angegriffenen individuellen Nutzer von Kaspersky-Lab-Produkten an allen von einem Schädling der Klasse Trojan-Ransom angegriffenen Nutzern.

Die Top 10 setzen sich zum größten Teil aus berüchtigten Trojanern zusammen, die in den letzten Jahren in Erscheinung getreten sind: CTB-Locker, CryptoWall, Shade, Cryakl, TeslaCrypt, Scatter, Cryrar. Doch auch zwei neue Verschlüsselungsschädlinge, die erst im Jahr 2016 auf den Plan getreten sind, und zwar Locky und Crysis, gehören jetzt schon zu den zehn am weitesten verbreiteten Schädlingen ihrer Art.

Die neuen erpresserischen Verschlüsselungsprogramme, die wir im Laufe des Jahres 2016 entdeckt haben, sind ihren Vorgängern auffallend ähnlich. Die gängigsten Codierungsschemata, die typischerweise von Ransomware verwendet werden, sind schon allgemein bekannt und die Kriminellen müssen nicht mit neuen, unorthodoxen Methoden aufwarten, wenn sie neue Trojaner entwickeln. Die Programmierer von Ransomware verwenden heute bevorzugt langzeiterprobte Methoden bei der Implementierung der Dateiverschlüsselung und konzentrieren ihre Anstrengungen vielmehr auf neue Techniken, um ein Reverse Engineering zu vermeiden und die Detektion zu verhindern.

Gleichzeitig haben wir aber auch sehr viele neue Verschlüsselungsprogramme entdeckt, die eindeutig von „unqualifizierten" Programmierern entwickelt wurden. Diese Familien zeichnen sich normalerweise aus durch Code von minderer Qualität, viele Fehler und Schwachstellen in der Kryptografie, die Verwendung primitiver Algorithmen und Methoden und manchmal sogar durch Grammatikfehler in den Lösegeldforderungen. Die Samples erreichen selten eine hohe Auflage, aber über die reine Zahl dieser neuen Familien von „Amateur"-Ransomware kann man nicht einfach hinwegsehen. Offensichtlich zieht die Gier nach dem schnellen Geld durch Erpressung und die ausführliche Berichterstattung über Ransomware in den Medien mehr und mehr Verbrecher an, die eigentlich auf andere Betrugsarten spezialisiert sind.



Top 5 der am weitesten verbreiteten Familien von Verschlüsselungstrojanern nach Quartalen (Anteil der angegriffenen Nutzer)

Der Anteil der von Teslacrypt betroffenen Nutzer ist rapide zurückgegangen – was nach der Stilllegung dieser Kampagne im zweiten Quartal 2016 auch zu erwarten war.

Locky hingegen, der erstmals im ersten Quartal 2016 in Erscheinung trat, ist auf dem aufsteigenden Ast. CTB-Locker führt das Feld nach dem Niedergang von Teslacrypt weiter an. Cryakl und Scatter, die beide in erster Linie russischsprachige Länder angreifen, verlieren immer weiter an Boden.

Verschlüsselungs-Ransomware und der Unternehmenssektor

Im Jahr 2016 fanden etwa 22,6 Prozent der Attacken von Verschlüsselungs-Ransomware auf individuelle Nutzer in einem Unternehmensumfeld statt. Die zehn im Unternehmenssektor am weitesten verbreiteten Verschlüsselungsschädlinge sind nahezu identisch mit denen, die im oben stehenden Ranking aufgelistet sind. Allerdings gibt es eine bemerkenswerte Ausnahme, und zwar ist die Rede von Trojan-Ransom.Win32.Rakhni, der 2,42 Prozent aller Unternehmensnutzer ins Visier nahm, die im Jahr 2016 von Verschlüsselungs-Ransomware angegriffen wurden.

Trojan-Ransom.Win32.Rakhni wird mit Hilfe von Trojan-Downloader.Win32.Rakhni in Umlauf gebracht. Bei diesem Downloader handelt es sich um eine ausführbare Datei, die in ein .docx-Dokument eingefügt wurde, das wiederum zumeist als Anhang an Spam-Mails verbreitet wird. Die Hintermänner von Rakhni greifen eindeutig den Unternehmenssektor (insbesondere Personalabteilungen) in russischsprachigen Ländern an, denn der Name der Word-Datei soll den Empfänger denken lassen, dass es sich dabei um eine Bewerbung handelt (zum Beispiel „Резюме Жанна.docx" = „Lebenslauf Jeanne.docx"). Wenn das Opfer die .docx-Datei öffnet, wird ihm das Icon eines PDF-Readers angezeigt. Mit einem Klick auf das Icon wird der schädliche Downloader ausgeführt. Um nicht umgehend Misstrauen zu erregen, zeigt der Trojaner dem Opfer einen scheinbar perfekten Lebenslauf an.

Менеджер по работе с клиентами

Общая информация

Заработная плата: **от 35 000 руб.**
Характер работы: На территории работодателя
График работы: Полный рабочий день

Образование: Высшее
Опыт работы: 11 лет 2 месяца
Возраст: 28 лет (11 февраля 1988)

Опыт работы 11 лет 9 месяцев

Период работы: сентябрь 2008 — по настоящее время
Должность: **Менеджер отдела прямых продаж**
Компания: ООО "Протек"
Обязанности: Оптово-розничная продажа дверей
стратегическое планирование и развитие продаж;
составление бюджетов продаж и расходов отдела;
анализ эффективности работы отдела;
разработка мероприятий по увеличению объемов продаж отдела;
оперативное управление отделом: организация работы, координация, контроль выполнения плана продаж, составление отчетов;
контроль дебиторской задолженности, работа с просроченной задолженностью;

Период работы: август 2007 — сентябрь 2008 (1 год 2 месяца)
Должность: **Специалист по документообороту**
Компания: ООО Биокад
Обязанности: Прием и распределение тел звонков, работа с оргтехникой, архивация документов, деловая переписка, организация и планирование деловых встреч руководителей, контроль исполнения приказов и распоряжений.

Период работы: январь 2005 — август 2007 (2 года 8 месяцев)
Должность: **Ассистент менеджера**
Компания: ООО ПКФ Эрион
Обязанности: Ведение делопроизводства, оформление документов при закупке/продаже товаров.

Образование

Образование: Высшее
Окончание: 2010 год
Учебное заведение: МЭСИ
Факультет: Менеджмент организации
Специальность: Менеджер по конкурентоспособности

Дополнительная информация

Иностранные языки: Английский (Базовый)
Водительские права: Категория B
Владение компьютером: Эксперт
Возможность командировок: Есть
Навыки и умения: Высокие коммуникативные навыки, хорошие аналитические способности, умение работать в команде и с большим объемом информации, знание 1С программы "Управление торговлей 8.0"

Lebenslauf, den Trojan-Downloader.Win32.Rakhni seinen Opfern anzeigt

Unterdessen fährt der Trojaner damit fort, die Haupt-Payload herunterzuladen – den Verschlüsselungsschädling Trojan-Ransom.Win32.Rakhni, der die Dateien chiffriert und die Lösegeldforderung anzeigt.

Die KSN-Daten belegen, dass die Kriminellen hinter Rakhni nicht wirklich daran interessiert sind, Einzelpersonen anzugreifen, und sie wissen ganz genau, wie sie ganz gezielt Unternehmen ins Visier nehmen. Diese Familie ist nicht in den allgemeinen Top 10 vertreten, aber im Unternehmenssektor gehört sie zu den am weitest verbreiteten erpresserischen Verschlüsselungsschädlingen.

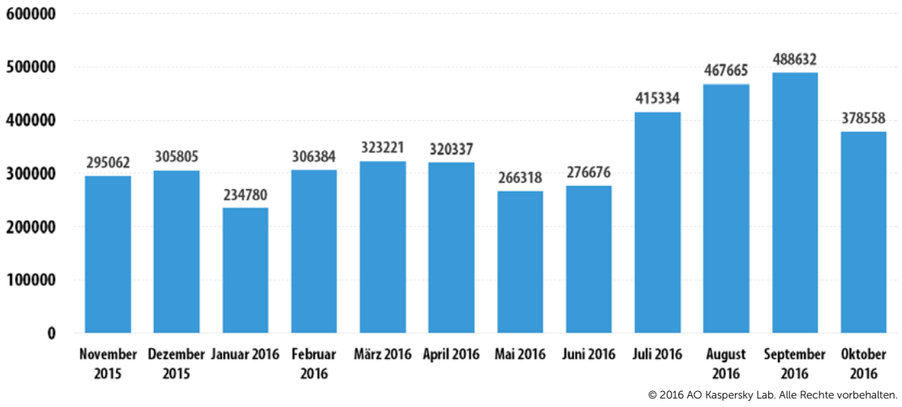
Online-Bedrohungen im Bankensektor

Die vorliegende Statistik basiert auf den Detektionen von Kaspersky Anti-Virus. Sie wurden von Nutzern der Produkte von Kaspersky Lab zur Verfügung gestellt, die ihre Zustimmung zur Übermittlung statistischer Daten gegeben haben.

Die Statistik für das Jahr 2016 beruht auf Daten, die zwischen November 2015 und Oktober 2016 gesammelt wurden.

Da ständig neue Vertreter von Bank-Trojanern erscheinen und die Funktionalität der bereits bekannten Bank-Schädlinge fortwährend verändert wird, haben wir im zweiten Quartal 2016 die Liste der Objekte, die zur Klasse der Bank-Bedrohungen gehören, grundlegend aktualisiert. Aus diesem Grund weicht die Zahl der Opfer von Finanzschädlingen von den in den letzten Jahren veröffentlichten Daten deutlich ab. Zum Vergleich haben wir die Statistik für das vorangegangene Jahr unter Berücksichtigung aller Schädlinge aus der aktualisierten Liste neu berechnet.

Im Jahr 2016 wehrten die Lösungen von Kaspersky Lab auf den Geräten von **2.871.965** KSN-Anwendern Ausführungsversuche von Software ab, die auf den Diebstahl von Finanzmitteln über den Online-Zugriff auf Bankkonten spezialisiert ist. Das ist ein um 46 Prozent höherer Wert als im Jahr 2015 (1.966.324).



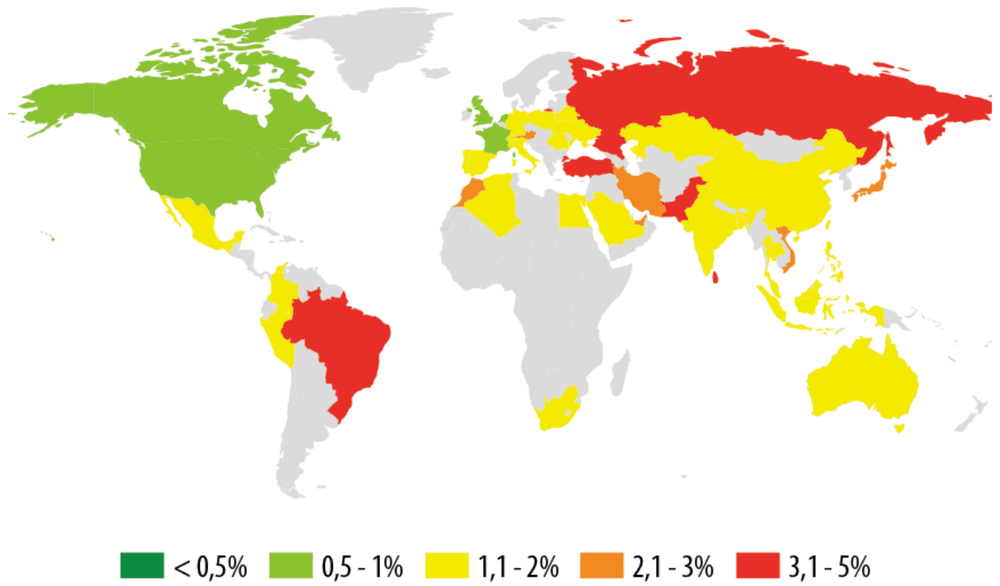
Zahl der von Finanzmalware angegriffenen Nutzer, November 2015 bis Oktober 2016

Ab Ende 2015 registrierten wir eine sinkende Zahl angegriffener Geräte, was der mangelnden Aktivität des Dyre-Botnets (auch bekannt als Dyreza) zuzuschreiben ist. Doch Mitte 2016 nahmen die Angriffe sukzessive wieder zu, und im September 2016 überstieg die monatliche Zahl der angegriffenen Geräte aufgrund einer gestiegenen Zahl von Angriffen auf mobile Online-Banking-Nutzer – zumeist Besitzer von Android-Geräten – sowohl die höchsten Monatswerte für 2014 als auch für 2015.

Geografie der Attacken

Um die Popularität von Finanzmalware unter Cyberkriminellen und den Grad des Risikos einer Infektion mit Bank-Trojanern, dem Computer in den verschiedenen Ländern der Welt ausgesetzt sind, beurteilen und vergleichen zu können, haben wir für jedes Land den Anteil der Nutzer von Kaspersky-Lab-Produkten, die im Berichtszeitraum mit dieser Bedrohung konfrontiert wurden, an allen Nutzern unserer Produkte im Land berechnet.

↺ ZURÜCK ZUM INHALT



Geografie der Attacken von Bankschädlingen im Jahr 2016
(prozentualer Anteil der von Bank-Trojanern angegriffenen Anwender
an allen von Schädlingen aller Art angegriffenen Anwendern)

Top 10 der Länder nach prozentualem Anteil der angegriffenen Anwender

	LAND*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER**
1	Russland	4,8
2	Brasilien	4,7
3	Türkei	4,5
4	Sri Lanka	4,5
5	Pakistan	3,8
6	Österreich	2,6
7	Vietnam	2,4
8	Vereinigte Arabische Emirate	2,3
9	Japan	2,2
10	Marokko	2,2

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 50.000 liegt und weniger als 7.000 Benachrichtigungen über Angriffsversuche von Bank-Schädlingen registriert wurden.

** Prozentualer Anteil individueller Anwender von Kaspersky-Lab-Produkten, die Angriffen von Bank-Trojanern ausgesetzt waren, an allen Nutzern von Kaspersky-Produkten in diesem Land.

Russland führt dieses Ranking an. Im Laufe des Jahres hatten es 4,8 Prozent der Nutzer von Kaspersky-Lab-Produkten in diesem Land mindestens einmal mit Bank-Trojanern zu. Diese Tatsache illustriert die Popularität von Finanz-Schädlingen im Verhältnis zu allen anderen Bedrohungen in diesem Land.

In Brasilien wurden 4,7 Prozent der angegriffenen Anwender mindestens einmal im Laufe des Jahres 2016 von Banking-Trojanern attackiert. In der Türkei waren es 4,5 Prozent, in Deutschland 2,0 Prozent, 1,7 Prozent in der Schweiz und 1,0 Prozent in Frankreich.

Top 10 der Banken-Schädlinge

In der folgenden Tabelle sind die zehn Schadprogramme aufgelistet, die im Jahr 2016 am häufigsten bei Attacken auf die Nutzer von Online-Banking- oder mobilen Banking-Systemen verwendet wurden (nach prozentualem Anteil der angegriffenen Nutzer):

	NAME*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN NUTZER**
1	Trojan-Banker.AndroidOS.Svpeng.q	8,8
2	Trojan-Banker.Win32.Gozi.gr	5,7
3	Trojan.BAT.Qhost.abp	4,5
4	Trojan-Spy.Win32.Zbot.pef	3,5
5	Trojan-Banker.AndroidOS.Agent.ai	2,8
6	Trojan-Spy.Win32.Zbot.vho	2,5
7	Trojan-Banker.AndroidOS.Asacub.e	1,9
8	Trojan-Banker.AndroidOS.Svpeng.r	1,8
9	Trojan.Win32.Qhost.afes	1,4
10	Trojan-Banker.AndroidOS.Hqwar.t	1,2

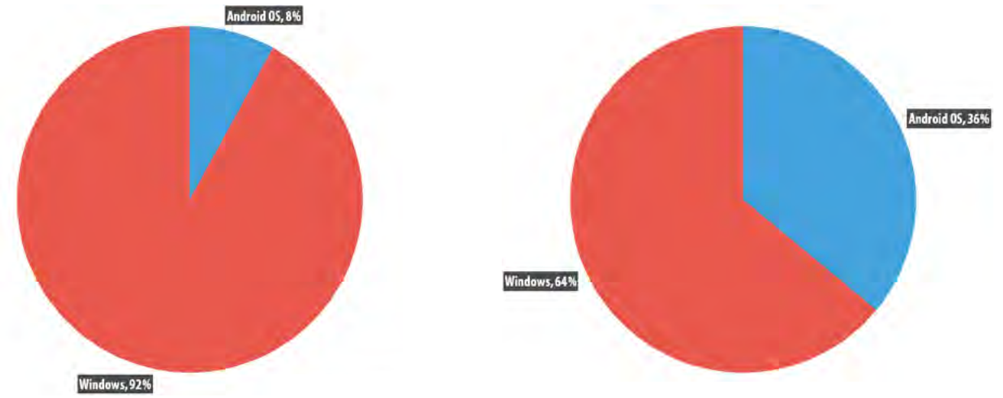
* Von Kaspersky-Lab-Produkten detektierte Objekte. Die Informationen stammen von Anwendern von Kaspersky-Lab-Produkten, die der Übermittlung von statistischen Daten zugestimmt haben.

** Prozentualer Anteil individueller Anwender, die von dem entsprechenden Schädling angegriffen wurden, an allen Anwendern, die von Finanz-Malware angegriffen wurden.

Fünf Vertreter aus den Top 10 der Bank-Trojaner versuchen, mobile Banking-Daten von Android-Geräten zu stehlen. Verglichen mit dem Jahr 2015 ist der Anteil der Attacken, die sich gegen das mobile Betriebssystem Android richten, um ein 4,5-Faches gestiegen. Das zeigt, dass die Cyberkriminellen das Verhalten der Nutzer ganz genau beobachten und nun von Angriffen auf Internet-Banking-Webseiten auf mobile Banken-Apps umschwenken.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
STATISTIK FÜR 2016



Anteile der von Finanz-Malware angegriffenen Geräte, 2015 bis 2016

Die Mehrheit der Schadprogramme aus den Top 10 für Windows funktionieren, indem sie HTML-Code in die Webseite einschleusen, die vom Browser angezeigt wird und alle Bezahl-Daten abfangen, die der Nutzer in die originalen oder die eingeschleusten Webformulare eingibt. Mobile Bank-Trojaner hingegen versuchen, das originale Fenster der mobilen Bank-App mit ihrem eigenen Phishing-Fenster zu überdecken und die Einmal-Authentifizierungscodes abzufangen, indem sie die eingehenden SMS kontrollieren.

Den ersten Platz im Rating nimmt Trojan-Banker.AndroidOS.Svpeng.q ein. Das liegt in erster Linie an der Verbreitungsmethode dieser Malware über das Werbenetzwerk Google AdSense, das von vielen großen Online-Portalen verwendet wird, unter anderem von großen Nachrichtenwebseiten, um den Nutzern zielgerichtete Werbung anzuzeigen. Offensichtlich haben die Svpeng-Autoren schädliche Werbung in diesem Netzwerk platziert. Der Trojaner lädt sich selbst herunter, sobald eine infizierte Werbung geladen wird, ganz egal, ob der Nutzer sie ausgewählt hat oder nicht.

Die Banktrojaner-Familie Svpeng ist Kaspersky Lab seit dem Jahr 2013 bekannt und sie verfügt über ein breites Spektrum an schädlichen Funktionen. Nachdem ein Schädling dieser Familie installiert und gestartet wurde, verschwindet er von der Liste der installierten Apps und erfragt Administratorenrechte auf dem Gerät (um es für Antiviren-Software oder den Nutzer schwerer zu machen, die Malware wieder zu entfernen). Svpeng ist in der Lage, Informationen über die Bankkarten der Nutzer mit Hilfe von Phishing-Fenstern zu stehlen, abzufangen, zu löschen und Textnachrichten zu senden – alles, was nötig ist, um Online-Banking-Systeme anzugreifen, die SMS zur Übermittlung der einmaligen Authentifizierungscodes nutzen.

Ein Vertreter aus der Familie Trojan-Banker.Win32.Gozi befindet sich auf Platz zwei. Er nutzt Techniken zur Einschleusung von Code in die Arbeitsprozesse populärer Webbrowser, um Rechnungsdaten zu stehlen, die auf den Webseiten von Internet-Banking-Systemen eingegeben wurden. Einige Samples dieser Familie können den MBR (Master Boot Record) infizieren und sich damit nachhaltig im Betriebssystem festsetzen, selbst wenn es zurückgesetzt wird. Die erste Version dieses Trojaners erschien vor zehn Jahren und seither hat der Schädling bedeutende Veränderungen durchgemacht. In diesem Jahr haben die Gozi-Entwickler ihrem kriminellen Spektrum neben dem Diebstahl von Bankdaten auch Erpressung mittels trojanischer Verschlüsselungsprogramme hinzugefügt. Wir haben entdeckt, dass der Code des Trojaners Nymaim Fragmente des Bankenschädlings Gozi enthält, die entfernten Zugriff auf infizierte Computer ermöglichen. Das bedeutet: wenn die Erpressungsopfer das Internet-Banking benutzen, so erpressen die Verbrecher nicht nur Geld von ihnen, sondern stehlen überdies auch alle verfügbaren Finanzmittel vom Bankkonto des Opfers.

Über einen langen Zeitraum hielt sich die Trojaner-Familie Zbot hartnäckig in den Top 3, doch mit dem Aufkommen von mobilen Bank-Trojanern hat sich die Situation in diesem Ranking geändert. Das heißt aber keinesfalls, dass Zbot nun in der Versenkung verschwunden ist. Er belegt vielmehr den vierten Platz und dient als Grundlage für eine große Zahl anderer Bank-Trojaner, unter anderem Citadel, Kins und ZeusVM.

Auf den Plätzen drei und neun befinden sich Vertreter der Trojaner-Familie Qhost. Es handelt sich dabei um eine der einfachsten Familien von Bank-Trojanern, was ihrer Effektivität allerdings keinen Abbruch tut. Diese zwei Vertreter modifizieren den Inhalt der Hosts-Datei auf dem Computer des Opfers, so dass alle Anfragen an eine Bank-Webseite über einen schädlichen Server laufen, von dem aus es möglich ist, „in die Konversation einzubrechen" und die Daten zu ersetzen, die der Nutzer im Browser sieht, ebenso wie die Daten, die an die Bank gesendet werden.

Länder, in denen Computer dem höchsten Risiko einer Infektion über das Internet ausgesetzt sind

Um den Grad des Infektionsrisikos via Internet zu bestimmen, dem Computer in verschiedenen Ländern ausgesetzt sind, hat das Kaspersky-Team für jedes Land berechnet, wie häufig Kaspersky Anti-Virus im Laufe des Jahres Alarm geschlagen hat. Die so erhaltenen Daten sind ein Indikator für die Aggressivität der Umgebung, in der die Computer in den verschiedenen Ländern arbeiten.

In diesem Rating werden nur Attacken von Schadobjekten der Klasse Malware berücksichtigt. Potenziell gefährliche und unerwünschte Programme wie etwa Programme der Klassen RiskTool und Adware fließen nicht in die Berechnungen mit ein.

↺ ZURÜCK ZUM INHALT

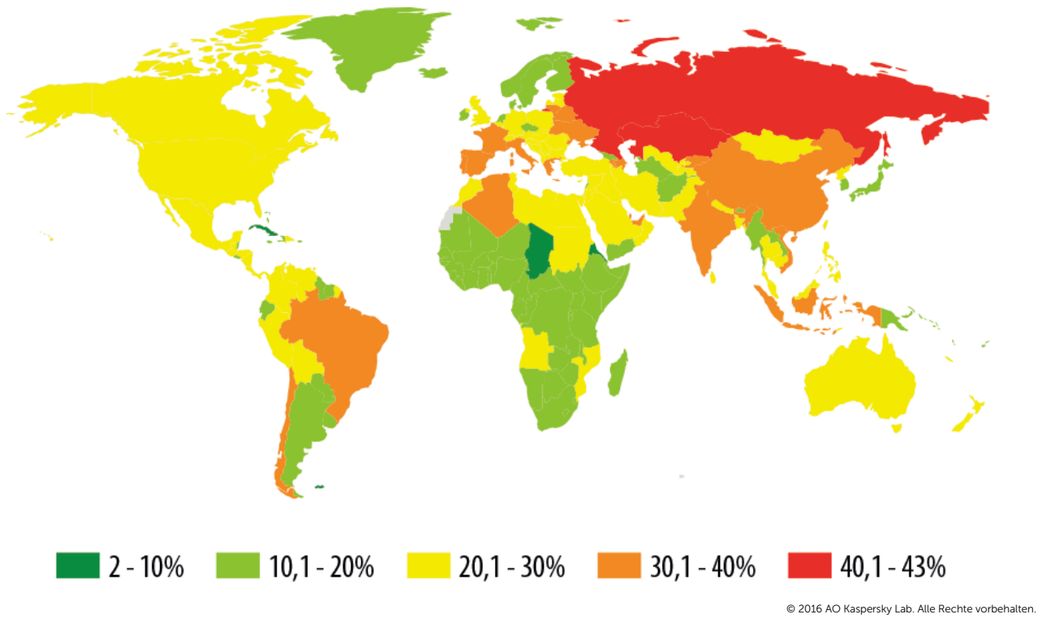
KASPERSKY SECURITY BULLETIN 2016/2017
STATISTIK FÜR 2016

Top 20 der Länder, in denen die Computer dem höchsten Risiko einer Infektion über das Internet ausgesetzt sind

	LAND*	PROZENTUALER ANTEIL INDIVIDUELLER KSN-TEILNEHMER**
1	Russland	42.15
2	Kasachstan	41.22
3	Italien	39.92
4	Ukraine	39.00
5	Brasilien	38.83
6	Aserbaidschan	38.81
7	Spanien	38.21
8	Weißrussland	38.04
9	Algerien	37.11
10	Vietnam	36.77
11	China	36.53
12	Portugal	35.86
13	Frankreich	34.74
14	Armenien	33.01
15	Griechenland	32.99
16	Chile	32.82
17	Indien	32.61
18	Katar	32.53
19	Indonesien	32.30
20	Moldawien	31.42

Die vorliegende Statistik basiert auf den Alarmen von Kaspersky Anti-Virus. Die Daten stammen von den Computern der KSN-Teilnehmer, die ihr Einverständnis zur Übermittlung von statistischen Daten gegeben haben.

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 50.000 liegt.
** Prozentualer Anteil individueller Anwender-PCs, die Web-Attacken durch Schadprogramme der Klasse Malware ausgesetzt waren, an allen Nutzern von Kaspersky-Produkten in diesem Land.



Geografie der schädlichen Web-Attacken im Jahr 2016 (nach Anteil der angegriffenen Nutzer)

Die Länder lassen sich nach dem Grad des Infektionsrisikos in drei Gruppen einteilen.

