KASPERSKY lab

KASPERSKY SECURITY BULLETIN 2015/2016

Kaspersky Lab Global Research and Analysis Team (GReAT)

DEUTSCHE VERSION

GREAT

ZURÜCK ZUM INHALT

INHALT

KASPERSKY SECURITY BULLETIN 2015/2016 4

» Jahresanalyse von Kaspersky Lab für 2015 und 2016 4

STATISTIK FÜR DAS JAHR 2015 6

» Das Jahr in Zahlen 7
» Von Cyberkriminellen ausgenutzte angreifbare Anwendungen 7
» Finanz-Malware 10
» Geografie der Attacken 12
» Top 10 der Bank-Malware-Familien 14
» 2015 – ein interessantes Jahr für Ransomware 16
» Zahl der angegriffenen Nutzer 17
» Top 10 der Trojan-Ransom-Familien 18
» Top 10 der von Malware des Typs Trojan-Ransom angegriffenen Länder 20
» Verschlüsselungsprogramme 21
» Zahl der neuen Verschlüsselungsprogramme der Klasse Trojan-Ransom 21
» Zahl der von Verschlüsselungsprogrammen angegriffenen Nutzer 22
» Top 10 der von Verschlüsselungsschädlingen angegriffenen Anwender 23
» Schadprogramme im Internet (Attacken über das Web) 24
» Top 20 der Schadprogramme im Internet 24
» Top 10 der Länder, auf deren Ressourcen Schadprogramme untergebracht sind 26
» Länder, in denen Computer dem höchsten Risiko einer Infektion über das Internet ausgesetzt sind 28
» Lokale Bedrohungen 31
» Top 20 der auf den Computern der Anwender entdeckten schädlichen Objekte 32
» Länder, in denen die Computer dem höchsten Risiko einer lokalen Infektion ausgesetzt waren 34
» Fazit 37

ENTWICKLUNG DER IT-BEDROHUNGEN IM UNTERNEHMENSBEREICH 40

» Das Jahr in Zahlen 41
» Zielgerichtete Attacken auf Unternehmen: APT und Kriminelle 41
» Statistik 46
» Web-Bedrohungen (Attacken über das Internet) 46
» Lokale Bedrohungen 48
» Besonderheiten bei Angriffen auf Unternehmen 50
» Exploits in Attacken auf Unternehmen 50
» Verschlüsselungsprogramme 53
» Angriffe auf PoS-Terminals 56
» Fazit 57
» Prognosen 58
» Was tun? 58

DIE TOP SECURITY STORIES 60

» Zielgerichtete Attacken und Malware-Kampagnen 60
» Datenlecks 70
» Smarte (aber nicht unbedingt sichere) Geräte 72
» Internationale Zusammenarbeit gegen Cyberkriminalität 74
» Angriffe auf Industrieobjekte 76
» Fazit 80

PROGNOSE: DAS ENDE VON APTS – WIE WIR SIE KENNEN 82

» Keine APTs mehr 83
» Der Ransomware-Alptraum geht weiter 84
» Gegen das Haus wetten: Finanz-Verbrechen auf höchstem Niveau 84
» Angriffe auf Sicherheitsanbieter 85
» Sabotage, Erpressung und Bloßstellung 86
» Wem trauen Sie? 86
» APT-Akteure am Ende 87
» Die Zukunft des Internets 88
» Die Zukunft der Beförderung 89
» Die Kryptokalypse naht 90

IMPRESSUM 91

KASPERSKY SECURITY BULLETIN 2015/2016

Autor: Stefan Rojacher

JAHRESANALYSE VON KASPERSKY LAB FÜR 2015 UND 2016

Mit dem Kaspersky Security Bulletin 2015/2016 veröffentlicht Kaspersky Lab seine Analyse der Cybergefahren und deren Entwicklungen für das Jahr 2015 sowie eine Prognose für zukünftige Internetgefahren und Angriffsszenarien.

Die Malware-Statistiken für das Jahr 2015 bieten einen Überblick über die Entwicklung von Cyberbedrohungen. Dabei stehen zwei Trends im Vordergrund: Zum einen breiten sich Banking-Trojaner auf neue Plattformen wie beispielsweise Android aus. Zum anderen wurde im Jahr 2015 ein starker Anstieg von Ransomware, also erpresserischer Schadsoftware verzeichnet. Die Geografie des Malware- und Infizierungsniveaus liefert daneben Aufschlüsse hinsichtlich regionaler Gefährdungen.

In Unternehmen wurden **58 Prozent** aller Rechner im vergangenen Jahr mindestens einmal angegriffen. Besonders die Finanzbranche stand im Visier der Cyberkriminellen. Der größte digitale Bankraub der Geschichte „Carbanak" ist dafür nur ein Beispiel.

Neben „Carbanak" machen noch zahlreiche weitere zielgerichtete Attacken wie „Equation" oder „Duqu 2.0" Schlagzeilen. Aber auch die Digitalisierung der Industrie und die Vernetzung kritischer Infrastrukturen sind wichtige Themen, die uns 2015 aus IT-Sicherheitsperspektive begleiteten.

Und was erwarten unsere Forensiker und Experten für das kommende Jahr?

Bei APTs (Advanced Persistent Threats) werden sich Veränderungen zeigen, während Ransomware ein Alptraum für Privatanwender und Unternehmen bleibt. Ein Blick in die weitere Zukunft zeigt, dass klassische Endpoint- und Netzwerklösungen für Cybersicherheit zukünftig um weitere, intelligente Ansätze ergänzt werden müssen.

STATISTIK FÜR DAS JAHR 2015

Autoren: Maria Garnaeva, Denis Makrushin, Jornt Van Der Wiel, Anton Ivanov, Yury Namestnikov

QUICK INFO

- DAS JAHR IN ZAHLEN
- VON CYBERKRIMINELLEN AUSGENUTZTE ANGREIFBARE ANWENDUNGEN
- FINANZ-MALWARE
- GEOGRAFIE DER ATTACKEN
- TOP 10 DER BANK-MALWARE-FAMILIEN
- 2015 – EIN INTERESSANTES JAHR FÜR RANSOMWARE
- ZAHL DER ANGEGRIFFENEN NUTZER
- TOP 10 DER TROJAN-RANSOM-FAMILIEN
- TOP 10 DER VON MALWARE DES TYPS TROJAN-RANSOM ANGEGRIFFENEN LÄNDER
- VERSCHLÜSSELUNGSPROGRAMME
- ZAHL DER NEUEN VERSCHLÜSSELUNGSPROGRAMME DER KLASSE TROJAN-RANSOM
- ZAHL DER VON VERSCHLÜSSELUNGSPROGRAMMEN ANGEGRIFFENEN NUTZER
- TOP 10 DER VON VERSCHLÜSSELUNGSSCHÄDLINGEN ANGEGRIFFENEN ANWENDER
- SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)
- TOP 20 DER SCHADPROGRAMME IM INTERNET
- TOP 10 DER LÄNDER, AUF DEREN RESSOURCEN SCHADPROGRAMME UNTERGEBRACHT SIND
- LÄNDER, IN DENEN COMPUTER DEM HÖCHSTEN 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
- FAZIT

DAS JAHR IN ZAHLEN

- Im Jahr 2015 wehrten die Produkte von Kaspersky Lab auf den Computern von **1.966.324** Anwendern Versuche ab, schädliche Software zu starten, die auf den Diebstahl von Geld via Online-Zugriff auf Bankkonten spezialisiert ist.
- Auf **753.684** Computern individueller Anwender wurden Ransomware-Schädlinge entdeckt. Dabei wurden **179.209** Computer von Erpresser-Programmen angegriffen.
- Im Laufe des gesamten Jahres erkannte Kaspersky Anti-Virus **121.262.075** individuelle schädliche Objekte (zum Beispiel Skripte, Exploits und ausführbare Dateien).
- Die Lösungen von Kaspersky Lab wehrten **798.113.087** Attacken ab, die von Internet-Ressourcen aus verschiedenen Ländern der Welt durchgeführt wurden.
- Im Laufe des Jahres waren **34,2 Prozent** der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt.
- Zur Durchführung der Angriffe über das Netz nutzten die Cyberverbrecher **6.563.145** individuelle Hosts.
- **24 Prozent** der von Kaspersky-Produkten blockierten Webattacken wurden unter Verwendung schädlicher Webressourcen durchgeführt, die sich in den USA befinden.
- Kaspersky Anti-Virus erkannte **4.000.000** schädliche und potenziell unerwünschte Programme auf den Computern der Anwender.

VON CYBERKRIMINELLEN AUSGENUTZTE ANGREIFBARE ANWENDUNGEN

Im Jahr 2015 beobachteten wir den Einsatz neuer Techniken zur Tarnung von Exploits, Shell-Code und Payloads, die dazu dienen, das Entdecken einer Infektion und die Analyse des Schadcodes zu erschweren. Insbesondere...

- **verwendeten Cyberkriminelle das Diffie-Hellman-Schlüsselaustauschprotokoll**.
- **versteckten Online-Gangster ein Exploit-Pack in einem Flash-Objekt**.

Eines der bedeutendsten Ereignisse des Jahres war die Entdeckung zweier Familien von kritischen Sicherheitslücken unter Android. Die Ausnutzung der **Stagefright**-Sicherheitslücken ermöglichte es einem Angreifer, der zuvor eine speziell aufbereitete MMS an die Nummer des Opfers geschickt hatte, entfernt willkürlichen Code auf dessen Gerät auszuführen. **Stagefright 2** wurde zu demselben Zweck ausgenutzt, doch bereits mit Hilfe einer speziell erstellten Mediadatei.

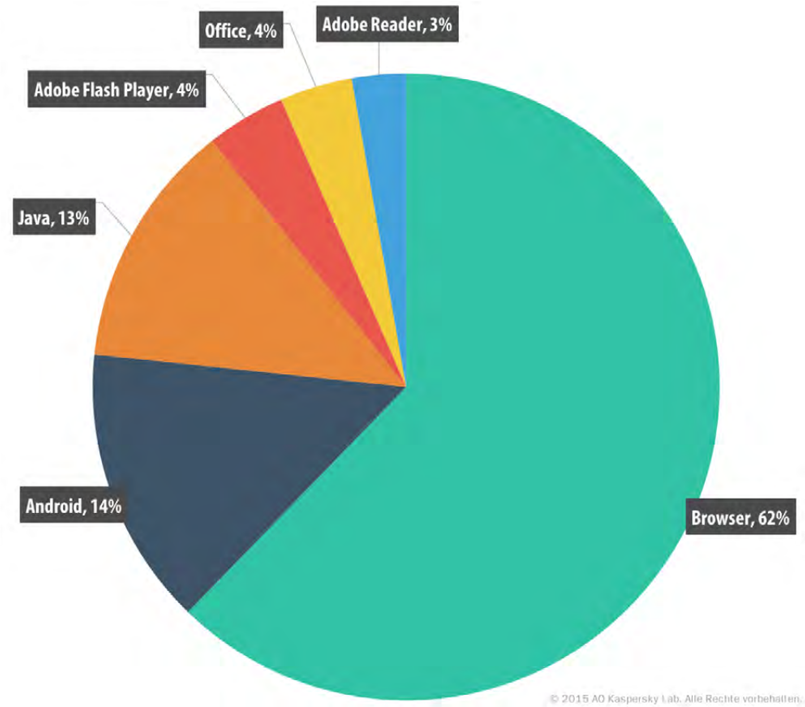
Im Jahr 2015 erfreuten sich Exploits für den Adobe Flash Player großer Beliebtheit unter Cyberkriminellen. Das lässt sich dadurch erklären, dass im Laufe des Jahres eine große Zahl von Sicherheitslücken in diesem Produkt gefunden wurde. Darüber hinaus wurden infolge des Hacking-Team-Datenlecks Informationen über unbekannte Sicherheitslücken im Flash Player öffentlich verfügbar, die sich auch Online-Gangster zunutze machten.

Die Entwickler verschiedener Exploit-Packs reagierten umgehend auf die Entdeckung neuer Sicherheitslücken im Adobe Flash Player und fügten ihren Produkten entsprechend neue Exploits hinzu. Es folgt das „dreckige Dutzend" der von Cyberkriminellen genutzten Sicherheitslücken im Adobe Flash Player, die jetzt in verbreiteten Exploit-Packs unterstützt werden:

1. CVE-2015-0310
2. **CVE-2015-0311**
3. **CVE-2015-0313**
4. **CVE-2015-0336**
5. **CVE-2015-0359**
6. **CVE-2015-3090**
7. **CVE-2015-3104**
8. **CVE-2015-3105**
9. **CVE-2015-3113**
10. **CVE-2015-5119**
11. **CVE-2015-5122**
12. **CVE-2015-5560**
13. **CVE-2015-7645**

Traditionell umfassen einige bekannte Exploit-Packs auch ein Exploit für eine Sicherheitslücke im Internet Explorer (CVE-2015-2419). Im Jahr 2015 wurde zudem die Ausnutzung einer Sicherheitslücke in Microsoft Silverlight (CVE-2015-1671) zur Infektion der Computer bekannt. Dieses Exploit erfreut sich unter den wichtigsten „Playern" auf dem Exploit-Markt allerdings keiner großen Beliebtheit.

ZURÜCK ZUM INHALT



© 2015 AO Kaspersky Lab. Alle Rechte vorbehalten.

Verteilung der Exploits, die Cyberkriminelle im Jahr 2015 bei ihren Attacken eingesetzt haben, nach Typen der angreifbaren Anwendungen

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.

Auch wenn der Anteil der Exploits für den Adobe Flash Player in unserem Rating nur vier Prozent beträgt, sind sie „in freier Wildbahn" recht häufig anzutreffen. Bei dieser Statistik ist aber unbedingt die Tatsache zu berücksichtigen, dass die Technologien von Kaspersky Lab Exploits auf verschiedenen Etappen ausfindig machen. Zu der Kategorie „Browser" (62 %) gehören auch Landing-Pages, die die Exploits „ausliefern". Unseren Beobachtungen zufolge sind das in den meisten Fällen Exploits für den Adobe Flash Player.

Im Laufe des Jahres konnten wir einen Rückgang der Fälle beobachten, in denen Java-Exploits zum Einsatz kamen. Während ihr Anteil Ende 2014 ganze 45 Prozent an allen blockierten Exploits betrug, so ging er innerhalb dieses Jahres nach und nach um 32 Prozentpunkte bis auf 13 Prozent zurück. Zum gegenwärtigen Zeitpunkt sind in keinem bekannten Exploit-Pack noch Java-Exploits vorhanden.

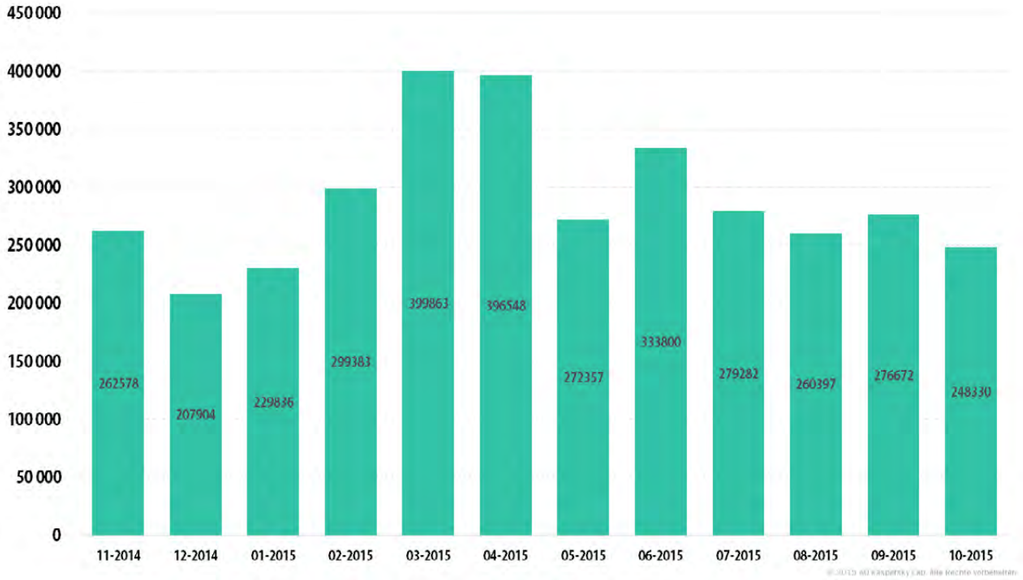
Gleichzeitig registrierten wir eine vermehrte Nutzung von Exploits für Microsoft Office – ihr Anteil stieg von ein auf vier Prozent. Unseren Beobachtungen zufolge wurden diese Exploits im Jahr 2015 mittels massenhafter Spam-Versendungen verbreitet.

FINANZ-MALWARE

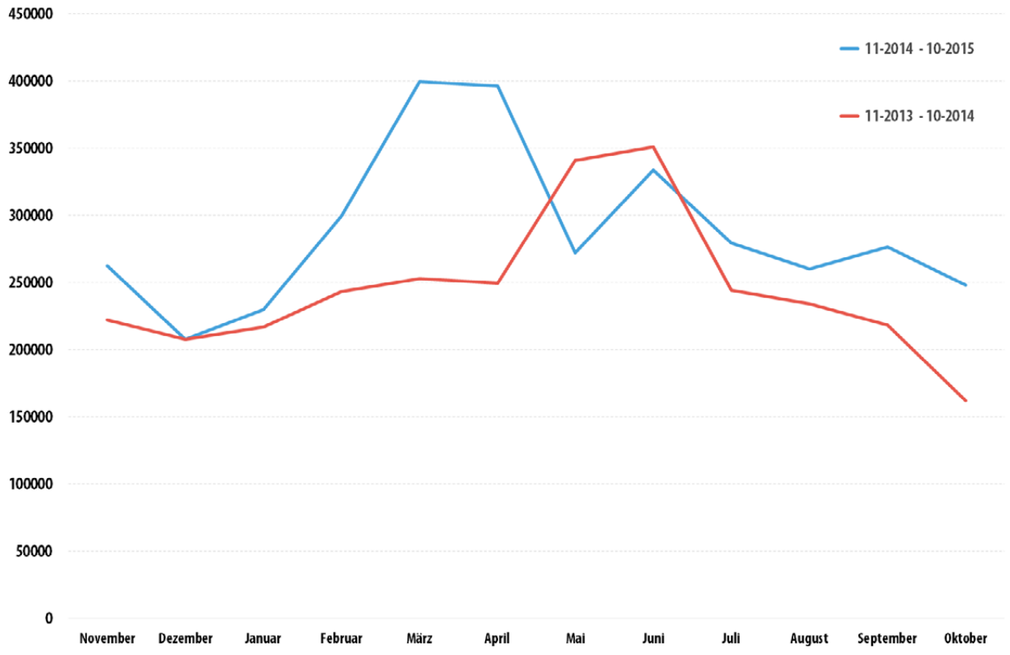
Die vorliegende Statistik basiert auf Daten über die von den Kaspersky-Lab-Produkten detektierten Objekten. Diese Daten stammen von Anwendern, die der Übermittlung statistischer Daten zugestimmt haben.

Die Jahresstatistik für 2015 basiert auf Daten aus dem Berichtszeitraum von November 2014 bis Oktober 2015.

Im Jahr 2015 wehrten die Lösungen von Kaspersky Lab auf den Computern von **1.966.324** Anwendern Versuche ab, schädliche Software zu starten, die auf den Diebstahl von Geld via Online-Zugriff auf Bankkonten spezialisiert ist. Im Vergleich zum Jahr 2014 (**1.910.520**) ist dieser Wert um 2,8 Prozent gestiegen.



Zahl der von Finanz-Malware angegriffenen Anwender, November 2014 bis Oktober 2015



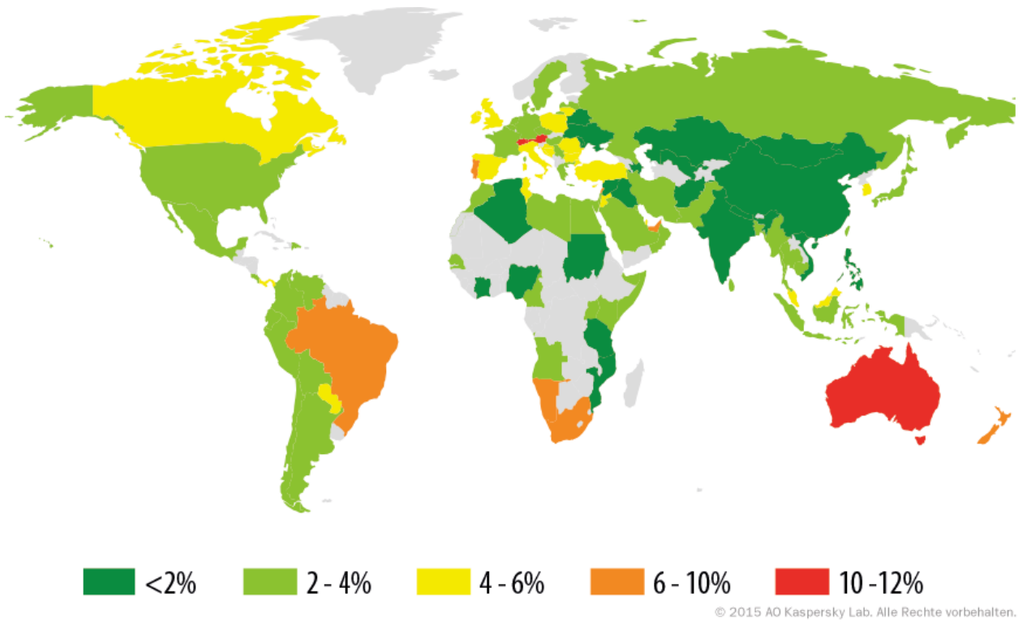
Zahl der von Finanz-Malware angegriffenen Anwender in den Jahren 2014 und 2015

Im Jahr 2015 nahm die Aktivität von Finanz-Malware in der Zeit von Februar bis April zu, mit maximalen Werten in den Monaten März und April. Eine weitere Spitze wurde im Juni registriert.

Im Jahr 2014 wurden die meisten Nutzer in den Monaten Mai und Juni von Finanzschädlingen angegriffen. Von Juni bis Oktober der Jahre 2014 und 2015 ging die Zahl der angegriffenen Anwender allmählich zurück.

GEOGRAFIE DER ATTACKEN

Um die Popularität von Finanz-Malware unter Cyberkriminellen einzuschätzen sowie das Risiko, dem die Computer der Anwender in den verschiedenen Ländern der Welt ausgesetzt sind, haben wir für jedes Land den prozentualen Anteil der Anwender von Kaspersky-Lab-Produkten, die im Berichtszeitraum mit dieser Bedrohung konfrontiert waren, an allen angegriffenen individuellen Anwendern unserer Produkte im Land berechnet.



Geografie der Attacken von Bank-Schädlingen im Jahr 2015 (prozentualer Anteil der von Bank-Trojanern angegriffenen Anwender an allen von Schädlingen angegriffenen Anwendern)

TOP-10 DER LÄNDER NACH PROZENTUALEM ANTEIL DER ANGEGRIFFENEN ANWENDER IM JAHR 2015

	LAND*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER**
1	Singapur	11,6
2	Österreich	10,6
3	Schweiz	10,6
4	Australien	10,1
5	Neuseeland	10,0
6	Brasilien	9,8
7	Namibia	9,3
8	Hongkong	9,0
9	Südafrika	8,2
10	Libanon	6,6

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 10.000 liegt.

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

Spitzenreiter in diesem Rating ist Singapur. In diesem Land hatten es 11,6 Prozent der Nutzer von Kaspersky-Lab-Produkten, die von Schädlingen angegriffen wurden, im Laufe des Jahres mindestens einmal mit Bank-Trojanern zu tun. Diese Tatsache illustriert die Popularität von Finanz-Schädlingen im Verhältnis zu allen anderen Bedrohungen in diesem Land.

In Spanien wurden 5,4 Prozent der angegriffenen Anwender mindestens einmal im Laufe des Jahres von Bank-Trojanern attackiert. In Italien waren es 5,0 Prozent, in Großbritannien 5,1 Prozent, in Deutschland 3,8 Prozent, in Frankreich 2,9 Prozent. In den USA betrug der entsprechende Wert 3,2 Prozent und in Japan waren es 2,5 Prozent.

In Russland hatten es 2,0 Prozent der angegriffenen Anwender mit Bank-Schädlingen zu tun.

TOP 10 DER BANK-MALWARE-FAMILIEN

Die Top 10 der Schadprogramm-Familien, die in Attacken auf Nutzer von Online-Banking-Systemen verwendet wurden, sehen für das Jahr 2015 folgendermaßen aus (nach Anzahl der angegriffenen Anwender):

	NAME*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER**
1	Trojan-Downloader.Win32.Upatre	42,36
2	Trojan-Spy.Win32.Zbot	26,38
3	Trojan-Banker.Win32.ChePro	9,22
4	Trojan-Banker.Win32.Shiotob	5,10
5	Trojan-Banker.Win32.Banbra	3,51
6	Trojan-Banker.Win32.Caphaw	3,14
7	Trojan-Banker.AndroidOS.Faketoken	2,76
8	Trojan-Banker.AndroidOS.Marcher	2,41
9	Trojan-Banker.Win32.Tinba	2,05
10	Trojan-Banker.JS.Agent	1,88

* 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.

Die überragende Mehrheit der Schädlingsfamilien aus den Top 10 verwendet eine für Bank-Trojaner typische Technik zur Einschleusung von willkürlichem HTML-Code in die vom Browser anzuzeigende Webseite. Die vom Nutzer dort in originale oder vom Trojaner hinzugefügte Web-Formulare eingegebenen Bezahldaten werden von den Cyberkriminellen abgefangen.

Die Schädlinge der Familie Trojan-Downloader.Win32.Upatre standen im Verlauf des gesamten Jahres an der Spitze dieses Ratings. Die Größe der Trojaner übersteigt 3,5 KB nicht, und ihre Funktion ist auf den Download einer „Payload" auf den infizierten Computer beschränkt – meist handelt es sich dabei um Vertreter der Trojan-Banker-Familie Dyre/Dyzap/Dyreza. Die Hauptaufgabe dieser Banktrojaner liegt im Diebstahl der Bezahldaten der Anwender. Zu diesem Zweck fängt Dyre die Bankdaten während einer Sitzung zwischen dem Browser des Opfers und der Web-Anwendung für das Online-Banking ab – das heißt, er setzt die Technik „Man-in-the-Browser" (MITB) um. Wir weisen darauf hin, dass dieser Schädling sich aktiv mittels eigens erstellter E-Mails verbreitet, die im Anhang den Downloader enthalten. Außerdem wurde der Downloader Trojan-Downloader.Win32.Upatre im Sommer auf kompromittierten Heimroutern **gefunden**, ein Beleg dafür, dass Cyberkriminelle diesen Trojaner sehr vielseitig einsetzen.

Ein anderer Stammgast in diesem Rating ist Trojan-Spy.Win32.Zbot (zweiter Platz), der ebenfalls seine Position behauptet. Dass er ständig in diesem Rating vertreten ist, ist kein Zufall. Die Trojaner der Familie Zbot gehörten zu den ersten, die Web-Einschleusungen zur Kompromittierung von Bezahldaten der Anwender von Online-Banking-Systemen einsetzten und den Inhalt der Bank-Webseiten modifizierten. Sie verschlüsselten ihre Konfigurationsdateien mehrfach. Die dechiffrierte Konfigurationsdatei wurde dabei nicht als Ganzes im Speicher verwahrt, sondern in einzelnen Teilen geladen.