1. **Gruppe mit erhöhtem Risiko (40 % und mehr)**
   Zu dieser Gruppe gehören für das Jahr 2016 die ersten zwei Länder aus den Top 20: Russland und Kasachstan.
2. **Risikogruppe (20 bis 39,9 %)**
   In dieser Gruppe sind 105 Länder vertreten, darunter Kanada (29,5 %), die Türkei (29,3 %), Polen (28,7 %), Rumänien (27,4 %), Mexiko (26,8 %), Australien (26,2 %), Deutschland (26,2 %), Belgien (25,3 %), Österreich (24,8 %), die USA (24 %), die Schweiz (23,6 %), Großbritannien (22,1 %), Ungarn (21,3 %) und Irland (20 %).
3. **Gruppe der beim Surfen im Internet sichersten Länder (0 bis 19,9 %)**
   Zu dieser Gruppe zählen die Tschechische Republik (19,6 %), Argentinien (19,5 %), Japan (17,7 %), Norwegen (15,9 %), Schweden (15,2 %), Georgien (14,6 %), die Niederlande (14,5 %) und Dänemark (12,2 %).

Im Jahr 2016 waren **31,9** Prozent der Computer von Internetnutzern mindestens einmal einer Webattacke durch Schadprogramme der **Klasse Malware** ausgesetzt.

LOKALE BEDROHUNGEN

Ein sehr wichtiger Indikator ist die Statistik der lokalen Infektionen der Computer. Zu diesen Daten gehören Objekte, die über die Infektion von Dateien oder mobilen Datenträgern in die Computer eindringen oder die ursprünglich nicht in offener Form auf den Computer gelangt sind (beispielsweise Programme im Zuge komplexer Installationen, verschlüsselte Dateien und so weiter). Zudem werden in dieser Statistik Objekte berücksichtigt, die nach dem ersten Systemscan durch Kaspersky Anti-Virus auf den Computern der Nutzer gefunden wurden. In diesem Abschnitt

↺ ZURÜCK ZUM INHALT

präsentiert das Kaspersky-Team statistische Daten, die auf der Arbeit des Echtzeit-Scanners der Kaspersky-Lösungen basieren. Hinzu kommen Statistiken über den Scan verschiedener Datenträger, darunter auch mobile Speichermedien (On-Demand Scanner).

Im Jahr 2016 spürte Kaspersky Anti-Virus insgesamt **4.071.588** individuelle schädliche und potenziell unerwünschte Programme auf (individuelle Programme bedeutet hier Programme mit eindeutigen Werten).

Top 20 der auf den Computern der Anwender entdeckten schädlichen Objekte

Wir haben nachfolgend die 20 Bedrohungen aufgeführt, die im Jahr 2016 am häufigsten auf den Computern der Anwender aufgespürt wurden. Programme der Klassen Adware und Riskware werden in diesem Rating nicht berücksichtigt.

	NAME*	PROZENTUALER ANTEIL DER INDIVIDUELLEN ANGEGRIFFENEN ANWENDER**
1	DangerousObject.Multi.Generic	42,32
2	Trojan.Win32.Generic	9,23
3	Trojan.WinLNK.Agent.gen	7,78
4	Trojan.WinLNK.StartPage.gena	6,25
5	Trojan.Script.Generic	5,86
6	Trojan.Win32.AutoRun.gen	4,78
7	Virus.Win32.Sality.gen	4.34
8	Trojan.WinLNK.Runner.jo	4,17
9	Worm.VBS.Dinihou.r	3,58
10	Trojan.WinLNK.Agent.ew	3,13
11	Trojan.Win32.Starter.yy	2,93
12	Trojan-Downloader.Script.Generic	2,80
13	Trojan.Win32.Autoit.cfo	2,27
14	Trojan.Win32.Wauchos.a	2,03
15	Virus.Win32.Nimnul.a	2,02
16	Trojan-Proxy.Win32.Bunitu.avz	1,90
17	Worm.Win32.Debris.a	1,83
18	Trojan.Win32.Hosts2.gen	1,80
19	Trojan-Dropper.VBS.Agent.bp	1,34
20	Trojan.WinLNK.StartPage.ab	1,26

Die Statistik basiert auf Daten der Module OAS und ODS von Kaspersky Anti-Virus, dessen Anwender der Übermittlung statistischer Daten zugestimmt haben.

* Malware-Detektionen der Module OAS und ODS von Kaspersky Anti-Virus, dessen Anwender der Übermittlung statistischer Daten zugestimmt haben.

** Prozentualer Anteil der einzelnen Computer, auf denen Kaspersky Anti-Virus das entsprechende Objekt erkannt hat, an allen mit Kaspersky-Produkten ausgestatteten Computern, auf denen Kaspersky Anti-Virus bei Programmen der Klasse Malware Alarm geschlagen hat.

Den ersten Platz belegen schädliche Programme des Typs DangerousObject.Multi.Generic (42,32 %), die mit Hilfe von Cloud-Technologien aufgespürt werden. Die Cloud-Technologien greifen dann, wenn es in den Antiviren-Datenbanken bisher keine Signaturen gibt und keine Heuristiken zur Erkennung von Schadprogrammen zur Verfügung stehen, in der Cloud von Kaspersky Lab aber bereits Informationen über das Objekt vorhanden sind. Auf diese Weise werden die allerneuesten Schadprogramme erkannt.

Der Anteil der Viren im Rating nimmt weiterhin ab. So war Virus.Win32.Sality.gen beispielsweise im letzten Jahr bei 5,53 Prozent der KSN-Anwender anzutreffen, im Jahr 2016 dagegen nur noch bei 4,34 Prozent. Der Wert von Virus.Win32.Nimnul.a lag 2015 bei 2,37 Prozent, im Jahr 2016 bei 2,02 Prozent. Bei den Objekten des Typs Trojan-Dropper.VBS.Agent.bp auf Platz 19 handelt es sich um ein VBS-Skript, das den Schädling Virus.Win32.Nimnul aus sich selbst extrahiert und ihn auf der Festplatte speichert.

Neben den Objekten der oben genannten Typen (durch Cloud-Technologien aufgespürte Schädlinge und Viren) sind auch Würmer in den Top 20 vertreten, die sich auf mobilen Speichermedien sowie deren Komponenten verbreiten. Ihre Anwesenheit im Rating lässt sich durch die Art ihrer Verbreitung und die Erstellung einer Vielzahl von Kopien erklären. Ein Wurm kann sich immer weiter ausbreiten, über einen langen Zeitraum hinweg, selbst wenn seine Steuerungsserver nicht mehr aktiv sind.

Trojan.Win32.Wauchos.a, ein Neueinsteiger in diesem Rating, ist beispielsweise eine Komponente der Wurm-Familie Worm.Win32.Debris, die den Trojaner auf externen Festplatten installiert. Dieser Trojaner kann andere Malware von den C&C-Servern nachladen, und es wurde beobachtet, wie er neue Versionen von Worm.Win32.Debris geladen hat.

Trojan-Proxy.Win32.Bunitu.avz ist ein für dieses Rating untypisches Objekt, da es zur Klasse Trojan-Proxy gehört und keinen Selbstverbreitungsmechanismus hat.

Bei den meisten Samples von Trojan.Win32.Hosts2.gen handelt es sich dieses Jahr um Hosts-Dateien, die den Zugriff auf Antiviren-Webseiten und -Server blockieren.

Länder, in denen die Computer dem höchsten Risiko einer lokalen Infektion ausgesetzt waren

Um zu bewerten, in welchen Ländern es die Anwender am häufigsten mit Cyberbedrohungen zu tun hatten, haben wir für jedes Land berechnet, wie häufig unsere Antiviren-Lösung im Laufe des Jahres bei den Anwendern Alarm geschlagen hat. Berücksichtigt wurden dabei detektierte Objekte, die direkt auf den Computern gefunden wurden oder auf Wechseldatenträgern, die an die Computer angeschlossen waren, zum Beispiel USB-Sticks, Speicherkarten aus Fotoapparaten und Mobiltelefonen oder externe Festplatten. Die folgende Statistik spiegelt das durchschnittliche Infektionsniveau der Computer in den verschiedenen Ländern der Welt wider.

↺ ZURÜCK ZUM INHALT

Top 20 der Länder nach Infektionsniveau der Computer

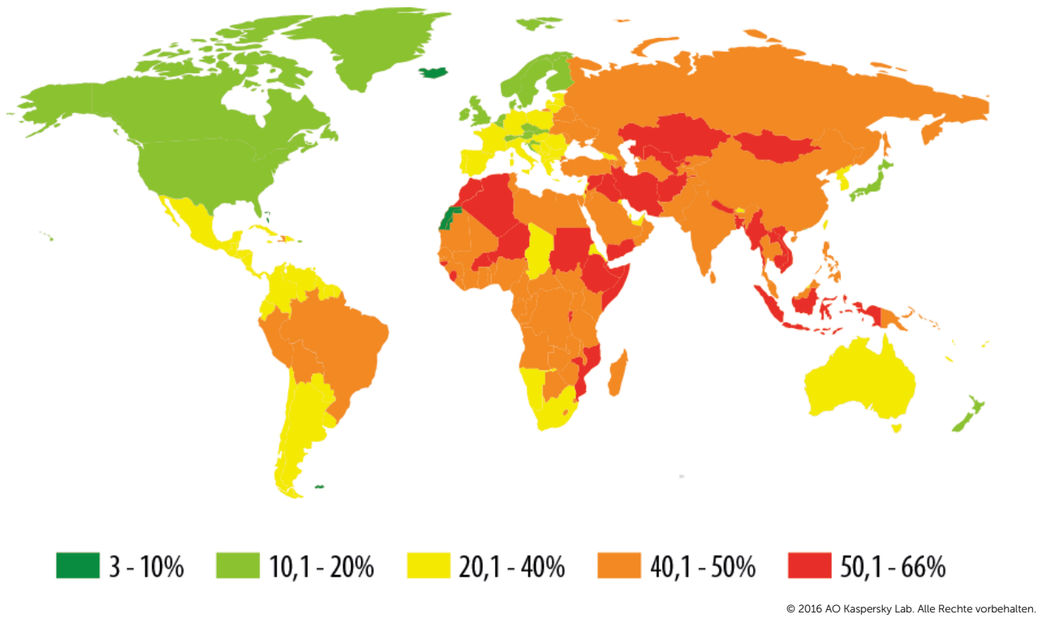
	LAND*	ANTEIL IN PROZENT**
1	Vietnam	65,69
2	Somalia	63,90
3	Afghanistan	61,05
4	Ruanda	60,17
5	Algerien	59,80
6	Laos	58,90
7	Äthiopien	57,75
8	Bangladesch	57,39
9	Nepal	57.35
10	Mongolei	56,89
11	Kambodscha	55.90
12	Indonesien	55,51
13	Mozambique	54,95
14	Usbekistan	54,03
15	Irak	53,97
16	Syrien	53,44
17	Marokko	53,39
18	Myanmar	53,11
19	Kasachstan	53,02
20	Niger	52,96

Die Statistik basiert auf Daten von Kaspersky Anti-Virus, dessen Anwender der Übermittlung statistischer Daten zugestimmt haben.

* Aus unseren Berechnungen haben wir die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 50.000 liegt.

** Prozentualer Anteil von individuellen Anwender-PCs, auf denen lokale Bedrohungen der Klasse Malware blockiert wurden, an allen individuellen Nutzern von Kaspersky-Produkten in diesem Land.

Durchschnittlich wurde in den Ländern aus den Top 20 bei 36,8 Prozent der KSN-Anwender, die uns Informationen zur Verfügung stellten, mindestens einmal ein schädliches Objekt auf dem Computer gefunden – auf der Festplatte oder auf angeschlossenen mobilen Datenträgern.

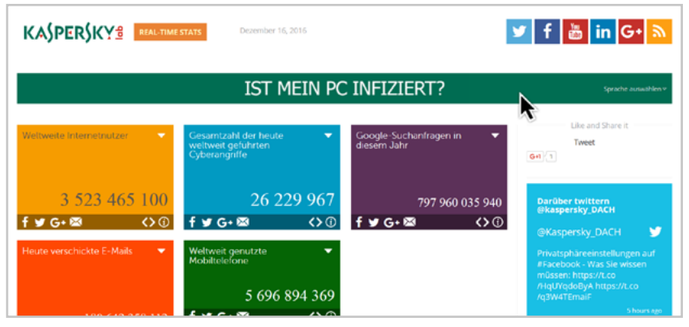


Geografie der schädlichen lokalen Infektionen im Jahr 2016 (nach Anteil der angegriffenen Nutzer)

Auch bei den lokalen Bedrohungen lassen sich alle Länder in verschiedene Kategorien einteilen.

- **Maximales Infektionsniveau (über 60 %):** vier Länder aus den Top 20.
- **Hohes Infektionsniveau (41 bis 60 %):** Zu dieser Gruppe gehören Iran (51,9 %), Indien (50,4 %), Weißrussland (48,7 %), China (48,6 %), die Ukraine (47,9 %), Saudi Arabien (44 %), Russland (43,6 %), die Türkei (42 %) und Brasilien (41,3 %).
- **Mittleres Infektionsniveau (21 bis 40,99 %):** In dieser Gruppe sind vertreten: Moldawien (40,8 %), Armenien (40,4 %), Mexiko (39,1 %), Südafrika (30,5 %), Polen (29 %), Serbien (28,6 %), Bulgarien (27,4 %), Spanien (27 %), Griechenland (26,2 %), Israel (24,8 %), Italien (24,8 %), Ungarn (23,4 %) und Frankreich (21,1 %).

Real-Time Stats



↺ ZURÜCK ZUM INHALT

Die 10 Länder mit den geringsten Computer-Infektionsraten waren:

	LAND	ANTEIL IN PROZENT*
1	Dänemark	10,4
2	Schweden	13,0
3	Niederlande	13,9
4	Japan	13,9
5	Norwegen	14,5
6	Irland	15,1
7	Tschechische Republik	15,2
8	Schweiz	15,75
9	Vereinigte Staaten	16,48
10	Neuseeland	16,78

Durchschnittlich wurden 16 Prozent der Computer in den zehn sichersten Ländern mindestens einmal im Laufe des Jahres angegriffen.

Cyberbedrohungen Echtzeitkarte

KASPERSKY SECURITY BULLETIN 2016/2017. RÜCKBLICK

Autor(en): David Emm, Roman Unuchek, Kirill Kruglov

QUICK INFO

ZIELGERICHTETE ATTACKEN

Zielgerichtete Attacken sind zu einem festen Bestandteil der Bedrohungslandschaft geworden, daher überrascht es nicht, dass diese Art von Attacken auch in unserem Jahresrückblick eine bedeutende Rolle spielt.

Hier eine Zusammenstellung der wichtigsten APT-Kampagnen, über die wir in diesem Jahr berichteten.

BlackEnergy

Das Jahr begann mit einem sich langsam zusammensetzenden Gesamtbild der Cyberattacke BlackEnergy auf den ukrainischen Energiesektor. Der Schaden, den diese Attacke anrichtete, machte sie zu etwas Einmaligem: Hackern war es gelungen, die Stromverteilungssysteme in der Westukraine abzuschalten. Sie starteten ein Wiper-Programm in den angegriffenen Systemen, um den Inhalt der infizierten Computer zu löschen und führten eine Telefon-DDoS-Attacke auf den technischen Support der angegriffenen Unternehmen durch. Die Experten von Kaspersky Lab beleuchteten verschiedene Aspekte der Aktivität der Gruppe, die hinter diesem Vorfall steckt. Eine dieser Analysen behandelt das Tool, das benutzt wurde, um in die Systeme einzudringen. Wer Genaueres über diese Attacke erfahren möchte, dem empfehlen wir den Bericht des amerikanischen SANS-Institute, der in Zusammenarbeit mit dem ICS-CERT erstellt wurde.

In einer massiven Attacke deaktivierte BlackEnergy die Stromverteilung, löschte Software und startete eine DDoS-Attacke.

Operation Blockbuster

Kaspersky Lab war einer der Investigatoren der Operation „Blockbuster" – einer gemeinsamen Studie einiger großer Unternehmen auf dem Gebiet der Cybersicherheit. Untersuchungsgegenstand war die Tätigkeit der Lazarus Group (den entsprechenden Bericht von Kaspersky Lab finden Sie hier), die vermutlich südkoreanischer Herkunft ist und unter anderem in die skandalträchtige Attacke auf Sony Pictures im Jahr 2014 verwickelt war.

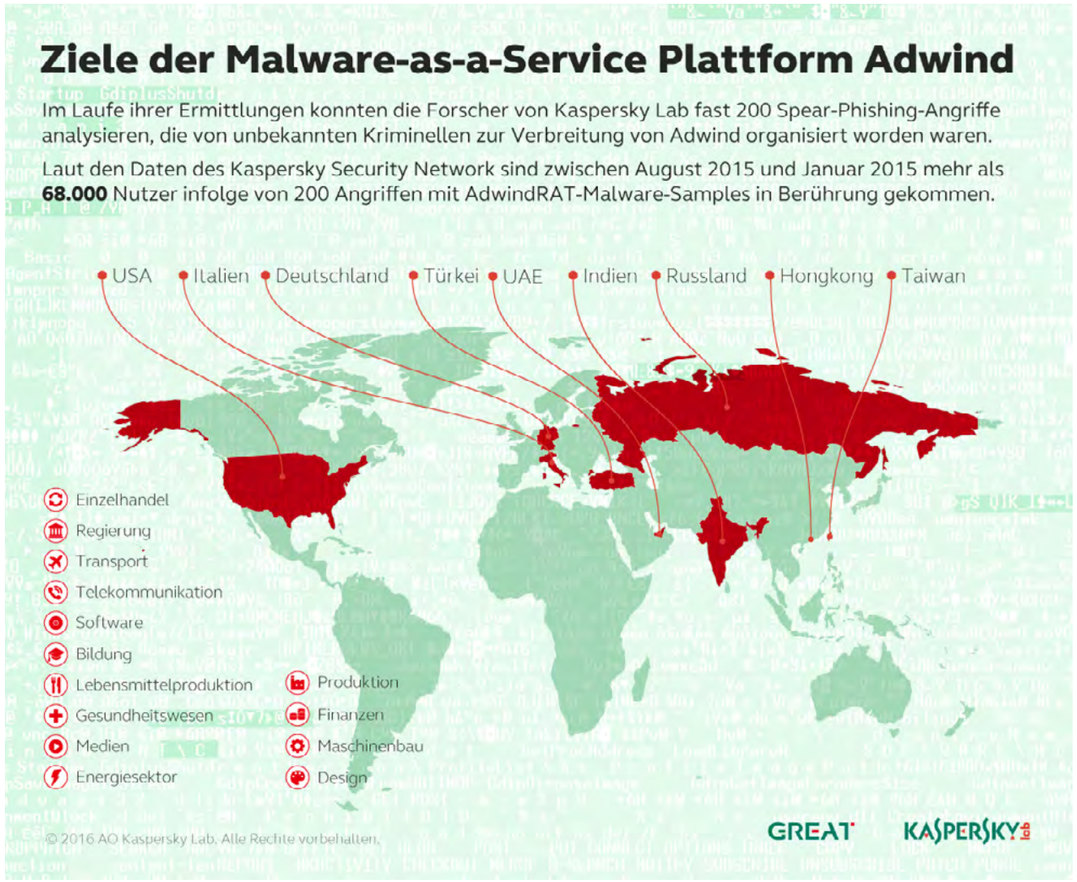
Die Existenz der Lazarus Group lässt sich bis ins Jahr 2009 zurückverfolgen. Wirklich aktiv wurde sie allerdings erst im Jahr 2011. Diese Gruppe ist verantwortlich für so bekannte Attacken wie Troy, Dark Seoul (Wiper) und WildPositron. Die Gruppe griff insbesondere Unternehmen, Finanzorganisationen sowie Radio- und Fernsehsender an.

↺ ZURÜCK ZUM INHALT

Adwind

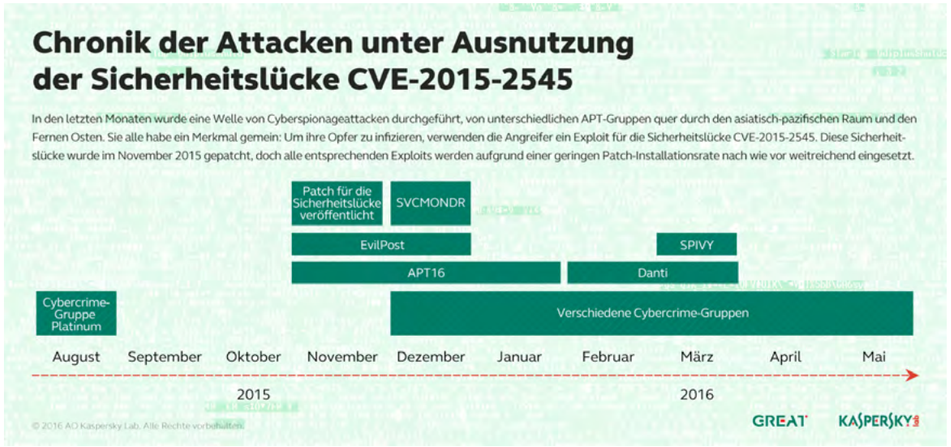
Auf dem Security Analyst Summit im Februar 2016 stellten unsere Experten Details ihrer Ermittlungsarbeit zu der Aktivität des Fernsteuerungs-Trojaners Adwind vor, einem Plattform übergreifenden, multifunktionalen RAT (Remote Access Tool), das über einen einzelnen Malware-as-a-Platform-Service verbreitet wurde. Dieser Trojaner hatte seit seinem Erscheinen im Jahr 2012 viele Namen – AlienSpy, Frutas, Unrecom, Sockrat, JSocket und jRat. Wir glauben, dass dieses Schadprogramm in den Jahren zwischen 2013 und 2016 in Angriffen auf mehr als 443.000 Einzelpersonen sowie auf kommerzielle und nicht kommerzielle Organisationen auf der ganzen Welt eingesetzt wurde. Eines der wichtigsten Merkmale, das Adwind von anderen kommerziellen Schädlingen unterscheidet, ist die Tatsache, dass die Malware offen als bezahlpflichtiger Service verbreitet wird, wobei die Kunden eine Gebühr für die Nutzung der schädlichen Software zahlen. Unseren Schätzungen zufolge hatte das System zum Ende des Jahres 2015 etwa 1.800 Kunden. Das macht es zu einer der größten Malware-Plattformen, die es derzeit gibt.

Adwinds Miet-Malware hatte 1.800 Kunden.



Attacken unter Verwendung von Exploits zu der Sicherheitslücke CVE-2015-2545

Im Mai berichteten wir über eine Welle von Cyberspionageangriffen, die von unterschiedlichen APT-Gruppen quer durch den asiatisch-pazifischen Raum und den Fernen Osten durchgeführt wurden. Sie alle haben ein Merkmal gemein: sie nutzen die Sicherheitslücke CVE-2015-2545 aus. Diese Schwachstelle ermöglicht einem Angreifer die Ausführung von willkürlichem Code unter Verwendung einer speziell erstellten EPS-Grafikdatei. Sie verwendet PostScript und kann die Adressverwürfelung (ASLR) und Data Execution Prevention (DEP) umgehen – in Windows integrierte Schutzmethoden. Es war bereits bekannt, dass die Cybercrime-Gruppen Platinum, APT16, EvilPost und SPIVY dieses Exploit benutzen. Etwas später wurde es außerdem von der Danti- und der SVCMONDR-Gruppe verwendet. Einen Überblick über die APTs, die diese Sicherheitslücke ausnutzen, finden Sie hier.



Einer der verblüffendsten Aspekte dieser Attacken ist die Tatsache, dass sie erfolgreich eine Sicherheitslücke ausnutzen, die Microsoft im September 2015 gepatcht hatte. In unseren Prognosen für das Jahr 2016 sagten wir voraus, dass APT-Kampagnen künftig weniger Mühe darauf verwenden werden, raffinierte Tools zu entwickeln und dafür aktiver gebrauchsfertige Malware einsetzen werden, um ihre Ziele zu erreichen. Dies ist ein Paradebeispiel dafür: hier wird eine bekannte Sicherheitslücke ausgenutzt, anstatt ein Zero-Day-Exploit zu entwickeln.

Das unterstreicht einmal mehr, dass Unternehmen ihrem Patch-Management mehr Aufmerksamkeit widmen müssen, um ihre IT-Infrastruktur zu sichern.

Mehr als sechs APT-Gruppen nutzen dieselbe Sicherheitslücke aus – die bereits im Jahr 2015 gepatcht wurde.

Operation Daybreak

Selbstverständlich wird es immer APT-Gruppen geben, die ihren Nutzen aus Zero-Day-Exploits zu ziehen versuchen. Im Juni 2016 berichteten wir über eine Cyberspionage-Kampagne mit dem Codenamen Operation Daybreak, für die eine Gruppe namens ScarCruft verantwortlich war und die ein bis dahin unbekanntes Exploit für den Adobe Flash Player (CVE-2016-1010) einsetzte. Diese Gruppe

↺ ZURÜCK ZUM INHALT

ist relativ neu und hat es bisher geschafft, unter dem Radar abzutauchen. Wir glauben, dass die Gruppe früher möglicherweise eine andere Zero-Day-Schwachstelle (CVE-2016-0147) ausgenutzt hat, die im April gepatcht wurde. Zu den Zielen der Gruppe gehören eine asiatische Strafverfolgungsbehörde, eines der weltgrößten Handelsunternehmen, eine Firma aus dem Bereich mobile Werbung und App-Monetarisierung in den USA, Einzelpersonen, die mit dem Weltleichtathletikverband IAAF in Verbindung stehen, sowie ein Restaurant in einem der exklusivsten Einkaufszentren von Dubai.

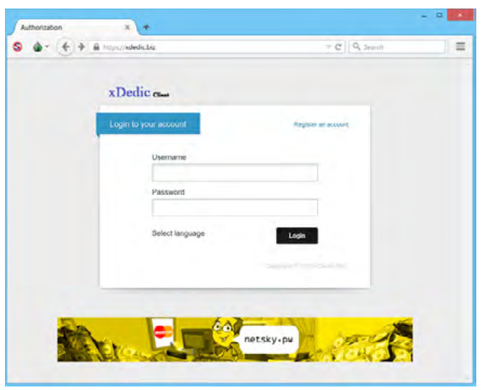
Es gibt keine hundertprozentige Sicherheit. Daher ist es entscheidend, Abwehrmechanismen so weit zu verbessern, dass es für einen Angreifer zu teuer wird, sie zu durchbrechen und er aufgibt oder sich ein anderes Ziel sucht. Die beste Verteidigung gegen zielgerichtete Attacken ist ein vielschichtiger Ansatz, der traditionelle Antiviren-Technologien mit Patch-Management, Host-basierten Intrusion-Prevention-Systemen und einer Whitelisting-Strategie, die auf standardmäßigem Verbieten basiert (default deny), vereint. Einer Studie des Australian Signals Directorate zufolge hätten 85 Prozent der analysierten zielgerichteten Attacken durch die Bereitstellung vier simpler Mitigationsstrategien verhindert werden können: Einsatz von Weißen Listen für Anwendungen, Aktualisieren von Anwendungen, Aktualisieren des Betriebssystems und Einschränken von administrativen Rechten.

Die Cyberspionagekampagne Operation Daybreak von ScarCruft nutzte eine unbekannte Zero-Day-Sicherheitslücke aus: CVE-2016-1010.

xDedic

In diesem Jahr stellte Kaspersky Lab Untersuchungen zu einer aktiven cyberkriminellen Handelsplattform namens xDedic an – ein Online-Schwarzmarkt für die Zugangsdaten von gehackten Servern rund um den Globus, die alle über das Remote Desktop Protocol (RDP) verfügbar sind. Ursprünglich dachten wir, dass dieser Markt bis zu 70.000 Server umfasst, aber neue Daten deuten darauf hin, dass der xDedic-Markt weitaus größer war und die Zugangsdaten für 176.000 Server enthielt. Zu xDedic gehört auch eine Suchmaschine, mit deren Hilfe potenzielle Käufer so gut wie alles finden können, Regierungs- und Unternehmensnetzwerke eingeschlossen, und zwar für nicht mehr als acht US-Dollar pro Server. Für diesen niedrigen Preis erhalten die „Kunden" Zugriff auf die Daten, die auf diesen Servern gespeichert sind, und können sie zudem als Ausgangspunkt für weitere zielgerichtete Attacken benutzen.

Untergrund-Marktplätze sind nichts Neues. Neu ist der Grad der Spezialisierung. Und auch wenn das Model der xDedic-Besitzer nichts ist, was einfach nachgeahmt werden kann, gehen wir davon aus, dass künftig andere spezialisierte Märkte auftreten werden.



xDedic war Umschlagsplatz für mindestens 70.000 gehackte Server – und die meisten Opfer hatten keine Ahnung.

Dropping Elephant

Zielgerichtete Attacken müssen nicht technisch ausgefeilt sein, um Erfolg zu haben. Im Juli 2016 berichteten wir über eine Gruppe mit dem Namen Dropping Elephant (auch bekannt als „Chinastrats" und „Patchwork"). Mit Hilfe einer Kombination aus Social Engineering, altem Exploit-Code und PowerShell-basierter Malware gelang es dieser Gruppe, ihren Opfern – meist hochgestellte diplomatische Einrichtungen und Wirtschaftsorganisationen, die mit den auswärtigen Beziehungen Chinas in Verbindung stehen – sensible Daten zu stehlen. Die Angreifer setzten dabei eine Kombination aus Spear-Phishing-Mails und Wasserloch-Attacken ein.

Der Erfolg der Gruppe Dropping Elephant ist verblüffend, bedenkt man, dass keine Zero-Day-Exploits oder raffinierten Techniken verwendet wurden, um prominente Opfer anzugreifen. Dropping Elephant ist ein klares Beispiel dafür, wie effektiv geringe Investitionen sowie die Nutzung gebrauchsfertiger Toolsets sein können, wenn sie mit qualitativ hochwertigem Social Engineering kombiniert werden.

Der Erfolg solcher Attacken kann verhindert werden, wenn Sicherheitsupdates angewendet werden und das Sicherheitsbewusstsein der Mitarbeiter geschärft wird.

Dropping Elephant demonstrierte die furchteinflößende Effizienz von hochwertigem Social Engineering.

Operation Ghoul

Der Erfolg von Social Engineering als Methode, einen Fuß in die Tür einer angegriffenen Organisation zu bekommen, spielte auch bei der Operation Ghoul eine große Rolle – die Gruppe hinter einer Reihe von Attacken, über die wir im Juni 2016 berichteten. Die Angreifer versendeten Spear-Phishing-Mails, die schädliche Anhänge enthielten.

Diese Nachrichten, die in erster Linie an Manager aus der obersten oder mittleren Führungsebene vieler Unternehmen gesendet wurden, sahen so aus, als kämen sie von einer Bank in den Vereinigten Arabischen Emiraten. Die Mitteilungen enthielten angeblich eine Zahlungsankündigung der Bank sowie ein angehängtes gepacktes SWIFT-Dokument.

Doch dieses Archiv enthielt in Wahrheit Malware. Den Informationen zufolge, die von auf Sinkehole-Server umgeleiteten C2-Servern erhalten wurden, sind die meisten angegriffenen Organisationen in der Industrie und im Ingenieurswesen angesiedelt. Aber auch Unternehmen aus den Bereichen Transport, Pharmazie, Fertigung, Handel und Bildung wurden angegriffen.

Die Operation Ghoul bestätigte diese Effizienz – durch äußerst zielgerichtetes Phishing gefolgt von kommerzieller Malware.

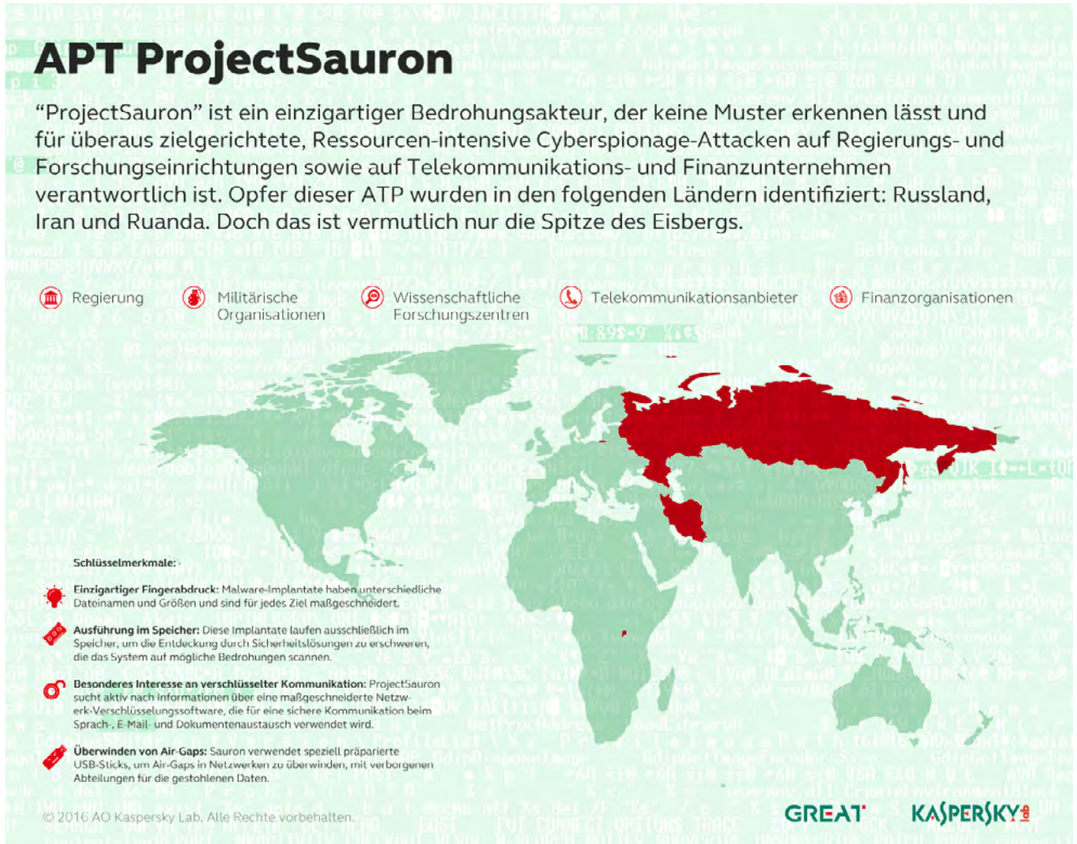
↺ ZURÜCK ZUM INHALT

Die von der Gruppe Operation Ghoul verwendete Malware basiert auf dem kommerziellen Spyware-Kit Hawkeye, das offen im Dark Web verkauft wird. Ist diese Malware installiert, so sammelt sie interessante Daten vom Computer des Opfers, unter anderem die Tastatureingaben, Daten aus der Zwischenablage, Zugangsdaten für FTP-Server, Kontodaten aus den Browsern, Messaging-Apps und E-Mail-Programmen sowie Informationen über die installierten Programme.

Der andauernde Erfolg von Social Engineering als Methode, einen Fuß in die Tür von Organisationen zu bekommen, zeigt, wie wichtig es ist, dass Unternehmen das Sicherheitsbewusstsein ihrer Mitarbeiter schärfen und die Mitarbeiterschulung zu einer zentralen Komponente ihrer Sicherheitsstrategie machen.

ProjectSauron

Im September deckten wir die Aktivität von ProjectSauron auf, einer Gruppe, die seit Juni 2011 vertrauliche Daten von Organisationen in Russland, Iran, Ruanda – und vermutlich auch in anderen Ländern – stiehlt.



Der Aufwand und die Kosten, die Nachhaltigkeit und das Endziel der Operation (das heißt der Datendiebstahl bei staatsbezogenen Organisationen) legen den Schluss nahe, dass das ProjectSauron eine von einem Nationalstaat unterstützte Kampagne ist.

Technische Details deuten darauf hin, dass die Angreifer von anderen hoch entwickelten ATP-Gruppen gelernt haben, unter anderem von Duqu, Flame, Equation und Regin, indem sie einige ihrer innovativsten Techniken übernahmen und ihre Taktiken verbesserten, um nicht entdeckt zu werden. Alle schädlichen Komponenten sind auf jedes Opfer individuell zugeschnitten, so dass deren Wert als Kompromittierungsindikatoren (Indicators of Compromise, IoC) für andere Opfer gegen Null geht.

↺ ZURÜCK ZUM INHALT

ProjectSauron hat die Bedrohungslandschaft für immer verändert – eine fortschrittliche modulare Spionageplattform mit individuellen Tools für jedes Opfer.

Schlüsselmerkmale von ProjectSauron:

1. ProjectSauron ist eine modulare Plattform zur Durchführung langfristiger Cyberspionage-Kampagnen.
2. Alle Module und Netzwerkprotokolle verwenden starke Verschlüsselungsalgorithmen wie RC6, RC5, RC4, AES, Salsa20, etc..
3. ProjectSauron verwendet eine modifizierte Lua-Scripting-Engine, um die eigentliche Plattform und ihre Plug-ins zu implementieren.
4. Es gibt mehr als 50 verschiedene Plug-in-Typen.
5. Die Hintermänner von ProjectSauron haben großes Interesse an Software zur Verschlüsselung der Kommunikation, die weitreichend von den angegriffenen Regierungsorganisationen verwendet wird. Sie stehlen Chiffrierungsschlüssel, Konfigurationsdateien und IP-Adressen der Server der Schlüsselinfrastruktur, die mit der Verschlüsselungssoftware in Verbindung stehen.
6. ProjectSauron kann Daten unter Umgehung von Air-Gaps in Netzwerken stehlen, mit Hilfe eines speziellen USB-Speichersticks, auf dem die Daten in einem für das Betriebssystem unsichtbaren Bereich verwahrt werden.
7. Die Plattform macht umfangreichen Gebrauch vom DNS-Protokoll zum Herausziehen der Daten und für den Statusbericht in Echtzeit.
8. Die APT ist seit Juni 2011 aktiv und blieb es bis April 2016.
9. Der ursprüngliche Infektionsvektor, über den in die Netzwerke der Opfer eingedrungen wird, bleibt unbekannt.
10. Die Angreifer verwenden legitime Software-Lieferkanäle, um sich in den infizierten Netzwerken zu bewegen.

Der einmalige Einsatz von einzigartigen Methoden wie zum Beispiel Steuerungsserver und Chiffrierungsschlüssel in Kombination mit der Übernahme von innovativsten Techniken anderer bedeutender APT-Gruppen ist neu.

Derartige Bedrohungen können nur dann effektiv abgewehrt werden, wenn multiple Schutzebenen bereitgestellt werden, die Sensoren zum Aufspüren der allergeringsten Anomalie im organisatorischen Arbeitsablauf beinhalten, kombiniert mit Threat Intelligence und forensischer Analyse.

Weitere Beschreibungen der verfügbaren Methoden zur Abwehr solcher Bedrohungen finden Sie hier.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
RÜCKBLICK

FINANZBEDROHUNGEN

Für Cyberkriminelle gehören Angriffe auf Bankkunden zu den direktesten Wegen, um an Geld zu kommen. Typischerweise setzen die Angreifer Social Engineering ein, um ihre Opfer dazu zu bringen, persönliche Informationen preiszugeben oder Malware zu installieren, die die Daten abfängt (das heißt also Passwörter), mit denen das Opfer auf sein Bankkonto zugreift. Im Jahr 2016 wehrten die Lösungen von Kaspersky Lab auf den Geräten von **2.871.965** KSN-Anwendern (Kaspersky Security Network) Ausführungsversuche von Software ab, die auf den Diebstahl von Finanzmitteln über den Online-Zugriff auf Bankkonten spezialisiert ist.

Es sind aber nicht nur die Bankkunden, die von Cyberkriminellen angegriffen werden. In den vergangenen Jahren konnten wir beobachten, dass die Zahl der Angriffe auf Banken und andere Finanzinstitutionen selbst zunimmt. Die bekannteste Kampagne dieser Art ist vermutlich Carbanak, die für zielgerichtete Attacken typische Infiltrationstechniken einsetzte, um Geld zu stehlen. In diesem Jahr gab es weitere Angriffe auf Finanzinstitutionen.

Im Februar 2016 deckte Kaspersky Lab die Aktivitäten anderer APT-Gruppen auf, die Finanzinstitutionen angriffen. Die Gruppe hinter Metel setzte Spear-Phishing und Browser-Exploits ein, um in das Unternehmensnetzwerk von Banken einzudringen und die Kontrolle über die wichtigsten Computer innerhalb des IT-Systems der Bank zu erhalten. Durch diesen Grad des Zugriffs war es möglich, das Zurücksetzen von Geldautomaten-Transaktionen zu automatisieren: Bandenmitglieder waren in der Lage, mit Hilfe von Debitkarten Geld von Bankomaten zu stehlen, ohne dabei den Umsatz auf der Karte zu beeinträchtigen und konnten dadurch zahlreiche Transaktionen an verschiedenen Geldautomaten durchführen. Unsere Ermittlungen ergaben, dass die Angreifer in mehreren russischen Städten in Autos umherfuhren und Geld von den Geldautomaten verschiedener Banken stahlen.

Sie arbeiteten ausschließlich nachts und stahlen Geld an verschiedenen Orten. Wir entdeckten Metel in über 30 Finanzinstitutionen, aber unser Incident Response Team konnte die infizierten Netzwerke säubern, bevor wirklich großer Schaden entstehen konnte. Die Hintermänner von Metel sind allerdings noch immer aktiv und wir meinen, dass die Malware vermutlich sehr viel weiter verbreitet ist.

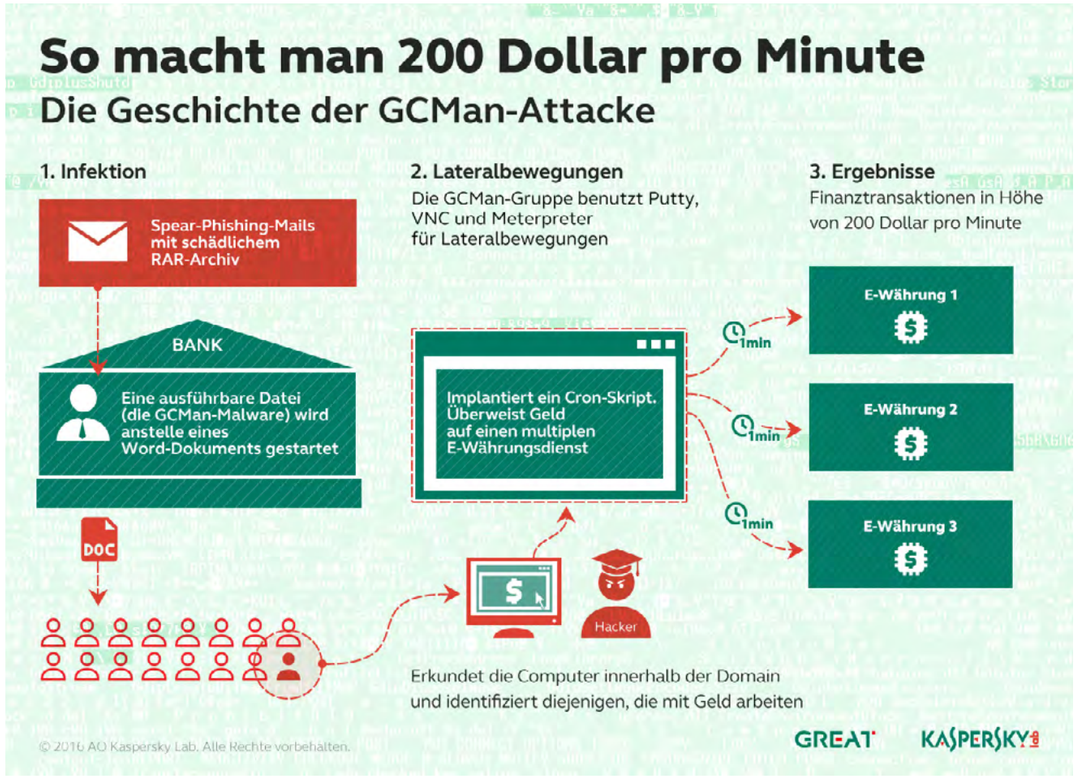
Metel führte zielgerichtete Attacken auf Banken durch und entsandte dann Teams, um das Bargeld von den Geldautomaten in der Nacht abzuheben.

GCMAN (so genannt, da die Malware auf Code basiert, der mit einem GCC-Compiler erstellt wurde) ist ein weiteres Beispiel für eine Finanzbedrohung. Die Gruppe infiltriert Finanzinstitutionen mit Hilfe von Spear-Phishing-E-Mails, die eine schädliche RAR-Datei enthalten. Wird das Archiv geöffnet, so startet eine ausführbare Datei, die zur Erstinfektion führt. Hat die Gruppe in einer Organisation erst einmal Fuß gefasst, verwendet sie legitime Pen-Test-Tools wie zum Beispiel Putty, VNC und Meterpreter, um sich seitwärts durch die Organisation bewegen zu können, bis sie strategisch wichtige Computer findet, die sie für den Transfer des Geldes zu digitalen Währungsdiensten nutzen kann. Zu diesem Zweck implantieren die Angreifer ein Cron-Skript in einen der Bankenserver (Cron dient der zeitbasierten Ausführung von Prozessen in Unix-basierten Betriebssystemen), das es ihnen ermöglicht, Finanztransaktionen in Höhe von 200 US-Dollar pro Minute abzuschließen. Dieses Skript wird minütlich aufgerufen, um seine Transaktionen direkt an ein vorgeschaltetes Zahlungsabwicklungssystem zu senden. Glücklicherweise entdeckten die Finanzinstitute die verdächtige Aktivität und stornierten die Transaktionen: Hätten sie das nicht getan, hätten die Angreifer erfolgreich Geld an verschiedene E-Währungsdienste überwiesen, ohne die Transaktionen irgendeinem System innerhalb der Bank zu melden. Die Forscher von Kaspersky Lab arbeiteten mit drei Finanzinstituten in Russland zusammen,

*ALLE NAMEN IN DIESEM COMIC SIND FREI ERFUNDEN. JEDE ÄHNLICHKEIT IST REIN ZUFÄLLIG.

deren Rechner mit der GCMAN-Malware infiziert waren. Doch wir glauben, dass diese Bedrohung wahrscheinlich sehr viel weiter verbreitet ist.

GCMAN beobachtete die infizierten Opfer 18 Monate lang, bevor die Malware angriff, indem sie legitime Tools benutzte, um tiefer in die Organisation einzudringen.



Wir haben festgestellt, dass die tatsächliche Attacke schon etwa 18 Monate vor Entdeckung der Malware stattgefunden hatte. Die Gruppe schleuste SQL-Code in kommerzielle Software ein, die auf einem der öffentlichen Webserver der Bank lief, und kehrte anderthalb Jahre später wieder zurück, um ihren Nutzen aus den Informationen zu ziehen, die sie gesammelt hatten, um die Bank zu infiltrieren. Zwei Monate vor diesem Vorfall hatten Unbekannte verschiedene Passwörter für einen Admin-Account auf einem Bankserver ausprobiert: sie waren sehr hartnäckig, beschränkten ihre Versuche aber auf Samstage und erlaubten sich nur drei Anläufe pro Woche, immer in dem Bemühen, unter dem Radar der Sicherheitsteams in den angegriffenen Institutionen abzutauchen. Die Aktivitäten der GCMAN-Gruppe warfen Licht auf einen aufkommenden Trend innerhalb der Bedrohungslandschaft: die Verwendung legitimer Tools an Stelle von maßgeschneiderten Malware-Modulen.

Legitime Tools können ebenso effektiv sein. Sie lösen seltener falschen Alarm aus und bieten den Cyberkriminellen eine schnellere Rendite. Es ist wichtig, dass die IT-Sicherheitsteams in Organisationen das berücksichtigen, wenn sie die Sicherheitsstrategie des Unternehmens überdenken.

↺ ZURÜCK ZUM INHALT

Weitere Informationen über die Kampagnen von Metel und GCMAN finden Sie hier.

Selbstverständlich operieren Banken nicht in der Isolation. Internationale Geldtransfers machen ein Interbanken-Netzwerk erforderlich, genannt SWIFT (Society for Worldwide Interbank Financial Telecommunication).

Im Februar 2016 benutzten Hacker die SWIFT-Zugangsdaten von Mitarbeitern der Zentralbank von Bangladesch, um gefälschte Anweisungen an die Federal Reserve Bank of New York zu senden und Millionen von US-Dollar auf verschiedene Bankkonten in Asien zu überweisen. Den Hackern gelang es auf diese Weise, 81 Millionen US-Dollar auf Konten der Rizal Commercial Banking Corporation auf den Philippinen und weitere 20 Million US-Dollar an die Pan Asia Banking Corporation zu überweisen. Die Verluste wären noch viel größer gewesen, wäre den Angreifern nicht ein Rechtschreibfehler in der Zahlungsanweisung unterlaufen: sie schrieben „fandation" an Stelle von „foundation". Die Federal Reserve Bank bemerkte den Fehler und die Zentralbank von Bangladesch konnte weitere Transaktionen in Höhe von 850 Millionen US-Dollar stornieren. Die ganze Geschichte lesen Sie hier. Nach dem Bankraub von Bangladesch kamen weitere Angriffe auf Banken unter Verwendung von SWIFT-Zugangsdaten ans Tageslicht.

Nach dem Diebstahl von 100 Millionen US-Dollar waren viele Banken gezwungen, ihre Authentifizierungs- und SWIFT-Update-Mechanismen zu verbessern.

Die Gruppe hinter Metel war nicht die einzige, die Geldautomaten angriff. Malware für Bankautomaten ist nichts Neues, aber die Zahl solcher Schadprogramme ist in den letzten Jahren gestiegen. Die bemerkenswerteste unter ihnen war bis zum Jahr 2016 Tyupkin. Um die Kontrolle über den Geldautomaten zu übernehmen, verschafften sich die Angreifer physischen Zugriff darauf und starteten eine bootbare CD auf der Maschine

Im Mai 2016 berichteten wir über eine neue Version der Bankautomaten-Malware Skimer. Dieser Bericht war das Ergebnis einer Incident-Response-Ermittlung, die wir im vergangenen Jahr durchgeführt haben. Diese Malware trat erstmals im Jahr 2009 in Erscheinung, doch sie wurde nun umgestaltet – ebenso wie die Taktiken der Cybergangster, die sie benutzen. Die neue Version greift Ziele auf der ganzen Welt an. Wir haben Attacken in den folgenden Ländern aufgedeckt: in den Vereinigten Arabischen Emiraten, in Frankreich, in den USA, Russland, Macau, China, den Philippinen, in Spanien, Deutschland, Georgien, Polen, Brasilien und der Tschechischen Republik.

Anstatt sich an die alteingesessene Methode zu halten und einen gefälschten Kartenleser in den Geldautomaten zu montieren, übernehmen die Angreifer die Kontrolle über den gesamten Automaten. Sie beginnen mit der Installation der Skimer-Malware auf dem Bankomaten – entweder, indem sie physisch auf ihn zugreifen oder indem sie das interne Netzwerk der Bank kompromittieren. Das Schadprogramm infiziert den Kern des Geldautomaten: den Teil des Geräts, der für die Interaktion mit der weiter gefassten Banken-Infrastruktur, für die Kartenverarbeitung und die Bargeldausgabe verantwortlich ist. Im Gegensatz zu einem traditionellen Karten-Skimmer gibt es keine physischen Anzeichen für eine Infektion, so dass die Angreifer in aller Ruhe Daten von den Karten abgreifen können, die an dem Geldautomaten benutzt werden (inklusive der Kontonummer und PIN eines Kunden), oder auch direkt Geld stehlen können.

Unsichere Bankautomaten sind zu einem Hauptziel von Cyberattacken geworden.

Die Angreifer erwecken einen Automaten zum Leben, indem sie eine Karte einführen, die bestimmte Einträge auf dem Magnetstreifen enthält. Nachdem Skimer die Karte gelesen hat, ist die Malware in der Lage, einen hart codierten Befehl auszuführen oder Befehle über ein spezielles Menü zu empfangen, das von der Karte aktiviert wurde. Die Benutzeroberfläche von Skimer erscheint erst auf dem Display, nachdem die Karte ausgeworfen wurde und auch nur dann, wenn innerhalb von 60 Sekunden der korrekte Sitzungsschlüssel eingegeben wird. Das Menü bietet 21 verschiedene Optionen, unter anderem Bargeldausgabe, Abgreifen von Details zu den Karten, die in den Automaten eingesteckt wurden, Selbstlöschung und Aktualisierung. Die Cyberkriminellen können die Kartendetails auf dem Chip ihrer Karte speichern oder die zusammengetragenen Daten ausdrucken.

Die Angreifer achten penibel darauf, keine Aufmerksamkeit auf sich und ihren Schädling zu lenken. Statt direkt Geld vom Automaten abzuheben – was umgehend auffallen würde – warten sie ab (manchmal mehrere Monate), bevor sie in Aktion treten. In den meisten Fällen sammeln sie Daten von den ausgelesenen Karten, um diese zu klonen. Sie benutzen die geklonten Karten dann später an anderen, nicht infizierten Geldautomaten und heben gelegentlich Geld von den Konten der Opfer ab, ohne dass ein Zusammenhang zu dem kompromittierten Bankautomaten hergestellt werden kann.

Die Zunahme von Angriffen auf Geldautomaten in den letzten Jahren spiegelt eine natürliche Evolution der bereits etablierten Methode unter Einsatz von physischen Kartenlesern wider, die Daten von den Karten lesen, die in manipulierte Geldautomaten eingeführt werden. Leider laufen auf vielen Bankomaten Betriebssysteme mit bekannten Sicherheitsschwächen. Dadurch wird die physische Sicherheit umso wichtiger.

Um die Banken dabei zu unterstützen, sich selbst zu schützen, empfiehlt Kaspersky Lab: regelmäßige AV-Scans, die Nutzung von Whitelisting-Technologien, eine gute Gerätemanagement-Policy, vollständige Festplattenverschlüsselung sowie einen Schutz des Geldautomaten-BIOS mit einem Passwort, das ausschließlich das Booten von der Festplatte erlaubt. Außerdem raten wir dazu, das Geldautomaten-Netzwerk von der restlichen Bankeninfrastruktur zu isolieren. Eine unserer Expertinnen hat eine **Tiefenanalyse über das Knacken von Geldautomaten veröffentlicht** und erläutert, was getan werden müsste, um die Geräte sicher zu machen.

Doch selbstverständlich ermitteln wir nicht nur in Fällen von Angriffen, die bereits stattgefunden haben. Wir setzen uns auch mit aufkommenden Technologien auseinander und fragen uns, wie Cybergangster diese zu ihren Zwecken missbrauchen könnten. Kürzlich haben wir die Ergebnisse unserer Untersuchung der potenziellen Authentifizierungsmethoden veröffentlicht, zu denen neben Einmal-Passwörtern und Biometrie auch die kontaktlose Authentifizierung via **NFC** gehört. Es mag den einen oder anderen überraschen, dass wir zwölf Hersteller aufgetan haben, die bereits jetzt gefälschte Fingerabdruck-Scanner (das heißt also biometrische Skimmer) anbieten und mindestens drei weitere Anbieter, die an Geräten arbeiten, mit denen Cyberkriminelle Daten von Handvenen- und Iriserkennungssystemen abgreifen können. Den Bericht finden Sie **hier**.