Vertreter der Familie Trojan-Banker.Win32.ChePro wurden erstmals im Oktober 2012 entdeckt. Damals griffen die Trojaner hauptsächlich Nutzer in Brasilien, Portugal und Russland an, aktuell werden sie in Attacken auf User in vielen Ländern eingesetzt. Die meisten Samples von ChePro sind Downloader, die für eine erfolgreiche Infektion eines Systems andere Dateien benötigen. In der Regel sind das Bank-Schädlinge, die das Erstellen von Screenshots, das Protokollieren der Tastatureingaben und das Auslesen des Kopierpuffer-Inhalts ermöglichen. Damit verfügen sie über eine Funktionalität, mit der sie bei Angriffen auf praktisch jedes beliebige Online-Banking-System eingesetzt werden können.

In diesem Rating sind auch zwei Familien mobiler Bank-Trojaner vertreten, und zwar Faketoken und Marcher. Die Schädlinge dieser Familie stehlen Bezahldaten von mobilen Android-Geräten.

DER FEIND IN MEINEM SMARTPHONE

Die Vertreter der Familie Trojan-Banker.AndroidOS.Faketoken funktionieren in Kooperation mit Bank-Trojanern für PCs. Um sie in Umlauf zu bringen, setzen die Cyberkriminellen Social Engineering ein. Wenn ein Bankkunde mit seinem infizierten PC eine Online-Banking-Seite besucht, verändert der Trojaner diese Seite und fordert den Anwender auf, eine Android-App herunterzuladen, die die Transaktion angeblich schützt. Tatsächlich führt der angebotene Link aber zur Faketoken-App. Nachdem sich Faketoken auf dem Smartphone des Opfers eingenistet hat, erhalten die Verbrecher über den mit einem Bank-Trojaner infizierten Computer des Anwenders Zugriff auf das Bankkonto, und mit dem infizierten mobilen Gerät fangen sie die mTAN ab.

Der zweite mobile Bank-Trojaner ist Trojan-Banker.AndroidOS.Marcher. Nachdem er ein mobiles Gerät infiziert hat, wartet er auf den Start von genau zwei Apps: einer Anwendung für das mobile Banking einer europäischen Bank und Google Play. Ruft der Anwender Google Play auf, zeigt Marcher dem Anwender ein gefälschtes Google-Play-Fenster an, in dem er seine Kreditkartendaten eingeben soll, die dann den Online-Gangstern in die Hände fallen. Genau so geht der Trojaner auch vor, wenn der Nutzer eine Banking-App öffnet.

Auf Position zehn des Ratings befindet sich die Familie Trojan-Banker.JS.Agent. Bei den Vertretern dieser Familie handelt es sich um schädlichen JS-Code, der das Resultat einer Einschleusungsprozedur in die Online-Banking-Seite ist. Die Aufgabe dieses Codes besteht darin, die Bezahldaten abzufangen, die der Nutzer in das Formular auf der Online-Banking-Seite eingibt.

2015 – EIN INTERESSANTES JAHR FÜR RANSOMWARE

Die Klasse Trojan-Ransom bezeichnet Malware, die auf eine unautorisierte Modifizierung von Nutzerdaten ausgerichtet ist, die diese Daten unbrauchbar macht (beispielsweise Verschlüsselungsprogramme), oder die die normale Funktionsfähigkeit eines Computers blockiert. Für die Entschlüsselung der Dateien oder das Zurücksetzen des Computers in seinen alten – funktionsfähigen – Zustand fordern die Betreiber der Malware normalerweise ein Lösegeld von den Opfern.

Seit ihrem Auftauchen in Form von CryptoLocker im Jahr 2013 hat die Ransomware einen weiten Weg zurückgelegt. Im Jahr 2014 entdeckten wir beispielsweise die erste Ransomware-Version für Android. Nur ein Jahr später entfielen bereits 17 Prozent aller erkannten Infektionen auf Android-Geräte.

Das Jahr 2015 sah auch die erste Ransomware für Linux, die in der Klasse Trojan-Ransom.Linux zu finden ist. Auf der positiven Seite ist zu vermerken, dass den Malware-Autoren ein kleiner Fehler bei der Umsetzung unterlief, wodurch es möglich ist, die Dateien zu entschlüsseln, ohne Lösegeld zahlen zu müssen.

Leider treten immer weniger von solchen Implementationsfehlern auf. Das veranlasste **das FBI zu der folgenden Erklärung**: „Die Ransomware ist so gut[...]. Um ehrlich zu sein, raten wir den Anwendern häufig, das Lösegeld einfach zu bezahlen." Dass das nicht immer eine gute Idee ist, wurde dieses Jahr ebenfalls deutlich, als die niederländische Polizei **zwei Personen festnehmen konnte**, die verdächtigt wurden, hinter der CoinVault-Malware zu stecken. Etwas später erhielten wir alle 14.000 Chiffrierungsschlüssel, die wir unserem **neuen Entschlüsselungstool hinzufügten**. Alle CoinVault-Opfer konnten ihre Dateien entschlüsseln, ohne dass sie etwas dafür zahlen mussten.

2015 ist aber auch das Geburtsjahr von TeslaCrypt. TeslaCrypt ist dafür bekannt, die grafische Benutzeroberfläche anderer Ransomware-Familien zu benutzen, ursprünglich die von CryptoLocker, später die von CryptoWall. Dieses Mal wurde die HTML-Seite von CryptoWall 3.0 vollständig kopiert und nur die URLs wurden geändert.

ZAHL DER ANGEGRIFFENEN NUTZER

Das folgende Diagramm zeigt die Zunahme der Nutzer im Laufe des Jahres, bei denen Malware der Klasse Trojan-Ransom entdeckt wurde:

Zahl der von Malware der Klasse Trojan-Ransom angegriffenen Nutzer (Q4/2014 bis Q3/2015)

Insgesamt wurden im Jahr 2015 auf **753.684** Computern Ransomware-Schädlinge entdeckt. Ransomware wird also mehr und mehr zu einem Problem.

TOP 10 DER TROJAN-RANSOM-FAMILIEN

In diesem Rating sind die Top 10 der vorherrschenden Ransomware-Familien vertreten. Die Liste besteht aus Browser-basierten Erpresser- oder Blocker-Familien und einigen berühmt-berüchtigten Familien von Verschlüsselungsprogrammen. Die so genannten Windows-Blocker, die den Zugriff auf ein System einschränken (beispielsweise die Familie Trojan-Ransom.Win32.Blocker) und dann ein Lösegeld verlangen, waren vor einigen Jahren überaus populär, als sie ihren Siegeszug in Russland antraten, um sich dann Richtung Westen auszubreiten. Doch heute sind sie nicht mehr so weit verbreitet und daher auch nicht in den Top 10 vertreten.

	NAME*	PROZENTUALER ANTEIL DER ANWENDER**
1	Trojan-Ransom.HTML.Agent	38,0
2	Trojan-Ransom.JS.Blocker	20,7
3	Trojan-Ransom.JS.InstallExtension	8,0
4	Trojan-Ransom.NSIS.Onion	5,8
5	Trojan-Ransom.Win32.Cryakl	4,3
6	Trojan-Ransom.Win32.Cryptodef	3,1
7	Trojan-Ransom.Win32.Snocry	3,0
8	Trojan-Ransom.BAT.Scatter	3,0
9	Trojan-Ransom.Win32.Crypmod	1,8
10	Trojan-Ransom.Win32.Shade	1,8

* Die vorliegende Statistik basiert auf den Alarmen von Kaspersky-Lab-Produkten auf den Computern der KSN-Teilnehmer, die ihr Einverständnis zur Übermittlung statistischer Daten gegeben haben.

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

Den ersten Platz belegt Trojan-Ransom.HTML.Agent (38 %). An zweiter Stelle steht die Familie Trojan-Ransom.JS.Blocker (20.7 %). Es handelt sich hierbei um Webseiten, die den Browser blockieren und unterschiedliche unerwünschte Inhalte enthalten, meist auch die Erpresser-Mitteilung (zum Beispiel die „Warnung" einer Strafverfolgungsbehörde). Oder sie enthalten JavaScript-Code, der den Browser blockiert und eine Nachricht anzeigt.

Auf der dritten Position befindet sich Trojan-Ransom.JS.InstallExtension (8 %), eine den Browser blockierende Webseite, die dem Nutzer die Installation einer Chrome-Erweiterung beschert. Bei dem Versuch, die Seite zu schließen, wird eine mp3-Datei mit der folgenden Sprachmitteilung abgespielt: „Um die Seite zu schließen, klicken Sie auf den Button ‚Hinzufügen'". Die auf diese Weise angebotenen Erweiterungen fügen dem Nutzer keinen Schaden zu, doch sie sind äußerst lästig, und es ist nahezu unmöglich, sie abzulehnen. Diese Art von Erweiterungsverbreitung wird von Partner-Programmen betrieben. Diese ersten drei Familien sind insbesondere in Russland vorherrschend, ebenso wie in einigen Ländern der ehemaligen Sowjetunion.

Wenn man sich einmal anschaut, wo genau Ransomware am weitesten verbreitet ist (nicht nur die drei oben erwähnten Familien), so kommt man auf das Ländertrio Kasachstan, Russland und Ukraine.

Die Familie **Cryakl** war im dritten Quartal 2015 recht aktiv, mit Spitzenwerten von bis zu 2.300 Infektionsversuchen pro Tag. Eine interessante Besonderheit von Cryakl ist das Verbreitungsschema dieser Malware-Familie. Anstatt die gesamte Datei zu verschlüsseln, chiffriert Cryakl lediglich die ersten 29 Bytes plus drei weitere Blöcke, die sich irgendwo willkürlich in der Datei befinden. Dadurch soll die Verhaltens-basierte Detektion umgangen werden, und die Verschlüsselung der ersten 29 Bytes zerstört den Header.

Cryptodef auf Platz sechs ist die berüchtigte Cryptowall-Ransomware. Cryptowall wird im Gegensatz zu den anderen hier besprochenen Familien am häufigsten in den USA gefunden: Tatsächlich gibt es in den USA dreimal mehr Infektionen als in Russland. Cryptowall wird via Spam-Mails verbreitet, mit denen Nutzer ein ZIP-Archiv bekommen, das seinerseits ein JavaScript enthält. Bei Ausführung lädt das JavaScript Cryptowall herunter und beginnt, die Dateien zu verschlüsseln. Auch die Erpressermitteilung hat sich geändert. Jetzt gratuliert der Schädling den Opfern dazu, „nun Teil der großen Cryptowall-Gemeinschaft zu sein".

Verschlüsselungsprogramme können nicht nur als ausführbare Dateien bereitgestellt werden, sondern auch unter Verwendung simpler Skript-Sprachen, wie im Fall der Familie **Trojan-Ransom.BAT.Scatter**. Die Scatter-Familie erschien im Jahr 2014 und entwickelte sich schnell weiter, wobei sie die Funktionalität eines E-Mail-Wurms und eines Trojan-PSW bekam. Bei der Verschlüsselung werden zwei Paare von asymmetrischen Schlüsseln verwendet, die die Chiffrierung der Nutzerdateien ermöglichen, ohne ihre privaten Schlüssel aufzudecken. Die Malware bedient sich umbenannter legitimer Tools zur Verschlüsselung der Dateien.

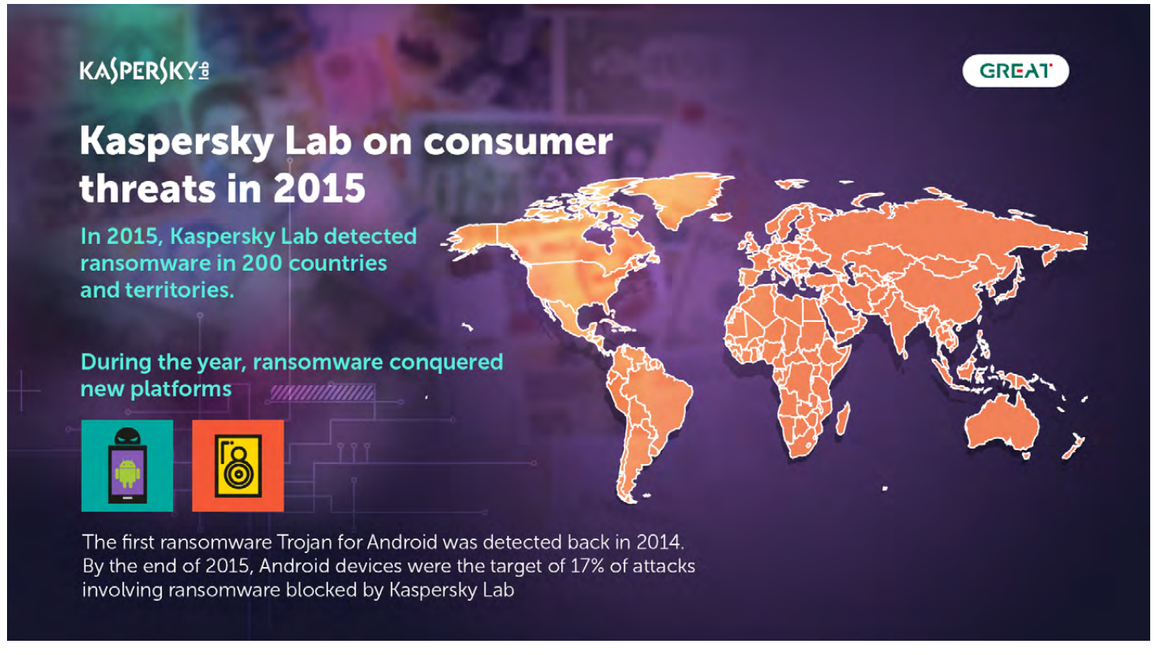
Das Verschlüsselungsprogramm **Trojan-Ransom.Win32.Shade**, das ebenfalls in Russland sehr weit verbreitet ist, kann vom C&C-Server eine Liste mit den URLs zusätzlicher Malware erhalten. Daraufhin lädt es diese Schadprogramme herunter und installiert sie im System. Alle C&C-Server dieser Familie werden im Netzwerk Tor gehostet. Es wird außerdem vermutet, dass Shade über ein Partnerprogramm verbreitet wird.

TOP 10 DER VON MALWARE DES TYPS TROJAN-RANSOM ANGEGRIFFENEN LÄNDER

	NAME*	PROZENTUALER ANTEIL DER VON RANSOM-WARE ANGEGRIFFENEN NUTZER**
1	Kasachstan	5,47
2	Ukraine	3,75
3	Russische Föderation	3,72
4	Niederlande	1,26
5	Belgien	1,08
6	Weißrussland	0,94
7	Kirgisien	0,76
8	Usbekistan	0,69
9	Tadschikistan	0,69
10	Italien	0,57

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 10.000 liegt.

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



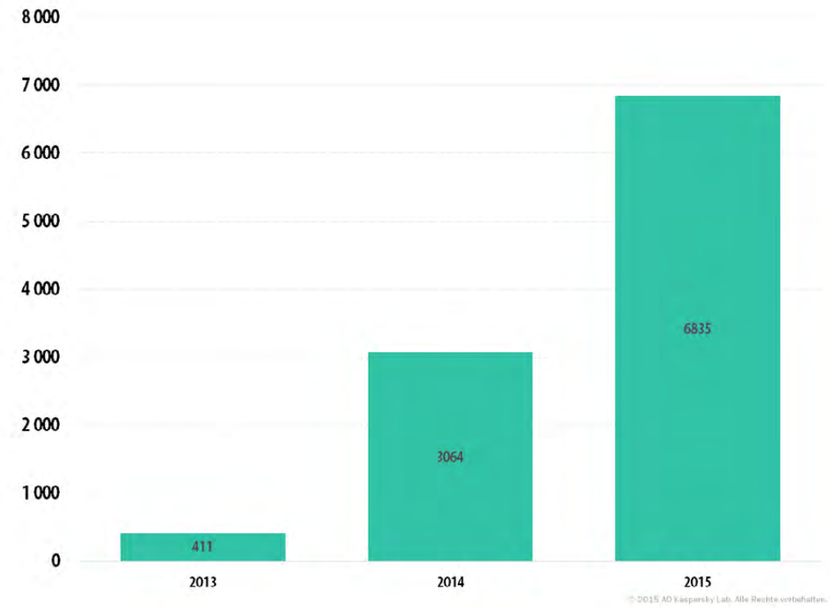
ZURÜCK ZUM INHALT

VERSCHLÜSSELUNGSPROGRAMME

Obwohl die Verschlüsselungsprogramme unter Cyberkriminellen heute nicht so populär sind wie Blocker-Software, fügen sie den Anwendern doch größeren Schaden zu. Daher macht es durchaus Sinn, sie hier auch gesondert zu behandeln.

ZAHL DER NEUEN VERSCHLÜSSELUNGSPROGRAMME DER KLASSE TROJAN-RANSOM

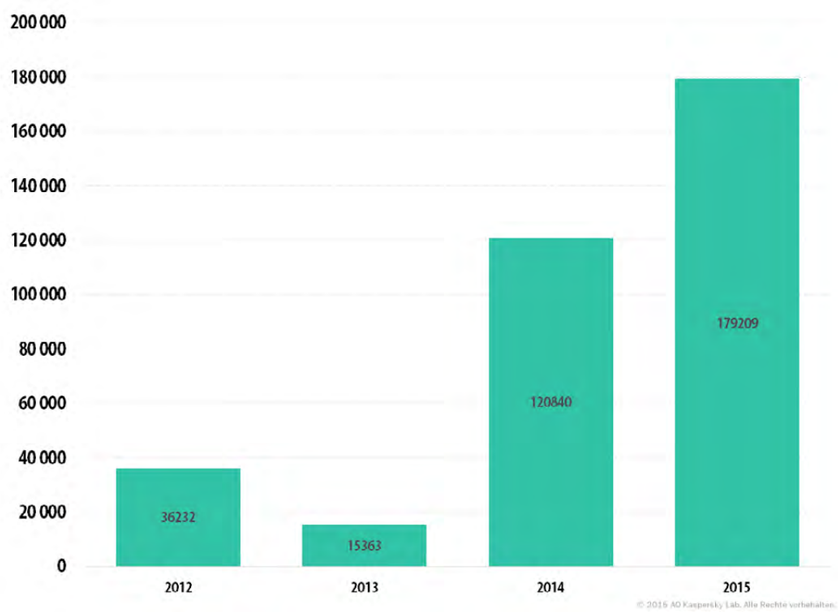
Die folgende Grafik zeigt die Zunahme der neu entwickelten Modifikationen von Verschlüsselungsprogrammen pro Jahr.



Zahl der Modifikationen von Verschlüsselungsprogrammen der Klasse Trojan-Ransom in der Virenkollektion von Kaspersky Lab (2013 bis 2015)

Die Gesamtzahl der Modifikationen von Verschlüsselungsprogrammen beträgt aktuell mindestens 11.000. Im Jahr 2015 wurden zehn neue Familien von Verschlüsselungsprogrammen entwickelt.

ZAHL DER VON VERSCHLÜSSELUNGSPROGRAMMEN ANGEGRIFFENEN NUTZER



Zahl der von Verschlüsselungs-Malware der Klasse Trojan-Ransom angegriffenen Nutzer (2012 bis 2015

Im Jahr 2015 wurden **179.209** individuelle Anwender von Verschlüsselungsschädlingen angegriffen. Etwa 20 Prozent dieser Angriffe ereigneten sich im Unternehmenssektor.

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.

TOP 10 DER VON VERSCHLÜSSELUNGSSCHÄDLINGEN ANGEGRIFFENEN ANWENDER

	LAND*	PROZENTUALER ANTEIL DER VON VERSCHLÜSSELUNGS-MALWARE ANGEGRIFFENEN NUTZER
1	Niederlande	1,06
2	Belgien	1,00
3	Russische Föderation	0,65
4	Brasilien	0,44
5	Kasachstan	0,42
6	Italien	0,36
7	Lettland	0,34
8	Türkei	0,31
9	Ukraine	0,31
10	Österreich	0,30

* Aus den Berechnungen sind die Länder ausgenommen, in denen die Zahl der Nutzer von Kaspersky-Produkten unter 10.000 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.

Der erste Platz wird von den Niederlanden belegt. Die am weitesten verbreitete Familie von Verschlüsselungsschädlingen ist **CTB-Locker** (Trojan-Ransom.Win32/NSIS.Onion). Im Jahr 2015 wurde ein Partner-Programm gestartet, das sich CTB-Locker zunutze macht, und neue Sprachen wurden hinzugefügt, unter anderem Niederländisch. In der Regel werden die Computer mit schädlichen Anhängen infiziert. Es sieht so aus, als wäre auch ein niederländischer Muttersprachler in die Infektionskampagne involviert, da die E-Mails in relativ gutem Niederländisch geschrieben sind.

Eine ähnliche Situation liegt in Belgien vor. Auch dort ist CTB-Locker die am weitesten verbreitete Verschlüsselungs-Malware.

In Russland führt Trojan-Ransom.Win32.Cryakl die Liste der Verschlüsselungsprogramme an, die Anwender angreifen

SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)

Die statistischen Daten in diesem Abschnitt basieren auf dem Modul Kaspersky Anti-Virus, das Windows-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.

TOP 20 DER SCHADPROGRAMME IM INTERNET

Im Laufe des gesamten Jahres erkannte Kaspersky Anti-Virus **121.262.075** individuelle schädliche Objekte (zum Beispiel Skripte, Exploits und ausführbare Dateien).

Von allen Schadprogrammen, die im Jahr 2015 an Internet-Attacken beteiligt waren, hat das Kaspersky-Team nachfolgend die 20 aktivsten aufgeführt. Wie auch schon im vergangenen Jahr belegen Werbeprogramme und ihre Komponenten zwölf Positionen in den Top 20. Im Laufe des Jahres wurden auf 26,1 Prozent aller Computer, auf denen Kaspersky Anti-Virus Alarm geschlagen hat, Werbeprogramme und deren Komponenten registriert. Die Zunahme der Werbeprogramme, ihre aggressive Verbreitungsart und ihre Mechanismen zur Abwehr der Erkennung durch Antivirenprogramme setzen den Trend des Jahres 2014 fort.

Auch wenn aggressive Werbung den Anwendern Unannehmlichkeiten bereitet, fügt Adware ihren Computern keinen Schaden zu. Aus den nachfolgenden Top 20 der Bedrohungen haben wir daher Programme der Klassen Adware und Riskware ausgeschlossen. Auf die schädlichen Objekte in der Hitliste entfielen 96,6 Prozent der Attacken von Schadprogrammen.

	NAME*	PROZENTUALER ANTEIL AN ALLEN ATTACKEN**
1	Malicious URL	75,76
2	Trojan.Script.Generic	8,19
3	Trojan.Script.Iframer	8,08
4	Trojan.Win32.Generic	1,01
5	Expoit.Script.Blocker	0,79
6	Trojan-Downloader.Win32.Generic	0,69
7	Trojan-Downloader.Script.Generic	0,36
8	Trojan.JS.Redirector.ads	0,31
9	Trojan-Ransom.JS.Blocker.a	0,19
10	Trojan-Clicker.JS.Agent.pq	0,14
11	Trojan-Downloader.JS.Iframe.diq	0,13
12	Trojan.JS.Iframe.ajh	0,12
13	Exploit.Script.Generic	0,10
14	Packed.Multi.MultiPacked.gen	0,09
15	Exploit.Script.Blocker.u	0,09
16	Trojan.Script.Iframer.a	0,09
17	Trojan-Clicker.HTML.Iframe.ev	0,09
18	Hoax.HTML.ExtInstall.a	0,06
19	Trojan-Downloader.JS.Agent.hbs	0,06
20	Trojan-Downloader.Win32.Genome.qhcr	0,05

* 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.

Die Top 20 bestehen zu einem großen Teil aus schädlichen Objekten, die in der Regel bei Drive-by-Attacken eingesetzt werden. Sie werden mit heuristischen Methoden als Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic und andere detektiert. Solche Objekte belegen sieben Positionen in unserem Rating.

Unter Malicious URL 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).

Als Trojan.JS.Redirector.ads (8. Platz) erkennt Kaspersky Anti-Virus ein Skript, das Cyberkriminelle auf infizierten Web-Ressourcen platzieren. Es leitet die Browser auf andere Webseiten, beispielsweise auf die Ressourcen von Online-Kasinos. Dass diese Objekte in unserem Rating gelandet sind, sollte Administratoren von Web-Ressourcen daran erinnern, wie einfach die automatische Infektion ihrer Seiten selbst mit den allerkomplexesten Programmen sein kann.

Bei Trojan-Ransom.JS.Blocker.a (9. Platz) handelt es sich um ein Skript, das mit Hilfe der regelmäßigen Aktualisierung einer Seite versucht, den Browser zu blockieren und eine Mitteilung anzuzeigen, die den Nutzer zur Zahlung einer „Strafe" auffordert, weil er sich anstößige Inhalte angesehen hat. Das Geld soll in eine angegebene elektronische Brieftasche überwiesen werden. Dieses Skript ist in erster Linie auf Porno-Webseiten anzutreffen und es wird von Kaspersky Anti-Virus hauptsächlich in Russland und anderen GUS-Staaten aufgespürt.

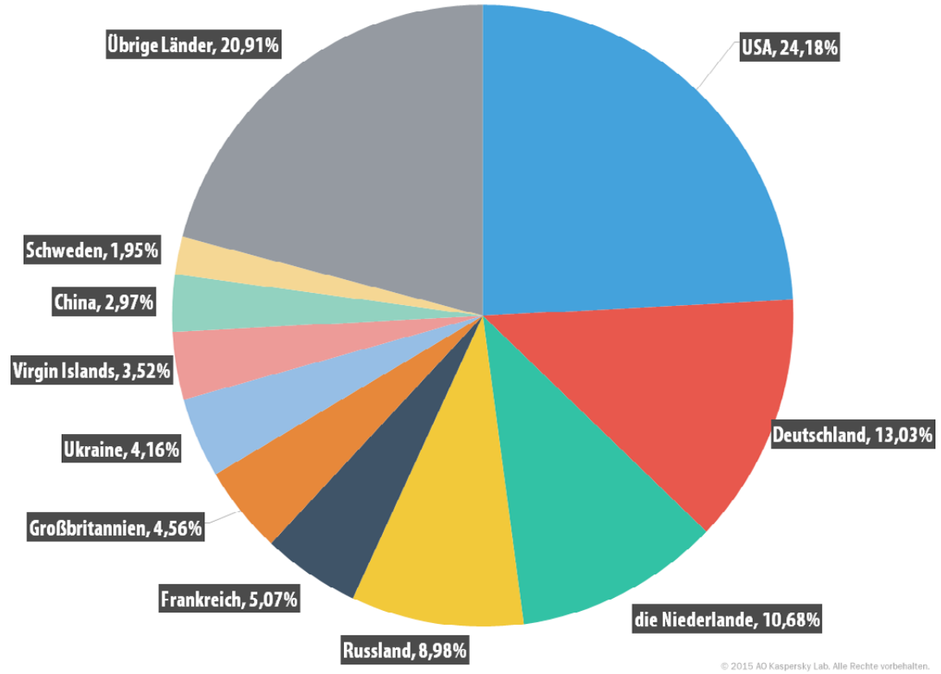
Das Skript, das unsere Schutzlösungen als Trojan-Downloader.JS.Iframe.diq (11. Platz) erkennen, findet sich auch auf infizierten WordPress-, Joomla- und Drupal-Webseiten. Die Kampagne zur massenhaften Infektion von Webseiten mit diesem Skript begann im August 2015. An den Server der Cyberkriminellen übermittelt das Skript zunächst Informationen über den Header der infizierten Seite sowie die aktuelle Domain und die Adresse der Seite, von der aus der Anwender auf die Seite mit dem Skript gewechselt ist. Daraufhin wird mit Hilfe eines iframe ein anderes Skript in den Browser des Anwenders geladen, das Informationen über das Betriebssystem auf dem Computer des Nutzers sammelt, über die Zeitzone und über das Vorhandensein von Adobe Flash Player. Danach und nach einer Reihe von Umleitungen landet der Anwender auf einer Webseite, die ihm die Installation eines Werbeprogramms anbietet, das als Update für den Adobe Flash Player getarnt ist. Alternativ wird er zur Installation eines Browser-Plug-ins aufgefordert.