Neue biometrische Skimmer greifen Authentifizierungsmethoden der nächsten Generation an – Fingerabdruck-, Handvenen- und Iriserkennungssysteme.

DAS INTERNET DER DINGE

Heutzutage sind wir umgeben von intelligenten Geräten. Eine zunehmende Zahl von Haushaltsgegenständen ist heute intelligent: Telefone, Fernseher, Thermostate, Kühlschränke, Babyphones, Fitnessarmbänder und sogar Kinderspielzeug. Einige Häuser werden sogar mit integrierter „Intelligenz" gebaut. Doch die Liste der smarten Geräte beschränkt sich nicht auf Apparate rund um unser Heim, sie umfasst auch Autos, medizinische Ausrüstung, Überwachungskameras und Parkuhren. Das allgegenwärtige Wi-Fi (wenn auch nicht immer so allgegenwärtig, wie wir es uns manchmal wünschen) bringt alle diese Geräte online, als Teil des Internet der Dinge (IoT).

Das Risiko, ausnahmslos alles ohne Rücksicht zu verbinden – müssen wir im Jahr 2016 noch mehr sagen?

Alle diese Dinge wurden geschaffen, um uns das Leben leichter zu machen. Seitdem verbundene Alltagsgeräte in der Lage sind, ohne menschliche Interaktion automatisch Daten zu sammeln und zu übertragen, können sie weitaus effektiver arbeiten. Doch eine Welt aus verbundenen Alltagsgegenständen bietet Cyberkriminellen auch eine größere Angriffsfläche. Sind die IoT-Geräte nicht gesichert, können die persönlichen Daten, die sie austauschen, kompromittiert werden, sie können entweder selbst angegriffen oder für einen Angriff missbraucht werden.

Leider lassen sich Sicherheitsfeatures nur schwer verkaufen. Verbundene Geräte werden von verschiedenen Anbietern hergestellt, in einem offenen Markt, in dem die Rendite entscheidend ist. In einem wettbewerbsorientierten Markt haben meist die Dinge Vorrang, die den Kunden das Leben erleichtern. Hinzu kommt, dass Konnektivität meist bereits bestehenden Kommunikationsnetzwerken hinzugefügt wird, die nicht mit dem Gedanken an Sicherheit im Hinterkopf erschaffen wurden. So spielt Sicherheit im Entwicklungsstadium oftmals keine Rolle – wenn sie denn überhaupt eine Rolle spielt. Das Problem der Sicherheit wurde häufig immer erst dann in Angriff genommen, nachdem etwas Negatives passiert war, das die Auswirkungen von Sicherheitslücken deutlich gemacht hat.

In den letzten Jahren haben Forscher Sicherheitsprobleme in verschiedenen verbundenen Geräten behandelt. Vielleicht erinnern Sie sich noch daran, dass einer unserer Sicherheitsforscher sein eigenes Zuhause unter die Lupe nahm, um herauszufinden, wie angreifbar er wirklich ist. Im letzten Jahr demonstrierten Charlie Miller und Chris Valasek, wie es möglich sein konnte, sich drahtlosen Zugriff auf die kritischen Systeme eines Jeep Cherokee zu verschaffen, den Wagen vollständig unter Kontrolle zu bringen und ihn von der Straße abzubringen! Vasilios Hioureas von Kaspersky Lab und Thomas Kinsey von Exigent Systems führten Untersuchungen zu potenziellen Sicherheitsschwächen in Videoüberwachungsanlagen durch. In jüngerer Zeit meldete ein Hersteller eine Sicherheitslücke in einer seiner Insulinpumpen, die es einem Angreifer ermöglichen könnte, das Gerät abzuschalten oder die Dosis zu ändern. Auch alltägliche Haushaltsgeräte wie Kinderspielzeug, Babyphones und Türklingeln gaben Anlass zur Sorge.

Im Februar zeigten wir, wie leicht es ist, sich Zugriff auf das interne Netzwerk eines Krankenhauses zu verschaffen und die Kontrolle über ein MRT-Gerät zu übernehmen – sich somit persönliche Daten über die Patienten und ihre Therapie anzueignen und auf das Dateisystem des MRT-Gerätes zuzugreifen. Unser Experte Sergey Lozhkin präsentierte seine Erkenntnisse auf dem diesjährigen Security Analyst Summit und arbeitete dabei die Schlüsselfaktoren heraus, die die Sicherheit von Krankenhaussystemen beeinträchtigen. Erstens konnte auf mit dem Internet verbundene medizinische Geräte mit Standard-Passwörtern zugegriffen werden. Auf einigen lief Windows XP und sie waren anfällig für Dutzende alter, ungepatchter Sicherheitslücken, die hätten genutzt werden können, um Krankenhaussysteme

↺ ZURÜCK ZUM INHALT

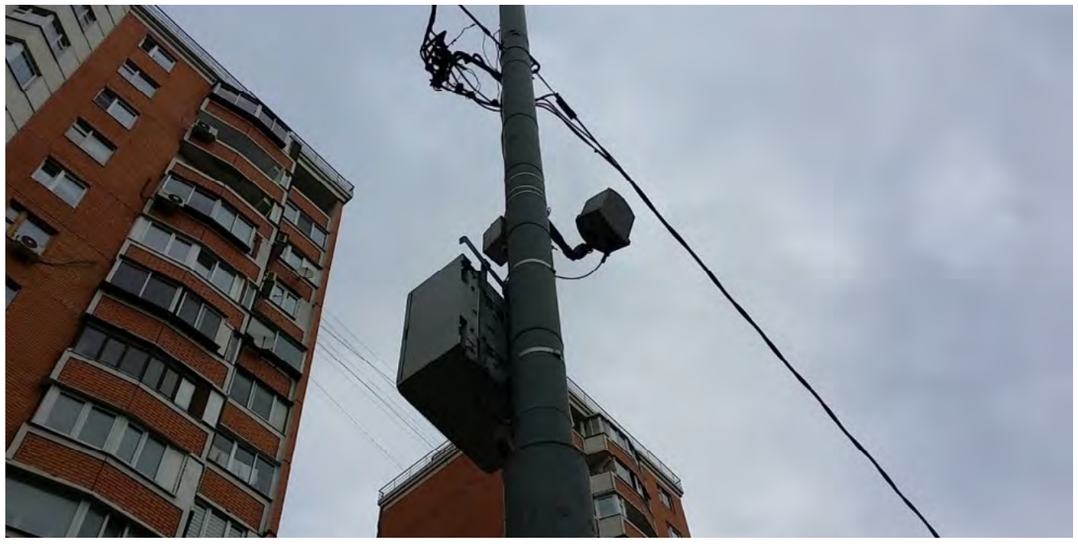
zu kompromittieren. Zweitens waren diese medizinischen Geräte nicht vom lokalen Netzwerk der Klinik getrennt. Hätte man sich also auf eins der Wi-Fi-Netze des Krankenhauses Zugriff verschafft (von einem schwachen Passwort geschützt), hätte man vollen Zugriff auf diese Geräte erhalten. Drittens machten es Sicherheitslücken in der Software-Architektur möglich, auf das Kontrollinterface und die persönlichen und krankheitsbezogenen Daten der Patienten zuzugreifen, wenn man sich zuvor mit dem Gerät verbunden und die Felder im Standard-Login-Bildschirm ausgefüllt hatte. Überdies war eine Kommandozeile in die Benutzeroberfläche implementiert, die Zugriff auf das Dateisystem des Gerätes ermöglichte. Den Bericht finden Sie hier.

Krankenhäuser sollten die folgenden Maßnahmen ergreifen, um ihre Systeme zu schützen:

- Verwendung starker Passwörter zum Schutz der externen Verbindungspunkte.
- Aktualisieren der IT-Sicherheitsrichtlinien, Entwicklung von Schwachstellen-Assessments und Patch-Systemen.
- Schutz medizinischer Ausrüstung im lokalen Netzwerk durch Passwörter, im Fall von unautorisiertem Eindringen in einen vertrauenswürdigen Bereich.
- Schutz der Infrastruktur vor Malware- und Hacker-Attacken mit Hilfe einer umfassenden Sicherheitslösung.
- Regelmäßige Sicherheitskopien kritischer Informationen und Speichern einer Kopie offline.

Im April veröffentlichte Kaspersky Lab eine Studie über Verkehrssensoren, die in den letzten Jahren in russischen Städten und anderorts buchstäblich aus dem Nichts auftauchten. Diese Sensoren können dazu beitragen, Geschwindigkeitsbegrenzungen durchzusetzen. Die Radarwarngeräte der Autofahrer reagierten auf die Signale der neuen Sensoren auf dieselbe Weise wie auf die Radarpistolen der Verkehrspolizei. Doch aus diesem Grunde waren die Sensoren nicht installiert worden. Sie sammeln Rohdaten über den Verkehr auf den Straßen (Anzahl der Autos auf jeder Spur, Durchschnittsgeschwindigkeit und so weiter) und geben sie zur Analyse an die zuständigen Behörden weiter.

Die Studie zu den Verkehrssensoren hat gezeigt, dass der Ansatz „Sicherheit durch Geheimhaltung" in einer verbunden Welt nicht funktioniert.



Unser Experte Denis Legezo fand heraus, dass der Datenverkehr nicht geschützt ist und manipuliert werden kann. Es gab keine Autorisierung, außer für Bluetooth, und selbst das war nicht sauber konfiguriert. Der Hersteller der Verkehrssensoren, die wir untersuchten, war bei seiner Unterstützung der Servicetechniker sehr großzügig und machte eine Menge von Informationen über die Geräte auf seiner offiziellen Webseite sowie auch an anderer Stelle öffentlich verfügbar.

↺ ZURÜCK ZUM INHALT

Das ist durchaus positiv. „Sicherheit durch Unklarheit" ergibt nicht unbedingt einen Sinn. Jeder halbwegs begabte Hacker findet das Befehlssystem so oder so heraus und kommt dann irgendwie an die Ingenieurssoftware heran. Daher sollte man viel eher Offenheit, ein Bug-Bounty-Programm und eine schnelle Reaktion auf gefundene Sicherheitslücken soweit es geht miteinander kombinieren – und sei es allein deshalb, weil die Zahl der Forscher immer größer sein wird als die der Mitarbeiter in irgendwelchen IT-Sicherheitsabteilungen. Den Bericht finden Sie **hier**.

Intelligente Städte sind ein komplexes, offenes Ökosystem, das ein „maßgeschneidertes Sicherheitskonzept" erforderlich macht.

Moderne Städte sind komplexe Ökosysteme, bestehend aus hunderten von unterschiedlichen Komponenten, darunter auch digitale. Intelligente Städte sollen ihren Bewohnern das Leben erleichtern, es komfortabler und sicherer machen. Doch wenn etwas gebraucht werden kann, so kann es auch missbraucht werden. Im September stellten wir unsere Forschungsergebnisse zu verschiedenen Aspekten intelligenter Städte vor. Unsere Experten Denis Makrushin und Vladimir Dashchenko verfassten auf der Grundlage ihrer Studien einen Bericht im Rahmen der internationalen gemeinnützigen Initiative „**Securing Smart Cities**", die von Kaspersky Lab unterstützt wird und zum Ziel hat, Experten im Bereich IT-Sicherheit von Technologien in intelligenten Städten zusammenzubringen. Ticketautomaten in Kinos, Terminals an Leihfahrradstationen, elektronische Warteschlangensysteme in Behörden, Buchungs- und Informationsterminals an Flughäfen sowie Informations- und Unterhaltungsterminals in Taxis mögen sich äußerlich klar voneinander unterscheiden, aber das Innenleben der meisten dieser Apparate ist gleich. Jeder dieser Terminals ist entweder ein Gerät auf Windows- oder auf Android-Basis. Der wichtigste Unterschied gegenüber gewöhnlichen Geräten ist eine spezielle Kiosk-Modus-Software, die auf öffentlichen Terminals läuft und als Benutzeroberfläche dient. Diese Software bietet einfachen Zugriff auf die speziellen Terminal-Funktionen, während sie den Zugriff auf andere Funktionen des Betriebssystems sperrt, unter anderem den Start eines Webbrowsers und den darauffolgenden Start einer virtuellen Tastatur. Der Zugriff auf diese Funktionen gibt einem Angreifer zahlreiche Möglichkeiten zur Kompromittierung des Systems in die Hand, genau so, als würde er vor einem PC sitzen. Die Studie hat gezeigt, dass fast jeder digitale öffentliche Kiosk eine oder mehrere Sicherheitsanfälligkeiten aufweist, die es einem Angreifer ermöglichen, auf verborgene Features des Betriebssystems zuzugreifen. Den Bericht finden Sie **hier.**

Die meisten öffentlichen Terminals verbergen ihr Betriebssystem hinter einer speziellen Benutzeroberfläche – doch die enthält Schwachstellen, die Angreifer hereinlassen.

Immer mehr Aspekte unseres Alltags werden digital. Wird die Sicherheit nicht schon im Entwicklungsstadium berücksichtigt, könnten die potenziellen Gefahren weitreichend sein – und das nachträgliche Anpassen von Sicherheitsmaßnahmen könnte sich als nicht unkompliziert erweisen. Damit die Bewohner sicher und komfortabel in intelligenten Städten leben können, müssen letztere wie Informationssysteme behandelt werden, deren Schutz einen maßgeschneiderten Ansatz und Fachkenntnisse erfordert.

Im Oktober benutzten Cyberkriminelle ein Botnet aus mit dem Internet verbundenen Heimgeräten (wie etwa IP-fähige Kameras, DVR-Player, Videoüberwachungskameras und Drucker), um eine **DDoS-Attacke gegen Dyn** zu initiieren – ein Unternehmen, das **DNS**-Services für Twitter, Amazon, PayPal, Netflix und andere bereitstellt. Der Angriff hatte zur Folge, dass die Webseiten dieser Unternehmen zusammenbrachen oder nur noch zeitweise erreichbar waren. Die Angreifer hatten verwundbare Geräte mit der Mirai-Malware infiziert. Dieses Schadprogramm war bereits vorher verwendet worden,

und zwar im Rahmen einer DDoS-Attacke gegen die Blog-Webseite des Sicherheitsforschers Brian Krebs – angeblich die leistungsstärkste DDoS-Attacke aller Zeiten (denn da der Quellcode von Mirai kürzlich online veröffentlicht wurde, bedeutet es nicht, dass die Attacke von denselben Hackern durchgeführt wurde wie die auf Dyn). Schätzungen zufolge umfasst das Mirai-Botnet etwa 550.000 Bots. Die Angreifer benutzten voreingestellte Standardpasswörter, um auf die Online-Geräte zuzugreifen. War der Schadcode in ein Gerät geschrieben, wurde es Teil des Mirai-Botnets. Wie bei jeder anderen DDoS-Attacke auch verwendeten die Angreifer die kompromittierten Geräte, um die Webseite des auserwählten Opfers mit Traffic zu überschwemmen und so einen normalen Betrieb unmöglich zu machen.

Das Internet wurde von Küchengeräten übertölpelt.

Wie auch bei vielen anderen Attacken unter Beteiligung von kompromittierten IoT-Geräten machten sich die Hintermänner dieses Angriffs die Tatsache zunutze, dass viele Leute die Standardzugangsdaten des Herstellers nicht ändern, wenn sie ein smartes Gerät kaufen. Dadurch können sich Angreifer problemlos Zugriff auf das Gerät verschaffen, indem sie einfach das bekannte Standardpasswort ausprobieren. Hinzu kommt, dass es für viele Geräte keine Firmware-Updates gibt. IoT-Geräte sind auch ein beliebtes Ziel für Cyberverbrecher, da sie meistens rund um die Uhr und sieben Tage in der Woche mit dem Internet verbunden sind.

Der beste Ratschlag für jeden, der zu Hause mit dem Internet verbundene beziehungsweise IoT-Geräte verwendet, lautet: das Standardpasswort auf allen Geräten muss geändert werden (und durch ein einmaliges, komplexes Passwort ersetzt werden), um zu verhindern, dass aus der Ferne darauf zugegriffen wird. Dazu zählen auch Heimrouter, die das Einfallstor in das Heimnetzwerk sind. Angesichts solcher Nachrichten werden viele vielleicht versucht sein, alle Geräte vom Internet zu trennen, aber in der heutigen zunehmend vernetzten Welt ist das nicht realistisch. Es ist allerdings immer gut, die Funktionalität eines smarten Geräts zu überprüfen und alle Funktionen zu deaktivieren, die nicht benötigt werden. Doch eine gute Passwort-Organisation trägt viel dazu bei, Cyberkriminelle von Ihren Geräten fernzuhalten. Diese Art von groß angelegten Attacken unterstreicht einmal mehr die Tatsache, dass Hersteller den Sicherheitsaspekt bereits im Entwicklungsstadium berücksichtigen müssen – und nicht erst nachträglich.

MOBILE BEDROHUNGEN

Die wichtigsten mobilen Bedrohungen im Jahr 2016 waren Werbe-Trojaner, die in der Lage sind, Rootrechte auf einem infizierten Gerät zu benutzen. Auch wenn es nichts grundsätzlich Neues für derartige Malware ist, sich mit Superuser-Rechten auszustatten, haben im Jahr 2016 immer mehr und mehr Android-Trojaner diese Rechte eingesetzt, mit denen sie alles nur Erdenkliche auf dem Gerät tun können. Um Rootrechte auf einem Gerät zu erhalten, müssen Trojaner Sicherheitslücken im System ausnutzen. Da viele Geräte nicht regelmäßig aktualisiert werden, erhalten sie auch nicht die entsprechenden Patches für diese Sicherheitslücken. Aus diesem Grunde sagen wir eine Zunahme bezüglich Anzahl und Raffinesse von Trojanern vorher, die diese Rechte nutzen.

Die letzten Android-Updates beseitigten nicht nur Schwachstellen, sondern sie enthielten auch neue Sicherheitsfunktionen, die die Trojaner schnell zu umgehen lernten. Wir erwarten, dass künftig mehr neue Sicherheitsfeatures erfolgreich unterlaufen werden. Einige dieser Funktionen könnten Attacken von mobiler Ransomware unterbrechen, daher wird sich deren Verhalten parallel dazu ändern.

> Der Feind in meinem Smartphone

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
RÜCKBLICK

Malware mit Rootrechten

Die populärsten und gefährlichsten mobilen Trojaner im Jahr 2016 waren Werbe-Trojaner, die Superuser-Rechte auf dem Gerät benutzen können. Die meisten dieser Schädlinge stammten aus den Familien Trojan.AndroidOS.Ztorg und Trojan.AndroidOS.Iop.

Im Laufe des gesamten Jahres 2016 hielt das Wachstum dieser Malware an und sie verdoppelten gegenüber dem vorangegangenen Jahr die Zahl ihrer Vertreter in den Top 30 der populärsten Trojaner (mit 22 Positionen im Jahr 2016 verglichen mit elf Positionen im Jahr 2015).

Um Superuser-Rechte zu erhalten, können die Schädlinge verschiedene Exploits verwenden oder bereits existierende Superuser-Rechte, wenn das Gerät früher schon gerootet wurde.

Die Trojaner nutzen die Rootrechte in erster Linie für zwei Dinge. Erstens können sie sich selbst in einem Systemverzeichnis verstecken, was bedeutet, dass es fast unmöglich wird, sie zu löschen. Einige von ihnen sind sogar in der Lage, das Recovery Image zu infizieren, wodurch es unmöglich wird, sie über ein Zurücksetzen auf die Werkseinstellungen zu löschen. Zweitens nutzen sie die Superuser-Rechte, um heimlich, still und leise verschiedene Apps zu installieren und zu starten, die aggressiv Werbung anzeigen. Bei den meisten dieser neu installierten Apps handelt es sich um nicht-schädliche Anwendungen mit Werbeeinblendungen, doch in manchen Fällen wurde auch neue Malware installiert, unter anderem die modulare Backdoor.AndroidOS.Triada, die in den Zygote-Prozess eindringt. Dadurch setzt sich die Malware nachhaltig im System fest und kann SMS modifizieren, die von anderen Apps gesendet wurden, um dem Nutzer auf diese Weise Geld zu stehlen. Unter Verwendung von Rootrechten kann dieser Trojaner buchstäblich alles tun, unter anderem auch URLs in Browsern austauschen.

Immer mehr mobile Trojaner eignen sich Rootrechte an – um nicht gelöscht zu werden und um weitere Adware und Malware zu installieren.

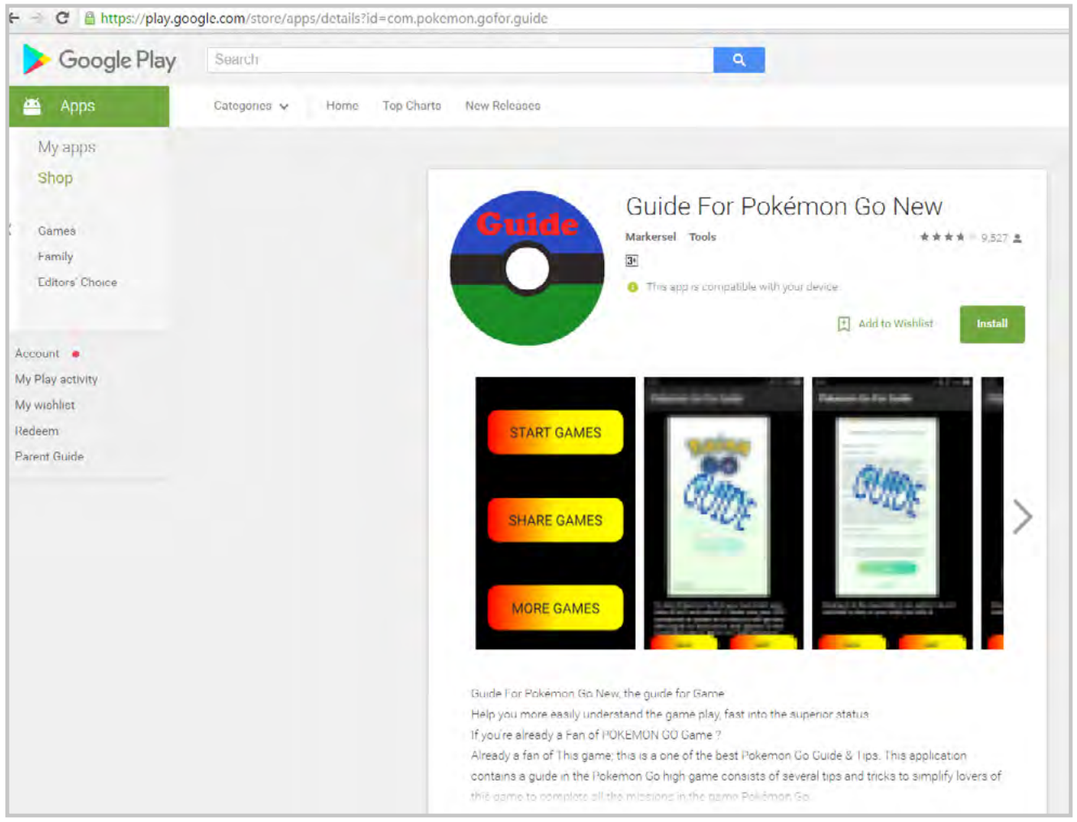
Ein Gerät, das mit einer Werbe-App infiziert wurde, ist aufgrund der Unmenge an lästiger Werbung und installierten Apps praktisch nicht mehr zu gebrauchen. Solche Trojaner lassen sich nur sehr schwer löschen und sie können heimlich neue Apps aus dem Google Play Store installieren, sogar kostenpflichtige.

Zumeist werden diese Schädlinge über Dritt-App-Stores verbreitet, doch manchmal sind sie auch schon auf niedrigpreisigen Geräten vorinstalliert. Im Laufe des Jahres konnten wir auch beobachten, dass sie über den Google Play Store verbreitet wurden. Laut der Google-Play-Statistik wurden sie in einigen Fällen über 100.000 Mal installiert. In einem Fall erreichten die Cyberkriminellen über 500.000 Installationen des Schädlings Trojan.AndroidOS.Ztorg.am über Google Play, wobei sie eine infizierte App benutzten, die sich als Anleitung für Pokemon GO ausgab.

Cyberkriminelle nutzen noch immer den Google Play Store aus

Cyberkriminelle haben weiterhin den Google Play Store missbraucht, um ihre Malware in Umlauf zu bringen. Innerhalb von nur einer Woche im Oktober entdeckten wir mehr als zehn neue Apps im Google Play Store, die mit Trojan.AndroidOS.Ztorg.am infiziert waren, einer neuen Modifikation von Trojan.AndroidOS.Ztorg.ad. Viele dieser neuen Apps wurden mehr als 100.000 Mal installiert.

Über Google Play verbreitete Malware wurde hunderttausende Male heruntergeladen.

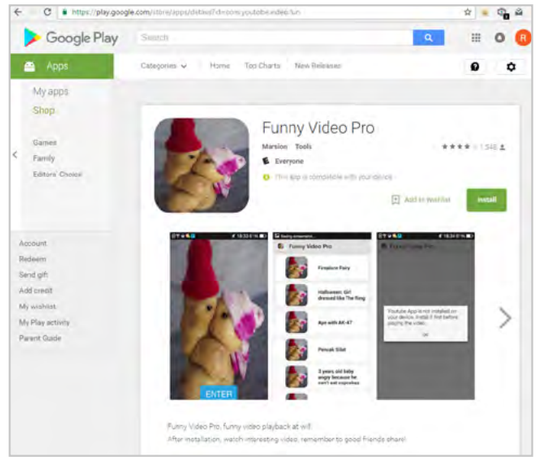


Trojan.AndroidOS.Ztorg.ad im Google Play Store

Doch nicht nur Malware, die Rootrechte nutzt, wird über Google Play in Umlauf gebracht, sondern auch Passwörter stehlende Trojaner. Im Oktober 2015 entdeckten wir Trojan-PSW.AndroidOS.MyVk.a im Google Play Store. Diese infizierte App wurde mehr als 100.000 Mal installiert und sah aus wie eine App zum Abspielen von Musik aus dem russischen sozialen Netzwerk VKontakte.

Tatsächlich aber stahl sie die Zugangsdaten der Nutzer zu diesem Sozialen Netzwerk. Im Laufe des Jahres luden Cyberbetrüger mehrfach neue Modifikationen dieses Trojaners in den Google Play Store hoch. Um einen Sicherheitsscan zu umgehen, luden sie zunächst eine saubere App ohne schädliche Funktionalität hoch. Es folgten einige saubere Updates, bevor sie schließlich an einem gewissen Punkt eine infizierte Version hochluden. Diese Methode wandten sie mindestens zwei Mal an.

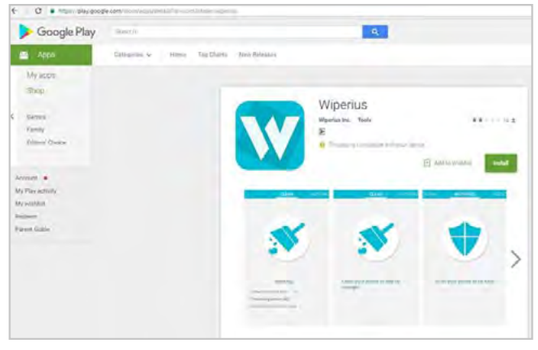
Ein Android-Trojaner installierte und aktualisierte eine saubere App, bevor er seine Ziele schließlich mit einem infizierten Update angriff.



Trojan.AndroidOS.Ztorg.am im Google Play Store

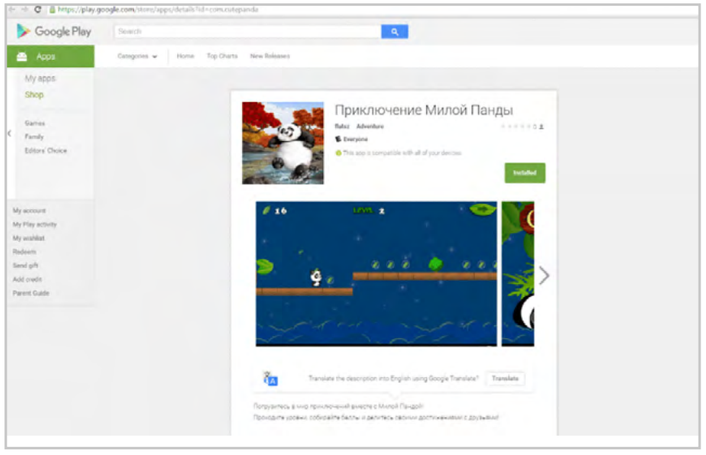
Ein weiteres Beispiel für Zugangsdaten stehlende Malware aus dem Google Play Store ist HEUR:Trojan-Spy.AndroidOS.Instealy.a. Damit präparierte Apps gaben vor, den Nutzer wissen zu lassen, wer sein Profil besucht hat. Tatsächlich aber missbrauchten sie den Authentifikationsprozess, um sich mit Instagram zu verbinden.

Aber nicht nur Malware mit Rootrechten und Passwort stehlende Trojaner wurden über den Google Play Store verbreitet. Wir beobachteten auch Fälle, in denen Cyberkriminelle diesen Kanal nutzten, um Trojan-Ransom.AndroidOS.Pletor.d in Umlauf zu bringen.



Trojan-Ransom.AndroidOS.Pletor.d im Google Play Store

Ursprünglich verschlüsselten die Vertreter der Familie Trojan-Ransom.AndroidOS.Pletor die Dateien der Nutzer auf dem infizierten Gerät, doch diese Modifikation blockiert das infizierte Gerät lediglich und fordert von dem Anwender Geld. Interessant ist, dass Pletor von derselben Cybercrime-Gang entwickelt wurde wie auch der mobile Banktrojaner Acecard. Im Dezember 2015 missbrauchte diese Gruppe den Google Play Store, um Trojan-Downloader.AndroidOS.Acecard.b zu verbreiten – einen Trojaner, der den Schädling Trojan-Banker.AndroidOS.Acecard.a herunterlädt und installiert.



Eine mit Trojan-Downloader.AndroidOS.Acecard.b infizierte App im Google Play Store

Nicht nur den Google Play Store

Während Werbe-Trojaner Exploits einsetzten, um nach der Infektion Superuser-Rechte zu erhalten, gab es auch einige Fälle, in denen Malware Exploits verwendete, um sich auszubreiten.

Unsere Kollegen von Bluecoat **entdeckten**, dass Trojan-Ransom.AndroidOS.Fusob von Exploits verbreitet wurde. Das Exploit-Kit konnte schädliche Apps herunterladen und installieren. Einige Zeit später **fanden wir heraus**, dass Cyberkriminelle versuchten, wohlbekannte Sicherheitslücken auszunutzen, um Schadprogramme zu verbreiten.

Eine weitere interessante Methode, um die Geräte der Nutzer zu infizieren, wurde angewandt, um den Bankenschädling Trojan-Banker.AndroidOS.Svpeng zu verbreiten. In diesem Fall missbrauchten Cyberkriminelle das **Werbenetzwerk Google AdSense**, um Trojan-Banker.AndroidOS.Svpeng.q an die Nutzer zu bringen. Svpeng kann **über ein Phishing-Fenster** Informationen über die Bankkarten des Nutzers stehlen und Textnachrichten abfangen, löschen und senden. Die Verbreitung über eines der größten Online-Werbenetzwerke machte Svpeng im Jahr 2016 zu dem populärsten Banktrojaner für Android. Überdies wurde er nach den Trojanern mit Rootrechten zum zweitpopulärsten Trojaner insgesamt.

Trojaner wurden auch über Werbenetzwerke verbreitet.

Umgehen von Sicherheitsfunktionen

Wie bereits erwähnt, entdeckten einige Trojaner im Jahr 2016 neue Wege, um einige Sicherheitsfeatures in Android zu umgehen.

In den neuesten Android-Versionen fragt das Betriebssystem den Nutzer beim SMS-Versand an eine Premium-Nummer um Erlaubnis. Der SMS-Trojaner Tiny zeigt über diesem Dialogfenster sein eigenes Fenster an, wobei er die Buttons auf dem Originalfenster nicht verdeckt.

Dieselbe Technik wurde auch von dem Schädling **Trojan-Banker.AndroidOS.Asacub** verwendet. In diesem Fall überdeckt der Trojaner das Standard-Systemfenster mit der Anfrage nach Administratorenrechten für das Gerät mit seinem eigenen Fenster inklusive Buttons. Auf diese Weise verbirgt der Trojaner den Erhalt von zusätzlichen Rechten im System vor dem Nutzer und veranlasst ihn mittels Betrug, diese Rechte zu bestätigen. Zudem wurde Asacub auch die Funktionalität eines SMS-Messengers hinzugefügt, und der Schädling bietet nun seine Dienste an Stelle der Standard-SMS-App des Geräts an. Dadurch kann der Trojaner Systemeinschränkungen umgehen, die mit Android 4.4 eingeführt wurden, und jede eingehende SMS löschen oder vor dem Nutzer verbergen.

Im Juni 2016 **entdeckten wir** eine neue Modifikation des Schädlings Trojan-Banker.AndroidOS.Gugi, die in der Lage ist, zwei neue Sicherheitsfeatures zu umgehen, die in Android 6 hinzugefügt wurden: berechtigungsbasiertes Überlagern von Apps und dynamische Berechtigungsanfrage für gefährliche In-App-Aktivität wie die Arbeit mit SMS oder das Durchführen von Anrufen. Diese Modifikation nutzt keine Sicherheitslücken aus, sondern arbeitet ausschließlich mit Social Engineering.

Die Trojaner Gugi und Asacub fanden Wege, neue Android-Sicherheitsfeatures zu umgehen.

Mobile Ransomware

Die populärste mobile Ransomware im Jahr 2016 war **Trojan-Ransom.AndroidOS.Fusob**. Am intensivsten wurde sie in Deutschland, den USA und in Großbritannien verbreitet. In der GUS und einigen Nachbarländern funktioniert sie hingegen nicht. Die Verbrecher verlangen normalerweise zwischen 100 und 200 US-Dollar, um das Gerät zu entsperren. Das Lösegeld muss in Form von Codes von vorausbezahlten iTunes-Karten entrichtet werden. Zwischen November 2015 und März 2016 ist die Popularität dieses Trojaners enorm gestiegen, mit einer Zunahme der angegriffenen Nutzer um ein Zwölffaches. Dann ging die Zahl der angegriffenen Anwender allerdings fast wieder auf das Vorjahresniveau zurück.

Zahl der individuellen, von Trojan-Ransom.AndroidOS.Fusob angegriffenen Nutzer

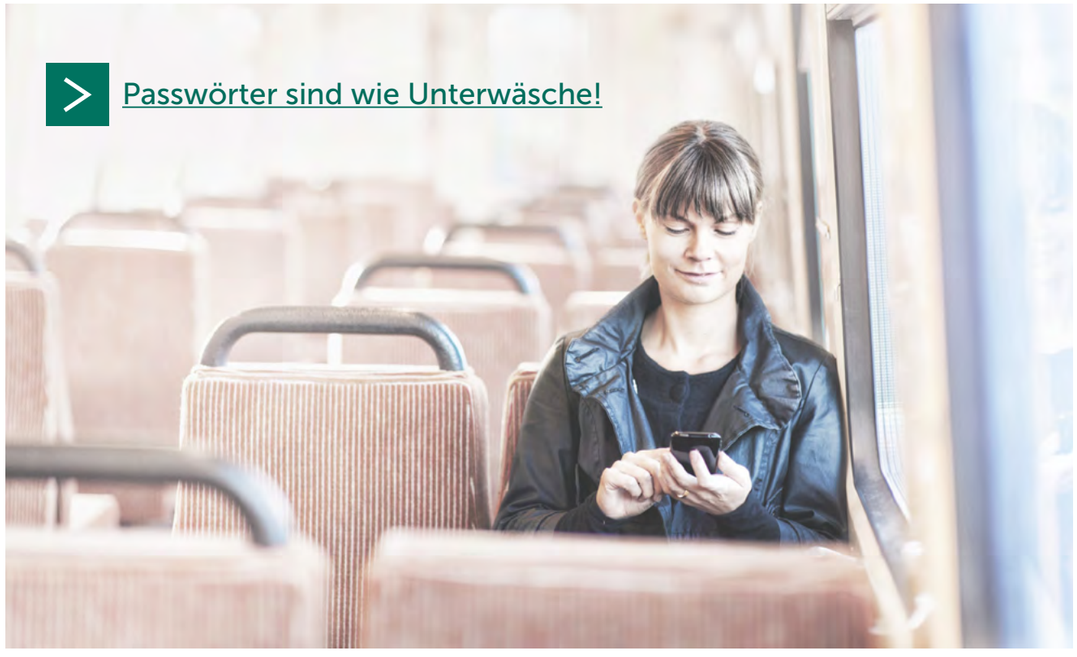
Während mehr Nutzer von mobilen Bankschädlingen als von mobiler Ransomware angegriffen werden, verhält es sich bei der Zahl der gesammelten Installationspakete umgekehrt. Beginnend mit dem zweiten Quartal 2016 ist die Zahl der Programme des Typs Trojan-Ransom höher als die des Typs Trojan-Banker.

Die ersten mobilen Erpressertrojaner verschlüsselten die Dateien der Nutzer und verlangten für die Dechiffrierung ein Lösegeld. Die meisten modernen trojanischen Erpresserprogramme für Android verschlüsseln hingegen keine Dateien mehr. Sie zeigen lediglich ihr eigenes Fenster über allen anderen Apps an und überdecken damit sogar Systemdialoge. Das Verschlüsseln von Dateien auf mobilen Geräten ist deswegen aus der Mode gekommen, weil es von den meisten Nutzerdaten auf mobilen Geräten normalerweise ein Backup in der Cloud gibt. Erpresser-Trojaner, die alle anderen Fenster mit ihrem eigenen Fenster überdecken, funktionieren auch und es ist sehr schwer, einen solchen Trojaner wieder loszuwerden.

Mobile Ransomware überdeckt Daten eher, als dass sie sie verschlüsselt, da es meist ein Backup in der Cloud gibt.

Trojan-Ransom.AndroidOS.Congur, eine der populärsten mobilen Ransomware-Familien in China, blockiert das infizierte Gerät auf andere Art: Das Schadprogramm erfragt direkt nach dem Start Geräteadministratorenrechte und ändert dann den PIN-Code oder richtet einen ein (falls es vorher keinen gab). Es fordert die Nutzer auf, die Cyberkriminellen via QQ-Messenger zu kontaktieren und den neuen Geräte-PIN-Code herauszufinden. Diese Methode ist äußerst simpel, aber trotzdem effektiv.

Trojanische Erpresserprogramme gehören zu den technisch einfachsten und den effektivsten Trojanern überhaupt. Daher erwarten wir ein weiteres Wachstum dieser Schädlingsgattung und das Erscheinen vieler neuer Ransomware-Familien im nächsten Jahr.



Passwörter sind wie Unterwäsche!

↺ ZURÜCK ZUM INHALT

Persönliche Informationen sind ein wertvolles Gut, daher ist es keine Überraschung, dass Cybergangster Online-Provider angreifen, um Daten en gros im Rahmen einer einzigen Attacke zu stehlen. Wir haben uns längst an den stetigen Strom von Sicherheitslecks gewöhnt, über die in den Massenmedien berichtet wird. Dieses Jahr bildete keine Ausnahme, mit Datenlecks bei beautifulpeople.com, Tumblr, dem Hacker-Forum nulled.io (was die Tatsache unterstreicht, dass nicht nur legitime Systeme angegriffen werden), Kiddicare, VK.com, Sage, dem offiziellen DotA-2-Forum, Yahoo, Brazzers, Weebly und der Tesco Bank.

Einige dieser Attacken endeten mit dem Diebstahl großer Datenmengen und bewiesen damit einmal mehr, dass viele Unternehmen keine adäquaten Maßnahmen ergreifen, um sich selbst zu schützen. Es geht nicht einfach darum, das Unternehmensperimeter vor Angriffen zu verteidigen.

So etwas wie hundertprozentige Sicherheit gibt es nicht. Daher kann auch niemand garantieren, dass nicht in das System eingebrochen werden kann, insbesondere dann nicht, wenn sich eine Lücke mit Hilfe eines Insiders auftut oder wenn ein Interner dazu gebracht wird, irgendetwas zu tun, was die Unternehmenssicherheit gefährdet.

Doch jede Organisation, die persönliche Daten verwaltet, hat die Pflicht, effektiv für die Sicherheit dieser Daten zu sorgen. Dazu gehört auch das Hashen und Salten der Kundenpasswörter und das Verschlüsseln anderer sensibler Daten.

Nutzer haben keine direkte Kontrolle über die Sicherheit der persönlichen Daten, die sie Online-Providern anvertrauen. Aber sie können den Schaden beschränken, der durch ein Sicherheitsleck bei einem Online-Provider entstehen kann, indem sie einmalige und komplexe Passwörter verwenden. Ein ideales Passwort ist mindestens 15 Zeichen lang und besteht aus einer Mischung aus Buchstaben, Zahlen und Symbolen der gesamten Tastatur. Sollte das eine allzu knifflige Aufgabe sein, so finden Sie hier einen Leitfaden zum Erstellen sicherer, aber leicht zu merkender Passwörter. Alternativ kann man eine Passwort-Manager-App verwenden, die alle Passwörter automatisch verwaltet.

Leider werden viel zu häufig leicht zu erratende Passwörter verwendet, meist ein und dasselbe für zahlreiche Online-Accounts. Wird dann das Passwort für ein Konto geknackt, so sind alle Online-Kennwörter des Opfers angreifbar. Dieses Problem geriet im Mai 2016 in den öffentlichen Fokus, als ein unter dem Namen „Peace" bekannter Hacker versuchte, 117 Millionen LinkedIn-Zugangsdaten zu verkaufen, die einige Jahre zuvor gestohlen worden waren. Mehr als eine Million der gestohlenen Passwörter lautete: „123456".

Der Diebstahl der LinkedIn-Daten offenbarte eine Million Accounts mit dem Passwort „123456".

Im Juli haben wir ein Jahr nach der Attacke, die zum Diebstahl von Nutzerdaten führte, einen Blick auf die Auswirkungen des Ashley-Madison-Lecks geworfen, und jedem, der sich mit dem Gedanken trägt, online nach der großen Liebe zu suchen, einige gute Ratschläge mit auf den Weg gegeben (sowie nützliche Tipps zur Verwaltung jedes beliebigen Online-Accounts).

Das Passwort-Problem bleibt aktuell. Wählen wir ein Passwort, das zu leicht zu erraten ist, öffnen wir dem Identitätsdiebstahl Tür und Tor. Das Problem wird verschärft, wenn wir ein und dasselbe Passwort für viele Online-Accounts verwenden. Daher bieten viele Provider,

darunter auch Apple, Google und Microsoft nun Zwei-Faktoren-Authentifizierung an. Dabei muss der Nutzer einen Code eingeben, der von einem Hardware-Token generiert oder auf ein mobiles Gerät gesendet wird, um auf eine Seite zugreifen zu können oder um zumindest Änderungen an den Account-Einstellungen vorzunehmen. Zwei-Faktoren-Authentifizierung erhöht die Sicherheit ganz bestimmt, aber nur, wenn sie auch wirklich gefordert und nicht nur als Option angeboten wird.

Bedenkt man die möglichen Auswirkungen, die eine Sicherheitslücke haben kann, überrascht es kaum, dass die zuständigen Behörden diesem Problem nun größere Aufmerksamkeit widmen. Das britische Information Commissioner's Office (ICO) erlegte dem Unternehmen Talk Talk im Zusammenhang mit einer Attacke auf die britische Telekommunikationsgruppe im Oktober 2015 kürzlich eine Strafe in Rekordhöhe von 400.000 britischen Pfund auf, da das Unternehmen es „versäumt hatte, die grundlegendsten Cybersicherheitsmaßnahmen zu ergreifen". Nach dem Willen des ICO soll diese Rekordstrafe „anderen als Mahnung dienen, dass Cybersicherheit keine IT-Angelegenheit, sondern Chefsache ist".

Die Datenschutz-Grundverordnung (General Data Protection Regulation, GDPR) der Europäischen Union, die im Mai 2018 in Kraft treten soll, verlangt von Unternehmen, den Behörden Datenlecks zu melden und sieht empfindliche Strafen für das Versäumnis vor, persönliche Daten angemessen zu sichern. Eine Zusammenfassung der Verordnung finden Sie hier. Es bleibt zu hoffen, dass dadurch gewährleistet wird, dass Unternehmen Datenlecks rechtzeitig melden. Dieses Problem trat in diesem Jahr besonders deutlich hervor, als Dropbox vielen seiner Nutzer eine Nachricht mit der Aufforderung schickte, ihre Passwörter zu ändern. Das Sicherheitsleck bei Dropbox im Jahr 2012 führte nicht nur zum Durchsickern von E-Mail-Adressen, sondern auch von Passwörtern. Dropbox informierte seine Nutzer über den Diebstahl der Mail-Adressen, nicht aber über den Verlust der Passwörter – jedenfalls nicht zu diesem Zeitpunkt. Glücklicherweise waren die Passwörter gehasht und gesaltet. Zudem bietet Dropbox eine Zwei-Schritte-Verifizierung an.

Einige Unternehmen hoffen, vollständig auf Passwörter verzichten zu können. Apple ermöglicht die Autorisierung per Fingerabdruck für iTunes-Käufe und Bezahlvorgänge mit Apple Pay. Samsung hat bekannt gegeben, die Authentifizierung mittels Fingerabdruck, Stimme und Iriserkennung für Samsung Pay einzuführen. Amazon hat die Technologie „selfie-pay" angekündigt. MasterCard und HSBC berichten über die Einführung von Gesichts- und Stimmerkennung zur Autorisierung von Transaktionen. Der wichtigste Vorteil liegt selbstverständlich darin, dass etwas ersetzt wird, was die Kunden sich merken müssen (ein Passwort), durch etwas, was sie haben – ohne die Möglichkeit, den Prozess abzukürzen (wie sie es tun, wenn sie ein schwaches Passwort wählen).

Biometrie erscheint vielen als die Authentifizierungsmethode der Zukunft. Doch sie ist kein Sicherheits-Patentrezept. Biometrie kann ausgetrickst werden, wie wir schon mehrfach diskutiert haben (hier, hier und hier), und biometrische Daten können gestohlen werden. Hilfreicher wäre es, nicht Passwörter, sondern Nutzernamen durch biometrische Daten zu ersetzen. Unerlässlich ist eine Multi-Faktoren-Authentifikation, eine Kombination aus drei Komponenten: etwas, was man weiß, etwas, was man hat und etwas, was man ist.

Eine über Passwörter hinausgehende Authentifizierung ist für die Sicherheit von essenzieller Bedeutung.

Kaspersky Cybersecurity Index

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
RÜCKBLICK

CYBERSICHERHEIT IN DER INDUSTRIE: BEDROHUNGEN UND VORFÄLLE

2016 war kein Jahr, das durch besonders viele oder besonders kritische Cybersicherheitsvorfälle in der Industrie in Erinnerung bleiben wird. Doch einige interessante Fälle gab es, auf die wir in unserem Jahresbericht näher eingehen wollen.

Vorfälle

In diesem Jahr gelangten zwei Cybersicherheitsvorfälle in Kernkraftwerken ans Licht der Öffentlichkeit. Der erste Fall ereignete sich Ende April, als das Betreiberunternehmen des deutschen Kernkraftwerks Gundremmingen über eine Infektion mit dem Wurm Kido (alias Conficker) auf den Rechnern der Brennelemente-Lademaschine in Block B berichtete. Glücklicherweise hatte der Wurm keinen Einfluss auf die technologischen Prozesse und das Kraftwerk wurde nicht beschädigt.

Die zuständigen Aufsichtsbehörden und das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden informiert. Alle kritischen Systeme und Geräte wurden überprüft und es wurden keine weiteren Hinweise auf eine schädliche Infektion gefunden. Infolge des Vorfalls wurden die Sicherheitsmaßnahmen ausgeweitet. Das Ereignis wurde der Kategorie N (normal) des deutschen Meldesystems zugeordnet. Die Gefährdungseinstufung gemäß der Internationalen Bewertungsskala für nukleare Ereignisse (INES) lautete „Abweichung" (Ereignis ohne oder mit geringer sicherheitstechnischer Bedeutung).

Die Infektionsquelle konnte nicht ausgemacht werden, aber der Pressesprecher des Kernkraftwerks berichtete, dass etwa 18 in dem Büro-Netzwerk verwendete USB-Sticks gefunden wurden, die ebenfalls mit dem Wurm Kido infiziert waren. Er sagte, dass kein Schaden verursacht wurde, weil alle kritischen Kontrollsysteme entkoppelt seien und die gesamte Systemarchitektur mehrfach gegen DoS abgesichert und vor Manipulation geschützt sei.

Auch wenn die Kido-Infektion in diesem Fall keinen ernsthaften Schaden angerichtet hat (glücklicherweise), wäre es naiv zu glauben, dass nur zielgerichtete und speziell maßgeschneiderte Malware dazu in der Lage ist. Ende 2015 wurden ukrainische Stromverteilungsanlagen von einer hochgradig koordinierten Cyberattacke getroffen. Die Angreifer verschickten Phishing-Mails mit Exploits an Personen im administrativen oder im IT-Netzwerk der Stromversorger. Sobald die ersten Computer infiziert waren, suchten und fanden die Angreifer einen Weg in das OT-Netzwerk und schafften es, die Stromversorgung zu unterbrechen. Außerdem, und das ist in diesem Fall besonders

wichtig, schnitten sie den Remote-Zugriff auf das Stromnetz ab. Durch das Löschen spezieller technischer Software und durch Manipulation des Bootsektors des Systems machten es die Angreifer unmöglich, das System aus der Ferne zu verwalten und zu reparieren.

Die Idee dahinter ist die folgende: selbst wenn die Malware keine technologischen Prozesse beeinflusst, aber eine Dienstverweigerung kritischer Hilfssysteme wie SCADA, OPS-Gateway, Remote-Zugriff, etc. auslöst, so wird das Industrielle Kontrollsystem (ICS) vermutlich gemäß den letzten Einstellungen weiterlaufen, aber es gibt keine Möglichkeit, den Prozess im Notfall zu kontrollieren oder zu korrigieren.

Vor Monaten **erklärte** Yukiya Amano, Generaldirektor der Internationalen Atomenergieorganisation (IAEA), dass vor zwei bis drei Jahren ein Atomkraftwerk von Hackern angegriffen wurde. Amano sagte dass „das tatsächlich passiert ist und es verursachte einige Probleme. Obwohl das Kraftwerk nicht heruntergefahren werden musste, wurden einige Vorsorgemaßnahmen notwendig". Aber es ist nicht nur das Problem, dass Mängel in der Cybersicherheit Störungen in AKWs verursachen. Offensichtlich besteht hier ein größeres Problem, das die Kommunikation und die Transparenz zwischen den ICS-Betreibern und der Cybersicherheits-Community betrifft. Am Ende des Tages haben Cybersicherheitsexperten keine Chance, die Probleme von ICS-Betreibern zu analysieren und die Anbieter können keine proaktiven Maßnahmen implementieren, die diese Probleme verringern würden.

Angriffe auf ICS, die der Sicherheitsbranche nicht gemeldet werden, können nicht analysiert werden und niemand lernt etwas daraus.

Proof-of-Concept-Malware auf SPS-Basis

Im August stellten Forscher aus dem Team von OpenSource Security auf der Black Hat 2016 einen Proof-of-Concept-Wurm (PoC) für speicherprogrammierbare Steuerungen (SPS) vor. Der ausschließlich als SPS-Programm geschriebene Wurm ist in der Lage, autonom speicherprogrammierbare Steuerungen zu identifizieren und sich im Netzwerk von einer SPS zur nächsten auszubreiten. Er kann zudem den Input und Output einer SPS manipulieren und Dienstverweigerungen bei SPS auslösen, sich mit Steuerungsservern verbinden und als Proxy für die Ausweitung des Angriffs dienen.

Der interessanteste Teil dieser Machbarkeitsstudie sind die Techniken, die verwendet werden, um eine speicherprogrammierbare Steuerung zu infizieren. Das PoC wurde für Siemens-S7-1200-Controller entwickelt, die über die Zugriffsschutzfunktion verfügen. Ist diese Funktion aktiviert, so verhindert sie, dass jemand ohne Passwort unter Verwendung des Protokolls S7CommPlus auf die speicherprogrammierbare Steuerung zugreifen kann und damit auch, dass ein Unbefugter den Code auf der SPS liest und modifiziert. Doch standardmäßig ist dieser Zugriffsschutz deaktiviert. Ist die Funktion angeschaltet, ist die einzige Möglichkeit für einen Wurm, eine SPS zu infizieren, das Passwort mittels Brute-Forcing zu knacken oder es auf irgendeine andere Weise zu kapern.

Wenn das Zugriffsschutzfeature aber deaktiviert ist, gibt es noch immer zwei weitere Schutzmechanismen, die den Zugriff auf die SPS einschränken sollen:

- Know-how-Schutz, der verbietet, das SPS-Programm von einem Gerät zu entfernen oder zu modifizieren.
- Kopierschutz, der das Kopieren des SPS-Programms auf ein anderes SPS-Gerät verbietet.

Die Zugriffsverifizierung für beide Schutzmechanismen, den „Know-how-Schutz" und den „Kopierschutz", wurde clientseitig implementiert (innerhalb des TIA-Portals). Das bedeutet, dass ein einfaches, selbstgeschriebenes Tool unter Umgehung der Authentifikationsüberprüfungen Blöcke auf

↺ ZURÜCK ZUM INHALT

der SPS lesen und schreiben kann. Siemens hat eine **Warnung** veröffentlicht und einen entsprechenden Patch für die S7-1200-Firmware bereitgestellt.

Die wichtige Lektion, die wir dabei lernen, lautet: jedes unautorisierte Gerät oder jeder Bedrohungsakteur mit Zugriff auf ein ICS-Netzwerk kann problemlos ganze Kontrollsysteme kompromittieren. Überdies sind SPS-Geräte anfälliger für Attacken (insbesondere für DoS), da sie normalerweise außer mit SCADA oder technischer Software mit nichts und niemandem kommunizieren. Aus diesem Grund gibt es nur geringen oder gar keinen Schutz vor unautorisiertem Zugriff, falschem Input oder schädlichen Manipulationen.