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 **798.113.087** Attacken über das Internet, die im Jahr 2015 blockiert wurden, verwendeten die Cyberkriminellen **6.563.145** individuelle Hosts, das sind 16 Prozent weniger als im Jahr 2014.

Insgesamt 80 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 im Jahr 2015

Die Besetzung der ersten vier Plätze hat sich gegenüber dem Vorjahr nicht geändert. Frankreich ist von dem siebten auf den fünften Platz (5,07 %) aufgestiegen, die Ukraine dagegen fiel von Position fünf auf Position sieben zurück (4,16 %). Nicht mehr in dem Rating vertreten sind Kanada und Vietnam. Die Neueinsteiger sind China und Schweden auf den Rängen neun respektive zehn.

Diese Top 10 zeigen, dass es Cyberkriminelle vorziehen, ihrer Tätigkeit in Industrienationen nachzugehen und dort auch das Hosting in Anspruch zu nehmen, wo der Markt der Hosting-Dienstleistungen gut entwickelt ist.

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.

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	48,90
2	Kasachstan	46,27
3	Aserbaidschan	43,23
4	Ukraine	40,40
5	Vietnam	39,55
6	Mongolei	38,27
7	Weißrussland	37,91
8	Armenien	36,63
9	Algerien	35,64
10	Katar	35,55
11	Lettland	34,20
12	Nepal	33,94
13	Brasilien	33,66
14	Kirgisien	33,37
15	Moldawien	33,28
16	China	33,12
17	Thailand	32,92
18	Litauen	32,80
19	Vereinigte Arabische Emirate	32,58
20	Portugal	32,31

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 10.000 liegt.

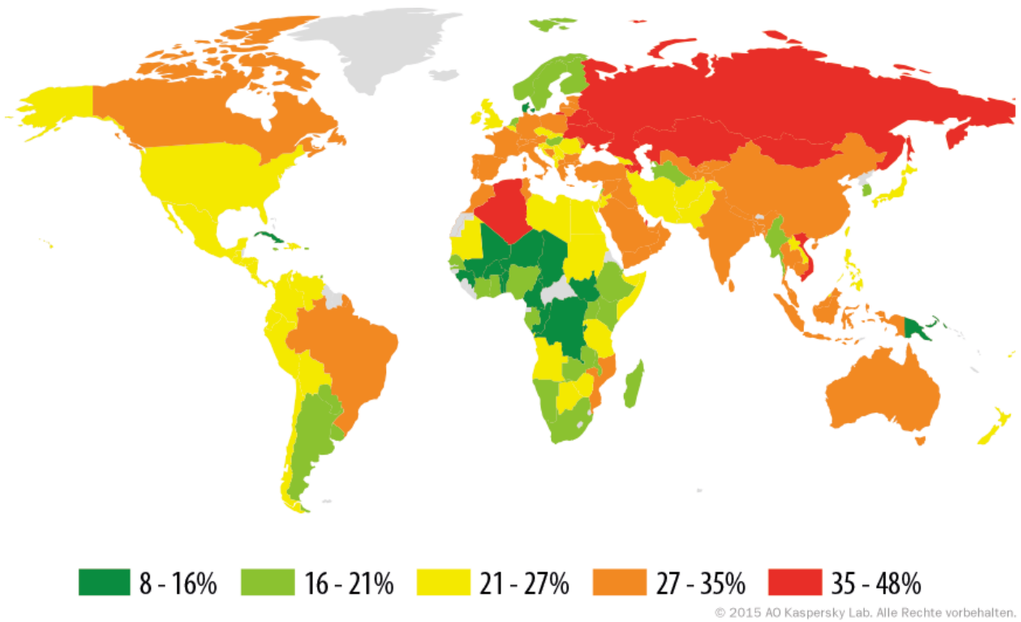
** Prozentualer Anteil individueller Anwender-PCs, die Web-Attacken ausgesetzt waren, an allen Nutzern von Kaspersky-Produkten in diesem Land.

Die ersten drei Länder in diesem Rating blieben gegenüber dem Jahr 2014 unverändert. Russland ist nach wie vor Spitzenreiter, allerdings ging der prozentuale Anteil individueller Anwender dort um 4,9 Prozentpunkte zurück.

Nicht mehr in den Top 20 vertreten sind Deutschland, Tadschikistan, Georgien, Saudi-Arabien, Österreich, Sri Lanka und die Türkei. Neu eingestiegen sind Lettland, Nepal, Brasilien, China, Thailand, die Vereinigten Arabischen Emirate und Portugal.

Alle Länder der Welt lassen sich nach dem Grad des Infektionsrisikos beim Surfen im Netz in drei Gruppen einteilen.

1. **Gruppe mit erhöhtem Risiko**
   Zu dieser Gruppe mit Werten von über 41 Prozent gehören die ersten drei Länder aus den Top 20 – Russland, Kasachstan und Aserbaidschan. Diese Gruppe ist kleiner geworden, im Jahr 2014 umfasste sie noch neun Länder.
2. **Risikogruppe**
   In dieser Gruppe mit Werten zwischen 21 und 40,9 Prozent sind 109 Länder vertreten, unter anderen: Frankreich (32,1 %), Deutschland (32,0 %), Indien (31,6 %), Spanien (31,4 %), die Türkei (31,0 %), Griechenland (30,3 %), Kanada (30,2 %), Italien (29,4 %), die Schweiz (28,6 %), Australien (28,0 %), Bulgarien (27,0 %), die USA (26,4 %), Georgien (26,2 %), Israel (25,8 %), Mexiko (24,3 %), Ägypten (23,9 %), Rumänien (23,4 %), Großbritannien (22,4 %), Tschechien (22,0 %), Irland (21,6 %) und Japan (21,1 %).
3. **Gruppe der beim Surfen im Internet sichersten Länder** (0 bis 20,9 %)
   Zu dieser Gruppe zählen 52 Länder, darunter auch Kenia (20,8 %), Ungarn (20,7 %), Malta (19,4 %), die Niederlande (18,7 %), Norwegen (18,3 %), Argentinien (18,3 %), Singapur (18,2 %), Schweden (18 %), Südkorea (17,2 %), Finnland (16,5 %) und Dänemark (15,2 %).



Risiko einer Infektion über das Internet

Im Jahr 2015 waren **34,2 Prozent** der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt.

Die Gefahrenstufe ist innerhalb des Jahres durchschnittlich um 4,1 Prozentpunkte gesunken. Dieser Trend des gleichmäßigen Rückgangs begann im Jahr 2014 und setzt sich nun schon das zweite Jahr in Folge fort. Dafür können verschiedene Faktoren verantwortlich sein:

- Erstens leisten nun auch Browser und Suchmaschinen, deren Entwickler sich um die Sicherheit der Anwender kümmern, ihren Beitrag im Kampf gegen schädliche Webseiten.
- Zweitens bevorzugen immer mehr Anwender mobile Geräte und Tablets zum Surfen im Netz.
- Drittens überprüfen viele Exploit-Packs nun, ob auf einem Computer eines unserer Produkte läuft. Finden sie ein Kaspersky-Produkt, so versuchen sie gar nicht erst, den Computer anzugreifen.

ZURÜCK ZUM INHALT

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 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 2015 spürte Kaspersky Anti-Virus insgesamt **vier Millionen** schädliche und potenziell unerwünschte Programme auf. Das sind doppelt so viel wie im vorangegangenen Jahr.

TOP 20 DER AUF DEN COMPUTERN DER ANWENDER ENTDECKTEN SCHÄDLICHEN OBJEKTE

Wir haben nachfolgend die 20 Bedrohungen aufgeführt, die im Jahr 2015 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 ANGEGRIFFENEN ANWENDER**
1	DangerousObject.Multi.Generic	39,70
2	Trojan.Win32.Generic	27,30
3	Trojan.WinLNK.StartPage.gena	17,19
4	Trojan.Win32.AutoRun.gen	6,29
5	Virus.Win32.Sality.gen	5,53
6	Worm.VBS.Dinihou.r	5,40
7	Trojan.Script.Generic	5,01
8	DangerousPattern.Multi.Generic	4,93
9	Trojan-Downloader.Win32.Generic	4,36
10	Trojan.WinLNK.Agent.ew	3,42
11	Worm.Win32.Debris.a	3,24
12	Trojan.VBS.Agent.ue	2,79
13	Trojan.Win32.Autoit.cfo	2,61
14	Virus.Win32.Nimnul.a	2,37
15	Worm.Script.Generic	2,23
16	Trojan.Win32.Starter.lgb	2,04
17	Worm.Win32.Autoit.aiy	1,97
18	Worm.Win32.Generic	1,94
19	HiddenObject.Multi.Generic	1,66
20	Trojan-Dropper.VBS.Agent.bp	1,55

* Die Statistik basiert auf Daten 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 Malware Alarm geschlagen hat.

Den ersten Platz belegen schädliche Programme des Typs DangerousObject.Multi.Generic (39,70 %), 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 6,69 Prozent der Anwender anzutreffen, im Jahr 2015 dagegen nur noch bei 5,53 Prozent. Der Wert von Virus.Win32.Nimnul.a lag 2014 bei 2,8 Prozent, im Jahr 2015 bei 2,37 Prozent. Bei den Objekten des Typs Trojan-Dropper.VBS.Agent.bp auf Platz 20 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.

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.

TOP 20 DER LÄNDER NACH INFEKTIONSNIVEAU DER COMPUTER

	LAND*	ANTEIL IN PROZENT**
1	Vietnam	70,83
2	Bangladesch	69,55
3	Russland	68,81
4	Mongolei	66,30
5	Armenien	65,61
6	Somalia	65,22
7	Georgien	65,20
8	Nepal	65,10
9	Jemen	64,65
10	Kasachstan	63,71
11	Irak	63,37
12	Iran	63,14
13	Laos	62,75
14	Algerien	62,68
15	Kambodscha	61,66
16	Ruanda	61,37
17	Pakistan	61,36
18	Syrien	61,00
19	Palästinensische Gebiete	60,95
20	Ukraine	60,78

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 10.000 liegt.

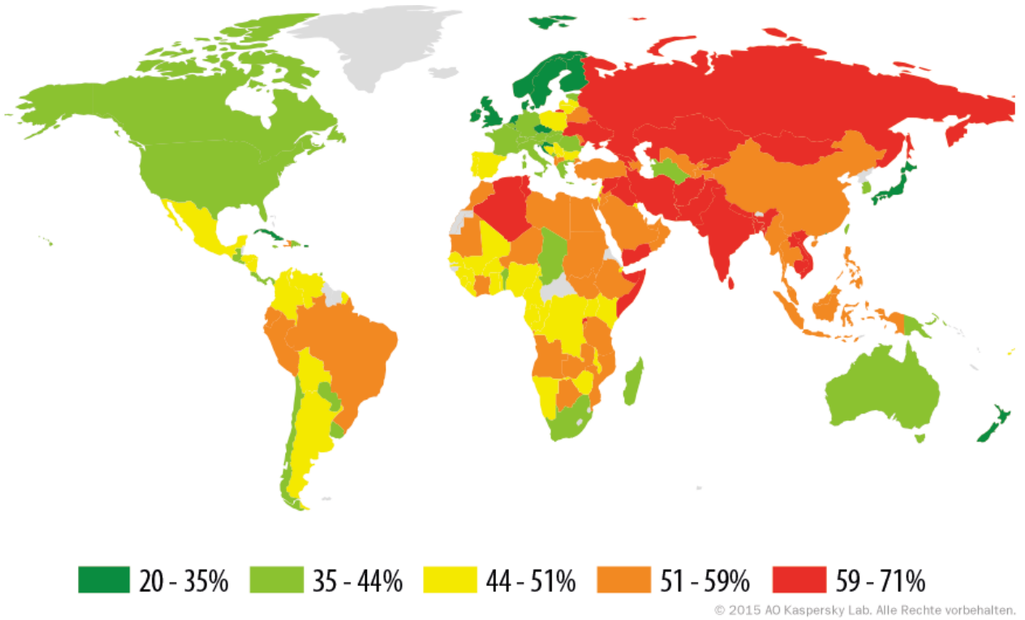
** Prozentualer Anteil von Anwender-PCs, auf denen lokale Bedrohungen blockiert wurden, an allen Nutzern von Kaspersky-Produkten in diesem Land.

ZURÜCK ZUM INHALT

Den ersten Platz in diesem Rating belegt das dritte Jahr in Folge Vietnam. Die Mongolei und Bangladesch haben im Jahr 2015 die Plätze getauscht: Während die Mongolei vom zweiten auf den vierten Platz abrutschte, stieg Bangladesch von Rang vier auf Rang zwei auf. Russland, das im vergangenen Jahr gar nicht in den Top 20 vertreten war, belegt nach den Ergebnissen für das Jahr 2015 gleich den dritten Platz.

Nicht mehr in den Top 20 vertreten sind Indien, Afghanistan, Ägypten, Saudi Arabien, der Sudan, Sri Lanka, Myanmar und die Türkei. Neueinsteiger sind Russland, Armenien, Somalia, Georgien, Iran, Ruanda, die Palästinensischen Gebiete und die Ukraine.

Durchschnittlich wurde in den Ländern aus den Top 20 bei 67,7 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 –, gegenüber 58,7 Prozent im Jahr 2014.



Risiko einer lokalen Infektion

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

- **Maximales Infektionsniveau** (über 60 %)
  Zu dieser Gruppe gehören 22 Länder, unter anderem Kirgisien (60,77 %) und Afghanistan (60,54 %).
- **Hohes Infektionsniveau** (41 bis 60 %)
  98 Länder, darunter Indien (59,7 %), Ägypten (57,3 %), Weißrussland (56,7 %), die Türkei (56,2 %), Brasilien (53,9 %), China (53,4 %), die Vereinigten Arabischen Emirate (52,7 %), Serbien (50,1 %), Bulgarien (47,7 %), Argentinien (47,4 %), Israel (47,3 %), Lettland (45,9 %), Spanien (44,6 %), Polen (44,3 %), Deutschland (44,0 %), Griechenland (42,8 %), Frankreich (42,6 %), Korea (41,7 %) und Österreich (41,7 %).
- **Mittleres Infektionsniveau** (21 bis 40,9 %)
  45 Länder, darunter Rumänien (40,0 %), Italien (39,3 %), Kanada (39,2 %), Australien (38,5 %), Ungarn (38,2 %), die Schweiz (37,2 %), die USA (36,7 %), Großbritannien (34,7 %), Irland (32,7 %), die Niederlande (32,1 %), Tschechien (31,5 %), Singapur (31,4 %), Norwegen (30,5 %), Finnland (27,4 %), Schweden (27,4 %), Dänemark (25,8 %) und Japan (25,6 %).

TOP 10 DER LÄNDER MIT DEN GERINGSTEN COMPUTER-INFEKTIONSRATEN (LOKALE INFEKTIONEN)

	LAND*	ANTEIL IN PROZENT**
1	Kuba	20,8
2	Seychellen	25,3
3	Japan	25,6
4	Dänemark	25,8
5	Schweden	27,4
6	Finnland	27,4
7	Andorra	28,7
8	Norwegen	30,5
9	Singapur	31,4
10	Tschechien	31,5

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

Gegenüber dem Jahr 2014 gab es in dieser Liste einige Veränderungen. Neu hinzugekommen ist Andorra, nicht mehr im Rating vertreten ist Martinique. Durchschnittlich wurden 26,9 Prozent der Computer in den zehn sichersten Ländern mindestens einmal im Laufe des Jahres angegriffen. Im Vergleich zum Vorjahr ist dieser Wert um 3,9 Prozentpunkte gestiegen.

FAZIT

Auf der Grundlage einer Analyse unserer Statistik können wir grob bestimmen, in welche Hauptrichtungen sich die Cyberkriminalität entwickeln wird:

- Ein Teil der Personen, die im Cybercrime-Milieu aktiv sind, werden versuchen, das Risiko einer strafrechtlichen Verfolgung zu minimieren und von Malware-Angriffen auf die aggressive Verbreitung von Adware umsteigen.
- Bei der in massenhaften Attacken eingesetzten Schadsoftware wird der Anteil vergleichsweise einfacher Programme steigen. Das versetzt die Cyberkriminellen in die Lage, ihre Malware schnell zu aktualisieren und damit die Effizienz zu steigern.
- Cyberkriminelle haben Nicht-Windows-Plattformen erschlossen, und zwar Android und Linux: Für diese Plattformen wurden mittlerweile praktisch alle Arten von Schadprogrammen entwickelt und werden auch verwendet.
- Im Rahmen ihrer Tätigkeit setzen Cyberkriminelle aktiv moderne Anonymisierungs-Technologien ein, wie etwa Tor zum Verbergen der Steuerungsserver und Bitcoins für die Durchführung von Finanz-Transaktionen.

Ein immer größerer Teil der Alarme von Kaspersky Anti-Virus entfällt auf die „Grauzone“: In erster Linie sind das verschiedene Werbeprogramme und ihre Module. In unserem Rating der Web-Bedrohungen für das Jahr 2015 belegen die Vertreter dieser Programm-Art zwölf Positionen in den Top 20. Im Laufe des Jahres wurden auf 26,1 Prozent aller Computer, auf denen Kaspersky Anti-Virus Alarm geschlagen hat, Werbeprogramme und deren Komponenten registriert. Die Zunahme der Werbeprogramme, ihre aggressive Verbreitungsart und ihre Mechanismen zur Abwehr der Erkennung durch Antivirenprogramme setzen den Trend des Jahres 2014 fort. Die Verbreitung solcher Adware bringt nicht wenig Geld, und im Rennen um die höchsten Einnahmen setzen ihre Schöpfer manchmal Methoden und Technologien ein, die für Malware charakteristisch sind.

Im Jahr 2015 nahm die Popularität von Exploits für den Adobe Flash Player unter Virenautoren zu. Unseren Beobachtungen zufolge laden Landing-Pages mit Exploits am häufigsten gerade Exploits für den Adobe Flash Player. Das hat zwei Gründe: Erstens wurde im Laufe des Jahres eine große Zahl von Sicherheitslücken in diesem Produkt gefunden. Zweitens wurden infolge des Hacking-Team-Datenlecks **Informationen** über unbekannte Sicherheitslücken im Flash Player öffentlich verfügbar, die sich auch Online-Gangster zunutze machten.

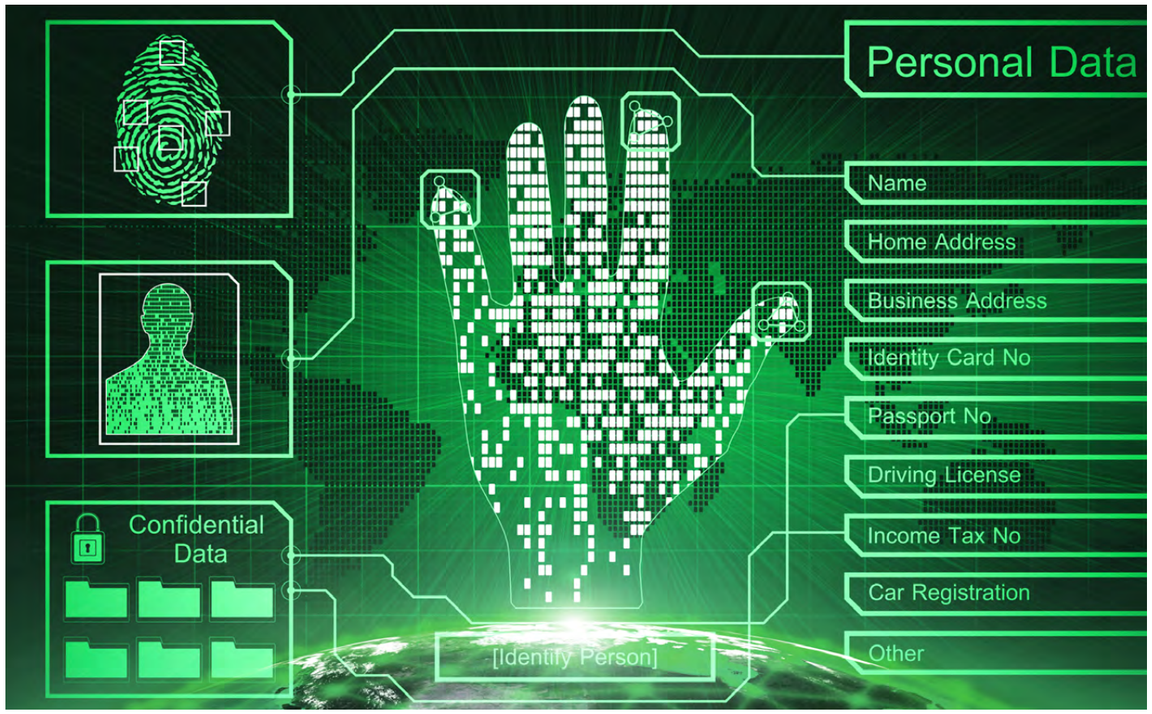
Im Lager der Bank-Trojaner gab es eine interessante Veränderung. Die unzähligen Modifikationen des Trojaners ZeuS, die lange Jahre den ersten Platz belegten, wurden nun von dem Schadprogramm Trojan-Banker.Win32.Dyreza verdrängt. Im Laufe des ganzen Jahres 2015 befand sich Upatre an der Spitze des Ratings der Schädlinge, die auf den Diebstahl von Geld bei Online-Banking-Systemen spezialisiert sind. Auf den betroffenen Computer lädt dieser Downloader Bank-Trojaner einer Familie, die unter den Namen Dyre/Dyzap/Dyreza bekannt ist. An allen Bankbedrohungen betrug der Anteil der von Dyreza angegriffenen Anwender über 40 Prozent. Der Bank-Schädling verwendet ein effektives Schema zur Web-Einschleusung mit dem Ziel, Zugriffsdaten für Online-Banking-Systeme zu stehlen.

Wir weisen zudem darauf hin, dass zwei Familien von mobilen Bank-Trojanern in den Top 10 der Bankschädlinge für das Jahr 2015 vertreten sind, und zwar Faketoken und Marcher. Ausgehend von den Trends ist zu vermuten, dass mobile Bank-Trojaner im nächsten Jahr einen deutlich größeren Anteil an unserem Rating haben werden.

Bei den Erpresser-Trojanern gab es im Jahr 2015 eine Reihe von Veränderungen:

1. Während die Popularität von Schadprogrammen, die die Funktionsfähigkeit des Computers blockieren, nach und nach abnimmt, stieg die Zahl der von Verschlüsselungsprogrammen attackierten Nutzer innerhalb des Jahres um 48,3 Prozent. Das Chiffrieren von Dateien anstelle des simplen Blockierens des Computers ist eine Methode, die es dem Opfer in den meisten Fällen unmöglich macht, den Zugriff auf seine Informationen wiederherzustellen. Besonders aktiv nutzen Cyberkriminelle Verschlüsselungsschädlinge in Attacken auf Unternehmensanwender, die viel eher zum Zahlen des Lösegelds bereit sind als normale Heimanwender. Eine Bestätigung hierfür ist auch das Erscheinen des ersten Verschlüsselungstrojaners unter Linux im Jahr 2015, der sich gegen Web-Server richtet.
2. Die Verschlüsselungsschädlinge werden dabei immer modularer – neben der reinen Chiffrierungsfunktionalität legten sie sich auch eine Funktionalität zum Diebstahl von Daten von den Computern ihrer Opfer zu.
3. Während die Online-Verbrecher gerade erst beginnen, ihre Aufmerksamkeit auf Linux zu richten, wurde der erste Erpresser-Trojaner für Android bereits 2014 entdeckt. Im Jahr 2015 nahm die Zahl der Attacken auf Android stetig zu, und auf das gesamte Jahr gesehen wurden 17 Prozent aller Angriffe von Erpresser-Programmen auf Geräten unter dem mobilen Betriebssystem Android blockiert.
4. Die Bedrohung breitet sich über den gesamten Globus aus: Die Produkte von Kaspersky Lab entdeckten in 200 Ländern und Gebieten Erpresser-Trojaner, also praktisch überall.

Für das Jahr 2016 erwarten wir eine weitere Entwicklung von Verschlüsselungsschädlingen, die sich gegen Nicht-Windows-Plattformen richten: einen Anstieg des Anteils von Android und das Erscheinen von erpresserischen Verschlüsselungsprogrammen für Mac OS. Wenn man bedenkt, dass Android auch aktiv in Gebrauchselektronik verwendet wird, ist es durchaus möglich, dass wir schon bald mit den ersten Angriffen von Verschlüsselungsschädlingen auf „smarte“ Geräte zu rechnen haben.



CYBERTHREAT REAL-TIME MAP

ENTWICKLUNG DER IT-BEDROHUNGEN IM UNTERNEHMENSBEREICH

Autoren: Yury Namestnikov

QUICK INFO

- DAS JAHR IN ZAHLEN
- ZIELGERICHTETE ATTACKEN AUF UNTERNEHMEN: APT UND KRIMINELLE
- STATISTIK
- WEB-BEDROHUNGEN (ATTACKEN ÜBER DAS INTERNET)
- LOKALE BEDROHUNGEN
- BESONDERHEITEN BEI ANGRIFFEN AUF UNTERNEHMEN
- EXPLOITS IN ATTACKEN AUF UNTERNEHMEN
- VERSCHLÜSSELUNGSPROGRAMME
- ANGRIFFE AUF POS-TERMINALS
- FAZIT
- PROGNOSEN
- WAS TUN?

Ende 2014 veröffentlichte Kaspersky Lab seine **Vorhersagen bezüglich der Entwicklung im Bereich Cyber-(Un)-Sicherheit für das Jahr 2015**. Vier von neun unserer Prognosen betrafen direkt Bedrohungen für die Geschäftswelt. Und unsere Vorhersagen erwiesen sich als richtig – drei von vier Punkten haben sich bereits bewahrheitet:

- Cyberkriminelle entdecken APTs – ja
- APT-Gruppen spalten sich auf und streuen ihre Angriffe – ja
- Eskalation der Angriffe auf Geldautomaten und PoS-Terminals – ja
- Attacken auf virtuelle Zahlungssysteme – nein

Schauen wir uns einmal anhand der wichtigsten Ereignisse des Jahres 2015 an, welche neuen Trends wir in Verbindung mit IT-Sicherheit im Unternehmensbereich beobachten konnten.

DAS JAHR IN ZAHLEN

- Im Jahr 2015 wurde auf **58 Prozent** der Unternehmenscomputer mindestens einmal eine Malware-Attacke abgewehrt, das sind drei Prozentpunkte mehr als im vorangegangenen Jahr.
- 29 Prozent der Computer, also fast **jeder dritte Rechner** in einer Unternehmensumgebung, wurden mindestens einmal über das Internet attackiert.
- Bei Angriffen auf Unternehmen werden drei Mal häufiger Exploits zu Office-Anwendungen eingesetzt als bei Attacken auf Heimanwender.
- Kaspersky Anti-Virus schlug auf **26 Prozent** der Computer von Unternehmensanwendern Alarm (detektiert wurden Objekte auf den Computern oder daran angeschlossenen Wechselmedien wie USB-Sticks, Speicherkarten, Mobiltelefone, externe Festplatten oder Netzwerkfestplatten).

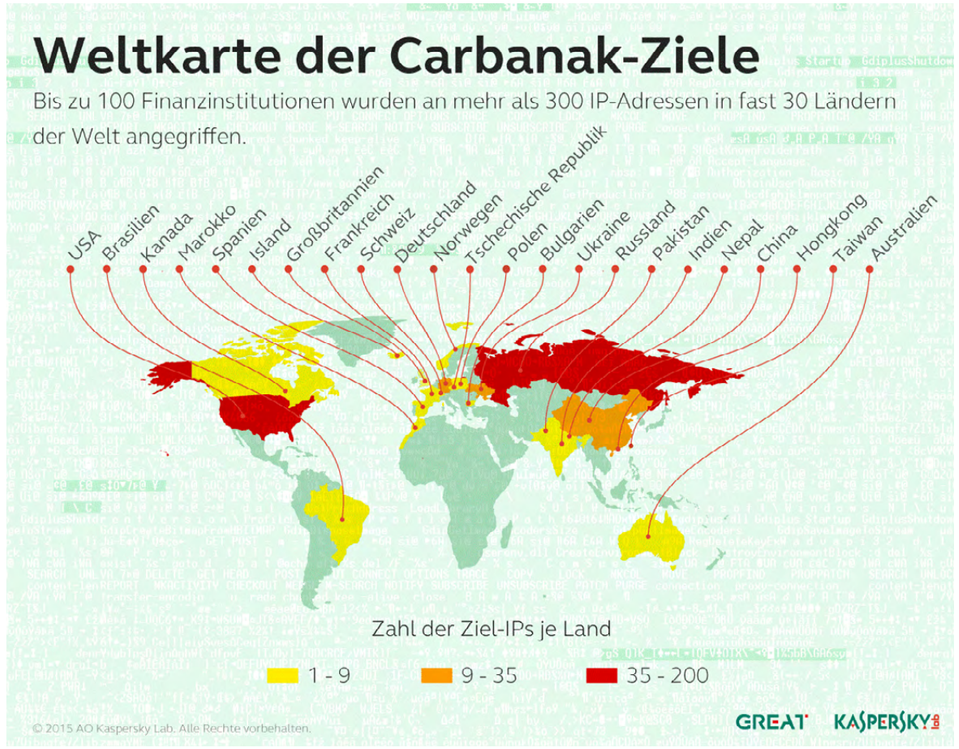
ZIELGERICHTETE ATTACKEN AUF UNTERNEHMEN: APT UND KRIMINELLE

Das Jahr 2015 war geprägt von einer Reihe von Angriffen des Typs APT auf Unternehmen. Die Cyberwaffen und Methoden, die die Cyberkriminellen einsetzten, waren denen sehr ähnlich, auf die wir bei der Analyse von APT-Attacken stießen. Doch hinter den Angriffen standen keine staatlichen Strukturen, sondern Cyberkriminelle. Obwohl die Cyberverbrecher für sie untypische Methoden einsetzten, blieb der Sinn hinter den Angriffen unverändert – das Erzielen von finanziellen Vorteilen.

Ein anschauliches Beispiel für zielgerichtete Angriffe des Typs APT auf Finanzorganisationen ist die Operation **Carbanak**. Es handelte sich dabei um einen echten Banküberfall in digitaler Form:

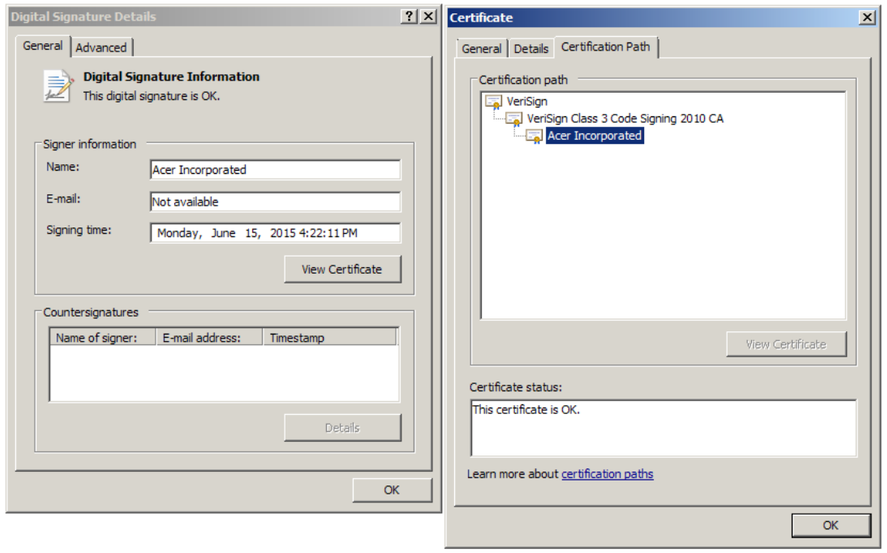
Cyberkriminelle drangen in das Netz der betroffenen Bank ein und suchten nach kritisch wichtigen Systemen, mit Hilfe derer sie Geldmittel aus der angegriffenen Finanzorganisation herausschleusen konnten. Nachdem sie eine Bank um eine bedeutende Summe erleichtert hatten (zwischen 2,5 und 10 Millionen US-Dollar), machten sich die Bankräuber auf die Suche nach dem nächsten Opfer.

Die meisten Opfer dieser Schadkampagne sind in Osteuropa ansässig. Weltweit wurden mehr als 100 Opfer dieses Angriffs gezählt, und die Gesamtverluste der betroffenen Organisationen (in erster Linie Banken) könnten bis zu einer Milliarde US-Dollar betragen.



Man darf nicht vergessen, dass Informationen ebenfalls einen großen Wert darstellen können, insbesondere wenn sie bei Geschäftsabschlüssen oder beim Handel an verschiedenen Waren-, Wertpapier- oder Devisenbörsen benutzt werden, unter anderem auch beim Handel mit Kryptowährungen. Ein Beispiel für eine zielgerichtete Attacke, die auf das Abgreifen derartiger Informationen ausgerichtet sein könnte, ist **Wild Neutron** (auch bekannt als Jripbot und Morpho). Diese Kampagne **erregte erstmals im Jahr 2013 allgemeine Aufmerksamkeit**, als der Bedrohungsakteur erfolgreich so bekannte Unternehmen wie Apple, Facebook, Twitter und Microsoft angriff. Nachdem über diese Vorfälle ausführlich in den Massenmedien berichtet worden war, stellten die Organisatoren der Cyberspionage-Operation ihre Aktivität ein. Doch etwa ein Jahr später registrierte Kaspersky Lab ein Wiederaufleben der Aktivität von Wild Neutron.

Unsere Untersuchungen ergaben, dass im Laufe der Cyberspionage-Kampagne Computer von Nutzern in elf Ländern infiziert wurden, und zwar in Russland, Frankreich, in der Schweiz, in Deutschland, Österreich, Slowenien, Palästina, den Vereinigten Arabischen Emiraten, in Kasachstan, Algerien und den USA. Zu den Zielen gehörten Anwaltskanzleien, Investmentfirmen, Bitcoin-Unternehmen, große Unternehmensgruppen, die meist auf dem Markt der Fusionen und Firmenübernahmen (M&A) tätig sind, IT-Unternehmen, Firmen aus dem Gesundheitswesen, Immobilienfirmen sowie individuelle Anwender.



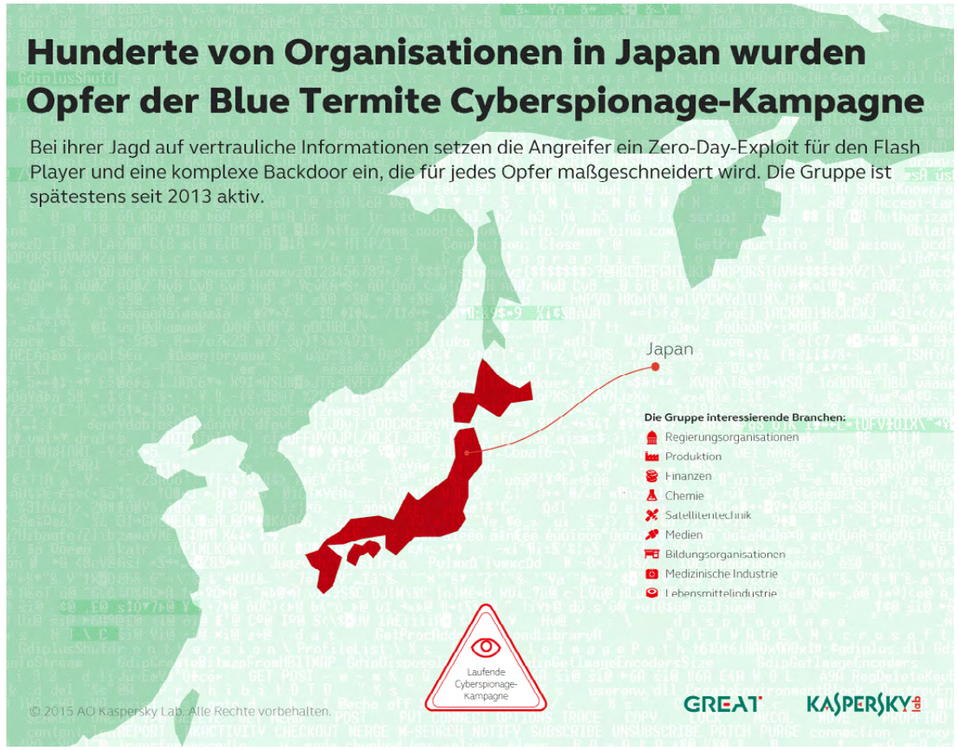
Signatur der Firma Acer im Wild-Neutron-Installer

Im Rahmen der Wild Neutron-Kampagne wurde ein gestohlenes, Code signierendes Zertifikat der Firma Acer verwendet.
Der Trend zur Streuung von APT-Attacken wird sehr anschaulich durch die veränderten Angriffsziele der Cybercrime-Gruppe **Winnti** illustriert. Lange Zeit wurde angenommen, dass dieser vermeintlich chinesische Bedrohungsakteur in erster Linie Spielehersteller angreift. Doch beginnend mit dem Frühjahr 2015 erhielten wir Informationen, die darauf hinwiesen, dass die Cyberkriminellen, nachdem sie ihre Tools und Methoden überarbeitet hatten, nun versuchten, Gewinne durch Attacken auf andere Ziele zu erhalten. Ihr Interesse galt nicht mehr allein der Unterhaltungsindustrie:

Der Akteur hatte es jetzt auch auf Unternehmen aus den Bereichen Pharmazie und Telekommunikation abgesehen. Bei einer Analyse der neuen Winnti-Angriffswelle stellte sich wie im Fall von Wild Neutron heraus, dass das Winnti-Rootkit mit einem gestohlenen Zertifikat signiert war, das einer Unterabteilung eines riesigen japanischen Konzerns gehörte.

Das Jahr 2015 zeichnete sich bezüglich der Attacken und der Angreifer gegenüber dem Vorjahr auch jeweils durch eine größere geografische Ausdehnung aus. Während einer laufenden Ermittlung eines Vorfalls im Mittleren Osten stießen die Experten von Kaspersky Lab auf die Aktivität einer bis dahin unbekannten Gruppe, die zielgerichtete Attacken durchführte. Die Gruppe wurde auf den Namen **Desert Falcons** getauft, und sie ist die erste arabische Gruppe, die vollwertige Cyberspionage-Operationen durchführt. Zum Zeitpunkt der Entdeckung betrug die Zahl der Opfer etwa 300, darunter auch Finanzorganisationen.

Die Gruppe **Blue Termite** hingegen griff Unternehmen in Japan an:



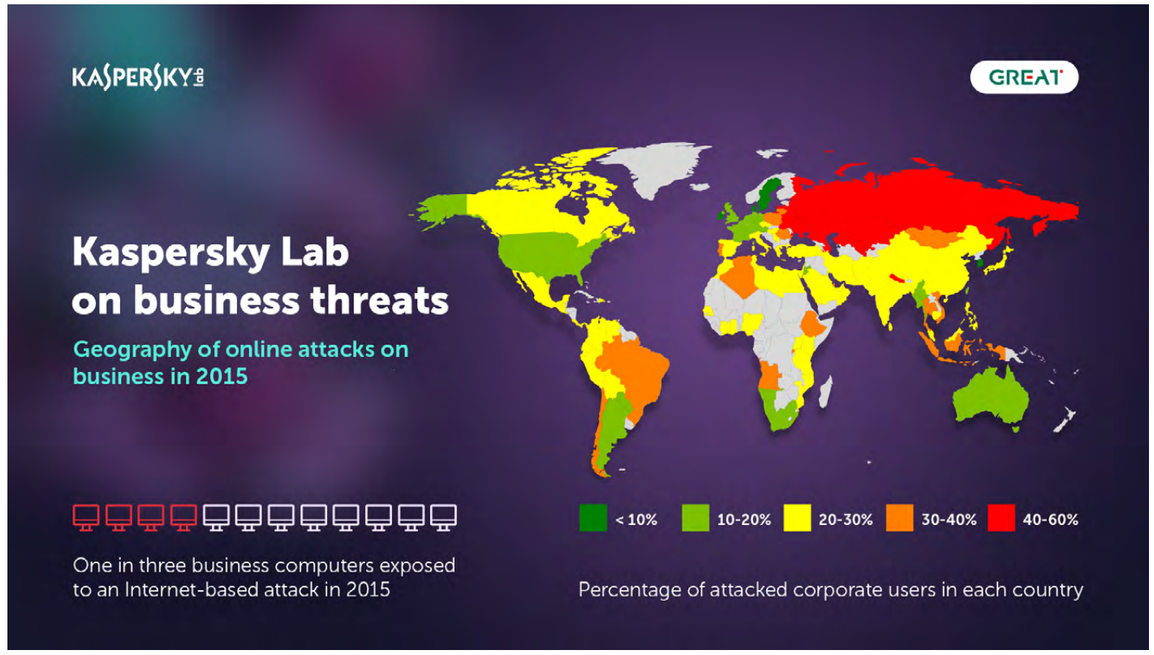
Informationen über zielgerichtete Attacken auf Unternehmen finden Sie in den folgenden Berichten von Kaspersky Lab: **Carbanak**, **Wild Neutron**, **Winnti**, **DarkHotel 2015**, **Desert Falcons**, **Blue Termite** und **Grabit**. Abonnenten des **Kaspersky Intelligence Service** stehen alle Untersuchungsergebnisse im Detail zur Verfügung (intelreports@kaspersky.com).

Die Analyse der aufgeführten Attacken erlaubt es uns, gewisse Rückschlüsse auf die Entwicklungstendenzen zielgerichteter Attacken auf Unternehmen zu ziehen:

- Im Visier der Cybergangster stehen Organisationen, die Geld verwahren und verwalten: Banken, Fonds und Unternehmen, die in unterschiedlichen Formen mit der Börse in Verbindung stehen, unter anderem mit Börsen, an denen Kryptowährungen gehandelt werden.
- Die Angriffe werden sorgfältig geplant und vorbereitet. Die Cyberkriminellen studieren die Interessen ihrer potenziellen Opfer (das heißt der Mitarbeiter der angegriffenen Unternehmen) und finden heraus, welche Webseiten sie aller Wahrscheinlichkeit nach regelmäßig besuchen. Sie ermitteln die Kontakte der Opfer und sie finden heraus, mit welchen Lieferanten und Dienstleistern das Unternehmen zusammenarbeitet.

- Die in der Vorbereitungsphase zusammengetragenen Daten werden aktiv eingesetzt. Die Angreifer hacken die vorher ausgespähten legitimen Webseiten und die Accounts der Anwender, die sie aus den Geschäftskontakten der Mitarbeiter des angegriffenen Unternehmens beziehen. Diese Webseiten/Accounts werden im Laufe weniger Stunden ausgenutzt, denn von dort aus wird der Schadcode verbreitet, woraufhin die Infektion abgeschlossen ist. Solch ein Schema gibt Online-Verbrechern die Möglichkeit, eine gehackte Ressource über mehrere Monate wiederholt zu benutzen.
- Die aktive Verwendung signierter Dateien und legaler Software zum Sammeln von Informationen aus dem angegriffenen Netz.
- Streuung der Attacken, Angriffe auf kleine und mittelständische Unternehmen.
- Geografische Ausdehnung der gegen Unternehmen gerichteten Attacken: umfangreicher Angriff in Japan, APT-Gruppen aus der arabischen Welt.

Wenngleich die Zahl der APT-Attacken, hinter denen Cyberkriminelle stecken, verhältnismäßig gering ist, hat die Entwicklungstendenz dieser Bedrohungen zweifellos Einfluss auf die Ansätze und Methoden, die in Angriffen „gewöhnlicher" Cyberkrimineller auf Unternehmen zum Einsatz kommen.



STATISTIK

Unsere allgemeine Statistik zu Unternehmensanwendern (Geografie der Attacken, Rating der detektierten Objekte) stimmt im Prinzip mit der Statistik zu den Heimanwendern überein. Das ist auch nicht überraschend, denn Unternehmensanwender existieren nicht in einer isolierten Umgebung, und ihre Computer werden zu Angriffsobjekten von Cyberkriminellen, die Schadprogramme verbreiten, ohne dass auf bestimmte Charakteristika der Angegriffenen geachtet würde. Solche Attacken/Schädlinge bilden die Mehrheit, und die Daten zu Attacken, die sich gezielt gegen Unternehmensanwender richten, beeinflussen die allgemeine Statistik nur wenig.

Im Jahr 2015 wurde mindestens eine Malware-Attacke auf **58 Prozent** der in einer Unternehmensumgebung genutzten Computer abgewehrt, das sind drei Prozentpunkte mehr als im vergangenen Jahr.

WEB-BEDROHUNGEN (ATTACKEN ÜBER DAS INTERNET)

Im Jahr 2015 waren 29 Prozent aller Computer in einer Geschäftsumgebung mindestens einer Attacke über das Internet ausgesetzt.

TOP 10 DER SCHADPROGRAMME, ANGRIFFE ÜBER DAS INTERNET

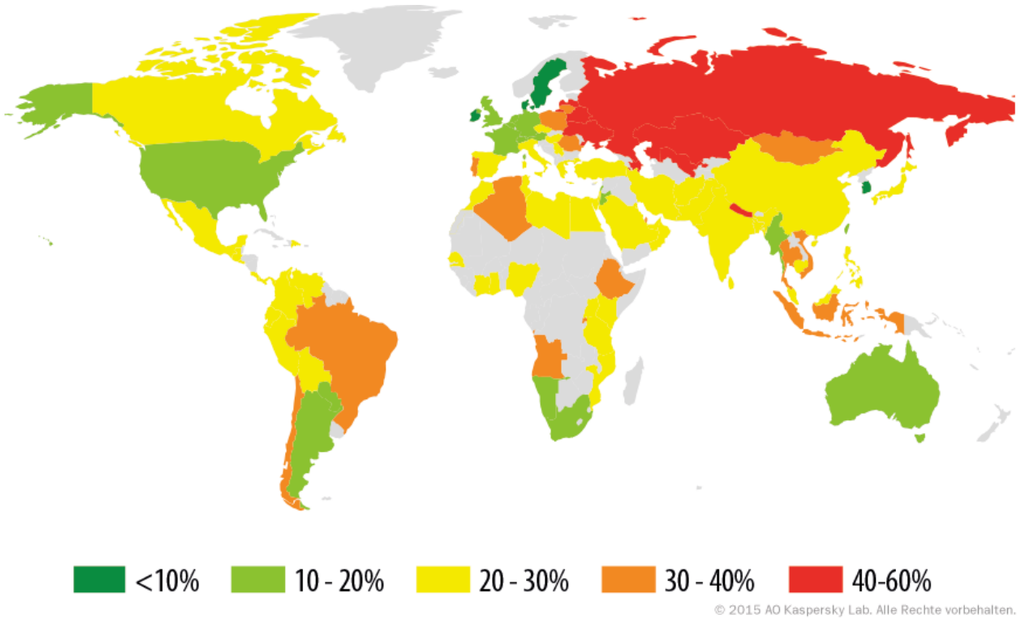
In diesem Rating sind nur Schadprogramme vertreten. Wir haben Werbeprogramme hier ausgeschlossen, die zwar lästig sind und dem Nutzer Unannehmlichkeiten bereiten, dem Computer jedoch keinen Schaden zufügen.

	NAME*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN COMPUTER**
1	Malicious URL	57 %
2	Trojan.Script.Generic	24,7 %
3	Trojan.Script.Iframer	16,0 %
4	Exploit.Script.Blocker	4,1 %
5	Trojan-Downloader.Win32.Generic	2,5 %
6	Trojan.Win32.Generic	2,3 %
7	Trojan-Downloader.JS.Iframe.diq	2,0 %
8	Exploit.Script.Generic	1,2 %
9	Packed.Multi.MultiPacked.gen	1,0 %
10	Trojan-Downloader.Script.Generic	0,9 %

* Von Kaspersky Anti-Virus erkannte Objekte. Die Informationen stammen von KSN-Teilnehmern, die der Übermittlung der Daten zu statistischen Zwecken zugestimmt haben.
** Anteil der Computer, die von dem jeweiligen Schädling angegriffen wurden, an allen angegriffenen Computern.

Praktisch die gesamte Top 10 setzt sich aus Objekten zusammen, die bei Drive-by-Attacken eingesetzt werden, das heißt verschiedene Trojan-Downloader und Exploits.

GEOGRAFIE DER ATTACKEN



Geografie der Attacken über Web-Ressourcen im Jahr 2015 (prozentualer Anteil der angegriffenen Unternehmensanwender im Land)

LOKALE BEDROHUNGEN

Kaspersky Anti-Virus schlug auf **26 Prozent** der Computer von Unternehmensnutzern Alarm (es wurden Objekte auf den Computern oder daran angeschlossenen mobilen Datenträgern entdeckt, etwa auf USB-Sticks, Speicherkarten, Mobiltelefonen, externen Festplatten und Netzwerkfestplatten).

TOP 10 DER SCHADPROGRAMME, LOKALE BEDROHUNGEN

In diesem Rating sind ebenfalls nur Schadprogramme vertreten. Wir haben auch hier Werbeprogramme ausgeschlossen, die zwar lästig sind und dem Nutzer Unannehmlichkeiten bereiten, dem Computer jedoch keinen Schaden zufügen.

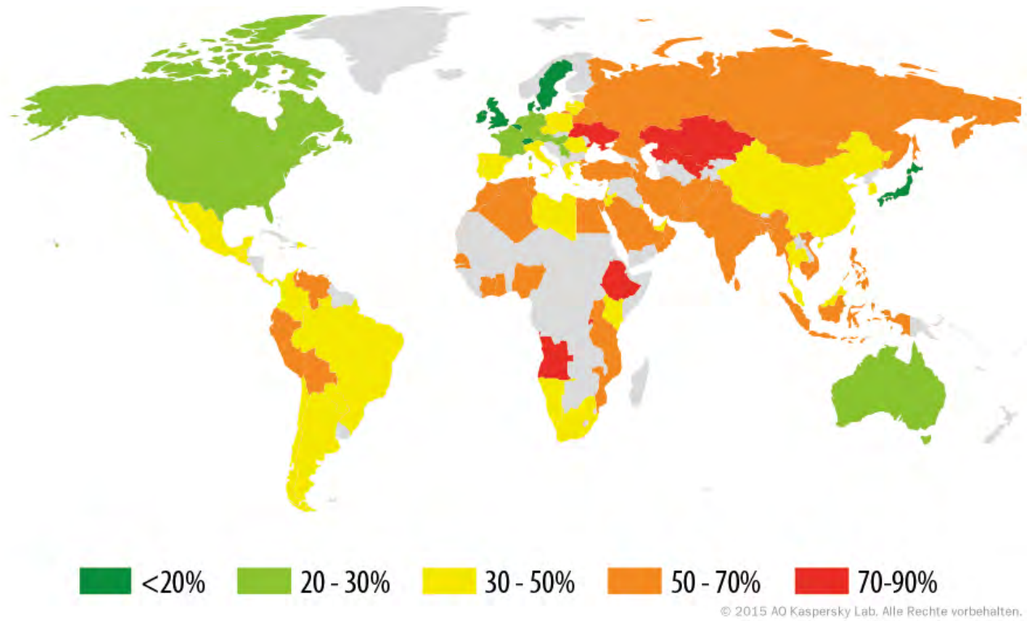
	NAME*	PROZENTUALER ANTEIL DER ANGEGRIFFENEN COMPUTER**
1	DangerousObject.Multi.Generic	23,1 %
2	Trojan.Win32.Generic	18,8 %
3	Trojan.WinLNK.StartPage.gena	7,2 %
4	Trojan.Win32.AutoRun.gen	4,8 %
5	Worm.VBS.Dinihou.r	4,6 %
6	Net-Worm.Win32.Kido.ih	4,0 %
7	Virus.Win32.Sality.gen	4,0 %
8	Trojan.Script.Generic	2,9 %
9	DangerousPattern.Multi.Generic	2,7 %
10	Worm.Win32.Debris.a	2,6 %

* Die Statistik basiert auf Daten der Module OAS und ODS von Kaspersky Anti-Virus, dessen Anwender zugestimmt haben, dass die Software statistische Informationen zu Auswertungszwecken sammelt.
** 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 Alarm geschlagen hat.

Auf Platz eins befinden sich verschiedene Schadprogramme des Typs DangerousObject.Multi.Generic, 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. Bei Unternehmen, die über keinerlei Rechte verfügen, irgendwelche Statistiken in die Cloud zu senden, deaktiviert Kaspersky Lab die Cloud-Technologien nicht, sondern setzt das Kaspersky Private Security Network ein. Auf diese Weise erhalten die Computer im Netz ebenfalls den Schutz aus der Cloud.

Bei den übrigen Vertretern im Rating handelt es sich in erster Linie um sich selbst verbreitende Programme und ihre Komponenten.

GEOGRAFIE DER LOKALEN BEDROHUNGEN



Geografie der entdeckten lokalen Bedrohungen im Jahr 2015 (prozentualer Anteil der angegriffenen Unternehmensanwender im Land)

BESONDERHEITEN BEI ANGRIFFEN AUF UNTERNEHMEN

Die allgemeine Statistik zu Unternehmensanwendern spiegelt nicht die Spezifika von Angriffen auf Unternehmen wider, denn sie wird von mehreren Faktoren beeinflusst, wie zum Beispiel der Infektionswahrscheinlichkeit von Computern in einem bestimmten Land oder der Beliebtheit des einen oder anderen Schädlings unter Cyberkriminellen.