Zero-Days in ICS-Software und -Hardware

Laut Daten vom **US ICS CERT** wurden der Organisation im Haushaltsjahr 2015 (von Oktober 2015 bis September 2016) 427 Sicherheitslücken gemeldet – gegenüber 245 gemeldeten Sicherheitslücken im vorangegangenen Jahr. Ungefähr 25 Prozent dieser Sicherheitslücken waren auf eine unzureichende Eingabeüberprüfung zurückzuführen und 27 Prozent auf schwache Zugriffskontrolle. Die Existenz anderer signifikanter Schwachstellenkategorien – die Konfiguration oder den Betrieb betreffend – wird häufig von den Anbietern bestritten. Schwachpunkte wie Standard-Zugangsdaten, Standard-Sicherheitseinstellungen (die meist deaktiviert sind), verborgene API oder nicht dokumentierte Funktionalität sind äußerst gefährlich, da es keine besonderen technischen Fähigkeiten erfordert, sie auszunutzen, während sie gleichzeitig umfassenden Zugriff auf ein Kontrollsystem bieten.
Die schlechte Nachricht: nachdem ein Schwachstellenbericht an einen Hersteller gesendet wurde, vergeht unheimlich viel Zeit, bis der entsprechende Patch bereitgestellt wird. Manchmal passiert das nie, da der Hersteller **behauptet, das verwundbare Produkt sei ein Auslaufmodell**. Für den Betreiber einer ICS bedeutet das, entweder enorme Kosten für die Modernisierung auf sich zu nehmen, oder ein hohes Risiko einzugehen, kompromittiert zu werden.

Die Zeit zwischen dem Melden einer ICS-Sicherheitslücke und der Veröffentlichung eines Patches ist häufig zu lang.

Als Fazit möchten wir unterstreichen, wie wichtig es ist, dass die IT-Sicherheits-Communities ihren Beitrag zu der Cybersicherheit von ICS leisten. In den letzten Jahren beobachten wir ein deutlich gestiegenes Interesse an Themen, die die Sicherheit von industriellen Steuerungssystemen betreffen. Jedes Jahr wird eine beträchtliche Zahl an Forschungsberichten, aber auch an Tools und Frameworks veröffentlicht. Auch Kaspersky Lab hat in diesem Jahr einen Überblick über die Cybersicherheit in der Industrie und die entsprechende Bedrohungslandschaft publiziert. So wird es Cybersicherheitsexperten aus anderen Gebieten (nicht ICS) möglich, schnell auf den Zug aufzuspringen und ihre Erfahrungen und ihr Wissen beizusteuern.

KASPERSKY SECURITY BULLETIN. DIE STORY DES JAHRES. DIE RANSOMWARE-REVOLUTION

Autor(en): Fedor Sinitsyn, Anton Ivanov, Santiago Pontiroli, David Emm

QUICK INFO

↺ ZURÜCK ZUM INHALT

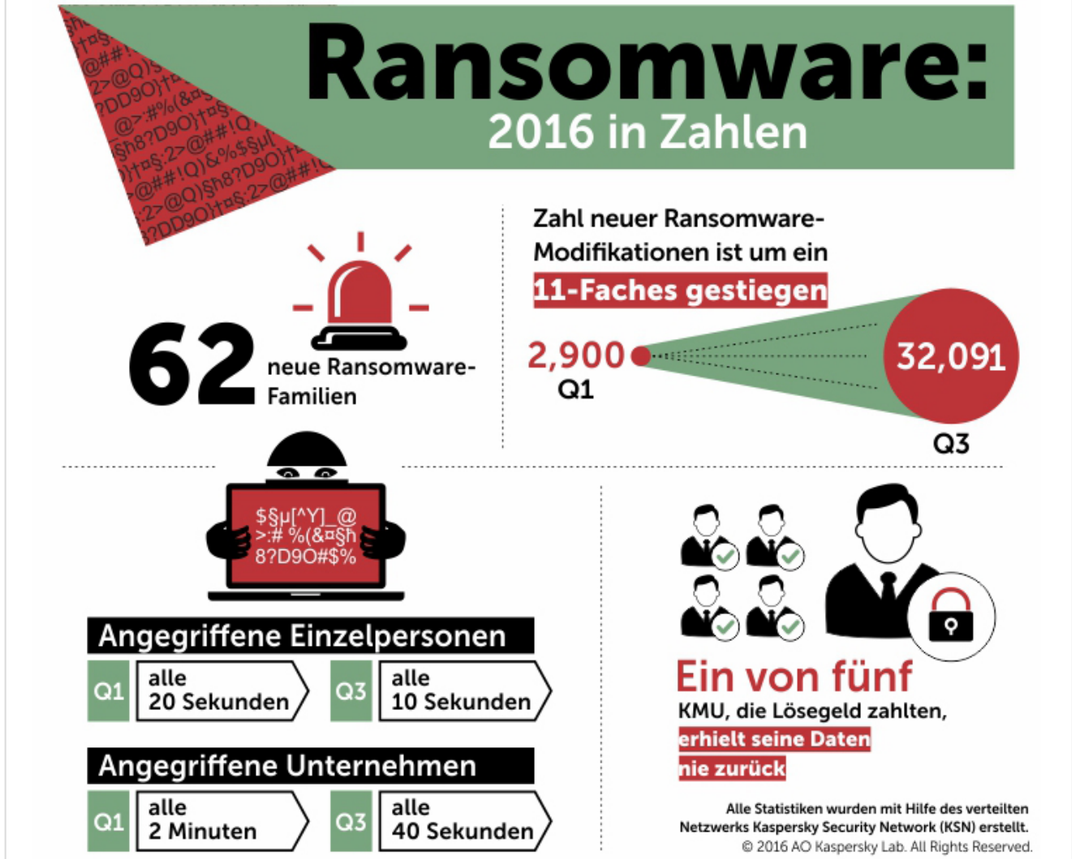
KASPERSKY SECURITY BULLETIN 2016/2017
DIE STORY DES JAHRES. DIE RANSOMWARE-REVOLUTION

EINLEITUNG

Im Jahr 2016 hat Ransomware ihren verheerenden Marsch um den gesamten Globus fortgesetzt und dabei Daten und Geräte, Heimanwender und Unternehmen fest in ihren Klammergriff genommen.

Die Zahlen sprechen für sich:

- Insgesamt 62 neue Ransomware-Familien sind in Erscheinung getreten.
- Die Zahl der Ransomware-Modifikationen hat um das 11-Fache zugenommen: von 2.900 neuen Modifikationen im Januar bis März auf 32.091 im Juli bis September.
- Zu Beginn des Jahres wurde alle 20 Sekunden ein Privatnutzer von Ransomware angegriffen. Gegen Ende des Jahres hatte sich die Frequenz auf alle 10 Sekunden erhöht.
- Zu Beginn des Jahres wurde alle zwei Minuten ein Unternehmen von Ransomware angegriffen, Ende September bereits alle 40 Sekunden.
- Eines von fünf kleinen und mittleren Unternehmen, die das geforderte Lösegeld gezahlt haben, hat seine Daten nie zurückerhalten.



Im Jahr 2016 haben aber auch Komplexität, Raffinesse und Vielfalt von Ransomware zugenommen, was sich beispielsweise an den folgenden Fakten festmachen lässt: Wandel bei der Entdeckung von Finanz-Software, Programmierung in Scripting-Sprachen, Beschreiten neuer Infektionswege, zunehmende Zielgerichtetheit und für technisch weniger Versierte das Angebot, fertige Ransomware-as-a-Service-Lösungen, Ressourcen oder Zeit bereitzustellen – all das mit Hilfe eines gedeihenden und immer effizienter werdenden Untergrund-Ökosystems.

Gleichzeitig begann sich die Welt im Jahr 2016 im Kampf gegen Ransomware zusammenzutun:

Das Projekt NoMoreRansom.org startete im Juli und brachte die niederländische Polizei, Europol, Intel Security und Kaspersky Lab an einen Tisch. Weitere 13 Organisationen kamen im Oktober hinzu. Zu den Ergebnissen dieser Zusammenarbeit gehören unter anderem eine Reihe von kostenlosen Dechiffrierungstools, die bisher tausenden Ransomware-Opfern dabei geholfen haben, ihre Daten wiederherzustellen.

Das ist nur die Spitze des Eisbergs und es gibt noch viel zu tun. Gemeinsam können wir weitaus mehr erreichen als jeder einzelne von uns für sich allein.

Was ist Ransomware?

Es gibt zwei Arten von Ransomware. Bei der am weitesten verbreiteten Art von Ransomware handelt es sich um Verschlüsselungssoftware. Solche Programme chiffrieren die Daten auf dem Gerät des Opfers und verlangen Geld als Gegenleistung für das Versprechen, die Daten wiederherzustellen. Die den Bildschirm blockierenden Programme hingegen beeinträchtigen die auf dem Gerät gespeicherten Daten nicht. Dafür verhindern sie, dass das Opfer auf sein Gerät zugreifen kann. Die auf dem gesamten Bildschirm angezeigte Lösegeldforderung kommt typischerweise als Nachricht irgendeiner Strafverfolgungsbehörde daher, in der es heißt, das Opfer habe auf illegale Webinhalte zugegriffen und müsse nun ein Verwarnungsgeld zahlen. Einen Überblick über beide Ransomware-Arten finden Sie **hier**.

„Die meisten Erpresser-Programme basieren auf einer merkwürdigen Vertrauensbeziehung zwischen dem Opfer und den Angreifern. Sie stützt sich auf das Versprechen, dass das Opfer, nachdem die Lösegeldzahlung beim Erpresser eingegangen ist, seine gekaperten Dateien zurückerhält. Die Cyberkriminellen haben dabei ein erstaunliches Maß an Professionalität an den Tag gelegt, was die Erfüllung dieses Versprechens angeht."

GReAT, Prognosen für 2017

↺ ZURÜCK ZUM INHALT

RANSOMWARE: DIE WICHTIGSTEN TRENDS UND ENTDECKUNGEN DES JAHRES 2016

Neuerscheinungen und Auslaufmodelle

Neuerscheinungen: Im Jahr 2016 sagte die Welt „Hallo" zu Cerber, Locky und CryptXXX – sowie zu 44.287 neuen Ransomware-Modifikationen

Cerber und **Locky** gaben ihr Debüt im frühen Frühjahr. Bei beiden handelt es sich um bösartige, aggressive Ransomware-Familien, die – in erster Linie mittels Spam-Attachments und Exploit-Kits - weit verbreitet werden. Sie haben sich mit Angriffen auf Individuen und Unternehmen gleichermaßen rasch selbst als „wichtige Player" auf der Cybercrime-Bühne etabliert. Kurz darauf folgte CryptXXX. Alle drei Familien entwickeln sich fortwährend weiter und zeigen der Welt, was Ransomware – über die alt eingesessenen Schädlinge wie CTB-Locker, CryptoWall und Shade hinaus – bedeutet.

Die Ransomware-Familie Locky hat sich bisher in 114 Ländern verbreitet.

Stand Oktober 2016: Die Top 10 der von Kaspersky-Lab-Produkten detektierten Ransomware-Familien:

	NAME	OBJEKTE*	PROZENTUALER ANTEIL DER NUTZER**
1	**CTB-Locker**	Trojan-Ransom.Win32.Onion Trojan-Ransom.NSIS.Onion	25,32
2	**Locky**	Trojan-Ransom.Win32.Locky Trojan-Dropper.JS.Locky	7,07
3	**TeslaCrypt** (aktiv seit Mai 2016)	Trojan-Dropper.JS.Locky	2,85
4	**Scatter**	Trojan-Ransom.Win32.Scatter Trojan-Ransom.BAT.Scatter Trojan-Downloader.JS.Scatter Trojan-Dropper.JS.Scatter	2,79
5	**Cryakl**	Trojan-Ransom.Win32.Cryakl	2,79
6	**CryptoWall**	Trojan-Ransom.Win32.Cryptodef	2,36
7	**Shade**	Trojan-Ransom.Win32.Shade	1,73
8	**(generic verdict)**	Trojan-Ransom.Win32.Snocry	1,26
9	**Crysis**	Trojan-Ransom.Win32.Crusis	1,15
10	**Cryrar/ACCDFISA**	Trojan-Ransom.Win32.Cryrar	0,90

* Die vorliegende Statistik basiert auf den von Kaspersky-Lab-Produkten detektierten Objekten, deren Nutzer ihre Zustimmung zur Übermittlung von statistischen Daten gegeben haben.
** Prozentualer Anteil der von einer konkreten Familie von Verschlüsselungs-Ransomware angegriffenen Nutzer an allen von Verschlüsselungs-Schädlingen angegriffenen Nutzern.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
DIE STORY DES JAHRES. DIE RANSOMWARE-REVOLUTION

Auslaufmodelle: Auf Wiedersehen Teslascrypt, Chimera und Wildfire – so schien es zumindest...

Die vermutlich größte Überraschung des Jahres 2016 war die Stilllegung von TeslaCrypt und die darauffolgende Veröffentlichung des Master Keys, vermutlich durch die Malware-Autoren selbst.

TeslaCrypt begeht Selbstmord – währenddessen erledigt die Polizei Encryptor RaaS und Wildfire.

Encryptor RaaS, einer der ersten Trojaner, der anderen Cyberkriminellen als Ransomware-as-a-Service-Modell zur Verfügung stand, wurde stillgelegt, nachdem ein Teil seines Botnetzes von der Polizei unschädlich gemacht worden war.

Im Juli wurden dann etwa 3.500 Schlüssel für die **Chimera**-Ransomware öffentlich gemacht – von Individuen, die behaupteten, hinter der Erpressersoftware Petya/Mischa zu stecken. Da Petya einen Teil des Chimera-Quellcodes für seine eigene Ransomware verwendete, könnte durchaus ein und dieselbe Gruppe für beide Bedrohungen verantwortlich sein, die ihre Produkte aktualisiert und Chaos gestiftet hat.

Auch die Familie **Wildfire**, deren Server beschlagnahmt wurden, und für die dank der gemeinsamen Anstrengungen von Kaspersky Lab, Intel Security und Europol ein Dechiffrierungsschlüssel entwickelt werden konnte, scheint nun unter dem Namen Hades wiederbelebt worden zu sein.

Missbrauch von „Weiterbildungs-Ransomware“

Wohlmeinende Forscher haben Ransomware zu Lernzwecken entwickelt, um Systemadministratoren ein Tool an die Hand zu geben, mit dem sie Angriffe von Erpressersoftware simulieren und ihre Abwehr auf den Prüfstand stellen können. Doch Cybergangster haben sich diese Tools schnell angeeignet, um sie zu ihren eigenen böswilligen Zwecken zu nutzen.

Zu „Lernzwecken“ entwickelte Ransomware bringt Ded_Cryptor und Fantom hervor – und viele andere Trojaner.

Die Entwickler der Lern-Ransomware **Hidden Tear & EDA2** veröffentlichten den Quellcode hilfsbereit auf GitHub. Unweigerlich erschienen daraufhin im Jahr 2016 zahlreiche bösartige Trojaner, die auf **eben diesem Code basieren**. Dazu zählt auch **Ded Cryptor**, der den Bildschirmhintergrund auf dem Computer des Opfers gegen ein Bild eines bösartig aussehenden Weihnachtsmannes austauschte und als Lösegeld satte zwei Bitcoins (etwa 1.300 €) verlangte. Ein anderes Programm dieser Art war **Fantom**, das einen täuschend echt aussehenden Windows-Update-Bildschirm anzeigte.

↺ ZURÜCK ZUM INHALT

Unkonventionelle Ansätze

- **Warum sich mit einer Datei herumschlagen, wenn du die ganze Festplatte haben kannst?**
  Zu den neuen Ansätzen im Bereich Ransomware-Attacken, die erstmals im Jahr 2016 beobachtet wurden, gehört die Verschlüsselung der Festplatte, wobei die Angreifer entweder den Zugriff auf die Dateien blockieren oder gleich alle Dateien auf einmal chiffrieren. Petya ist ein Beispiel für die Anwendung dieser Methode, wobei sie den Master Index (MFT) der Festplatte verschlüsselt und so einen Reboot unmöglich macht. Ein anderer Trojaner mit dem Namen Dcryptor, auch bekannt als Mamba, ging noch einen Schritt weiter und blockierte die gesamte Festplatte. Diese Ransomware ist ganz besonders unangenehm, da sie jeden Festplattensektor, inklusive Betriebssystem, geteilter Dateien und aller persönlicher Daten chiffriert – mit Hilfe einer Kopie der Open-Source-Software DiskCryptor.

Angreifer haben es heute auf Backups und Festplatten abgesehen – und sie knacken Passwörter mittels Brute-Forcing.

- **Die „manuelle“ Infektionstechnik**
  Die Infektion mit Dcrypter wird manuell vollzogen, wobei die Angreifer die Passwörter für den entfernten Zugriff auf den Rechner des Opfers via Brute-Forcing knacken. Wenn er auch nicht neu ist, so hat dieser Ansatz im Jahr 2016 doch deutlich an Beliebtheit zugelegt, häufig als Methode, um Server anzugreifen und sich Zutritt zu Unternehmenssystemen zu verschaffen. Ist der Angreifer erfolgreich, installiert und verschlüsselt der Trojaner die Dateien auf dem Server und möglicherweise auf allen von ihm aus erreichbaren Netzwerkteilen. Kaspersky Lab hat die Gruppe TeamXRat identifiziert, die diesen Ansatz nutzt, um ihre Ransomware auf brasilianischen Servern zu verbreiten.

- **Zwei-in-eins-Infektion**
  Im August entdeckten wir ein Sample von Shade, das mit einer unerwarteten Funktionalität ausgestattet war: es stellte sich heraus, dass ein Computer zu einem Finanzservice gehört, so wurde statt Ransomware ein Spionageprogramm heruntergeladen und installiert, möglicherweise mit einem längerfristigem Ziel als dem Diebstahl von Geld.

Bei Identifizierung von Finanz-Software lädt Shade Spyware herunter.

Ransomware in Skriptsprachen

Ein weiterer Trend, der unsere Aufmerksamkeit im Jahr 2016 auf sich zog, ist die zunehmende Zahl von Verschlüsselungsschädlingen, die in Skriptsprachen programmiert sind. Allein im dritten Quartal stießen wir auf mehrere Familien, die in Python geschrieben wurden, darunter HolyCrypt und CryPy, sowie Stampado – programmiert in der Automatisierungssprache AutoIt.

Eine lange Reihe von Dilettanten und Nachäffern

Viele der im Jahr 2016 neu entdeckten Erpressertrojaner waren von geringer Qualität: simpel gestrickt, mit Software-Mängeln und Flüchtigkeitsfehlern in den Lösegeldforderungen.

Ransomware von minderer Qualität erhöht das Risiko, dass die Daten für immer verloren sind.

Dieser Trend ging einher mit einer Zunahme nachgemachter Ransomware. Unter anderem fielen uns die folgenden Punkte auf:

- Bart kopiert die Lösegeldforderung und die Aufmachung von Lockys Bezahlseite.
- Eine auf AutoIt basierende Kopie von Locky (genannt AutoLocky) verwendete dieselbe Erweiterung – „.locky"
- Crusis (alias Crysis) benutzt die Erweiterung „.xtbl", die ursprünglich von Shade verwendet wurde.
- Xorist kopiert das gesamte Namensschema der von Crusis verschlüsselten Dateien.

Die prominenteste Kopie, die wir dieses Jahr fanden, ist möglicherweise Polyglot (alias MarsJoke). Dieser Schädling übernimmt vollständig das Erscheinungsbild und die Dateiverarbeitungsmethode von CTB-Locker.

Wir vermuten, dass sich diese Trends im Jahr 2017 verstärken werden.

„Doch mit der zunehmenden Popularität dieses Gewerbes wird auch das Niveau der Cyberverbrecher, die ein Stückchen vom Ransomware-Kuchen abhaben wollen, immer geringer. Wir befürchten daher, dass wir es mehr und mehr mit Ransomware zu tun bekommen, die diese Qualitätssicherung oder auch allgemeine Verschlüsselungsfähigkeiten vermissen lässt und daher dieses Versprechen auch nicht mehr einhalten kann. Wir erwarten eine Art von „Skiddie"-Ransomware, die Dateien oder den Zugriff auf das System sperrt, Dateien einfach löscht oder das Opfer dazu bringt, das Lösegeld zu zahlen, ohne irgendeine Gegenleistung dafür zu erbringen."

GReAT, Prognosen für 2017

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
DIE STORY DES JAHRES. DIE RANSOMWARE-REVOLUTION

DIE FLORIERENDE RANSOMWARE-INDUSTRIE

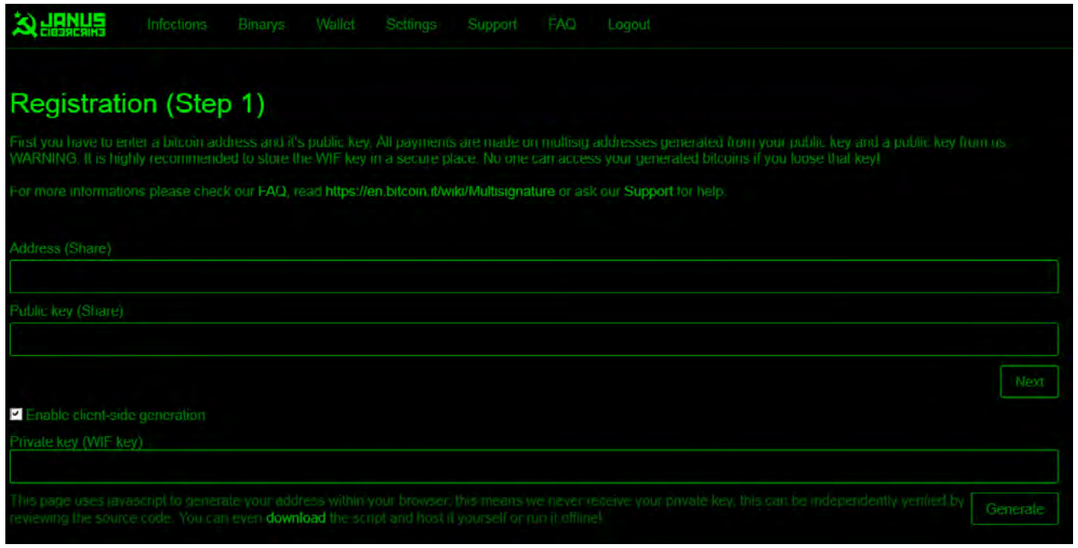
Der Aufstieg von Ransomware-as-a-Service

Ransomware-as-a-Service ist zwar kein neuer Trend, doch im Jahr 2016 hat sich dieses Ausbreitungsschema weiterentwickelt und immer mehr Ransomware-Entwickler bieten ihr schädliches Produkt jetzt „nach Bedarf" an. Dieser Ansatz hat sich als sehr reizvoll für Kriminelle erwiesen, denen es an technischen Fähigkeiten, Ressourcen oder Lust mangelt, ihre eigene Erpressersoftware zu entwickeln.

Ransomware wird im kriminellen Untergrund zunehmend vermietet.

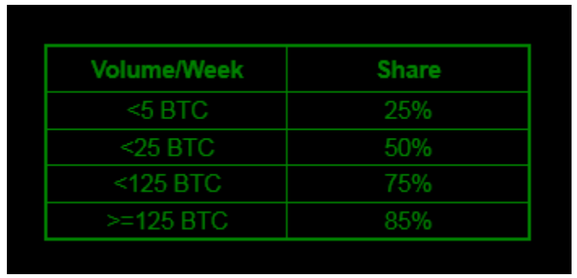
Bemerkenswerte Beispiele für Ransomware, die im Jahr 2016 auf den Plan trat und dieses Modell anwendet, sind die Schadprogramme Petya/Mischa und Shark, das später unter dem Namen Atom neu aufgelegt wurde.

Dieses Geschäftsmodell wird immer raffinierter:



Die Partner-Webseite der Ransomware Petya

Die Partner einigen sich dabei auf ein traditionelles Arrangement auf Kommissionsbasis. Laut Petya-„Preisliste" bleiben einem Angreifer von 125 in der Woche erpressten Bitcoins nach Abzug der Kommission 106,25 Bitcoins Gewinn.



Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Petya-Preisliste

Es gibt auch einmalige Nutzungsgebühren. Wer beispielsweise die Ransomware Stompado verwenden will, ist mit nur 39 US-Dollar dabei.

Da andere Kriminelle ihre Dienste unter anderem beim Spam-Versand und bei der Erstellung von Lösegeldforderungen anbieten, kann ein motivierter Angreifer jederzeit loslegen.

↺ ZURÜCK ZUM INHALT

Von Netzwerken auf Provisionsbasis zu Kunden-Support und Branding

Die wirklich „professionellen" Angreifer boten ihren Opfern einen Helpdesk und technischen Support an, um sie reibungslos durch den Kaufprozess von Bitcoins zu geleiten, mit denen dann das Lösegeld bezahlt werden soll. Manchmal sind sie sogar zu Verhandlungen bereit. Jeder weitere Schritt ermutigt das Opfer, zu zahlen.

Die Kriminellen bieten Kunden-Support an, um sicherzustellen, dass mehr Opfer zahlen.

Experten von Kaspersky Lab, die sich mit Ransomware in Brasilien beschäftigt haben, konnten zudem feststellen, dass die Markenentwicklung, also das Branding der Ransomware, von nicht unerheblicher Bedeutung ist. Diejenigen, die die Aufmerksamkeit der Medien auf sich ziehen und den Nutzern Angst einjagen wollen, entscheiden sich für aktuelle, reißerische Themen oder originelle Aufhänger. Dagegen widerstehen diejenigen, die lieber im Verborgenen agieren, der Versuchung des Ruhmes und hinterlassen ihren Opfern nur eine E-Mail mit den Kontaktdaten der Erpresser und eine Bitcoin-Adresse, an die gezahlt werden soll.

Es geht immer noch um Bitcoins

Das gesamte Jahr 2016 hindurch bevorzugten die führenden Ransomware-Familien wie gehabt Zahlungen in Bitcoins. Die meisten Lösegeldforderungen waren nicht übertrieben. Sie bewegten sich im Rahmen von durchschnittlich 300 US-Dollar, obwohl einige weitaus höher angesetzt – und auch bezahlt – wurden.

Im Rahmen anderer, meist regional beschränkter und maßgeschneiderter Operationen wurden lokale Zahlungsmethoden bevorzugt, obwohl das auch bedeutet, dass sich die Erpressung nicht so leicht verbergen lässt und nicht im allgemeinen Ransomware-Getöse untergeht.

RANSOMWARE NIMMT UNTERNEHMEN INS VISIER

In den ersten drei Monaten des Jahres 2016 richteten sich 17 Prozent der Ransomware-Attacken gegen Unternehmen – das bedeutet, dass alle zwei Minuten irgendwo auf der Welt ein Unternehmen von Erpressersoftware angegriffen wurde . Zum Ende des dritten Quartals 2016 war dieser Wert auf 23,9 Prozent gestiegen, was einer Attacke alle 40 Sekunden gleichkommt.

Alle 40 Sekunden wird ein Unternehmen von Ransomware angegriffen.

Gemäß den **Studien von Kaspersky Lab** wurde im Jahr 2016 eines von fünf Unternehmen weltweit Opfer eines IT-Sicherheitsvorfalls infolge einer Ransomware-Attacke.