Eine detaillierte Analyse offenbart jedoch die Besonderheiten der Attacken auf Unternehmensanwender:

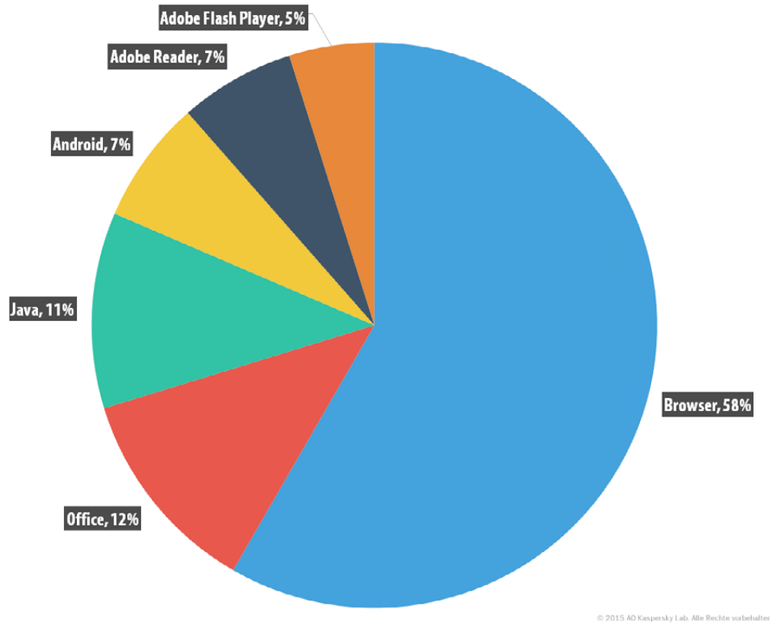
- Exploits zu Office-Anwendungen werden **drei Mal** häufiger als bei Angriffen auf Heimanwender eingesetzt
- Verwendet werden schädliche Dateien, die mit einem gültigen digitalen Zertifikat signiert sind
- Im Laufe der Attacken kommen allgemein verfügbare, legale Programme zum Einsatz, was es den Angreifern ermöglicht, länger unbemerkt zu bleiben

Zudem registrierten wir eine stetige Zunahme der Zahl von Unternehmenscomputern, die von schädlichen Verschlüsselungsprogrammen angegriffen werden.

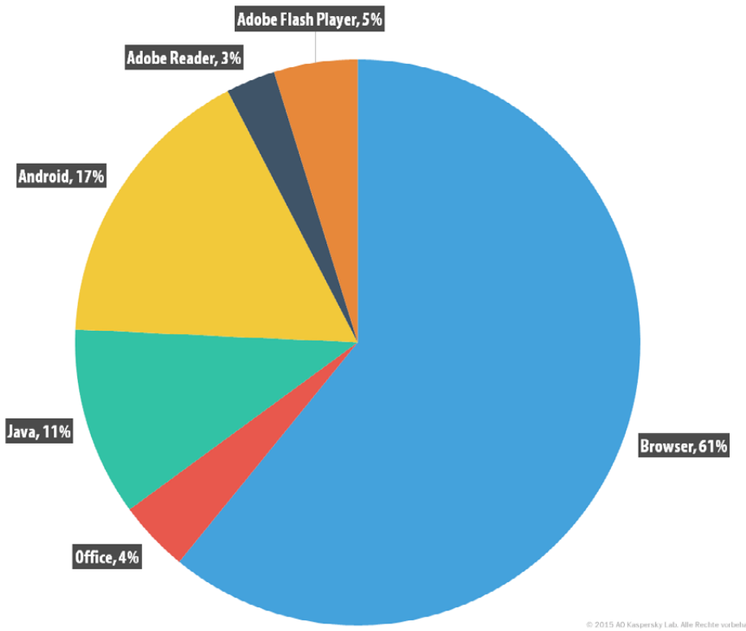
Die Rede ist hier bei weitem nicht immer von Angriffen des Typs APT: „Allerwelts-Cyberkriminelle" konzentrieren sich auf Unternehmensanwender – und manchmal auch auf einzelne Unternehmen.

EXPLOITS IN ATTACKEN AUF UNTERNEHMEN

Das Rating der angreifbaren Anwendungen basiert auf Daten über von unseren Produkten blockierte Exploits, die von Cyberkriminellen bei Attacken über das Internet oder über E-Mail eingesetzt werden, oder auch bei der Kompromittierung lokaler Anwendungen, darunter auch solche auf mobilen Geräten.



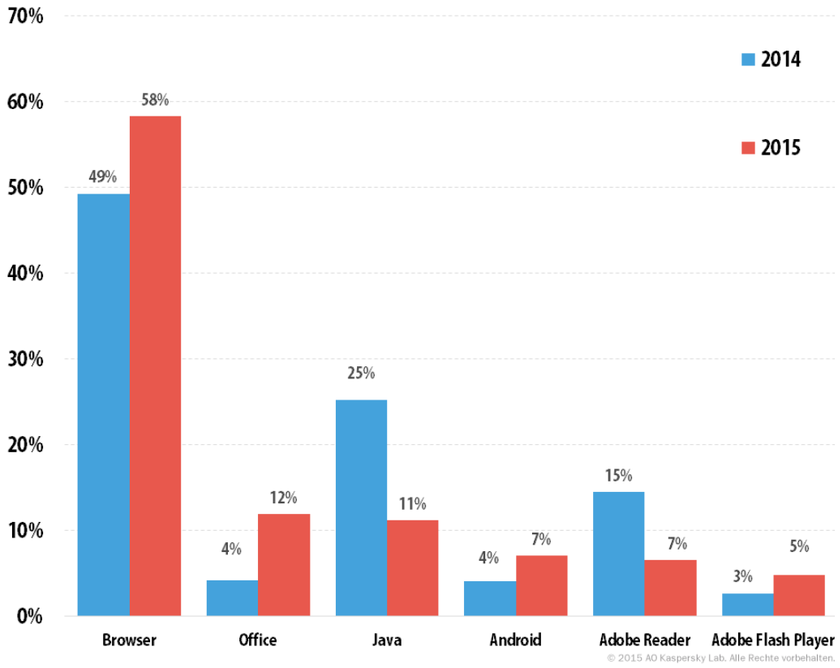
Verteilung der im Jahr 2015 von Cyberkriminellen bei Attacken auf Unternehmensanwendern eingesetzten Exploits nach Typen der angegriffenen Anwendungen



Verteilung der im Jahr 2015 von Cyberkriminellen bei Attacken auf Heimanwender eingesetzten Exploits nach Typen der angegriffenen Anwendungen

Bei der Gegenüberstellung der Exploits, die Online-Verbrecher für Attacken auf Heimanwender einerseits und auf Unternehmensanwender andererseits nutzen, springt vor allem die deutlich intensivere Nutzung von Exploits zu Office-Anwendungen bei Angriffen auf Unternehmen ins Auge. Liegt deren Anteil bei Angriffen auf Heimanwender nur bei vier Prozent, so beträgt der Prozentsatz der Exploits, die Sicherheitslücken in Office-Programmen ausnutzen, bei Angriffen auf Unternehmensnutzer zwölf Prozent aller innerhalb eines Jahres entdeckten Exploits.

Wie bei den Attacken auf Heimanwender steht auch bei den Unternehmensnutzern die Kategorie „Browser" auf Platz eins der Liste der am häufigsten von Exploits angegriffenen Anwendungen. Bei dieser Statistik ist aber unbedingt die Tatsache zu berücksichtigen, dass Kaspersky Lab Exploits auf verschiedenen Stufen detektiert. Zu der Kategorie „Browser" gehören auch Landing-Pages, die die Exploits „ausliefern". Unseren Beobachtungen zufolge sind das in den meisten Fällen Exploits für den Adobe Flash Player.



Verteilung der von Cyberkriminellen bei Attacken eingesetzten Exploits nach Typ der angegriffenen Anwendungen, 2014 und 2015

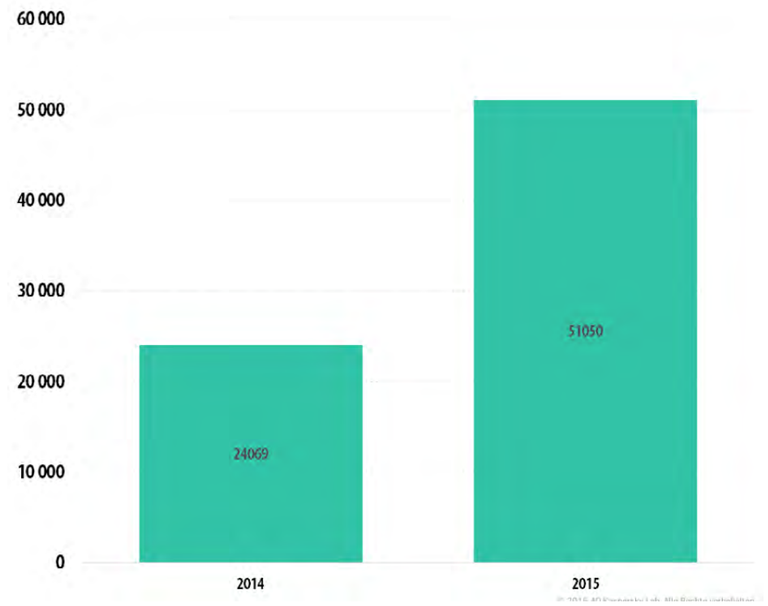
Im Vergleich zum Jahr 2014 ging der Anteil der Java- und PDF-Exploits deutlich zurück, und zwar um 14 respektive acht Prozentpunkte. Java-Exploits erfreuen sich nun geringerer Beliebtheit, obwohl im Laufe des Jahres einige Zero-Day-Sicherheitslücken gefunden wurden. Gleichzeitig gestiegen ist der Anteil der Angriffe unter Ausnutzung von Sicherheitslücken in Office-Anwendungen (plus 8 Prozentpunkte), Browsern (plus 9 Prozentpunkte), im Adobe Flash Player (plus 9 Prozentpunkte) und auch in Android (plus 3 Prozentpunkte).

Wie Analysen von Sicherheitsvorfällen zeigen, verwenden Cyberkriminelle sogar in zielgerichteten Attacken auf Unternehmen häufiger Exploits zu bereits bekannten Sicherheitslücken, was damit zusammenhängt, dass Patches in Unternehmensumgebungen meist nur mit großen Verzögerungen installiert werden. Die Zunahme des Anteils von Exploits, die sich gegen verwundbare Android-Apps richten, auf sieben Prozent zeugt von einem gesteigerten Interesse Cyberkrimineller an Unternehmensdaten auf den mobilen Geräten der Mitarbeiter.

VERSCHLÜSSELUNGSPROGRAMME

Verschlüsselungstrojaner wurden lange Zeit für eine Bedrohung gehalten, die nur Heimanwender betrifft. Jetzt aber richten Cyberkriminelle, die mit Daten verschlüsselnden Schädlingen ihr Geld verdienen, unseren Informationen zufolge ihre Aufmerksamkeit immer häufiger auf Unternehmen.

Im Jahr 2015 entdeckten die Lösungen von Kaspersky Lab Verschlüsselungsschädlinge auf mehr als **50.000 Rechnern** in Unternehmensnetzwerken, das sind **doppelt so viele wie im vorangegangenen Jahr**. Dabei ist unbedingt zu berücksichtigen, dass die reale Zahl von Vorfällen um ein Vielfaches höher ist: Diese Statistik bezieht nur die Resultate der Signatur-basierten und der heuristischen Erkennung mit ein, doch die Produkte von Kaspersky Lab erkennen Verschlüsselungstrojaner in den meisten Fällen mit Hilfe von verhaltensbasierten Methoden.



Anzahl der individuellen Unternehmensanwender, deren Rechner in den Jahren 2014 und 2015 von Verschlüsselungstrojanern attackiert wurden

Dass Cyberkriminelle, die mit Verschlüsselungsprogrammen operieren, nun ein spürbar gesteigertes Interesse an Attacken auf Unternehmen haben, hat vor allem zwei Gründe. Erstens ist das Lösegeld, das ein Unternehmen zu zahlen bereit ist, sicherlich deutlich höher als das, was ein Heimanwender zahlen kann. Und zweitens ist die Chance, dass das geforderte Lösegeld überhaupt gezahlt wird, im Falle einer angegriffenen Organisation sicherlich bedeutend höher, denn Unternehmen sind mitunter schlichtweg handlungsunfähig, wenn die Informationen auf einigen kritisch wichtigen Computern oder Servern verschlüsselt und nicht verfügbar sind.

Eines der interessantesten Ereignisse des Jahres 2015 war in diesem Kontext sicherlich das Erscheinen des ersten Verschlüsslungsprogramms für Linux (die Produkte von Kaspersky Lab detektieren es als Trojan-Ransom.Linux.Cryptor), das auf Webseiten spezialisiert ist, in erster Linie Webseiten von Online-Shops. Unter Ausnutzung einer Sicherheitslücke in den Web-Anwendungen verschafften sich Cyberkriminelle Zugriff auf die Webseiten und luden dort ein Schadprogramm hinauf, das die Daten auf dem Server verschlüsselte.

In den meisten Fällen führte das zum Zusammenbruch der Seite. Für die Dechiffrierung forderten die Online-Gangster ein Lösegeld in Höhe von einem Bitcoin. Die Menge der infizierten Webseiten wird auf 2.000 geschätzt. Bedenkt man die Häufigkeit von *nix-Servern in Business-Umgebungen, so ist die Vermutung nur naheliegend, dass sich die Angriffe von Verschlüsselungsschädlingen, die sich gegen Nicht-Windows-Plattformen richten, im nächsten Jahr fortsetzen werden.

TOP 10 DER FAMILIEN VON VERSCHLÜSSELUNGSTROJANERN

	FAMILIE	PROZENTUALER ANTEIL DER ANGEGRIFFENEN COMPUTER*
1	Scatter	21
2	Onion	16
3	Cryakl	15
4	Snocry	11
5	Cryptodef	8
6	Rakhni	7
7	Crypmod	6
8	Shade	5
9	Mor	3
10	Crypren	2

* Prozentualer Anteil der Computer, die von Schädlingen der entsprechenden Familie angegriffen wurden, an allen angegriffenen Computern.

Auf dem ersten Platz positionierten sich die Trojaner der Familie Scatter, die Dateien auf der Festplatte verschlüsseln und die chiffrierten Dateien mit der Erweiterung „.vault" zurücklassen. Bei den Programmen der Familie Scatter handelt es sich um modulare Schädlinge. Innerhalb kurzer Zeit hat sich diese Familie enorm weiterentwickelt Sie bekam neben der Möglichkeit, Dateien zu verschlüsseln, auch die Funktionalität eines E-Mail-Wurms und Trojan-PSW. Auf dem zweiten Platz im Rating der am weitesten verbreiteten Verschlüsselungsschädlinge befinden sich Programme der Familie **Onion**, die dafür bekannt sind, dass sich ihre Steuerungsserver im Netzwerk Tor befinden. Platz drei belegen die in Delphi geschriebenen verschlüsselnden Schadprogramme der Familie Cryakl, die erstmals bereits im April 2014 in Erscheinung traten.

In einigen Fällen besteht die Möglichkeit, die Daten wieder zu entschlüsseln, die mit diesen Schädlingen chiffriert wurden, insbesondere dann, wenn der Algorithmus irgendwelche Fehler enthält. Doch Daten zu entschlüsseln, die mit den neusten Versionen der in den Top 10 vertretenen Schadprogramme chiffriert wurden, ist zum gegenwärtigen Zeitpunkt nicht möglich.

Für ein Unternehmen kann die Infektion mit einem derartigen Programm den Stillstand der Geschäftstätigkeit bedeuten, wenn kritisch wichtige Daten verschlüsselt wurden oder infolge der Verschlüsselung die Funktion eines kritisch wichtigen Servers blockiert wurde. Die Folge einer solchen Attacke können erhebliche Verluste sein, vergleichbar mit den Schäden infolge der Attacken des Schadprogramms Wiper, das auf die Zerstörung von Daten in Unternehmensnetzwerken spezialisiert war.

Zur Bekämpfung derartiger Bedrohungen sollten unbedingt die folgenden Maßnahmen ergriffen werden:

- Einsatz einer Lösung zum Schutz vor Exploits
- Aktivieren der verhaltensbasierten Detektionsmethoden im Schutzprodukt (in den Produkten von Kaspersky Lab ist die Komponente „System Watcher" dafür verantwortlich)
- Einrichtung eines automatischen Backup-Prozesses

ANGRIFFE AUF POS-TERMINALS

Ein besonderes Thema für Unternehmen, insbesondere für Handel treibende, war im Jahr 2015 die Sicherheit von PoS-Terminals (Point Of Sale). Im Grunde genommen kann heute jeder beliebige Computer als PoS-Terminal verwendet werden, wenn ein spezielles Kartenlesegerät daran angeschlossen und eine spezielle Software installiert ist. Cyberkriminelle suchen gezielt nach solchen Computern und infizieren sie mit Schadprogrammen, die in der Lage sind, die über das Bezahlterminal eingegebenen Daten abzugreifen.

Weltweit wehrten die Produkte von Kaspersky Lab mehr als 11.500 Versuche ab, derartige Angriffe durchzuführen. Derzeit befinden sich in unserer Kollektion zehn Programm-Familien, die auf den Datendiebstahl von PoS-Terminals spezialisiert sind. Sieben davon sind in diesem Jahr aufgetaucht. Trotz der recht geringen Zahl der Angriffsversuche darf man die Gefahr nicht unterschätzen, die davon ausgeht, da schon durch eine einzige erfolgreiche Attacke zehntausende Kreditkartendaten gestohlen werden können. Es könnte deshalb so viele Opfer bei nur einem Angriff geben, da die Besitzer und Administratoren PoS-Terminals nicht als Objekte ansehen, die eines Schutzes bedürfen. Daher kann ein Terminal eine sehr lange Zeit infiziert bleiben, wobei das Schadprogramm ununterbrochen die am Terminal ausgelesenen Kreditkartendaten an die Angreifer sendet.

Dieses Problem ist insbesondere in solchen Ländern akut, in denen Karten mit EMV-Chip benutzt werden. Der Übergang zu Karten mit neuen Chip-Generationen soll es erheblich erschweren, an die Kreditkartendaten zu gelangen und die Karten zu fälschen, doch das kann noch sehr lange dauern. Daher sollten zumindest minimale Maßnahmen zum Schutz von POS-Geräten ergriffen werden, mittels derer sich die Sicherheits-Regel „standardmäßiges Ausführungsverbot für unbekannte Programme" umsetzen lässt.

Wir erwarten, dass Cyberkriminelle bald beginnen werden, mobile PoS-Geräte unter Android anzugreifen.

FAZIT

Unsere Daten zeigen, dass Cyberkriminelle bei Angriffen auf Unternehmen ganz anders vorgehen als bei Attacken auf Heimanwender. Bei Attacken auf Unternehmensanwender verwenden sie wesentlich häufiger Exploits zu Office-Anwendungen. Die angreifenden Schadprogramme sind häufig mit einem gültigen Zertifikat signiert und die Cyberkriminellen versuchen, sich verfügbare legale Programme zunutze zu machen, um über einen längeren Zeitraum unentdeckt zu bleiben. Außerdem stellten die Experten von Kaspersky Lab fest, dass die Zahl der Unternehmenscomputer, die von Verschlüsselungsschädlingen angegriffen werden, stetig zunimmt. Das betrifft nicht nur APT-Attacken: Ganz „gewöhnliche" Cyberkriminelle greifen zielgerichtet Unternehmensanwender an und manchmal auch die Computer in ganz bestimmten Firmen.

Die Anwendung von Methoden und Programmen aus der Welt der Advanced Persistent Threats (APT) durch cyberkriminelle Gruppierungen hebt ihre Attacken auf ein anderes Niveau und macht sie wesentlich gefährlicher. In erster Linie wenden Cyberkriminelle diese Methoden bei virtuellen Banküberfällen an, mit dem Ziel, riesige Summen zu stehlen. Mit Hilfe dieser Methoden können sie auch das Geld von Unternehmens-Bankkonten stehlen, nachdem sie sich Zugriff auf das Netzwerk der jeweiligen Organisation verschafft haben.

Bei ihren Attacken vertrauen die Verbrecher auf die Ausnutzung bereits bekannter Sicherheitslücken, was mit der verzögerten Installation von Software-Updates in Unternehmen zu erklären ist. Außerdem setzen Online-Kriminelle verstärkt signierte schädliche Dateien und legale Tools zur Schaffung eines Kanals zum Abgreifen von Informationen ein: Gebräuchlich sind zum Beispiel bekannte Fernwartungsprogramme, SSH-Clients und Software zur Passwort-Wiederherstellung.

Immer häufiger werden Unternehmensserver zum Angriffsziel Cyberkrimineller. Es werden nicht immer nur Daten von den Servern gestohlen, sondern es ist auch ein Fall bekannt, in dem die angegriffenen Server bei DDoS-Attacken eingesetzt wurden. Oder die Daten auf dem Server wurden einfach verschlüsselt und die Erpresser forderten ein Lösegeld für die Wiederherstellung. **Die jüngsten Ereignisse** haben gezeigt, dass das sowohl für Windows- als auch für Linux-Server gilt.

Viele Organisationen, die Attacken zum Opfer fielen, wurden mit der Forderung Cyberkrimineller konfrontiert, Lösegeld zu zahlen, damit diese eine DDoS-Attacke einstellen, verschlüsselte Daten wieder dechiffrieren oder gestohlene Informationen nicht veröffentlichen. Gerät ein Unternehmen in diese Situation, so muss es sich unbedingt an die Strafverfolgungsbehörden und an IT-Sicherheitsexperten wenden. Denn auch wenn sie das geforderte Lösegeld erhalten haben, bedeutet es nicht zwangsläufig, dass die Verbrecher ihr Wort halten, so wie im Fall einer **DDoS-Attacke auf ProtonMail**, die nach Zahlung des geforderten Lösegelds nicht eingestellt wurde.

PROGNOSEN

ZUNAHME VON ANGRIFFEN AUF FINANZORGANISATIONEN, FINANZIELLE MACHENSCHAFTEN AN VERSCHIEDENEN BÖRSEN

Im kommenden Jahr erwarten wir sowohl eine Zunahme der Attacken auf Finanzorganisationen als auch eine veränderte Qualität dieser Attacken. Cyberkriminelle könnten neben der Überweisung gestohlenen Geldes auf ihre Konten mit darauffolgender Monetarisierung auch neue Techniken anwenden, wie zum Beispiel Datenmanipulation auf Handelsplattformen, auf denen sowohl mit traditionellen als auch mit neuen Finanz-Werkzeugen gearbeitet wird, wie etwa Kryptowährungen.

ATTACKEN AUF DIE INFRASTRUKTUR

In eine Organisation einzudringen, ist nicht unbedingt einfach, allerdings befinden sich die wertvollen Daten mitunter gar nicht in der Organisation selbst, sondern auf Servern in Rechenzentren. Sich auf diese Elemente der Infrastruktur Zugriff zu verschaffen, wird im Jahr 2016 zu einer wichtigen Technik bei Attacken auf Unternehmen werden.

AUSNUTZUNG VON SICHERHEITSLÜCKEN IM INTERNET DER DINGE (IOT), MIT DEM ZIEL, INS UNTERNEHMENSNETZWERK EINZUDRINGEN

In praktisch allen modernen Unternehmensnetzwerken gibt es heute IoT-Geräte. Im Jahr 2015 durchgeführte Untersuchungen zeigen, dass es eine Reihe von Problemen mit der Sicherheit dieser Geräte gibt, die Cyberkriminelle offensichtlich auszunutzen versuchen, um so einen Fuß in die Tür von Unternehmensnetzwerken zu bekommen.

STRENGERE SICHERHEITSSTANDARDS, ZUSAMMENARBEIT MIT STRAFVERFOLGUNGSORGANEN

Die Antwort auf die zunehmende Zahl von Computervorfällen im Unternehmensbereich und die allgemeinen Veränderungen in der Landschaft der Cyberbedrohungen wird die Entwicklung neuer sowie die Aktualisierung bereits bestehender Sicherheitsstandards sein. Organisationen, die an der Unversehrtheit ihrer digitalen Werte interessiert sind, werden enger mit Strafverfolgungsbehörden zusammenarbeiten beziehungsweise von den oben erwähnten neuen Standards dazu verpflichtet werden. Dadurch könnte die Verfolgung von Cyberverbrechern effizienter werden und es könnte dazu führen, dass wir im Jahr 2016 von neuen Verhaftungen hören werden.

WAS TUN?

Das Jahr 2015 hat gezeigt, dass Cyberkriminelle APT-Methoden aktiv dazu verwenden, um in Unternehmensnetzwerke einzudringen. Wir sprechen hier auch über das Auskundschaften im Vorfeld, um die schwachen Glieder in der Infrastruktur auszumachen und Informationen über Mitarbeiter zu erhalten. Dabei geht es um den Einsatz von Spearphishing und Wasserloch-Attacken, um die aktive Nutzung von Exploits zur Ausführung von Code und zum Erhalt von Administratorenrechten sowie um die Verwendung nicht nur von trojanischen Programmen, sondern auch von legaler Software zur Verwaltung aus der Ferne, um das Studium des Netzes

und die „Wiederherstellung" von Passwörtern. All das macht die Entwicklung von Methoden und Techniken zum Schutz von Unternehmensnetzwerken erforderlich.

Um nun zu konkreten Empfehlungen überzugehen, möchten wir an allererster Stelle auf die **Top 35 der Mitigationsstrategien** verweisen, die vom Australian Signals Directorate (ASD) zusammengestellt wurde. Aufgrund einer umfassenden, detaillierten Analyse lokaler Attacken und Bedrohungen kam das ASD zu dem Schluss, dass nicht weniger als 85 Prozent aller Fälle von Eindringen in Computersysteme durch die Anwendung von vier Grundstrategien nahezu neutralisiert werden können. Drei dieser Strategien stehen in Zusammenhang mit dem Einsatz spezialisierter Schutzlösungen (die Produkte von Kaspersky Lab enthalten technische Lösungen, die die drei wichtigsten Strategien abdecken).

Die vier Grundstrategien, die die Wahrscheinlichkeit einer erfolgreichen zielgerichteten Attacke verringern:

- Einsatz von Weißen Listen für Anwendungen, um Schadsoftware und nicht genehmigte Programme an der Ausführung zu hindern
- Patchen von Anwendungen wie Java, PDF-Viewer, Flash, Webbrowser und Microsoft Office
- Patchen von Schwachstellen in Betriebssystemen
- Einschränken von administrativen Rechten bei Betriebssystemen und Anwendungen, basierend auf den Nutzeraufgaben

Detaillierte Informationen über die Strategien des ASD finden Sie in dem Dokument **über Mitigationsstrategien zur Abschwächung von Bedrohungen** in der Enzyklopädie der Securelist.

Ein zweiter wichtiger Faktor ist die Verwendung von Daten über aktuelle Bedrohungen, das heißt von so genannten Threat Intelligence Services (Kaspersky Lab stellt beispielsweise **Kaspersky Intelligence Services** bereit). Die rechtzeitige Konfiguration und Überprüfung des Netzes auf der Grundlage dieser Daten macht es möglich, sich vor einer Attacke zu schützen oder eine Attacke im Frühstadium zu erkennen.

Die grundlegenden Prinzipien zur Gewährleistung der Sicherheit in Unternehmensnetzwerken bleiben unverändert:

- Schulung des Personals. Nicht nur der Sicherheitsbeauftragte hat sich um die IT-Sicherheit zu kümmern, sondern auch jeder einzelne Mitarbeiter ist dazu verpflichtet
- Justieren der Sicherheitsprozesse: Das Sicherheitssystem muss auf sich entwickelnde Bedrohungen adäquat reagieren
- Einsatz neuer Technologien und Methoden: Mit jeder zusätzlichen Schutzschicht kann das Risiko des Eindringens ins Netzwerk verringert werden

DIE TOP SECURITY STORIES

Autoren: David Emm, Andrey Nikishin und Alexander Gostev

QUICK INFO

- ZIELGERICHTETE ATTACKEN UND MALWARE-KAMPAGNEN
- DATENLECKS
- SMARTE (ABER NICHT UNBEDINGT SICHERE) GERÄTE
- INTERNATIONALE ZUSAMMENARBEIT GEGEN CYBERKRIMINALITÄT
- ANGRIFFE AUF INDUSTRIEOBJEKTE
- FAZIT

Das Jahresende ist traditionell eine Zeit der Reflektion – wir ziehen Bilanz, bevor wir uns dem zuwenden, was vor uns liegt. Auch Kaspersky Lab präsentiert wie gewohnt einen Rückblick auf die Ereignisse, die die Bedrohungslandschaft im Jahr 2015 geprägt haben.