- **42 Prozent aller kleinen und mittleren Unternehmen** wurden in den letzten zwölf Monaten von Ransomware angegriffen.
- 32 Prozent dieser Unternehmen zahlten Lösegeld.
- Eines von fünf dieser Unternehmen erhielt seine Dateien nicht zurück, auch nicht nach der Zahlung des Lösegeldes.
- 67 Prozent der von Ransomware angegriffenen Unternehmen verloren ihre gesamten oder einen Teil ihrer Geschäftsdaten, und eines von vier versuchte wochenlang, den Zugriff auf die Daten wiederherzustellen.

Eines von fünf KMUs erhielt seine Daten – auch nach Zahlung des Lösegeldes – nie zurück.

Social Engineering und menschliche Fehlbarkeit spielen eine Schlüsselrolle bei der Angreifbarkeit von Unternehmen. In einem von fünf Fällen mit bedeutendem Datenverlust war der Schaden auf Sorglosigkeit oder mangelndes Sicherheitsbewusstsein der Mitarbeiter zurückzuführen.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
DIE STORY DES JAHRES. DIE RANSOMWARE-REVOLUTION

„Wir haben es zunehmend mit zielgerichteter Ransomware zu tun, wobei kriminelle Gruppen ihre Ziele sorgfältig aufgrund der Daten, die diese Ziele besitzen, und/oder aufgrund der Abhängigkeit von der Verfügbarkeit dieser wertvollen Daten auswählen und sie dann mittels Spear-Phishing angreifen."

John Fokker, Team-Koordinator bei der Dutch National High Tech Crime Unit"

Einige Branchen sind stärker betroffen als andere, aber unsere Studien zeigen, dass ausnahmslos alle potenziell gefährdet sind.

Keine Branche ist mehr sicher vor Ransomware.

	BRANCHE	PROZENTUALER ANTEIL DER RANSOMWARE-ATTACKEN
1	Bildung	23
2	IT/Telekommunikation	22
3	Unterhaltung/Medien	21
4	Finanzdienste	21
5	Baugewerbe	19
6	Regierung/Öffentlicher Sektor/ Verteidigung	18
7	Fertigung	18
8	Transport	17
9	Gesundheitswesen	16
10	Einzelhandel/Großhandel/Freizeit	16

Bedeutende Angriffe im Jahr 2016

- **Krankenhäuser haben sich zu einem Hauptziel entwickelt**, mit potenziell verheerenden Auswirkungen: Operationen mussten abgesagt, Patienten in andere Krankenhäuser verlegt werden und so weiter.
  - Das eklatanteste Beispiel für eine Ransomware-Attacke ereignete sich im März, als Cyberkriminelle die Computer des Hollywood Presbyterian Medical Center in Los Angeles so lange blockierten, bis das Krankenhaus 17.000 US-Dollar zahlte.
  - Innerhalb weniger Wochen wurde eine Reihe von Krankenhäusern in Deutschland angegriffen.
  - In Großbritannien haben 28 Einrichtungen des National Health Service eingeräumt, im Jahr 2016 angegriffen worden zu sein.
- **Der Hosted Desktop und Cloud Provider VESK** zahlte fast 23.000 US-Dollar Lösegeld, um den Zugriff auf seine Systeme nach einem Angriff im September wiederherzustellen.
- **Führende Medien**, unter anderem die New York Times, die BBC und AOL, wurden im März 2016 von Malware attackiert, die Ransomware auslieferte.
- Die University of Calgary in Kanada, ein führendes Forschungszentrum, räumte ein, um die 16.000 US-Dollar bezahlt zu haben, um die E-Mails wiederherzustellen, die eine Woche lang verschlüsselt waren.
- Ein kleines Polizeirevier in Massachusetts bezahlte letztlich 500 US-Dollar Lösegeld (in Bitcoin), um wichtige fallbezogene Daten zurückzuerhalten, nachdem ein Beamter einen verseuchten E-Mail-Anhang geöffnet hatte.
- **Selbst der Motorsport war betroffen:** Ein führendes NASCAR-Team verlor Daten im Wert von Millionen von US-Dollar infolge einer TeslaCrypt-Attacke im April.

ABWEHR

Durch Technologie

Die neusten Versionen der Kaspersky-Lab-Produkte für kleinere Unternehmen wurden um eine Anti-Kryptomalware-Funktionalität erweitert. Zudem wurde ein neues, kostenloses Anti-Ransomware-Tool für Unternehmen jeder Art zum Download und zum Gebrauch bereitgestellt, ganz unabhängig davon, welche Sicherheitslösung verwendet wird.

Ein neues, kostenloses, AV-unabhängiges Anti-Ransomware-Tool ist jetzt verfügbar.

Das Anti-Ransomware-Tool für Unternehmen von Kaspersky Lab ist eine „leichte" Lösung, die parallel zu anderer Antiviren-Software laufen kann. Das Tool verwendet zwei Komponenten, die für die Detektion von Trojanern in einem frühen Stadium benötigt werden: das verteilte Netzwerk Kaspersky Security Network sowie System Watcher, eine Komponente, die die Aktivität von Anwendungen überwacht.

Das Kaspersky Security Network überprüft mit hoher Geschwindigkeit die Reputation von Dateien und Website-URLs über die Cloud. System Watcher beobachtet das Verhalten von Programmen und bietet proaktiven Schutz vor bisher unbekannten Trojaner-Versionen. Am wichtigsten ist, dass das Tool in der Lage ist, eine Sicherheitskopie von Dateien zu erstellen, die von verdächtigen Apps geöffnet wurden. Außerdem kann es Änderungen zurücksetzen, wenn sich die von einem Programm vorgenommenen Aktionen als schädlich erweisen.

↺ ZURÜCK ZUM INHALT

Durch Zusammenarbeit: Die Initiative „NoMoreRansom.org"

Am 25. Juli 2016 gaben die niederländische Polizei, Europol, Intel Security und Kaspersky Lab den Start des Projekts NoMoreRansom.org bekannt – eine nicht kommerzielle Initiative, die öffentliche und private Organisationen vereint. Ihr Ziel ist es, die Öffentlichkeit über die Gefahren zu informieren, die von Ransomware ausgehen, und den Opfern dabei zu helfen, ihre Daten wiederherzustellen.

Das Online-Portal stellt aktuell acht Entschlüsselungstools zur Verfügung, von denen fünf von Kaspersky Lab entwickelt wurden. Mit Hilfe dieser Tools können Daten wiederhergestellt werden, die von über 20 Arten von Kryptomalware verschlüsselt wurden. Zum gegenwärtigen Zeitpunkt haben über 2.500 Opfer ihre Daten zurückerhalten und dabei etwa eine Million US-Dollar an Lösegeld NICHT gezahlt.

„NoMoreRansom.org" hat bisher Daten von 2.500 Opfern wiederhergestellt – und die Erpresser damit um eine Million US-Dollar Lösegeld gebracht.

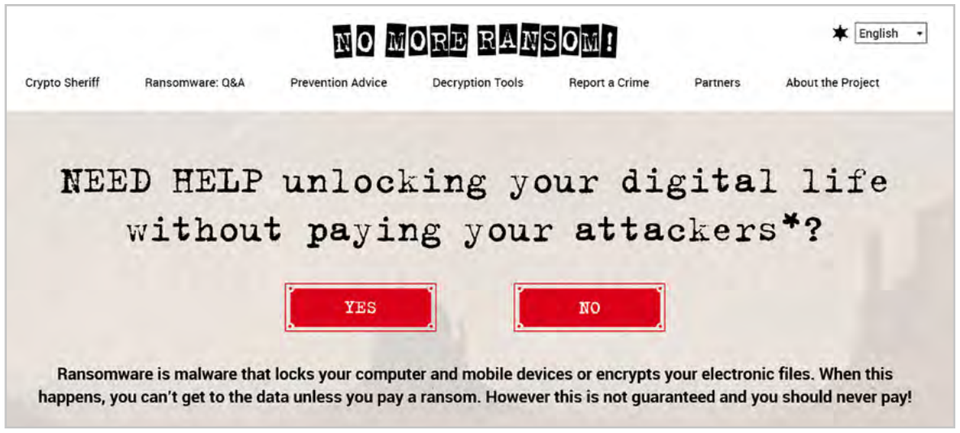
Im Oktober haben sich die Strafverfolgungsbehörden weiterer 13 Länder dem Projekt angeschlossen. Mit dabei sind jetzt auch Bosnien und Herzegowina, Bulgarien, Frankreich, Irland, Italien, Kolumbien, Lettland, Litauen, Portugal, Schweiz, Spanien, Großbritannien und Ungarn.

Eurojust und die Europäische Kommission unterstützen die Ziele des Projektes ebenfalls. Es wird erwartet, dass schon bald neue Partner aus dem privaten Sektor sowie auch Strafverfolgungsbehörden ihre Mitarbeit bekanntgeben werden.

„Öffentliche und private Partnerschaften sind der Kern und die Stärke der NMR-Initiative. Sie sind unerlässlich, um das Problem effektiv und wirkungsvoll anzupacken, da sie uns ein Potenzial und eine Reichweite bieten, die Strafverfolgungsbehörden allein nicht bieten können."

Steven Wilson, Leiter des EC3 von Europol

No more Ransom



Ransomware Paroli bieten – so bleibt man auf der sicheren Seite

1. Erstellen Sie regelmäßig Sicherheitskopien.
2. Verwenden Sie eine verlässliche Sicherheitslösung und denken Sie daran, Schlüsselfunktionen wie zum Beispiel System Watcher immer aktiviert zu haben.
3. Halten Sie die Software auf allen benutzten Geräten immer auf dem aktuellen Stand.
4. Behandeln Sie E-Mail-Anhänge oder Nachrichten von Personen, die Sie nicht kennen, mit Vorsicht. Sollten Sie Zweifel haben, öffnen Sie sie nicht.
5. Wenn Sie ein Unternehmen leiten, sollten Sie ihre Mitarbeiter und IT-Teams schulen; verwahren Sie sensitive Daten separat; beschränken Sie den Zugriff; und erstellen Sie Sicherheitskopien von allem, jederzeit.
6. Sollten Sie das große Pech haben, Opfer einer Ransomware-Attacke zu werden, verfallen Sie nicht in Panik. Verwenden Sie ein sauberes System, um auf der Webseite von „NoMoreRansom.org" nach einem Entschlüsselungstool zu suchen, das Ihnen dabei hilft, Ihre Daten wiederherzustellen.
7. Last but not least: Vergessen Sie nicht, dass eine Ransomware-Attacke eine strafbare Handlung ist. Melden Sie den Vorfall der Polizei vor Ort.

„Wir raten den Anwendern eindringlich dazu, Attacken zu melden. Jedes Opfer verfügt über ein wichtiges Beweisstück, das uns unschätzbare Erkenntnisse bietet. Im Gegenzug halten wir sie auf dem Laufenden und schützen sie vor zwielichtigen „Angeboten" Dritter, die Daten zu entschlüsseln. Aber wir müssen dafür sorgen, dass mehr Strafverfolgungsbehörden lernen, richtig mit digitaler Kriminalität umzugehen."

Ton Maas, Team-Koordinator bei der Dutch National High Tech Crime Unit

Warum Sie nicht zahlen sollten – ein Ratschlag von der Dutch National High Tech Crime Unit

1. Sie werden zu einer noch größeren Zielscheibe.
2. Kriminellen ist nicht zu trauen – möglicherweise bekommen Sie Ihre Daten auch dann nicht zurück, wenn Sie zahlen.
3. Die nächste Lösegeldforderung wird höher sein.
4. Sie ermutigen die Verbrecher.

Die Schätzungen basieren auf den folgenden Daten: 17 Prozent von 372.602 individuellen Nutzern, bei denen im ersten Quartal 2016 von Kaspersky-Lab-Produkten Ransomware-Attacken blockiert wurden, und 23,9 Prozent von 821.865 individuellen Nutzern, bei denen im dritten Quartal 2016 von Kaspersky-Lab-Produkten Ransomware-Attacken blockiert wurden.

KÖNNEN WIR DEN KAMPF GEGEN RANSOMWARE JEMALS GEWINNEN?

Wir glauben, ja – jedoch nur, wenn wir zusammenarbeiten. Ransomware ist ein lukratives kriminelles Geschäft. Um ihm Einhalt zu gebieten, muss die Welt sich vereinen, um die zerstörerische Kette der Kriminellen zu unterbrechen und es ihnen zunehmend zu erschweren, ihre Attacken durchzuführen und von ihnen zu profitieren.

KASPERSKY SECURITY BULLETIN. PROGNOSEN FÜR DAS JAHR 2017

Autor(en): Juan Andrés Guerrero-Saade,
Global Research and Analysis Team

QUICK INFO

UNSERE BILANZ

WAS HÄLT DAS JAHR 2017 BEREIT?

- Diese vermaledeiten APTs . . . .
  Der Aufstieg maßgeschneiderter und passiver Implantate
- Kurzfristige Infektionen
- Spionage goes mobile
- Die Zukunft von Finanzattacken
  Wie wir hören, möchten Sie eine Bank überfallen
- Robuste Bezahlsysteme
- Dreckige, verlogene Ransomware
- Der große rote Knopf
- Das übervölkerte Internet schlägt zurück
  Schwache Sicherheit im Internet der Dinge
- Die leise blinkenden Kästchen
- Wer zum Teufel sind Sie?
- Der Informationskrieg
- Das Abschreckungsversprechen
- Doppelung unter falschen Flaggen
- Welcher Datenschutz? Den Schleier lüften
- Das Spionage-Werbenetz
- Der Aufstieg des Selbstjustiz-Hackers

Schon wieder ist ein Jahr vergangen, und was die Ereignisse im Bereich IT-Sicherheit betrifft, so sollte es in die Geschichtsbücher eingehen. Dramen, Intrigen und Exploits haben das Jahr 2016 geprägt. Während wir die wichtigsten Ereignisse und Stories noch einmal Revue passieren lassen, werfen wir gleichzeitig einen Blick in die Zukunft, um die Umrisse der Bedrohungslandschaft des Jahres 2017 vorzuzeichnen.

Anstatt schlecht verhüllte Eigenwerbung zu betreiben, wollen wir unsere Vorhersagen basierend auf Trends treffen, die wir im Laufe unserer Forschungsarbeit beobachtet haben und damit Forschern und Besuchern des Threat-Intelligence-Universums gleichermaßen Stoff zum Nachdenken liefern.

Hunting the Hunter - Unser GReAT stellt sich vor

UNSERE BILANZ

Unsere Prognosen aus dem letzten Jahr haben sich keinesfalls als falsch herausgestellt, wobei einige Punkte noch früher als erwartet Realität geworden sind. Sollten Sie sie gerade nicht mehr parat haben, hier noch einmal unsere wichtigsten Vorhersagen für das Jahr 2016:

APTs: Wir sagten einen verminderten Fokus auf Nachhaltigkeit voraus. Gleichzeitig vermuteten wir, dass die Bemühungen der Angreifer, sich unsichtbar zu machen, zunehmen würden, indem sie Allerwelts-Malware in zielgerichteten Attacken einsetzen. Diese Vermutungen haben sich doppelt bestätigt: a) durch eine Zunahme von im Speicher aktiver Malware und dateiloser Schädlinge; b) durch die Unmenge bekannter zielgerichteter Attacken auf Aktivisten und Unternehmen, die auf Remote-Access-Trojanern basieren, wie zum Beispiel NJRat und Alienspy/Adwind.

Ransomware: 2016 kann als Jahr der Ransomware bezeichnet werden. Die Welt der Finanz-Malware, die darauf abzielt, Nutzer in die Irre zu führen und zu betrügen, hat sich praktisch vollständig in ein reines Ransomware-Universum verwandelt. Dabei werden Ressourcen für die Malware-Entwicklung zugunsten der effizienteren Erpressungsschemata von den weniger profitablen Versuchen abgezogen, die Nutzer zu betrügen.

Mehr Bankraube: Als wir uns den sich abzeichnenden Höhepunkt der Finanzkriminalität vorstellten, erstreckten sich unsere hypothetischen Überlegungen auf Angriffe auf Institutionen wie beispielsweise die Börse. Doch dann waren es die Attacken auf das SWIFT-Netzwerk, die diese Vorhersagen real werden ließen. Dank kluger, wohl platzierter Malware spazierten Millionenbeträge zur Tür hinaus.

Internet-Attacken: Vor kurzem drang die häufig missachtete Welt der Dinge mit Internetanschluss in Form eines IoT-Botnetzes in unser aller Leben vor. Das Botnetz war der Grund für Ausfälle bei großen Internet-Services, was besonders denjenigen Anbietern Bauchschmerzen bereitete, die von einem speziellen DNS-Provider abhängen.

Bloßstellung: Bloßstellungen und Erpressungen setzen sich im großen Stil fort, da strategische und wahllose Datenoffenlegungen links und rechts für Rufschädigungen sowie für persönliche und politische Probleme gesorgt haben. Wir müssen zugeben, dass wir vom Ausmaß und den Opfern einiger dieser Datenlecks ernsthaft überrascht waren.

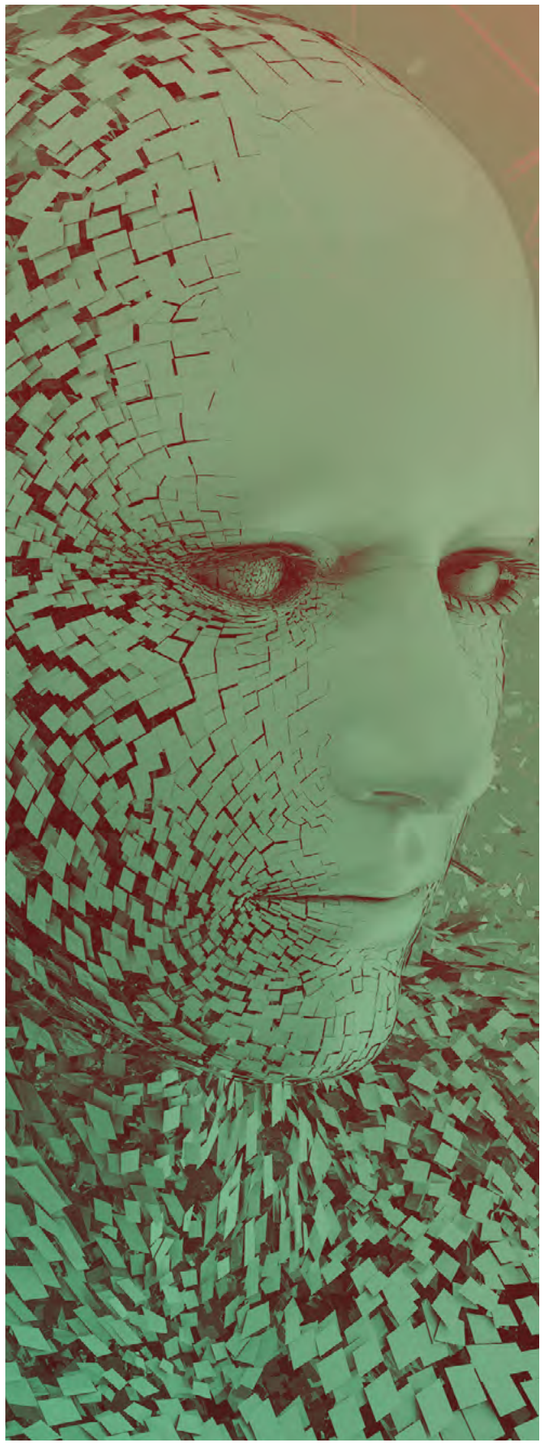
↺ ZURÜCK ZUM INHALT

WAS HÄLT DAS JAHR 2017 BEREIT?

Diese vermaledeiten APTs
Der Aufstieg maßgeschneiderter und passiver Implantate

Auch wenn es sehr schwierig sein mag, Unternehmen dazu zu bringen, Schutzmaßnahmen einzuführen, müssen wir doch zugeben können, wenn sich diese Maßnahmen langsam abnutzen oder gar wirkungslos werden. Indicators of Compromise (IoCs) sind eine großartige Methode, um Charakteristika bereits bekannter Malware, wie etwa Hashes, Domains oder Ausführungsmerkmale, zu teilen. Sie ermöglichen es Sicherheitsexperten, eine aktive Infektion zu erkennen. Doch die Cyberspionage-Elite, die in dieser kriminellen Branche die Trends setzt, hat Wege gefunden, diese allgemeinen Maßnahmen außer Kraft zu setzen. Dies ist auch mit der kürzlich bekannt gewordenen ProjectSauron APT nur allzu deutlich geworden. Es handelt sich bei dieser APT um eine wahrhaft maßgeschneiderte Malware-Plattform, deren einzelne Funktionen geändert und an jedes Opfer neu angepasst wurden. Dieses Vorgehen hilft den Sicherheitsexperten nicht gerade dabei, andere Infektionen zu detektieren. Das bedeutet nicht, dass die Security-Spezialisten jetzt vollkommen machtlos sind. Doch es ist nunmehr an der Zeit, eine weiter reichende Adaption guter Yara-Regeln voranzutreiben. Sie erlauben es uns, sowohl im gesamten Unternehmen zu scannen, zu inspizieren und ruhende Merkmale in Binärdateien zu identifizieren, als auch den Speicher nach Fragmenten bereits bekannter Attacken zu durchsuchen.

ProjectSauron hat noch eine weitere Tendenz bestätigt, von der wir angenommen hatten, dass sie bald auf dem Vormarsch sein würde, und zwar den Einsatz „passiver Implantate". Dabei handelt es sich um eine Netzwerk-gesteuerte Backdoor, die im Speicher sitzt oder als ein Hintertür-Treiber in einem Internet-Gateway oder einem Internet-zugewandten Server läuft und still darauf wartet, dass magische Bytes ihre Funktionalität zum Leben erwecken. Bis sie von ihren Herren aufgeweckt werden, zeigen passive Implantate wenige oder gar keine Anzeichen einer aktiven Infektion. Daher ist es äußerst unwahrscheinlich, dass sie von irgendjemandem gefunden werden, außer vielleicht von den paranoidesten unter den Sicherheitsforschern oder im Rahmen eines Incident-Response-Szenarios. Man darf nicht vergessen, dass diese Malware mit keiner vordefinierten Command-and-Control-Infrastruktur interagiert und daher eine weitaus anonymere Ausgangsposition bietet. Daher ist es das Tool der Wahl für die meisten vorsichtigen Angreifer, die von jetzt auf gleich einen Weg in ein Ziel-Netzwerk bereitstellen müssen.



Kurzfristige Infektionen

PowerShell hat sich zum Traum-Tool für Windows-Administratoren entwickelt. Allerdings bietet es auch dem ganzen Spektrum an Malware-Autoren fruchtbaren Boden, die auf heimliche Bereitstellung, Seitwärtsbewegung und Ausspähungsressourcen aus sind, die vermutlich nicht von Standardkonfigurationen aufgezeichnet werden.

Winzige PowerShell-Malware, die im Speicher oder der Registry untergebracht ist, hat alle Chancen, auf modernen Windows-Systemen ihren großen Tag zu feiern. Spinnt man die Sache weiter, so sind vorübergehende Infektionen zu erwarten: speicherresidente Malware, die für allgemeines Auskundschaften und den Diebstahl von Anmeldedaten jeglicher Art geschaffen wurde, aber keinen Anspruch auf Langlebigkeit und Nachhaltigkeit erhebt.

In hoch sensiblen Umgebungen könnten verborgene Angreifer absolut glücklich damit sein, so lange operieren zu können, bis ein Neustart ihre Infektion aus dem Speicher löscht – wenn das bedeutet, dass damit jeglicher Verdacht abgelenkt oder potenzielle Verluste durch das Entdecken ihrer Malware durch Sicherheitsexperten und Forscher vermieden werden können. Kurzfristige Infektionen werden die Notwendigkeit proaktiver und fortschrittlicher heuristischer Erkennungsmethoden in modernen Anti-Malware-Lösungen einmal mehr unterstreichen (siehe: Kaspersky System Watcher).

↺ ZURÜCK ZUM INHALT

Spionage goes mobile

Zahlreiche Bedrohungsakteure haben in der Vergangenheit mobile Malware-Implantate bereitgestellt, unter anderem Sofacy, Roter Oktober und CloudAtlas sowie auch die Kunden von HackingTeam und die mutmaßliche iOS-Malware-Suite Pegasus der NSO Group. Doch sie haben auch Kampagnen gefahren, die hauptsächlich auf Desktop-Toolkits basieren.

Da Desktop-Betriebssysteme aber immer weniger nachgefragt werden und immer mehr Durchschnittsnutzer ihr digitales Leben in ihre Hosen- und Handtaschen verlagern, gehen wir davon aus, dass die hauptsächlich mobilen Spionage-Kampagnen auf dem Vormarsch sind. Diese werden ganz sicher von verringerter Aufmerksamkeit und der Schwierigkeit profitieren, an forensische Tools für die neuesten mobilen Betriebssysteme zu kommen.

Vertrauen in das Signieren von Code und Integritätsprüfungen haben die Sichtbarkeit für Sicherheitsforscher in der mobilen Arena vermindert, aber das wird entschlossene und gut ausgestattete Angreifer nicht davon abhalten, ihre Ziele auch hier zu verfolgen.

Die Zukunft von Finanzattacken
Wie wir hören, möchten Sie eine Bank überfallen...

Als dieses Jahr die Nachricht von den Angriffen auf das Bezahlsystem SWIFT die Runde machte, versetzte allein die Kühnheit dieses Unterfangens die gesamte Finanzbranche in Aufruhr. Die Schadenssumme wurde mit jeder Menge Nullen und Punkten geschrieben und erreichte eine Größenordnung von vielen Millionen US-Dollar. Es handelte sich dabei um eine Art von natürlichem Entwicklungsschritt von Cybercrime-Playern wie der Carbanak-Gang und vielleicht auch einigen anderen interessanten Bedrohungsakteuren. Doch diese Fälle bleiben das Werk von APT-artigen Akteuren mit einer gewissen Verve und bewährtem Potenzial. Sicher sind sie aber nicht die einzigen, die eine Bank gerne um eine stattliche Summe erleichtern würden.

Mit zunehmendem Interesse der Cyberkriminellen wird unserer Vermutung nach eine Zunahme der Zwischenhändler bei SWIFT-Angriffen einhergehen, die sich in die bewährte Untergrundstruktur von gestaffelten kriminellen Unternehmen einfügen. Um einen derartigen Bankraub durchzuführen, benötigt man der Reihe nach Erstzugriff, spezialisierte Software, Geduld und schließlich ein Geldwäscheschema. Jeder dieser Schritte wird von bereits etablierten Kriminellen ausgeführt, die ihre Dienstleistungen gegen ein Honorar liefern, wobei der fehlende Teil die spezialisierte Malware zur Durchführung von SWIFT-Attacken ist. Wir erwarten die Kommerzialisierung dieser Angriffe durch spezialisierte Ressourcen, die in Untergrundforen zum Verkauf oder nach dem Schema As-a-Service angeboten werden.

↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
PROGNOSEN FÜR DAS JAHR 2017

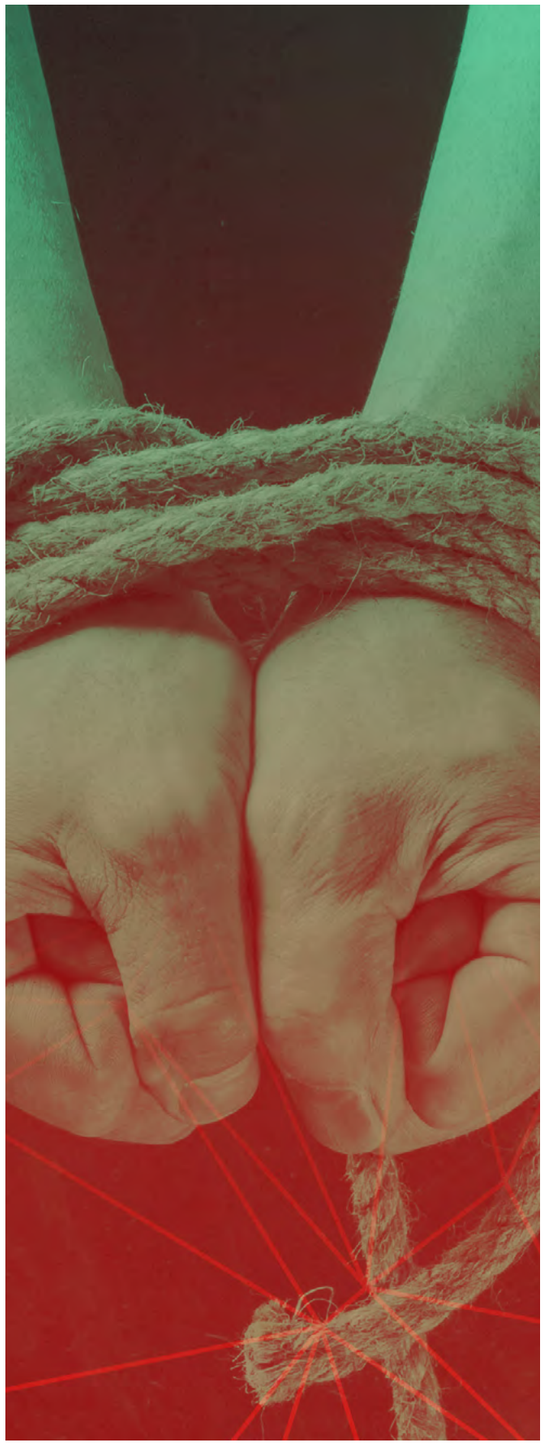
Robuste Bezahlsysteme

Da Bezahlsysteme immer populärer und immer besser angenommen werden, hatten wir ein größeres kriminelles Interesse an diesen Diensten erwartet. Doch es scheint, als seien diese Implementationen besonders widerstandsfähig. Und bis zum gegenwärtigen Zeitpunkt wurde von keinen umfassenden Attacken auf Systeme dieser Art berichtet.

Doch was für die Kunden eine Erleichterung sein mag, könnte den Anbietern von Bezahlsystemen selbst Kopfschmerzen bereiten. Cyberkriminelle sind es gewohnt, die Letztgenannten durch direkte Attacken auf die Bezahlsystem-Infrastruktur anzugreifen.

Ob diese Attacken nun in direkten finanziellen Verlusten resultieren oder einfach in Systemausfällen und -zusammenbrüchen – wir erwarten, dass sich Cyberverbrecher zunehmend mit diesen Systemen befassen werden, um mehr schändliche Aufmerksamkeit auf sich zu ziehen.

Dreckige, verlogene Ransomware



So sehr wir alle Ransomware hassen (und zwar aus gutem Grund), funktionieren die meisten Erpresserprogramme doch nur aufgrund einer merkwürdigen Vertrauensbeziehung zwischen dem Opfer und den Angreifern. Dieses kriminelle Ökosystem fußt auf dem Grundsatz, dass sich der Angreifer an eine stillschweigende Übereinkunft mit dem Opfer halten wird, die besagt, dass das Opfer, nachdem die Lösegeldzahlung beim Erpresser eingegangen ist, seine gekaperten Dateien zurückerhält. Die Cyberkriminellen haben dabei ein erstaunliches Maß an Professionalität an den Tag gelegt, was die Erfüllung dieses Versprechens angeht, so dass dieses Ökosystem gedeihen kann. Doch mit der zunehmenden Popularität dieses Gewerbes wird auch das Niveau der Cyberverbrecher, die ein Stückchen vom Ransomware-Kuchen abhaben wollen, immer geringer. Wir befürchten daher, dass wir es mehr und mehr mit Ransomware zu tun bekommen, die diese Qualitätssicherung oder auch allgemeine Verschlüsselungsfähigkeiten vermissen lässt und daher dieses Versprechen auch nicht mehr einhalten kann.

Wir erwarten eine Art von „Skiddie"-Ransomware, die Dateien oder den Zugriff auf das System sperrt, Dateien einfach löscht oder das Opfer dazu bringt, das Lösegeld zu zahlen, ohne irgendeine Gegenleistung dafür zu erbringen. An diesem Punkt wird sich Ransomware in keiner Weise mehr von Attacken unterscheiden, bei denen Daten gelöscht werden. Wir gehen davon aus, dass das Ransomware-Ökosystem die Auswirkungen einer „Vertrauenskrise" zu spüren bekommen wird. Das wird die größeren, professionelleren Banden nicht davon abhalten, ihre Erpresser-Kampagnen fortzusetzen. Doch es könnte dazu beitragen, dass in der aufkommenden Ransomware-Epidemie die Überzeugung vieler über Bord geworfen wird, dass der Vorschlag „Einfach das Lösegeld bezahlen" ein akzeptabler Rat für die Opfer ist.

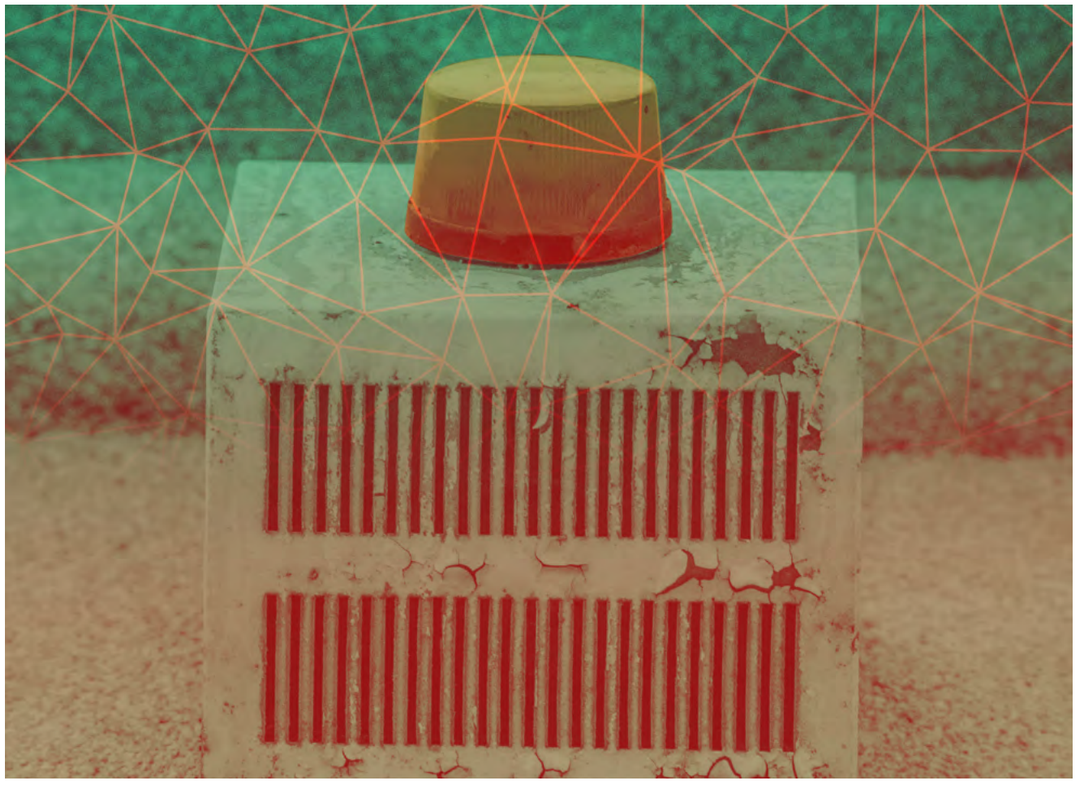
↺ ZURÜCK ZUM INHALT

KASPERSKY SECURITY BULLETIN 2016/2017
PROGNOSEN FÜR DAS JAHR 2017

Der große rote Knopf

Die berüchtigte Stuxnet-Malware hat vielleicht die Büchse der Pandora geöffnet, indem sie aufzeigte, welches Potenzial in Angriffen auf industrielle Steuerungssysteme liegt. Doch die Stuxnet-Kampagne war sorgfältig konzipiert, mit einem wachsamen Auge auf langandauernde Sabotage und sehr eng definierte Ziele. Selbst als sich die Infektion global ausbreitete, haben Payload-Checks den Kollateralschaden in Grenzen gehalten und ein industrielles Armageddon blieb aus. Seither dient jedes Gerücht oder jeder Bericht über einen Industrieunfall oder eine unerklärte Explosion als Nahrung für eine Cybersabotage-Verschwörungstheorie.

Nichtsdestoweniger ist ein durch Cybersabotage verursachter Industrieunfall sicherlich nicht ins Reich der Mythen zu verweisen. Solange kritische Infrastrukturen und Fertigungssysteme mit dem Internet verbunden bleiben – meist wenig oder gar nicht geschützt –, sind diese verlockenden Ziele durchaus dazu geeignet, gut ausgestattete Angreifer auf den Geschmack zu bringen, die darauf aus sind, Chaos zu stiften. Doch bei aller Panik sollte man auch bedenken, dass solche Attacken bestimmte Fähigkeiten und Absichten erfordern. Ein Cybersabotage-Angriff wird wahrscheinlich Hand in Hand mit zunehmenden geopolitischen Spannungen gehen und mit fest etablierten Bedrohungsakteuren, die auf zielgerichtete Zerstörung oder den Zusammenbruch kritisch wichtiger Dienste aus sind.



Das übervölkerte Internet schlägt zurück
Schwache Sicherheit im Internet der Dinge

So sehr wir alle Ransomware hassen (und zwar aus gutem Grund), funktionieren die meisten Schon seit Langem prophezeien wir, dass die schwache Sicherheit des Internets der Dinge uns eines Tages auf die Füße fallen wird. Und siehe da, nun ist dieser Tag gekommen. Wie das Mirai-Botnetz kürzlich deutlich gezeigt hat, wird Kriminellen durch die schwache Sicherheit Internet-fähiger Geräte unnötigerweise eine Möglichkeit eröffnet, Chaos zu stiften. Dabei ist die Wahrscheinlichkeit, zur Verantwortung gezogen zu werden, verschwindend gering. Für IT-Sicherheitsfanatiker ist das nicht wirklich eine Überraschung, aber der nächste Entwicklungsschritt könnte sich als besonders interessant erweisen. Denn wir sagen voraus, dass hackende Vigilanten die Dinge in die Hände nehmen werden.

Das Konzept, bekannte Sicherheitslücken zu patchen, hat einen gewissen unantastbaren Status als Bestätigung für die harte (und häufig unbezahlte) Arbeit von Sicherheitsforschern. Da die Hersteller von IoT-Geräten weiterhin unsichere Geräte auf den Markt werfen, die weitreichende Probleme verursachen, könnten Internet-Vigilanten die Dinge in die eigenen Hände nehmen. Und was könnte in diesem Fall effektiver sein, als den Ball zu den Herstellern selbst zurückzuspielen, indem sie diese verwundbaren Geräte massenhaft zerstören? Da IoT-Botnetze durch DDoS-Angriffe und die Verbreitung von Spam weiterhin Kopfschmerzen verursachen, könnte die natürliche Abwehrreaktion des Ökosystems darin bestehen, diese Geräte alle miteinander außer Gefecht zu setzen – sehr zum Leidwesen der Verbraucher und der Hersteller gleichermaßen. Das Internet der (unsicheren) Dinge könnte sehr wohl über uns zusammenbrechen.

↺ ZURÜCK ZUM INHALT

Die leise blinkenden Kästchen

Die schockierende Veröffentlichung der ShadowBrokers-Gruppe umfasste eine Fülle funktionierender Exploits für zahlreiche Firewalls von namhaften Herstellern. Kurze Zeit später wurde von Ausnutzungen in freier Wildbahn berichtet, während die Hersteller noch damit beschäftigt waren, die ausgenutzten Lücken zu verstehen und Patches herauszugeben. Doch das Ausmaß der Ausfälle muss erst noch vermessen werden. Was konnten die Angreifer mit diesen Exploits in der Hand erreichen? Welche Art von Implantaten mögen in den angreifbaren Geräten verborgen sein?

Schaut man über diese besonderen Exploits hinaus (und bedenkt man die Entdeckung einer Backdoor in Junipers ScreenOS Ende 2015), so ergibt sich ein größeres Problem der Geräteintegrität. Wenn es nämlich um Apparate gehen wird, die kritisch für Unternehmen sind, werden weitere Forschungen notwendig sein. Die entscheidende Frage bleibt: „Für wen arbeitet Ihre Firewall eigentlich?“

Wer zum Teufel sind Sie?

Falsche Flaggen und psychologische Kriegsführung gehören zu unseren ausgesprochenen Lieblingsthemen. Daher überrascht es nicht, dass wir die Entwicklung verschiedener Trends in diesen Bereichen vorhersehen...

Der Informationskrieg

Bei der Erstellung gefälschter Shops, die dazu dienen, Datenspeicher abzugreifen und die Opfer zu erpressen, haben Bedrohungsakteure wie Lazarus und Sofacy Pionierarbeit geleistet. Nachdem in den letzten paar Monaten recht erfolgreich Operationen im Rahmen eines Informationskriegs durchgeführt wurden, erwarten wir, dass diese zunehmen werden. Auf diese Weise sollen Meinungen rund um wichtige Prozesse manipuliert und allgemeines Chaos verursacht werden. Bedrohungsakteure, die gehackte Daten verschleudern, haben kaum etwas zu verlieren, wenn sie eine Geschichte über eine etablierte oder fingierte Hacktivisten-Gruppe zusammenschustern und so die Aufmerksamkeit von der Attacke selbst ablenken und die Inhalte ihrer Enthüllungen ins Zentrum rücken.

Die eigentliche Gefahr liegt an diesem Punkt nicht im Hacken oder dem Eindringen in die Privatsphäre, sondern vielmehr darin, dass – während sich Journalisten und Bürger daran gewöhnen, gestohlene Datenbanken als nachrichtentaugliche Fakten zu akzeptieren – sie damit clevereren Bedrohungsakteuren Tür und Tor öffnen. Diese versuchen, die Auswirkungen zu manipulieren, entweder durch Datenmanipulation oder durch Unterlassung. Die Verwundbarkeit gegenüber solchen Informationskriegs-Operationen ist zu jeder Zeit hoch und wir hoffen, dass die Urteilsfähigkeit obsiegen wird, während die Technik von immer mehr Playern adaptiert wird (oder von denselben Playern mit anderen Wegwerfmasken).

↺ ZURÜCK ZUM INHALT

Das Abschreckungsversprechen

Da Cyberattacken in internationalen Beziehungen eine immer größere Rolle spielen, wird die Zuweisung (Attribution) zu einem zentralen Punkt werden, wenn es darum geht, geopolitische Kurse festzulegen. Regierungsorganisationen werden sich noch den Kopf darüber zerbrechen müssen, welcher Zuweisungsstandard sich als ausreichend für Einsprüche oder öffentliche Anklagen erweisen wird. Eine genaue Attribution ist bei der nur bruchstückhaften Sichtbarkeit verschiedener öffentlicher und privater Institutionen nahezu unmöglich.

Es könnte sogar sein, dass eine „ungenaue Zuweisung" für solche Organisationen als gut genug angesehen wird. Während es sehr wichtig ist, zu absoluter Vorsicht zu raten, müssen wir immer im Hinterkopf behalten, dass es einen realen Bedarf nach Konsequenzen für das Betreten des Cyberattacken-Universums gibt. Unsere große Aufgabe besteht darin, sicherzustellen, dass Vergeltung keine weiteren Probleme verursacht, wenn clevere Akteure versuchen, diejenigen zu übervorteilen, die Attribution an erster Stelle sehen möchten.

Wir müssen auch bedenken, dass – wenn Vergeltung und Konsequenzen alltäglicher werden – der Missbrauch von Open-Source- und kommerzieller Malware extrem zunehmen wird, wobei Tools wie Cobalt Strike und Metasploit einen Mantel glaubhafter Bestreitbarkeit liefern, der bei proprietärer Malware nicht vorhanden ist.

Doppelung unter falschen Flaggen

Während die Beispiele aus dem Falsche-Flaggen-Report einige Fälle von APTs in freier Wildbahn umfassen, die Falsche-Flaggen-Elemente aufweisen, wurde zum gegenwärtigen Zeitpunkt nicht eine einzige echte Operation unter falschen Flaggen registriert. Darunter verstehen wir eine Operation von Bedrohungsakteur A, die sorgfältig und ausschließlich im Stil und mit den Ressourcen eines zweiten Bedrohungsakteurs B entwickelt wurde. Das geschieht in der Absicht, Vergeltungsgelüste bei dem Opfer gegenüber dem in diesem Fall unschuldigen Bedrohungsakteur B zu provozieren. Auch wenn es sein kann, dass so etwas bereits passiert, ohne dass die Sicherheitsforscher Kenntnis davon haben, ergibt diese Art von Operation gar keinen Sinn, solange Cyberattacken nicht de facto vergolten werden. Sobald Vergeltungsmaßnahmen (seien es Sanktionen, Vergeltungsschläge oder anderes) gängiger und impulsiver werden, gehen wir davon aus, dass echte Operationen unter falscher Flagge auf den Plan treten werden.

Wenn das der Fall sein wird, ist zu erwarten, dass Falsche-Flaggen-Angriffe größere Investitionen wert sein werden, vielleicht sogar dazu anstacheln, die Infrastruktur offenzulegen oder eifersüchtig bewachte proprietäre Toolkits zum Massengebrauch freizugeben. Auf diese Weise könnten schlaue Bedrohungsakteure kurzfristig überwältigende Verwirrung stiften, und zwar auch bei Forschern und Sicherheitsexperten, da dann Script-Kiddies, Hacktivisten und Cyberkriminelle plötzlich mit den proprietären Tools eines fortschrittlichen Bedrohungsakteurs hantieren. Das verleiht ihnen in der Menge der Attacken einen Mantel der Anonymität und kann damit die Zuweisungsmöglichkeiten einer vollstreckenden Behörde teilweise lähmen.

↺ ZURÜCK ZUM INHALT

Welcher Datenschutz? Den Schleier lüften

Das Beseitigen der letzten Reste von Anonymität im Cyberspace birgt große Möglichkeiten in sich – sei es für Werbetreibende oder für Spione. Für die Erstgenannten hat sich das Verfolgen mit nachhaltigen Cookies als sinnvolle Technik erwiesen. Das wird sich wahrscheinlich weiter ausbreiten, und zwar in Kombination mit Widgets und anderen harmlosen Ergänzungen zu gängigen Webseiten, die es Unternehmen ermöglichen, individuelle Nutzer auf ihrem Weg über ihre Domains hinaus zu verfolgen und so ein zusammenhängendes Bild ihres Surfverhaltens zu erstellen (mehr dazu siehe unten).

In anderen Teilen der Welt werden Angriffe auf Aktivisten und das Verfolgen von Aktivitäten in Sozialen Medien, die „Instabilität provozieren", weiterhin erstaunliche Raffinesse hervorbringen. Dicke Brieftaschen werden weiterhin gut aufgestellte, gänzlich unbekannte Unternehmen finanzieren, die über die letzten Neuheiten zum Verfolgen von Dissidenten und Aktivisten kreuz und quer durch die Weiten des Internets verfügen. Hinter diesen Aktivitäten steckt üblicherweise ein großes Interesse an den Tendenzen in Sozialen Netzwerken in ganzen geografischen Regionen und daran, wie sie von Dissidentenmeinungen beeinflusst werden. Möglicherweise werden wir sogar einen Akteur erleben, der es wagt, in ein Soziales Netzwerk einzubrechen, um dort eine Goldmine voller personenbezogener Daten und verfänglicher Informationen aufzutun.

Das Spionage-Werbenetz

Keine verbreitete Technologie ist so sehr dazu geeignet wie Werbenetzwerke, um wirklich zielgerichtete Attacken zu ermöglichen. Ihre Platzierung ist bereits absolut finanziell motiviert und es gibt wenig bis gar keine Regulierung, wie immer wiederkehrende Malvertising-Attacken auf bedeutende Webseiten bewiesen haben. Von Natur aus bieten Werbenetzwerke ein exzellentes Ziel-Profiling, mittels einer Kombination aus IPs, Browser-Fingerabdrücken, Surfinteressen und Login-Verhalten.

Diese Art von Nutzerdaten ermöglicht es einem Angreifer, ein Opfer selektiv zu infizieren. Es kann auch auf seine Payload umgeleitet werden und so kollaterale Infektionen und eine nachhaltige Verfügbarkeit von Payloads vermieden werden, die dazu geeignet ist, das Interesse von Sicherheitsforschern zu wecken.

Von daher erwarten wir, dass der Aufbau oder die Übernahme eines Werbenetzwerkes von fortgeschrittenen Cyberspionage-Akteuren – gemessen an den beträchtlichen Einnahmen – nur als kleine Investition angesehen wird, die bewirkt, dass die Ziele getroffen, die neuesten Toolkits aber geschützt werden.

↺ ZURÜCK ZUM INHALT

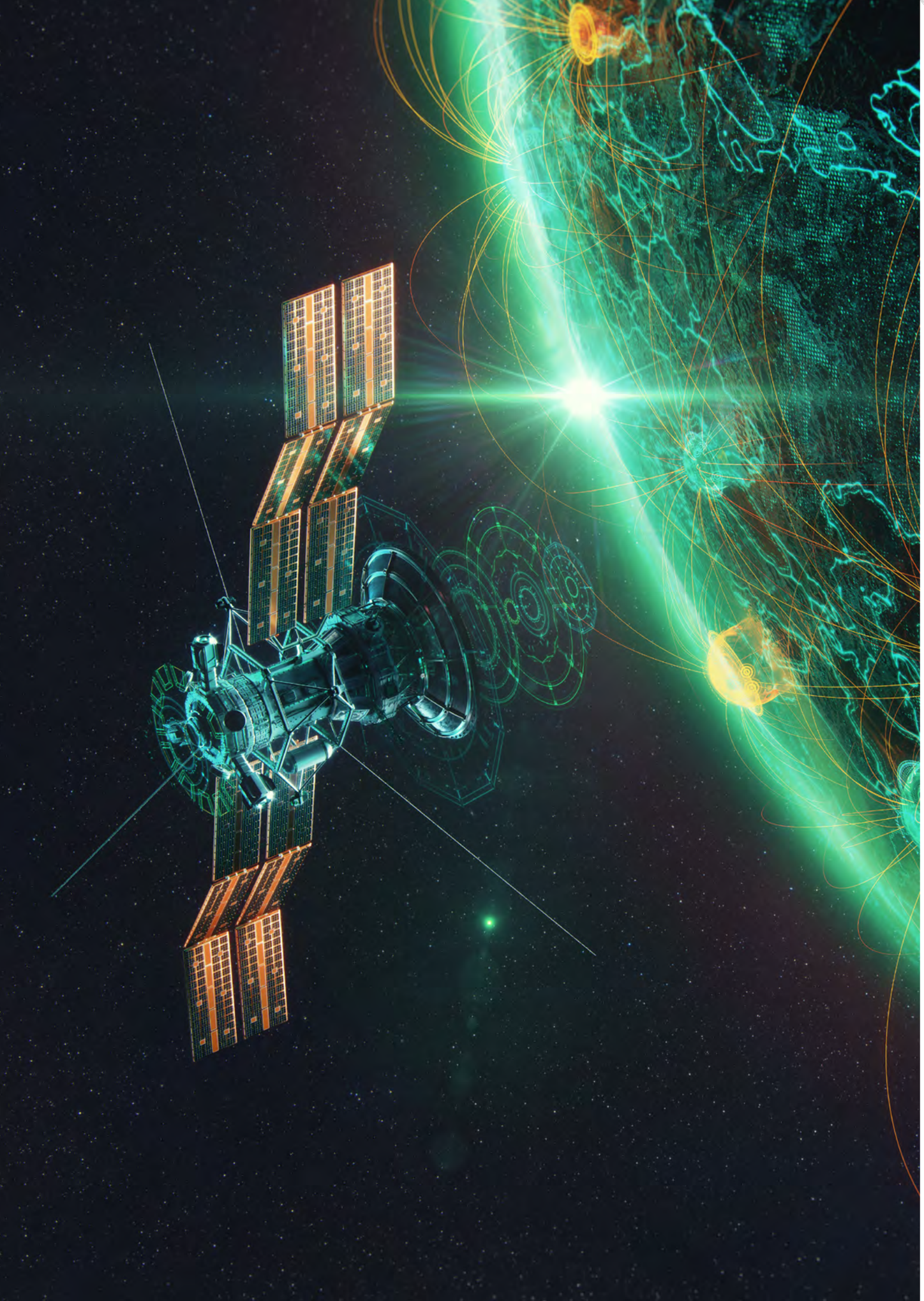
KASPERSKY SECURITY BULLETIN 2016/2017
PROGNOSEN FÜR DAS JAHR 2017

Der Aufstieg des Selbstjustiz-Hackers

Nachdem der mysteriöse Phineas Fisher im Jahr 2015 willkürliche Firmendaten der italienischen Überwachungsfirma HackingTeam online gestellt hatte, veröffentlichte er seinen Leitfaden für aufstrebende Hacker, die ungerechte Organisationen und zwielichtige Unternehmen außer Gefecht setzen wollen.

Er spricht damit das unterschwellige Empfinden an, dass die asymmetrische Macht des hackenden Vigilanten eine Kraft des Guten sei, ungeachtet der Tatsache, dass die Daten vom HackingTeam aktiven APT-Gruppen aktuelle Zero-Days lieferten und möglicherweise sogar eine neue und gierigere Klientel anlockte.

Während die Verschwörungsrhetorik in diesem Wahlzyklus zunimmt, angefeuert von dem Glauben, Datenlecks und das Durchsickern von Daten könnten den Ausschlag für das Informations-Ungleichgewicht geben, werden sich immer mehr Angreifer auf Selbstjustiz verlegen, indem sie Daten angreifbarer Organisationen hacken und durchsickern lassen.



Kaspersky Lab Global Research and Analysis Team (GReAT)

KASPERSKY SECURITY BULLETIN 2016/2017

DEUTSCHE VERSION

de.securelist.com/ | kaspersky.com/de

info@kaspersky.de
Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland
Tel.: +49 (0) 841 98 18 90
Fax: +49 (0) 841 98 189 100

V.i.S.d.P.: Stefan Rojacher

Auf YouTube ansehen

Werden Sie unser Fan auf Facebook

Folgen Sie uns auf Twitter

Treten Sie uns auf LinkedIn bei

Auf Slideshare ansehen

Lesen Sie unseren Blog

Treten Sie uns auf Threatpost bei

Schauen Sie sich uns auf Securelist an

Twitter.com/
Kaspersky_DACH

Facebook.com/
Kaspersky.Lab.DACH

Youtube.com/
KasperskyLabCE

Kaspersky Labs GmbH
Ingolstadt, Deutschland
www.kaspersky.de

Informationen
zur Internetsicherheit:
https://de.securelist.com/

Informationen zu Partnern
in Ihrer Nähe finden Sie hier:
http://www.kaspersky.com/de/partner_finden

KASPERSKY lab

THE POWER
OF PROTECTION