ZIELGERICHTETE ATTACKEN UND MALWARE-KAMPAGNEN

Zielgerichtete Attacken sind mittlerweile ein fester Bestandteil der Bedrohungslandschaft. Daher ist es keine Überraschung, dass sie auch in unserem Jahresrückblick eine wichtige Rolle spielen. Letztes Jahr haben wir in unserer **APT-Prognose** die unserer Meinung nach kommenden APT-Entwicklungstrends umrissen:

- Fusion von Cyberkriminalität und APT
- Aufspaltung größerer APT-Gruppen
- Sich entwickelnde Malware-Techniken
- Neue Methoden des Datendiebstahls
- Cyber-Wettrüsten

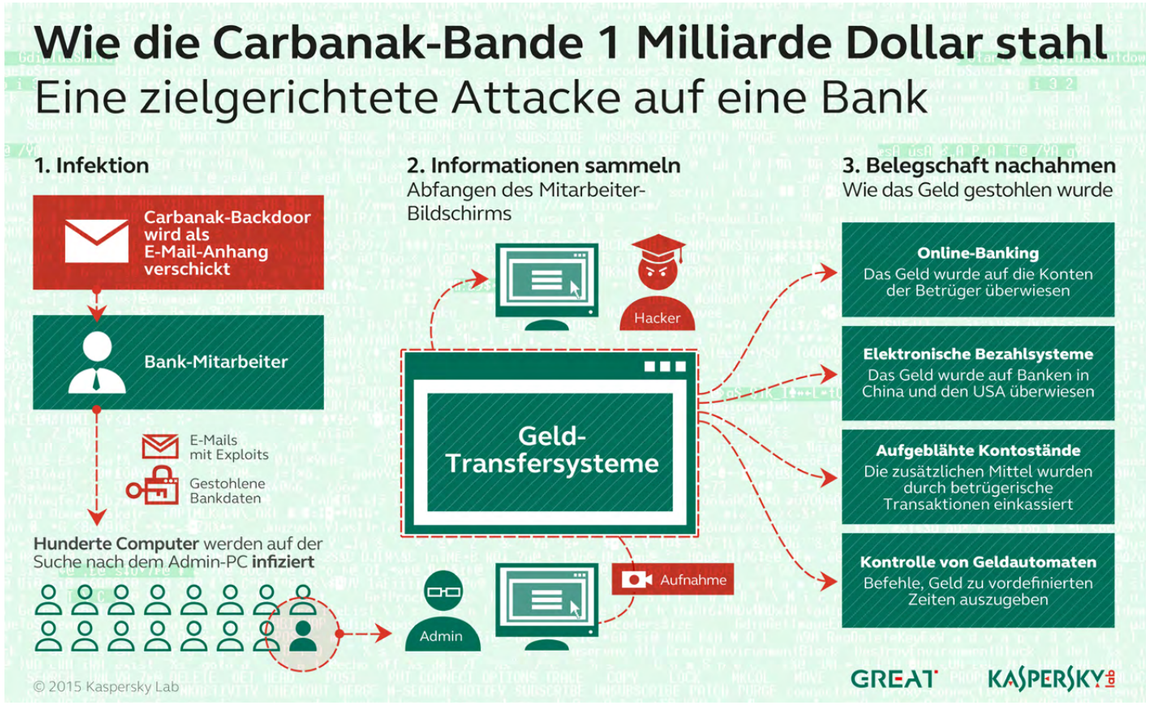
Hier die wichtigsten APT-Kampagnen, über die wir im Jahr 2015 berichtet haben.

Carbanak kombinierte Cyberkriminalität – in diesem Fall war es der Gelddiebstahl von Finanzinstituten – mit Techniken, die typisch sind für zielgerichtete Attacken. Die Kampagne wurde im Frühjahr 2015 aufgedeckt: Kaspersky Lab wurde gebeten, eine forensische Untersuchung eines Banksystems durchzuführen, nachdem einige Geldautomaten plötzlich „willkürlich" Geld ausgaben. Es stellte sich heraus, dass Computer in der Bank infiziert waren. Carbanak ist eine Backdoor, die auf Spionage, Datendiebstahl und die entfernte Kontrolle von infizierten Computern spezialisiert ist. Die Angreifer nutzten APT-typische Methoden, um die angegriffenen Rechner zu infizieren. So schickten sie beispielsweise Spear-Phishing-Mails an die Bankmitarbeiter. Sobald es den Angreifern gelungen war, sich erfolgreich im Netzwerk einzunisten, begannen sie es auszuspionieren. So konnten sie die Systeme identifizieren, die mit der Sachbearbeitung, der Buchhaltung und mit Geldautomaten zu tun haben und imitierten dann einfach die Aktivitäten der echten Mitarbeiter.

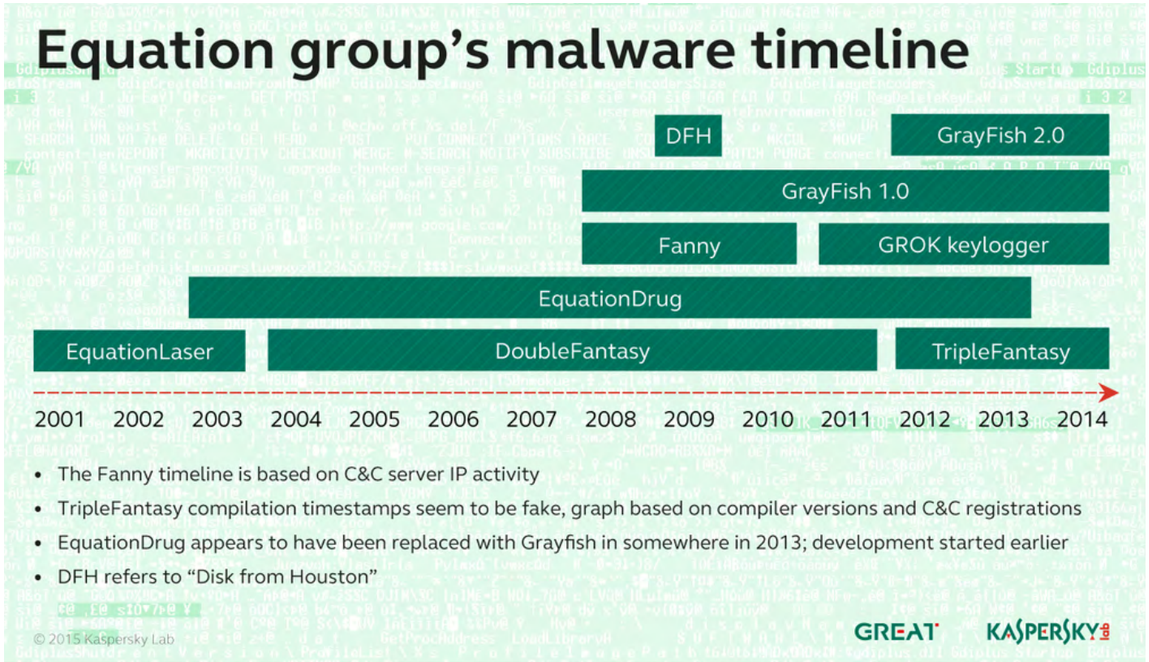
Carbanak hatte drei Methoden, Geld zu stehlen:

1. Abheben von Bargeld von einem Automaten
2. Überweisungen an die Cyberkriminellen über das SWIFT-Netzwerk
3. Eröffnung von gefälschten Konten und Nutzung von Kurierdiensten, um das Geld einzusammeln

Die Angreifer attackierten rund 100 Finanzinstitute und waren für Verluste von fast einer Milliarde US-Dollar verantwortlich.



Eine der am ausführlichsten diskutierten Nachrichten des ersten Quartals 2015 drehte sich um die **Cyberspionage-Gruppe Equation**. Die Angreifer hinter **Equation** infizierten erfolgreich tausende von Computern im Iran, in Russland, Syrien, Afghanistan, den USA und in anderen Ländern. Unter den Opfern waren Regierungsorganisationen und diplomatische Einrichtungen sowie Unternehmen aus den Bereichen Telekommunikation und Energiewirtschaft. Es handelt sich um eine der raffiniertesten APT-Kampagnen, die uns je untergekommen ist: Eines der vielen von der Gruppe entwickelten Module modifiziert die Firmware von Festplatten. Dadurch erzielten die Angreifer ein bisher noch nicht dagewesenes Niveau an Heimlichkeit und Nachhaltigkeit, das jede andere zielgerichtete Attacke in den Schatten stellt. Sicher ist, dass die Entwicklung des Codes in das Jahr 2001 oder früher zurückreicht. Es gibt auch Verbindungen zu den berüchtigten Attacken Stuxnet und Flame – beispielsweise befinden sich im Equation-Arsenal zwei Zero-Day-Schwachstellen, die später in Stuxnet verwendet wurden.



Im Laufe ihrer Ermittlungen zu einem Vorfall im Nahen Osten stießen die Experten von Kaspersky Lab auf die Aktivität einer bis dahin unbekannten Gruppe, die zielgerichtete Attacken durchführt. Die Gruppe erhielt den Namen Wüstenfalke, **Desert Falcon**. Sie ist die erste arabische Gruppierung, die vollwertige Cyberspionage-Operationen durchführt, die allem Anschein nach von der politischen Situation in der Region diktiert werden. Die ersten Anzeichen einer Aktivität von Desert Falcon lassen sich in das Jahr 2011 zurückverfolgen. Die ersten bekannten Infektionen datieren auf das Jahr 2013 und der Höhepunkt der Aktivität dieser Gruppe fällt auf den Zeitraum zwischen Ende 2014 und Anfang 2015. Die Gruppe hat über eine Million Dateien von mehr als 3.000 Opfern gestohlen. Darunter sind politische Aktivisten und politische Führer, Regierungen und Militärorganisationen, Massenmedien

ZURÜCK ZUM INHALT

und Finanzinstitute, die hauptsächlich in Palästina, Ägypten, Israel und Jordanien ansässig sind. Die Mitglieder der Gruppe Desert Falcon sind definitiv keine Anfänger, da sie die Schadprogramme für Windows und Android von Grund auf selbst entwickelten. Zudem waren die Attacken sehr kunstvoll organisiert und arrangiert, wobei Phishing-Mails, gefälschte Webseiten und gefälschte Accounts in Sozialen Netzwerken zum Einsatz kamen.

Im März 2015 veröffentlichten wir unseren Bericht über die APT **Animal Farm,** wenngleich schon im vergangenen Jahr entsprechende Tools auf der Bildfläche erschienen waren. Im März 2014 veröffentlichte die französische Zeitung **Le Monde** einen Artikel über ein Cyberspionage-Toolset, das vom Communications Security Establishment Canada (CSEC) entdeckt wurde: Dieses Toolset wurde in der Operation „Snowglobe" verwendet, die französischsprachige Medien in Kanada zum Ziel hatte, sowie in Griechenland, Frankreich, Norwegen und in einigen afrikanischen Ländern aktiv war. Das CSEC war der Meinung, die Operation sei möglicherweise von französischen Geheimdiensten initiiert worden.

Ein Jahr später veröffentlichten Sicherheitsforscher Analysen (**hier**, **hier** und **hier**) von Schadprogrammen, die viel mit „Snowglobe" gemein hatten: Insbesondere wurden auch einige Samples mit dem internen Namen „Babar" untersucht – ein Programmname, der auch vom CSEC erwähnt wurde. Aufgrund der Analysen und der Verbindungen zwischen ihnen taufte Kaspersky Lab die Gruppe hinter diesen Attacken auf den Namen Animal Farm.

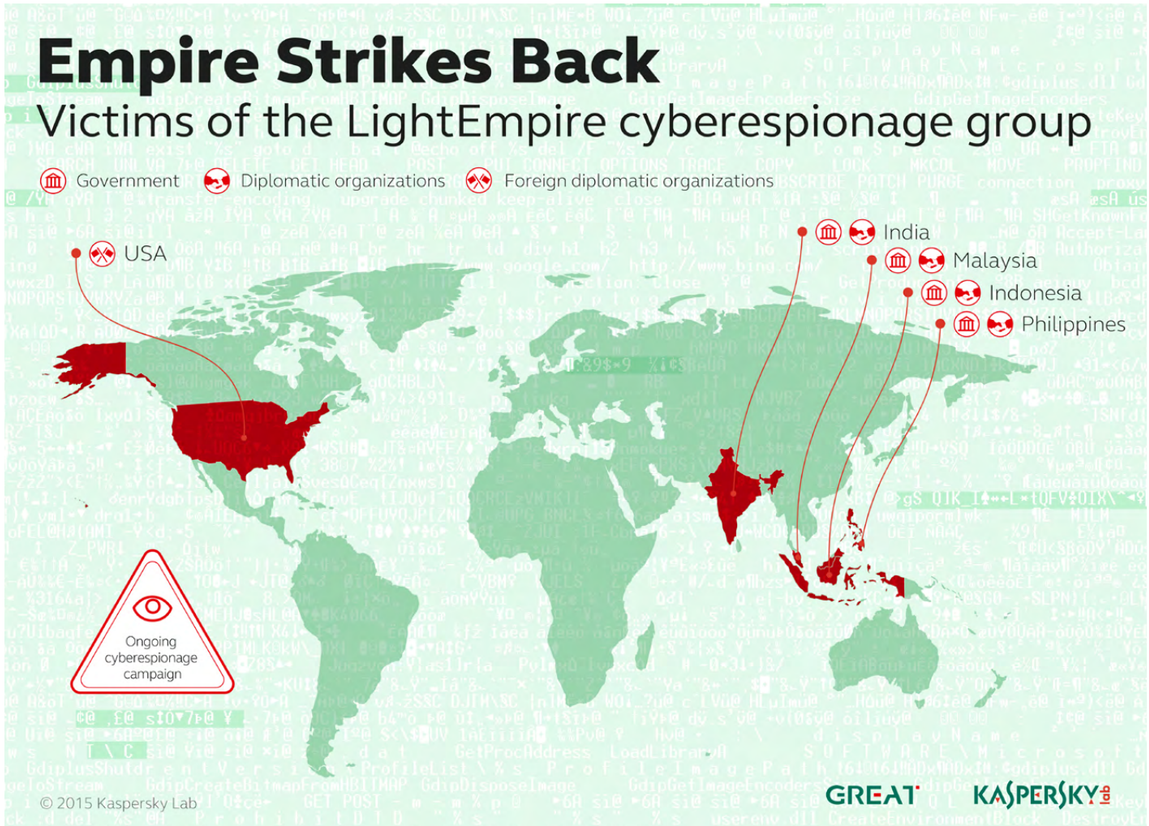
Im Arsenal der Gruppe befanden sich auch zwei der drei Zero-Day-Sicherheitslücken, die wir im Jahr 2014 gefunden hatten und die von Cyberkriminellen benutzt wurden: Eine Attacke beispielsweise, die die Webseite des syrischen Justizministeriums unter Verwendung von Exploits zu **CVE-2014-0515** kompromittierte, führte zum Download eines Tools von Animal Farm mit dem Namen „Casper". Ein interessantes Merkmal dieser Kampagne ist, dass mit „NBOT" eines seiner Programme darauf ausgerichtet ist, DDoS-Attacken (Distributed Denial of Service) durchzuführen. Das ist eher ungewöhnlich für APT-Gruppen. Eines der böswilligen „Tiere" auf dieser Farm hat den seltsamen Namen „Tafacalou" – möglicherweise ein Wort aus der okzitanischen Sprache, die unter anderem in Frankreich gesprochen wird.

Im April 2015 berichteten wir über das Erscheinen eines neuen Mitglieds der wachsenden „Duke"-Familie, zu der mittlerweile schon MiniDuke, CosmicDuke und OnionDuke gehören. Die **CozyDuke APT**, auch bekannt als „CozyBear", „CozyCat" und „Office Monkeys", greift Regierungsorganisationen und Unternehmen in den USA, Deutschland, Südkorea und Usbekistan an. Bei den Attacken kommen einige raffinierte Techniken zum Einsatz, unter anderem Verschlüsselung, Anti-Erkennungsmaßnahmen und eine gut designte Auswahl von Komponenten, die strukturell früheren Bedrohungen innerhalb der „Duke"-Familie ähneln. Doch eines der bemerkenswertesten Merkmale ist der Einsatz von Social Engineering. Einige der Spear-Phishing-Mails der Angreifer enthalten einen Link auf gehackte Webseiten, darunter höchst prominente legitime Webseiten, die ein ZIP-Archiv hosten. Dieses Archiv enthält wiederum eine RAR-SFX-Datei, die die Malware installiert, während ein leeres PDF-Dokument als Tarnung angezeigt wird. Bei einem anderen Ansatz wird ein präpariertes Flash-Video als E-Mail-Anhang verschickt.

Ein besonderes Beispiel für ein solches Video (dem die Malware auch einen ihrer Namen verdankt) ist „OfficeMonkeys LOL Video.zip". Wird die Datei ausgeführt, transportiert sie eine ausführbare Datei von CozyDuke auf den Computer, während zur Ablenkung ein „witziges" Video abgespielt wird, in dem Affen in einem Büro arbeiten. Das wiederum ermuntert die Opfer, das Video innerhalb des Büros weiterzuleiten, so dass immer mehr Computer infiziert werden. Der erfolgreiche Einsatz von Social-Engineering-Tricks – durch CozyDuke und so viele andere zielgerichtete Angreifer –, die Mitarbeiter dazu bringen, etwas zu tun, was die Unternehmenssicherheit gefährdet, unterstreicht einmal mehr, wie wichtig es ist, die Mitarbeiteraufklärung zu einer Kernkomponente jeder Sicherheitsstrategie eines Unternehmen zu machen.

Die **Naikon-APT** konzentrierte sich auf sensitive Ziele in Südostasien und rund um das Südchinesische Meer. Die Angreifer, die anscheinend chinesische Muttersprachler und seit mindestens fünf Jahren aktiv sind, attackieren Regierungsbehörden auf höchster Ebene sowie zivile und militärische Organisationen auf den Philippinen, in Malaysia, Kambodscha, Indonesien, Vietnam, Myanmar, Singapur, Nepal, Thailand, Laos und China. Wie so viele andere zielgerichtete Angriffskampagnen macht auch Naikon umfassenden Gebrauch von Social Engineering, um arglose Angestellte der angegriffenen Organisationen dazu zu bringen, die Malware zu installieren. Das Hauptmodul von Naikon ist ein Remote-Administration-Tool (RAT), also eine Fernwartungssoftware. Dieses Modul unterstützt 48 Befehle, um die Kontrolle über die infizierten Computer übernehmen zu können. Dazu gehören die Befehle, eine vollständige Inventur vorzunehmen, Daten herunter- und hochzuladen und Add-on-Module zu installieren. Obendrein setzt Naikon manchmal Keylogger ein, um an die Anmeldedaten der Mitarbeiter zu kommen. Jedem Zielland ist ein eigener Betreiber zugewiesen, der in der Lage ist, sich lokale kulturelle Gepflogenheiten zunutze zu machen – beispielsweise die „Sitte", private E-Mail-Accounts für die Arbeit zu verwenden. Die Angreifer benutzten zudem einen speziellen Proxyserver innerhalb der Landesgrenzen, um die Verbindungen mit den infizierten Computern zu koordinieren und die Daten an die Command-and-Control-Server (C2-Server) der Angreifer zu übermitteln. Sie finden unseren **Hauptbericht** sowie den **Nachfolgebericht** auf unserer Webseite.

Im Rahmen unserer Untersuchungen der Naikon-Kampagne deckten wir auch die Aktivität der **APT-Gruppe Hellsing** auf. **Hellsing** konzentrierte sich in erster Linie auf Regierungsorganisationen und diplomatische Einrichtungen in Asien: Die meisten Opfer befinden sich in Malaysia und auf den Philippinen, obwohl wir auch Opfer in Indien, Indonesien und den USA identifizieren konnten. Für sich gesehen ist Hellsing eine kleine und technisch eher unspektakuläre Cyberspionage-Gruppe (etwa 20 Organisationen wurden von Hellsing angegriffen). Interessant an dieser Gruppe ist allerdings, dass sie selbst im Visier einer Spear-Phishing-Attacke der APT-Gruppe Naikon stand – und beschloss, zurückzuschlagen! Die Antwort von Hellsing stellte die Authentizität des Absenders in Frage. Daraufhin erhielt die Hellsing-Gruppe eine Antwort von den Angreifern, doch sie öffneten den mitgeschickten Anhang nicht. Stattdessen sendeten sie kurz darauf den Angreifern eine E-Mail, die ihre eigene Malware enthielt. Es liegt auf der Hand, dass die Hellsing-Gruppe – nachdem sie entdeckt hatte, dass sie attackiert wird – versuchte, die Angreifer zu identifizieren und Informationen über ihre Aktivitäten zu sammeln. In der Vergangenheit konnten wir schon häufiger beobachten, wie sich APT-Gruppen versehentlich gegenseitig auf die Füße treten, beispielsweise, indem sie Adressbücher stehlen und dann jedem Adressaten auf den Listen massenhaft E-Mails schicken. Doch eine Attacke APT vs. APT ist ungewöhnlich.



Viele zielgerichtete Schadkampagnen richten sich gegen große Unternehmen, Regierungsbehörden oder andere Organisationen auf höchster Ebene. Daher könnte man leicht auf den Gedanken kommen, dass solche Organisationen die einzigen sind, die im Visier der Angreifer stehen. Doch eine der Kampagnen, über die wir letztes Quartal berichteten, hat eindeutig gezeigt, dass es nicht nur die „dicken Fische" sind, an denen die Cyberkriminellen interessiert sind.

Die **Cyberspionage-Kampagne Grabit** ist auf den Diebstahl von Daten aus kleinen und mittelgroßen Organisationen spezialisiert, die sich hauptsächlich in Thailand, Vietnam und Indien befinden, obwohl es nachweislich auch Opfer in den USA, den Vereinigten Arabischen Emiraten, der Türkei, Russland, China, Deutschland und anderswo gegeben hat. Zu den angegriffenen Branchen gehören die chemische Industrie, Nanotechnologie, Bildung, Landwirtschaft, Medien und Bauwirtschaft. Wir schätzen, dass die Gruppe hinter den Attacken in der Lage war, um die 10.000 Dateien zu stehlen. Zweifellos ist jedes Unternehmen ein potenzielles Ziel – aufgrund der eigenen Werte, die es zu stehlen gilt, oder als Einfallstor in eine andere Organisation.

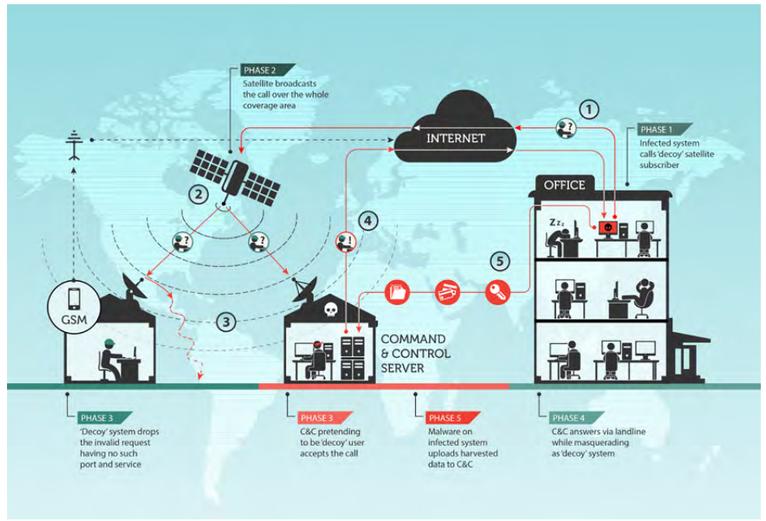
Die Experten von Kaspersky Lab stießen im Frühjahr 2015 während eines Sicherheitschecks auf einen Cyberangriff, der mehrere unserer internen Systeme betraf. Die nun folgenden, umfassenden Ermittlungen führten wiederum zur Entdeckung der neuen Malware-Plattform einer der kompetentesten, geheimnisvollsten und mächtigsten Gruppen in der APT-Welt, und zwar zu Duqu, manchmal auch als Stiefbruder von Stuxnet bezeichnet. Wir tauften diese neue Plattform auf den Namen **Duqu 2.0**. Im Fall von Kaspersky Lab machten sich die Angreifer eine Zero-Day-Schwachstelle im Windows-Kernel (von Microsoft am 9. Juni 2015 gepatcht) zunutze und möglicherweise bis zu zwei andere, aktuell gepatchte Sicherheitslücken, die zu der Zeit ebenfalls Zero-Day-Lücken waren. Das Hauptziel der Angreifer bestand darin, die Technologien von Kaspersky Lab, die laufenden Untersuchungen und interne Prozesse des Unternehmens auszuspionieren.

Doch Kaspersky Lab war nicht das einzige Ziel. Einige der Duqu-Infektionen werden mit den **P5+1-Veranstaltungen** und den Orten in Verbindung gebracht, an denen die Verhandlungen mit dem Iran über das Atomprogramm des Landes stattfanden: Der Bedrohungsakteur hinter Duqu scheint Angriffe auf die Veranstaltungsorte einiger dieser Gespräche auf höchster Ebene durchgeführt zu haben. Außerdem hat die Duqu-2.0-Gruppe auch ähnliche Angriffe auf die Veranstaltungen anlässlich des 70. Jahrestages der Befreiung von Auschwitz-Birkenau durchgeführt. Eines der hervorstechendsten Merkmale von Duqu 2.0 ist die kurze Lebensdauer und das Fehlen jeglicher Spuren im System. Die Malware nahm keine Veränderungen an der Festplatte oder den Systemeinstellungen vor: Die Malware-Plattform war so gestaltet worden, dass die Schadsoftware fast ausschließlich im Speicher infizierter Geräte überlebt. Das könnte darauf hinweisen, dass sich die Angreifer sicher waren, auch dann im System präsent zu bleiben, wenn ein individueller infizierter Computer neu gebootet und die Malware aus dem Speicher entfernt wurde. Die **Technische Dokumentation** und eine **Analyse des Persistenz-Moduls** finden Sie auf unserer Webseite.

Im August berichteten die Kaspersky-Experten über die **Blue-Termite-APT**, eine zielgerichtete Attacke, die darauf spezialisiert ist, Informationen von Organisationen in Japan zu stehlen. Dazu gehören Regierungsbehörden, lokale Verwaltungsämter, öffentliche Interessengruppen, Universitäten, Banken, Finanzdienstleister sowie Unternehmen aus den Bereichen Energie, Kommunikation, Schwerindustrie, Chemie, Automobilindustrie, Elektronik, neue Medien, Informationsdienste, Gesundheitswesen, Immobilien, Lebensmittel, Halbleiter, Robotertechnik, Bauwesen, Versicherungen, Transport und andere. Zu den prominentesten Zielen gehörte die Japanische Pensionskasse.

Die Malware wird auf das jeweilige Opfer zugeschnitten. Die Blue-Termite-Backdoor speichert Daten über sich selbst, unter anderen C2, API-Name, Anti-Analyse-Strings, Mutex-Werte sowie die MD5-Kontrollsummen der Backdoor-Befehle und die internen Proxy-Informationen. Die Daten werden in verschlüsselter Form gespeichert, wodurch die Analyse der Malware erschwert wird – für jedes einzelne Sample wird ein eigener Schlüssel benötigt. Die Hauptinfektionsmethode läuft wie bei so vielen zielgerichteten Angriffsattacken über Spear-Phishing-Mails.

Doch wir haben auch andere Infektionsmethoden erkannt, unter anderen Drive-by-Downloads unter Ausnutzung eines Flash-Exploits (CVE-2015-5119) – eines der Exploits, das infolge des **Hacking-Team-Leaks** bekannt geworden war. Mehrere japanische Webseiten wurden auf diese Weise kompromittiert. Wir registrierten auch einige Wasserloch-Attacken, darunter eine auf einer Webseite, die einem prominenten Mitglied der japanischen Regierung gehört.



Die Gruppe hinter der Cyberspionage-Kampagne **Turla** ist seit mehr als acht Jahren aktiv (unseren **Erstbericht**, die **darauf folgende Analyse** und die **Kampagnen-Übersicht** finden Sie auf **https://de.securelist.com/**) und hat hunderte Computer in mehr als 45 Ländern der Welt infiziert. Die Turla-Gruppe erstellt ein Profil ihrer Opfer und führt im Frühstadium Wasserloch-Attacken durch. Doch wie in unserem **jüngsten Report** beschrieben, macht sich die Gruppe für nachfolgende Operationen satellitengestützte Kommunikation zunutze, um ihren C2-Traffic (Command-and-Control) zu verwalten. Die von Turla verwendete Methode zum Abfangen der Downstream-Verbindungen erfordert kein gültiges Abonnement für einen satellitengestützten Internetzugang. Der wichtigste Vorteil besteht darin, dass die Verbindung anonym ist, und es damit sehr schwierig wird, die Angreifer zu identifizieren. Die Satellitenreceiver können sich überall in dem vom Satelliten abgedeckten Gebiet befinden (normalerweise ein großes Gebiet), und der tatsächliche Standort und die Hardware der C2-Server können nicht einfach identifiziert und physisch beschlagnahmt werden. Die Methode ist auch günstiger als das Mieten einer satellitengestützten Verbindung, und sie ist einfacher, als den Traffic zwischen dem Opfer und dem Satellitenbetreiber abzufangen und die Pakete auf dem Weg einzuschleusen.

Die Turla-Gruppe nutzt bevorzugt Provider von Satelliten-Internetverbindungen mit Sitz im Mittleren Osten und Afrika, unter anderem im Kongo, Libanon, Libyen, Niger, Nigeria, Somalia und den Vereinigten Arabischen Emiraten. Satellitenübertragungen von diesen Ländern decken normalerweise keine europäischen und nordamerikanischen Gebiete ab, was es Sicherheitsforschern sehr schwer macht, solche Attacken zu untersuchen. Die Nutzung von satellitengestützten Internetverbindungen ist eine interessante Entwicklung. Das Kapern von Downstream-Bandbreite ist günstig (ungefähr 1.000 US-Dollar Erstinvestition und zirka 1.000 US-Dollar Unterhaltungskosten pro Jahr), einfach umzusetzen und es bietet ein hohes Maß an Anonymität. Andererseits ist es nicht immer so zuverlässig wie traditionellere Methoden, zum Beispiel das Bullet-Proof-Hosting, multiple Proxy-Levels oder gehackte Webseiten – Methoden übrigens, die Turla ebenfalls ausnahmslos einsetzt. Dadurch ist es eher unwahrscheinlich, dass diese Methode verwendet wird, um umfangreiche Botnetze zu unterstützen. Doch sollte sich diese Methode unter APT-Gruppen oder Cyberkriminellen ausbreiten, so wird das ein ernsthaftes Problem für die IT-Sicherheit und die Strafverfolgungsbehörden darstellen.

Im August 2015 veröffentlichten wir ein **Update zu der Darkhotel-Kampagne**. Diese Attacken waren ursprünglich gekennzeichnet durch den Missbrauch gestohlener Zertifikate und die Bereitstellung von HTA-Dateien. Dabei setzten die Akteure ein breites Spektrum von Methoden ein und drangen in WLAN-Netze von Hotels ein, um Backdoors auf den Computern des Ziels zu platzieren. Während die Angreifer hinter dieser APT weiterhin auch die oben aufgezählten Methoden einsetzen, haben sie ihr Arsenal noch erweitert. Sie konzentrieren sich nun verstärkt darauf, die auserwählten Opfer durch Spear-Phishing zu ködern. Neben den HTA-Dateien stellen die Angreifer nun auch infizierte RAR-Dateien bereit, wobei sie einen RTLO-Mechanismus verwenden, um die echte Erweiterung der Datei zu verschleiern. Die Angreifer setzen zudem Flash-Exploits ein, unter anderem ein Zero-Day-Exploit von Hacking Team.

Die Gruppe hat zudem ihre geografische Reichweite ausgedehnt und greift nun auch Opfer in Nordkorea, Russland, Südkorea, Japan, Bangladesch, Thailand, Indien, Mosambik und Deutschland an.

LOGBOOK

DATENLECKS

Im Jahr 2015 wollte der Strom der Datenlecks kaum abreißen. Es überrascht kaum, dass derartige Vorfälle mittlerweile Routine sind: Persönliche Informationen sind ein wertvolles Gut, und zwar nicht nur für legitime Unternehmen, sondern auch für Cyberkriminelle. Zu den spektakulärsten Vorfällen in diesem Jahr gehören die Angriffe auf **Anthem**, **LastPass**, **Hacking Team**, das **Amt für Personalverwaltung der Vereinigten Staaten**, **Ashley Madison**, **Carphone Warehouse**, **Experian** und **TalkTalk**. Einige dieser Attacken endeten im Diebstahl eines großen Datenvolumens, was eindeutig zeigt, dass viele Unternehmen nicht in der Lage sind, adäquate Schritte zu unternehmen, um sich selbst zu schützen. Dabei geht es nicht nur einfach darum, die Unternehmensgrenzen zu

ZURÜCK ZUM INHALT

schützen. Es gibt keine hundertprozentige Sicherheit oder eine Garantie dafür, dass das System nicht kompromittiert wird, insbesondere dann nicht, wenn jemand innerhalb des Unternehmens dazu gebracht wird, etwas zu tun, was die Unternehmenssicherheit gefährdet. Aber jede Organisation, die persönliche Daten verwahrt, hat die Pflicht dafür zu sorgen, dass sie effizient geschützt werden. Das beinhaltet den Schutz von Passwörtern mittels Hash-Algorithmus und Salt sowie auch die Verschlüsselung anderer sensitiver Daten.

Andererseits können auch Kunden eines Online-Providers potenzielle, durch ein Sicherheitsleck entstehende Schäden einschränken, indem sie Passwörter benutzen, die einzigartig und komplex sind: Ein ideales Passwort ist mindestens 15 Zeichen lang und besteht aus einer Mischung von Buchstaben, Zahlen und Sonderzeichen. Alternativ kann man eine Passwort-Manager-App benutzen, die alles automatisch regelt.

Problematisch sind schwache Passwörter. Wenn wir ein Passwort wählen, das leicht zu erraten ist, so geben wir uns selbst dem Identitätsdiebstahl preis. Das Problem wird noch größer, wenn wir dasselbe Passwort für alle möglichen Online-Accounts verwenden – wird einer kompromittiert, so sind alle in Gefahr! Aus diesem Grund bieten viele Provider, unter anderem Apple, Google und Microsoft, nun eine Zwei-Faktoren-Authentifizierung an.

Dabei müssen die Kunden einen Code eingeben, der von einem Hardware-Token generiert oder an ein mobiles Gerät des Nutzers geschickt wird. Erst dann können sie auf eine Webseite zugreifen oder zumindest die Account-Einstellungen ändern. Die Zwei-Faktoren-Authentifizierung erhöht zweifellos die Sicherheit – aber nur, wenn sie vorgeschrieben wird, und eben nicht als Option zur Auswahl steht.

Der Diebstahl von persönlichen Daten kann für die Betroffenen ernsthafte Konsequenzen haben. Doch manchmal kann es auch zu regelrechten Kettenreaktionen kommen. Das **Hacking-Team-Leck** hatte die Veröffentlichung von 400 GB Daten zur Folge, darunter auch Exploits, die das italienische Unternehmen in seiner Überwachungssoftware verwendete. Einige dieser Exploits wurden in APT-Attacken eingesetzt, und zwar in den Kampagnen von Darkhotel und Blue Termite. Dem Leck folgte, wie zu erwarten war, eine Hektik, als es darum ging, die von den Hackern ausgenutzten Schwachstellen so schnell wie möglich zu beheben.

SMARTE (ABER NICHT UNBEDINGT SICHERE) GERÄTE

Das Internet wird immer mehr zum selbstverständlichen Teil unseres alltäglichen Lebens, und zwar buchstäblich, da die Zahl der Objekte zunimmt, die Teil unseres modernen Heims sind – Smart-TVs, intelligente Messgeräte, Babyfon, Wasserkocher und mehr. Vielleicht erinnern Sie sich daran, dass letztes Jahr einer unserer Sicherheitsforscher **sein eigenes Zuhause unter die Lupe nahm**, um herauszufinden, ob er wirklich cyber-sicher ist. Einen Nachfolgebericht zu dieser Studie finden Sie **hier**. Doch das „Internet der Dinge" umfasst mehr als nur Haushaltsgeräte.

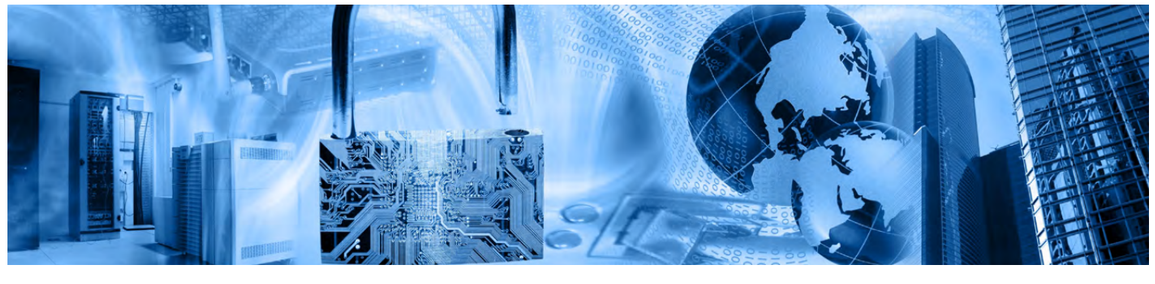
Forscher haben die möglichen Sicherheitsrisiken untersucht, die mit vernetzten Autos in Zusammenhang stehen. Im Juli 2014 **veröffentlichten Kaspersky Lab und IAB eine Studie, die die potenziellen Problemzonen von vernetzten Autos zum Inhalt hatte**. Bis zu diesem Jahr lag der Fokus auf dem Problem, mittels direkter physischer Verbindung auf das System des Autos zugreifen zu können. Das änderte sich, als die Forscher Charlie Miller und Chris Valasek einen Weg fanden, drahtlos auf die kritischen Systeme eines Jeep Cherokee zuzugreifen – und erfolgreich die Kontrolle übernahmen und ihn von der Straße abbrachten! (Lesen Sie die Geschichte **hier** nach!).

Diese Geschichte hebt einige der Probleme mit vernetzten Geräten hervor, die über die Autoindustrie hinausgehen und sich auf jedes vernetzte Gerät beziehen. Leider verkaufen sich Sicherheitsfeatures schlecht – auf einem Wettbewerbsmarkt haben meist die Dinge Vorrang, die den Kunden das Leben erleichtern. Hinzu kommt, dass Konnektivität häufig bereits existierenden Kommunikationsnetzwerken hinzugefügt wird, die nicht mit dem Gedanken an Sicherheit im Hinterkopf entwickelt wurden. Schließlich zeigt die Geschichte, dass die Sicherheit immer erst dann im Nachhinein angepasst wird, wenn irgendetwas Schlimmes passiert ist, was die Auswirkungen einer Sicherheitsschwachstelle deutlich aufzeigt. Lesen Sie mehr zu diesem Thema in einem **Blogpost von Eugene Kaspersky,** der nach der oben erwähnten Studie veröffentlicht wurde.

Solche Probleme gelten auch für „**Smart Cities**". Beispielsweise setzen Regierungen und Strafverfolgungsbehörden in den letzten Jahren immer mehr Video-Systeme ein, um öffentliche Plätze zu überwachen. Viele Video-Kameras sind drahtlos mit dem Internet verbunden, so dass die Polizei sie entfernt steuern kann. Doch das bedeutet nicht, dass sie auch zwangsläufig sicher sind: Cyberkriminelle haben die Möglichkeit, passiv die Sicherheits-Videofeeds einzusehen, Code in das Netzwerk einzuschleusen – und dabei den Kamerafeed durch gefälschtes Filmmaterial zu ersetzen – oder das System offline zu schalten. Zwei Sicherheitsforscher, Vasilios Hioureas von Kaspersky Lab und Thomas Kinsey von Exigent Systems, betrieben kürzlich Forschungen über potenzielle Sicherheitsschwachstellen in Videoüberwachungssystemen in einer Stadt. (Sie finden Vasilios' **Bericht** auf unserer Webseite).

Leider wurde seitens der Betreiber nicht versucht, die Markenbezeichnungen der Kameras zu verdecken, so dass die Machart und Modelle der Geräte problemlos identifiziert und die technischen Daten studiert werden konnten, um dann ein eigenes maßstabsgetreues Modell nachzubauen. Das verwendete Equipment gewährleistete wirkungsvolle Sicherheitskontrollen, aber diese Kontrollen wurden nicht sicher umgesetzt. Datenpakete, die durch die vermaschten Netze flossen, wurden nicht verschlüsselt, so dass ein Angreifer in der Lage gewesen wäre, seine eigene Version der Software zu erstellen und die durchlaufenden Daten zu manipulieren. Eine mögliche Ausnutzungsart für Angreifer könnte darin bestehen, das zu einer Polizeiwache zu sendende Bildmaterial zu fälschen. So könnte man einen Vorfall an einem Standort vortäuschen und die Polizeikräfte auf diese Weise von einem tatsächlichen Tatort irgendwo anders in der Stadt ablenken. Die Forscher informierten die für die Videoüberwachung zuständigen Stellen über dieses Problem, die bereits damit beschäftigt sind, das Sicherheitsproblem zu lösen. Ganz allgemein ist es überaus wichtig, dass eine von einem starken Passwort geschützte WPA-Verschlüsselung in diese Netzwerke implementiert ist. Ebenso wichtig ist, dass Markennamen von der Hardware entfernt werden, damit Angreifer nicht so leicht herausfinden, wie das Equipment funktioniert, und dass das Bildmaterial verschlüsselt durch das Netzwerk geschickt wird.

Das größere Problem hier ist, dass immer mehr Aspekte unseres täglichen Lebens digitalisiert werden. Wenn Sicherheit nicht als ein Teil des Entwicklungsprozesses angesehen wird, könnten die möglichen Gefahren weitreichend sein – und veraltete Sicherheitskonzepte könnten sich als nicht wirklich effektiv erweisen. Die von Kaspersky Lab unterstützte Initiative **Securing Smart Cities** soll denjenigen, die für die Entwicklung smarter Städte verantwortlich sind, helfen, die Cybersicherheit dabei nicht aus den Augen zu verlieren.



DIE TOP SECURITY STORIES

INTERNATIONALE ZUSAMMENARBEIT GEGEN CYBERKRIMINALITÄT

Cyberkriminalität ist heute ein fester Bestandteil des Lebens, der sich im Schatten unserer immer umfangreicher werdenden Online-Aktivitäten ausbreitet. Das zeigt sich auch in offiziellen Statistiken. In Großbritannien etwa bezieht das **Office for National Statistics** nun auch Cyberkriminalität in seine Schätzungen zum Umfang der Kriminalität ein. Das spiegelt die Tatsache wider, dass sich die Natur des Verbrechens in der Gesellschaft verändert. Während es keine Frage ist, dass Cyberkriminalität lukrativ sein kann, kommen Cyberkriminelle nicht immer ungestraft davon – und die Strafverfolgungsbehörden auf der ganzen Welt können einen großen Einfluss darauf haben. Internationale Zusammenarbeit ist ganz besonders wichtig, bedenkt man den globalen Charakter von Cyberverbrechen. In diesem Jahr gab es einige bemerkenswerte Polizeioperationen.

Im April war Kaspersky Lab an der **Abschaltung des Simda-Botnets** beteiligt, die vom Interpol Global Complex for Innovation koordiniert wurde. Die Ermittlungen wurden von Microsoft initiiert und dann auf andere Mitwirkende ausgeweitet, unter anderem Trend Micro, das Cyber Defense Institute, die National High Tech Crime Unit (NHTCU) der niederländischen Polizei, das FBI, die Police Grand-Ducale Section Nouvelles Technologies in Luxemburg und das Cybercrime Department „K" des russischen Innenministeriums, das vom National Central Bureau von INTERPOL in Moskau unterstützt wird. Im Rahmen der Zerschlagungsaktion wurden 14 C&C-Server konfisziert, die sich in den Niederlanden, den USA, Luxemburg, Polen und Russland befanden. Eine vorläufige Analyse einiger der abgefangenen Server-Logs förderte eine Liste von 190 Ländern zutage, die von der Aktivität des Simda-Botnets betroffen sind.

Im September verhaftete die **holländische Polizei zwei Männer, die verdächtigt werden, an Attacken der Ransomware CoinVault beteiligt zu sein**. Der Festnahme vorangegangen waren gemeinsame Ermittlungen von Kaspersky Lab, Panda Security und dem NHTCU. Diese Malware-Kampagne begann im Mai 2014 und setzte sich bis zum laufenden Jahr fort, wobei Opfer in mehr als 20 Ländern im Visier der Akteure standen. Die meisten wurden allerdings in den Niederlanden, in Deutschland, den USA, Frankreich und Großbritannien registriert. Die Angreifer verschlüsselten erfolgreich Dateien auf über 1.500 Windows-Computern und verlangten Zahlungen in Bitcoin, damit die Daten auf den betroffenen Rechnern wieder dechiffriert werden. Die für diese Erpressersoftware-Kampagne verantwortlichen Cyberkriminellen modifizierten ihre Machwerke mehrfach, um immer wieder neue Opfer angreifen zu können. Im November brachten Kaspersky Lab und das Niederländische NHTCU eine **Webseite auf den Weg, die als Anlaufstelle für Dechiffrierungsschlüssel dienen soll**. Außerdem stellten die Kaspersky-Experten auch ein **Entschlüsselungstool** online bereit, um den Opfern zu helfen, ihre Daten wiederherzustellen, ohne Lösegeld bezahlen zu müssen. Unsere Analyse über die Drehungen und Wendungen, die die CoinVault-Autoren vollziehen, finden Sie **hier**. Ransomware ist zum festen Inventar in der Bedrohungslandschaft geworden. Während dieser Fall zeigt, dass die Zusammenarbeit zwischen Forschern und Strafverfolgungsbehörden zu positiven Ergebnissen führen kann, ist es für Nutzer und Unternehmen gleichermaßen wichtig, Maßnahmen zu ergreifen, um die Risiken zu minimieren, die diese Art von Malware mit sich bringt. Ransomware-Kampagnen ergeben nur dann einen Sinn, wenn die Opfer zahlen. Im September löste ein **FBI-Agent eine Kontroverse aus, indem er Opfern nahelegte, Lösegelder zu zahlen, um ihre Daten wiederherzustellen**.

Während das eine pragmatische Lösung zu sein scheint (zumal es Situationen gibt, in denen eine Datenwiederherstellung unmöglich ist), ist es doch auch gleichzeitig eine gefährliche Strategie. Erstens gibt es keine Garantie dafür, dass die Betrüger tatsächlich die notwendigen Mechanismen zur Entschlüsselung der Daten bereitstellen. Zweitens fördert es ihr Geschäftsmodell und macht die weitere Entwicklung von Erpressersoftware nur umso wahrscheinlicher. Wir empfehlen daher Unternehmern und Heimanwendern gleichermaßen, regelmäßig Backups zu erstellen, um nicht in eine derart unangenehme Position zu geraten.

ANGRIFFE AUF INDUSTRIEOBJEKTE

Vorfälle mit Industrieobjekten, die auf Probleme mit der Cybersicherheit zurückzuführen sind, kommen relativ häufig vor. So wurden beispielsweise **laut Angaben des US-amerikanischen Internet Storm Centers CERT** im Finanzjahr 2014 in den USA 245 solcher Vorfälle registriert, und im Juli und August 2015 waren es 22. Unserer Meinung nach spiegeln diese Zahlen jedoch nicht die tatsächliche Situation wider – es gibt wesentlich mehr Cybervorfälle dieser Art. So wird ein Teil solcher Vorfälle von den Betreibern und Besitzern der Betriebe manchmal lieber unter den Teppich gekehrt, während sie von einem anderen Teil schlicht keine Kenntnis haben.

Schauen wir uns einmal zwei solcher Vorfälle genauer an, die im Jahr 2015 unsere Aufmerksamkeit auf sich zogen.

Der erste Vorfall ereignete sich in Deutschland in einem Stahlwerk. Ende 2014 gab das BSI, das Bundesamt für Sicherheit in der Informationstechnik, einen **Bericht zur Lage der IT-Sicherheit in Deutschland 2014** heraus. Darin wird ein Cybervorfall beschrieben, der sich in einem Stahlwerk in Deutschland ereignet hat. Infolge dieses Ereignisses wurde ein Hochofen physisch beschädigt. Das ist nach Stuxnet der zweite Fall einer Cyberattacke, die die physische Beschädigung einer Industrieanlage zur Folge hatte. Laut Erklärung des BSI erfolgte die initiale Infektion des Büronetzwerks dieses Betriebes durch Spear-Phishing. Daraufhin konnten sich die Hacker Schritt für Schritt Zugriff auf die Produktionsnetze verschaffen und die Anlage direkt angreifen. Leider stellte das BSI keine zusätzlichen Informationen zur Verfügung, und wir können nicht sagen, welche Schadsoftware genau eingesetzt wurde und was sie im Detail bewirkt hat.

Solche Heimlichkeit nützt nicht allen, denn die Betreiber ähnlicher Betriebe (außer deutschen vielleicht) sind dann nicht in der Lage, die Attacke zu studieren und entsprechende Gegenmaßnahmen zu ergreifen. Auch die Experten auf dem Gebiet Cybersicherheit bleiben unwissend und können ihren Kunden dementsprechend auch keine Schutzmethoden vorschlagen.

Ein anderer interessanter Fall ist der Angriff auf den Flughafen Frédéric Chopin in Warschau im Juni 2015. An einem Sonntag wurde das Computersystem, das die Abflüge der polnischen Fluggesellschaft LOT koordiniert, durch einen Hackerangriff für etwa fünf Stunden außer Gefecht gesetzt. Laut Angaben von **Reuters** wurde auf Grund dieses Vorfalls etwa ein Dutzend Flüge gestrichen.

Die Flughafenleitung ging trotzdem nicht mit Details zu diesem Angriff an die Öffentlichkeit, und verschiedene Experten äußerten – sich allein auf ihre Erfahrung stützend – ihre Meinung zu dem Vorfall. Ruben Santamarta, Principal Security Consultant bei IOActive, hatte schon vorher die Aufmerksamkeit auf **IT-Sicherheitsprobleme in der Luftfahrt** gelenkt. Sich auf Bestätigungen von LOT-Vertretern berufend geht er davon aus, dass die Fluggesellschaft Opfer einer zielgerichteten Attacke wurde: Das System war nicht mehr in der Lage, die Abflüge zu koordinieren, da die Schlüsselknoten des Back-Office kompromittiert worden waren oder die Attacke richtete sich gegen Bodenfunkstellen und führte dazu, dass es nicht mehr möglich war, den Upload von Daten (darunter auch die Abflugpläne) auf die Bordcomputer durchzuführen und zu validieren.

Unsere Experten haben ebenfalls auf den Vorfall reagiert: **Wir nehmen an**, dass hier zwei Angriffsszenarien möglich sind. Der Grund für den Vorfall könnte menschliches Versagen oder eine Fehlfunktion der Ausstattung gewesen sein. Oder aber dieser Angriff auf den verhältnismäßig kleinen Flughafen in Warschau war nur ein Vorbote umfangreicherer Aktionen Cyberkrimineller auf anderen großen Flughäfen der Welt.

Später wurde offiziell mitgeteilt, dass es sich um eine DDoS-Attacke gehandelt habe und nicht ins System eingedrungen worden sei. Detaillierte Informationen über diesen Vorfall werden nicht bekannt gemacht, und uns bleibt nichts anderes übrig, als den offiziellen Informationen Glauben zu schenken – oder über die wahren Gründe und Ziele des Angriffs zu spekulieren.

Wer auch immer hinter den Attacken stecken mag, über die wir berichtet haben, und was auch immer ihre Ziele sein mögen, sie beweisen doch einmal mehr, das Computer zu einem festen Bestandteil unseres Lebens geworden sind, und sie zeigen, wie angreifbar wichtige Infrastruktur-Objekte mit den Jahren geworden sind.

Leider verfolgen derzeit viele Staaten und Behörden eine Politik der Verschlossenheit. Unserer Meinung nach sind Transparenz und ein Informationsaustausch zum Thema Cyberattacken ein wichtiges Element beim Aufbau eines adäquaten Schutzes der Infrastruktur-Objekte – ohne dieses Wissen ist es sehr schwer, vor künftigen Bedrohungen zu schützen.

Zum Abschluss möchten wir noch auf eine Tendenz hinweisen, die bereits Einfluss auf uns alle hat und auch in den kommenden Jahren haben wird: Die in Industriebetrieben verwendeten Anlagen werden zunehmend mit dem Internet verbunden. Das Internet wurde schon vor geraumer Zeit erfunden, doch in den Produktionsprozessen wird es nun für uns sichtbar. Ohne Übertreibung kann man diese Tendenz eine industrielle Revolution nennen – es entsteht das „**Industrielle Internet der Dinge" oder die Industrie 4.0**. Dadurch kommen die Unternehmen in den Genuss vieler zusätzlicher Vorteile und die Produktion wird effektiver.

Um diesen Trend nicht zu verpassen, rüsten die Hersteller bewährte und zuverlässige Anlagen, die für eine Welt „ohne Internet" entwickelt wurden, einfach mit den notwendigen Sensoren und

Controllern aus, verbinden die Anlage mit dem Netz und schon haben sie eine „neue Ausrüstung". Doch sie vergessen dabei, dass immer, wenn ein beliebiges Gerät mit Funktionen zur Arbeit mit dem Internet ausgerüstet wird, auch neue Risiken und Bedrohungen auftreten, die mit der Cybersicherheit in Verbindung stehen. Nun sind es keine „physischen" Geräte mehr, sondern „cyberphysische" Geräte.

In der Welt der physischen Geräte wurden alle Industriegeräte, Instrumente, Verbindungsprotokolle und so weiter mit Blick auf die Funktionssicherheit projektiert, mit anderen Worten „idiotensicher" gemacht. Das bedeutete: Wenn ein Gerät den Anforderungen der Funktionssicherheit entsprechend projektiert wurde, darf es während des Betriebes keine Ausfälle geben und weder Menschen noch die Umwelt dürfen zu Schaden kommen – sofern die Funktionssicherheit nicht beeinträchtigt ist.

Die „Industrie 4.0" erhält eine ganz andere Sicherheitsdimension – nun geht es auch um IT-Sicherheit oder den Schutz vor absichtlicher Einflussnahme von außen. Man kann nicht einfach ein Objekt oder Gerät, das noch aus der „vor-WWW-Ära" stammt, an das Internet anschließen. Die Folgen könnten überaus beklagenswert sein – und sie sind es mitunter heute schon.

Ingenieure, die sich zu alten, „vorrevolutionären" Projektierungsprinzipien bekennen, bedenken häufig nicht, dass jetzt unter Umständen nicht ausschließlich Experten mit ihrem Gerät „arbeiten", die wissen, was man tun kann und was nicht, sondern auch Hacker, die sich nicht um „unerlaubte Aktionen mit einem entfernten Gerät" scheren. Das ist einer der Hauptgründe dafür, dass Unternehmen mit großem Erfahrungsschatz und langer Tradition jetzt gute und hinsichtlich der Funktionssicherheit zuverlässige Anlagen bauen, die den Betrieben kein ausreichendes Maß an Cybersicherheit gewährleisten können.

In der Welt der cyberphysischen Geräte sind die Elemente „cyber" und „physisch" eng miteinander verknüpft. Eine Cyberattacke kann einen technologischen Prozess zum Erliegen bringen, Anlagen beschädigen oder eine technische Katastrophe verursachen. Hacker sind eine reale Bedrohung, und alle, die mit dem Internet verbunden sind, können ihnen zum Opfer fallen.

Daher müssen die Hersteller bei der Entwicklung neuer vernetzter Industrieanlagen die Maßnahmen zum Schutz vor Cyberbedrohungen unbedingt ebenso sorgfältig ausarbeiten wie die Maßnahmen zur Gewährleistung der Funktionssicherheit.

FAZIT

Das Jahr 2015 war wohl das erste Jahr in der Geschichte des Internets, in dem Probleme des Netzwerkschutzes und der Sicherheit im Netz in Bezug auf jeden erdenklichen Wirtschaftssektor und hinsichtlich aller Bereiche unseres alltäglichen Lebens diskutiert wurden. Suchen Sie sich irgendein Gebiet der modernen Zivilisation aus – Finanzen, Industrieproduktion, Automobilindustrie, Flugzeuge, mobile Geräte, Gesundheitswesen und vieles mehr – und Sie finden garantiert zu jedem Thema eine Veröffentlichung aus diesem Jahr über einen Vorfall oder über Probleme in Zusammenhang mit Cybersicherheit.

Leider ist die Cybersicherheit untrennbar mit der Entwicklung des Terrorismus verbunden. Die Schutzmethoden und Überfallmöglichkeiten im Netz sind ins Zentrum des Interesses verschiedener illegaler Strukturen und Gruppierungen gerückt.

Fragen der Cybersicherheit werden nun auf diplomatischer Ebene und in den höchsten Regierungskreisen diskutiert. In diesem Jahr wurden Verträge über Cybersicherheit zwischen Russland und China abgeschlossen, zwischen China und den USA und zwischen China und Großbritannien. Im Rahmen dieser Verträge verpflichten sich die Staaten nicht nur zur Zusammenarbeit, sondern auch zur Verhinderung gegenseitiger Angriffe. Gleichzeitig wurde aktiv über die kürzlich erfolgte Revision des Wassenaar-Abkommens debattiert, die die Exporteinschränkung von Spionagesoftware betrifft. Eins der wichtigsten Themen des Jahres war die Nutzung von ungeschützten E-Mail-Diensten durch verschiedene Politiker auf der ganzen Welt, unter anderem auch durch die damalige Außenministerin der USA, Hillary Clinton.

All das hatte zur Folge, dass das Interesse an dem Problem der Cybersicherheit nicht nur seitens der Massenmedien enorm zunahm, sondern sich auch die Unterhaltungsindustrie diesem Thema widmete. Es wurden Spielfilme und Serien gedreht, und der eine oder andere Experte auf dem Gebiet Cybersicherheit wurde für eine Rolle besetzt oder spielte sich selbst.

Im Jahr 2015 wurde das Wort „Cybersicherheit" modern, doch das ist noch nicht die Lösung des Problems. Wir beobachten ein praktisch exponentielles Wachstum aller Größen, die mit Cybersicherheit zusammenhängen: eine Zunahme der Zahl der Attacken, der Zahl der Angreifer, der Opfer, der Ausgaben für die Abwehr und den Schutz, und eine Zunahme der Gesetze und Verträge, die die neuen Normen regeln und installieren. Für uns bedeutet das in erster Linie, dass die aufzuspürenden Attacken komplexer werden. Die Konfrontation ist in eine aktive Phase eingetreten, doch ein abschließendes Stadium ist noch weit, weit entfernt.

Über das, was uns in nächster Zukunft erwartet, berichten wir in unseren **Prognosen für das Jahr 2016**.

> HUNTING THE HUNTER - UNSER GREAT STELLT SICH VOR

PROGNOSE: DAS ENDE VON APTS – WIE WIR SIE KENNEN.

Autor: Juan Andrés Guerrero-Saade, GReAT bei Kaspersky Lab

QUICK INFO

- KEINE APTS MEHR
- DER RANSOMWARE-ALPTRAUM GEHT WEITER
- GEGEN DAS HAUS WETTEN: FINANZ-VERBRECHEN AUF HÖCHSTEM NIVEAU
- ANGRIFFE AUF SICHERHEITSANBIETER
- SABOTAGE, ERPRESSUNG UND BLOSSSTELLUNG
- WEM TRAUEN SIE?
- APT-AKTEURE AM ENDE
- DIE ZUKUNFT DES INTERNETS
- DIE ZUKUNFT DER BEFÖRDERUNG
- DIE KRYPTOKALYPSE NAHT

ZURÜCK ZUM INHALT

Jetzt, da sich das Jahr seinem Ende entgegen neigt, haben wir Gelegenheit, Bilanz zu ziehen, die Entwicklung der Branche zu bewerten und eine Vorhersage für die kommenden Jahre zu wagen, was die Entwicklung der Cyberbedrohungen angeht. Auf einem Treffen unserer Experten aus den GReAT- und Anti-Malware-Research-Team wurden viele Ideen diskutiert, und ich habe nun das Privileg, einige der bemerkenswertesten und plausibelsten – sowohl für die kommenden Jahre als auch für eine langfristige Zukunft, wie wir sie sehen – vorzustellen. Der Ausblick für das sich rasant entwickelnde Feld der Cybersicherheit bietet viele Denkanstöße und wird uns immer wieder vor neue Herausforderungen stellen. Indem wir sachliche Kriterien zugrunde legen, können wir vielleicht die übliche Science-Fiction-Panikmache über Bord werfen und einige präzise Vorhersagen treffen – sowohl für die nahe Zukunft als auch langfristig.

Global Research and Analysis Team

KEINE APTS MEHR

Bevor Sie nun anfangen zu jubeln, sollten wir darauf hinweisen, dass wir uns auf die Elemente „Advanced" – also fortschrittlich – und „Persistent" – also andauernd, nachhaltig – beziehen. Beides sind Elemente, die die Bedrohungsakteure mit Freude über Bord werfen würden, wenn sie sich dafür komplett unsichtbar machen könnten. Wir erwarten, dass die Nachhaltigkeit künftig eine weniger große Rolle spielen und einem größeren Fokus auf speicherresistente und dateilose Malware weichen wird. Der Gedanke dahinter ist, die in einem infizierten System hinterlassenen Spuren zu reduzieren und insgesamt eine Detektion zu vermeiden. Bei einem anderen Ansatz könnte es weniger wichtig werden, dass die Schadprogramme fortschrittlich und technisch besonders anspruchsvoll sind. Anstatt dass weiter in Bootkits, Rootkits und kundenspezifische Malware investiert wird, die dann doch von Antiviren-Forschern unschädlich gemacht wird, erwarten wir die Modifikation gebrauchsfertiger Schadprogramme. Das bedeutet zum einen, dass die Malware-Plattform bei Entdeckung nicht zerstört wird. Zum anderen bringt dieser Ansatz den zusätzlichen Vorteil mit sich, dass der Akteur sich und seine Absichten gut verbergen kann – in der unübersichtlichen Menge banaler Einsätze einer kommerziell verfügbaren Fernwartungssoftware. Wenn die Wirkung raffinierter, anspruchsvoller Malware nachlässt, werden viele Entscheidungen der Angreifer, die von Nationalstaaten gesponsert werden, durch die Kapitalrendite bestimmt – und nichts ist überzeugender als geringe Erstinvestitionen bei maximaler Rendite.

DER RANSOMWARE-ALPTRAUM GEHT WEITER

Wir erwarten, dass Ransomware künftig noch erfolgreicher sein und neue Grenzen überschreiten wird. Ransomware hat zwei Vorteile gegenüber traditionellen Bank-Bedrohungen: direkte Umsetzung in Bargeld und relativ geringe Kosten pro Opfer. Das hat zur Folge, dass gut ausgestattete Dritte wie etwa Banken nur ein geringes Interesse an Ransomware zeigen und relativ wenige Vorfälle den Strafverfolgungsbehörden gemeldet werden. Wir gehen nicht nur davon aus, dass Ransomware gegenüber Bank-Trojanern an Boden gewinnen wird, sondern wir erwarten zudem, dass Erpressersoftware auch auf anderen Plattformen auftaucht. Es wurden bereits schwache Versuche beobachtet, Ransomware auf mobile Plattformen (Simplelocker) und Linux (Linux.Encode.1) zu übertragen, aber die erstrebenswertere Plattform ist vermutlich Mac OS X. Wir meinen, dass Erpresser nicht nur den Rubikon überschreiten werden, um Macs anzugreifen, sondern dass sie auch „Mac-mäßige" Preise verlangen werden. Und dann, auf lange Sicht, ist es nicht unwahrscheinlich, dass auch Ransomware für das Internet der Dinge auftauchen wird. Dann wird man sich fragen müssen, wie viel man auszugeben bereit ist, um wieder Zugriff auf den eigenen Fernseher zu erhalten – oder auf den eigenen Kühlschrank, oder auf das eigene Auto.

GEGEN DAS HAUS WETTEN: FINANZ-VERBRECHEN AUF HÖCHSTEM NIVEAU

Das Aufkommen von Cyberkriminalität und APTs hat finanziell motivierte Verbrecher ermutigt, nicht mehr nur Heimanwender anzugreifen, sondern gleich Finanzinstitutionen selbst. Im letzten Jahr gab es viele Beispiele von Angriffen auf Point-of-Sale-Systeme und Geldautomaten, ganz zu schweigen von dem dreisten Carbanak-Banküberfall, bei dem hunderte Millionen US-Dollar gestohlen wurden. Wir erwarten, dass auch andere Cyberkriminelle in dieser Manier neue Wege beschreiten und alternative Bezahlsysteme (ApplePay und AndroidPay) ins Visier nehmen werden. Diese werden immer beliebter und eröffnen den Cyberkriminellen damit neue Wege der sofortigen

Monetarisierung. Ein anderer unausweichlicher Anziehungspunkt sind Börsen, die wahren Goldadern. Während Frontalangriffe schnelle Rendite versprechen, dürfen wir nicht die Möglichkeit

subtilerer Störungsmethoden übersehen, wie zum Beispiel einen Angriff auf die Algorithmen der Black Box, wie sie beim Hochfrequenzhandel verwendet wird, um nachhaltigere Gewinne zu erzielen, bei gleichzeitig geringerer Wahrscheinlichkeit, gefasst zu werden.

ANGRIFFE AUF SICHERHEITSANBIETER

Da die Angriffe auf Anbieter von Sicherheitslösungen zunehmen, sehen wir zukünftig auch folgende Angriffsszenarien: die Kompromittierung von Industriestandard-Reverse-Engineering-Tools wie IDA und Hiew, von Debugging-Tools wie OllyDbg und WinDbg oder von Virtualisierungstools wie die VMware Suite und VirtualBox. CVE-2014-8485, eine Sicherheitslücke in der String-Implementation in Linux, ist ein Beispiel für die verwundbare Landschaft nicht trivialer Forschungstools, die von Angreifern ausgenutzt werden können, wenn sie die Forscher selbst ins Visier nehmen. Auf ähnliche Weise ist das Teilen von Freeware-Forschungstools über Code-Repositorien wie Github ein Bereich, der dem Missbrauch viel Raum lässt, denn Nutzer werden gelegentlich Code auf ihr System laden und ihn dort ausführen, ohne auch nur einen Blick darauf zu werfen. Vielleicht sollten wir auch einen misstrauischen Blick auf populäre PGP-Umsetzungen werfen, die bereitwillig von der IT-Sicherheitscommunity aufgenommen wurden.

SABOTAGE, ERPRESSUNG UND BLOSSSTELLUNG

Vom Hacken von Promi-Nacktfotos zu den virtuellen Einbrüchen bei Sony und Ashley Madison und dem Hack von HackingTeam nehmen die Fälle von DOXing, öffentlicher Bloßstellung und Erpressung unbestreitbar zu. Hacktivisten, Kriminelle und Nationalstaat-gesponserte Angreifer gleichermaßen haben sich das strategische Veröffentlichen privater Fotos, Informationen, Kundenlisten und Code angeeignet, um ihre Ziele bloßzustellen. Während einige dieser Angriffe strategischer Natur sind, sind andere eher ein Produkt des Opportunismus, wenn ein schwacher Schutz ausgenutzt wird, um mit nicht vorhandenen Hacking-Fähigkeiten zu prahlen. Leider müssen wir davon ausgehen, dass diese Praxis weiterhin exponentiell zunehmen wird.

WEM TRAUEN SIE?

Das rarste Gut im heutigen Internetzeitalter ist vermutlich Vertrauen. Der Missbrauch von vertrauenswürdigen Ressourcen wird es noch seltener werden lassen. Angreifer werden weiterhin Open-Source-Bibliotheken und Ressourcen aus Whitelists für böswillige Zwecke nutzen. Wir meinen, dass eine andere Form von Vertrauen missbraucht werden wird, und zwar das der internen Ressourcen eines Unternehmens: Wenn clevere Angreifer darauf aus sind, ihre Reichweite in einem infizierten Netzwerk auszubauen, könnten sie Ressourcen angreifen, die auf das Intranet des Unternehmens beschränkt sind, indem sie Wasserloch-Attacken auf Sharepoint, Dateiserver oder ADP-Portale durchführen. Vielleicht werden wir sogar Zeuge einer Ausweitung des jetzt schon ungezügelten Missbrauchs vertrauenswürdiger Zertifikate, nämlich dann, wenn Angreifer mit einer schon komplett fertigen Zertifizierungsstelle aufwarten, um Zertifikate für ihre Malware auszugeben.

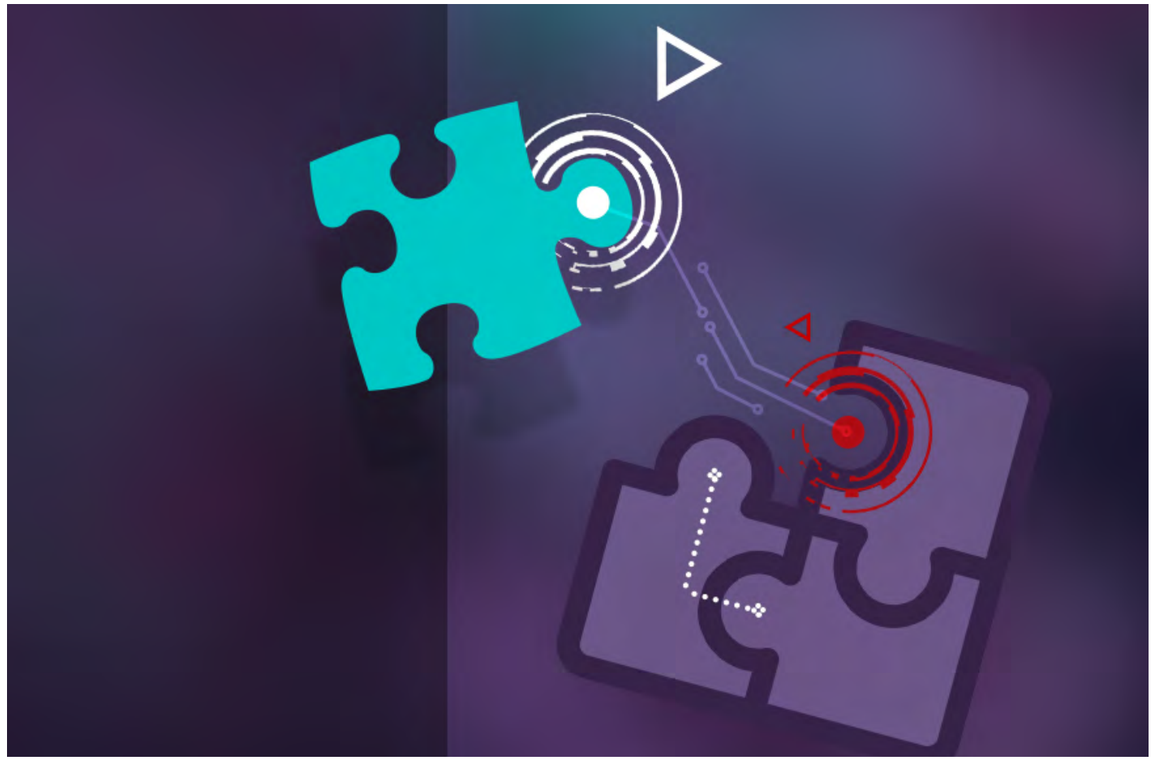
APT-AKTEURE AM ENDE

Dass Cyberspionage profitabel ist, ist auch Cyberkriminellen nicht entgangen, und wie wir es erwartet haben, bevölkern immer mehr Söldner die Szene. Dieser Trend wird sich verstärken, um die Nachfrage nach Cyberkapazitäten sowohl von Firmen als auch von bekannten APT-Akteuren zu decken, die wenige wichtige Aufgaben auslagern wollen, ohne dabei ihre Tools und ihre Infrastruktur einem Risiko auszusetzen. Wir könnten den Begriff „APT-as-a-Service" lancieren, aber vielleicht werden zielgerichtete Attacken interessanterweise eher einer Dienstleistung weichen, die wir als „Access-as-a-Service" bezeichnen möchten. Diese Dienstleistung beinhaltet den Verkauf des Zugriffs auf prominente Ziele, die bereits Cybersöldnern zum Opfer gefallen sind.

Wenn wir noch weiter in die Zukunft der Cyberspionage schauen, so sehen wir Mitglieder etablierter APT-Teams („APT-Onepercenters", wenn man so will), die möglicherweise aus dem Schatten treten werden. Das kann auf dem privaten Sektor der Fall sein, wenn sich der Trend des „Zurückhackens" weiter ausbreitet, oder es könnte passieren, dass die APT-Hacker ihr Insiderwissen mit einer größeren IT-Sicherheits-Community teilen, vielleicht indem sie unsere Konferenzen besuchen, um uns die andere Seite der Medaille zu zeigen. Bis dahin aber ist zu erwarten, dass der APT-Turm von Babylon noch um einige Sprachen erweitert wird.

DIE ZUKUNFT DES INTERNETS

Die Infrastruktur des Internets selbst hat in den vergangenen Jahren Anzeichen von Spannungen gezeigt und Risse bekommen. Sorgen um massive Router-Botnetze, das Abfangen des Routingprotokolls des Internets, BGP, massenhafte DNS-Attacken oder Server-gestützte DDoS-Angriffe reflektieren einen weltweiten Mangel an Zurechnungsfähigkeit und Durchsetzung. Schauen wir weiter in die Zukunft und berücksichtigen die langfristigen Vorhersagen, können wir uns vorstellen, wie das Internet aussehen könnte, wenn die Geschichte von einem global vernetzten Dorf noch mehr in Vergessenheit gerät. Wir könnten bei einem zersplitterten Internet enden, das durch nationale Grenzen geteilt wird. An diesem Punkt könnten Sorgen über die Verfügbarkeit aufkommen, Angst vor Angriffen auf die Service-Verbindungspunkte, die Zugriff zwischen verschiedenen Sektionen bieten, oder vor geopolitischen Spannungen, die sich auf die Kabel beziehen, welche große Teile des Internets miteinander verbinden. Vielleicht wird sich auch ein Schwarzmarkt für Konnektivität entwickeln. Und wenn die Technologien, die die Schattenseite des Internets mit Energie versorgen, immer mehr zum Mainstream werden und immer größere Akzeptanz erfahren, so könnten Entwickler mit Beteiligung am Schattenmarkt und an Foren auf ähnliche Weise bessere Technologien entwickeln, damit der Untergrund auch wirklich Untergrund bleibt.



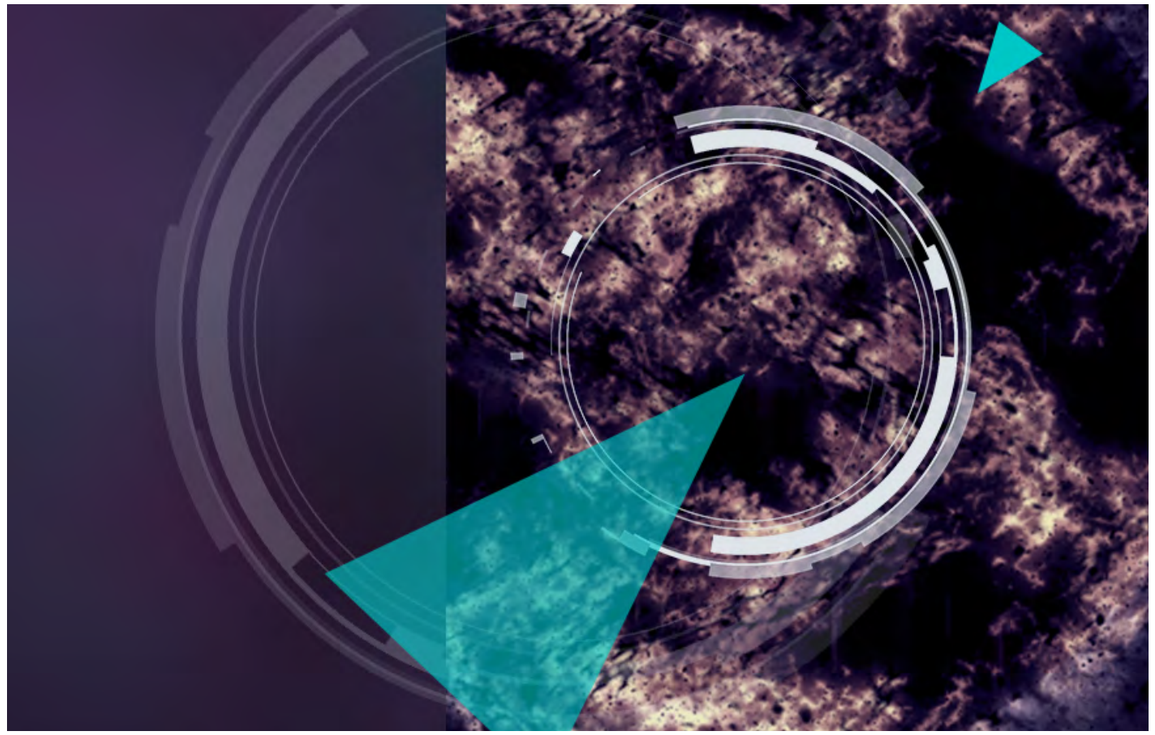
DIE ZUKUNFT DER BEFÖRDERUNG

Wenn Kapital und erstklassige Forschungsressourcen investiert werden, um autonome Vehikel sowohl für die private als auch für die kommerzielle Distribution zu entwickeln, werden wir das Aufkommen von verteilten Systemen beobachten können, die die Routen und den Verkehr einer großen Menge dieser Vehikel verwalten und steuern. Die Angriffe werden sich möglicherweise nicht gegen die Verteilungssysteme selbst richten, möglicherweise aber gegen die Protokolle, auf denen sie basieren, indem diese abgefangen und getäuscht werden (ein Proof-of-Concept zu den

Sicherheitslücken des weit verbreiteten Satcom-Systems von Global Star wurde in diesem Jahr von einem **Synack-Forscher auf der BlackHat-Konferenz präsentiert**). Vorhersehbare Absichten hinter diesen Attacken könnten unter anderem der Diebstahl hochwertiger Waren oder die Beeinträchtigung der Bewegungsfähigkeit sein, was Menschenleben kosten könnte.

DIE KRYPTOKALYPSE NAHT

Schließlich können wir die Wichtigkeit kryptografischer Standards gar nicht stark genug hervorheben, wenn es darum geht, den funktionalen Wert des Internets als Informationsaustausch- und Transaktionstool von beispiellosem Nutzen aufrechtzuerhalten. Diese kryptografischen Standards basieren auf der Erwartung, dass die Rechenleistung, die benötigt würde, um ihren verschlüsselten



Output zu knacken, schlicht über und jenseits unserer Möglichkeiten liegt. Doch was passiert, wenn wir einen Paradigmensprung bezüglich der Rechenmöglichkeiten vollziehen, wie es für künftige Durchbrüche im Quantencomputing versprochen wird? Auch wenn Quanten-Ressourcen nicht von Anfang an für gewöhnliche Cyberkriminelle verfügbar sein werden, markiert es doch das Ende der Zuverlässigkeit unserer aktuellen kryptografischen Standards und die Notwendigkeit, eine „Post-Quanten-Kryptografie" zu entwickeln und einzuführen. Bedenkt man, wie wenig die hochkarätige Kryptografie, die wir haben, angenommen oder wie schlecht sie häufig implementiert wird, so sehen wir keinen glatten Übergang vorher, durch den wir in der Lage wären, kryptografische Ausfälle aufzufangen.

SCHÜTZE DEINE WELT VOR CYBER-BEDROHUNGEN

KASPERSKY SECURITY BULLETIN 2015/2016

Kaspersky Lab Global Research and Analysis Team (GReAT)

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
© 2016 Kaspersky Labs GmbH.

Copyright bzw. Copyright-Nachweis für alle Beiträge bei der Kaspersky Labs GmbH. Reproduktion jeglicher Art – auch auszugsweise – nur mit schriftlicher Genehmigung der Kaspersky Labs GmbH.

Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion oder der Kaspersky Labs GmbH wieder. Alle Markennamen sind in der Regel eingetragene Warenzeichen der entsprechenden Hersteller oder Organisationen.

KASPERSKY lab
THE POWER OF PROTECTION

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

FOLLOW US

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

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/

© 2016 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber. Mac und Mac OS sind eingetragene Marken von Apple Inc. Cisco ist eine eingetragene Marke oder eine Marke von Cisco Systems, Inc. und/oder seinen Tochtergesellschaften in den USA und bestimmten anderen Ländern. IBM, Lotus, Notes und Domino sind Marken der International Business Machines Corporation und als solche in vielen Rechtsgebieten weltweit eingetragen. Linux ist das eingetragene Markenzeichen von Linus Torvalds in den USA und anderen Ländern. Microsoft, Windows, Windows Server und Forefront sind eingetragene Marken der Microsoft Corporation in den USA und anderen Ländern. Android™ ist eine Marke von Google, Inc. Die Marke BlackBerry ist Eigentum von Research In Motion Limited und in den USA eingetragen sowie als solche in anderen Ländern eingetragen bzw. ihre Eintragung wurde beantragt.

KASPERSKY lab

THE POWER
OF PROTECTION