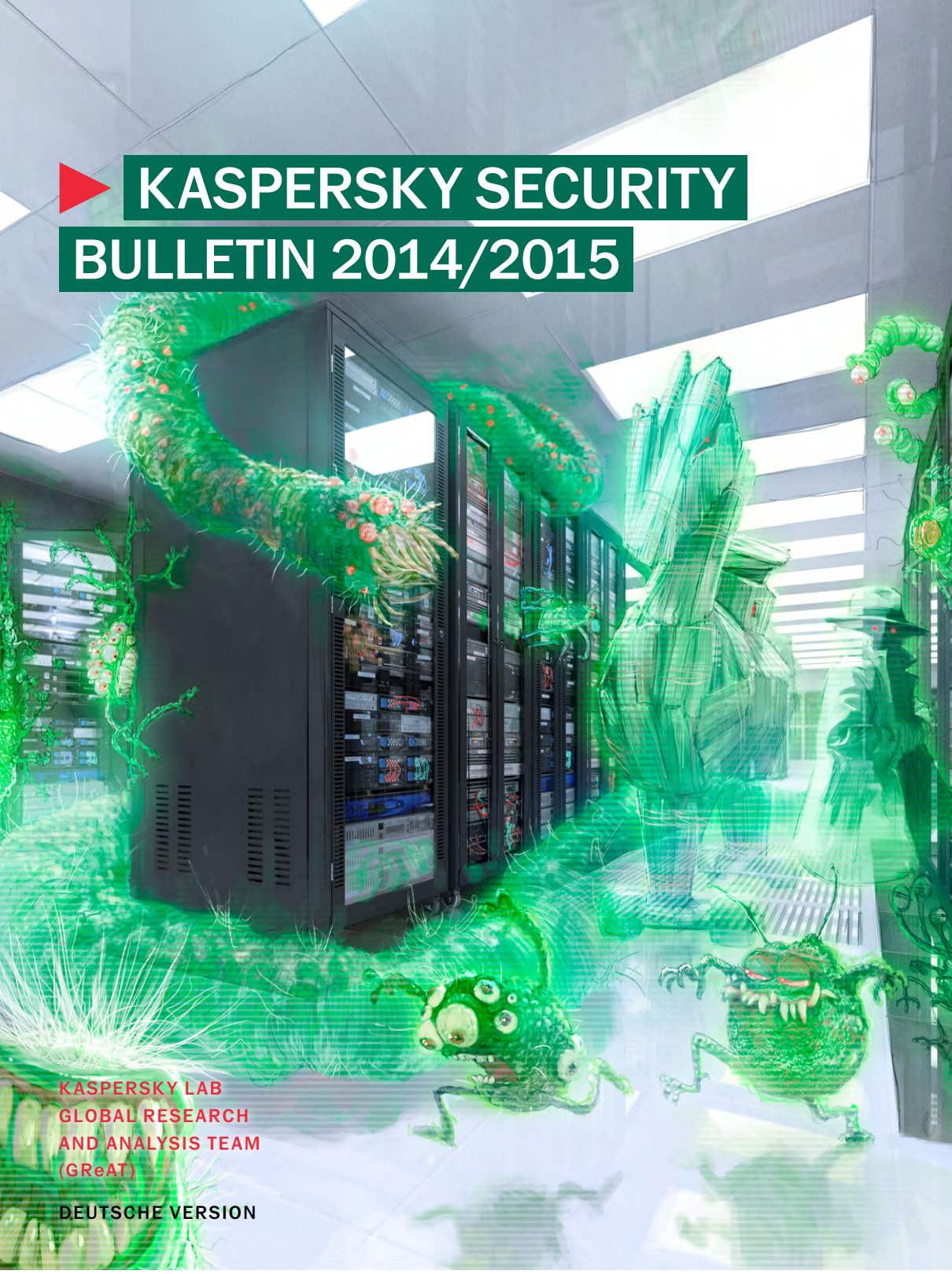
KASPERSKY SECURITY BULLETIN 2014/2015



KASPERSKY LAB
GLOBAL RESEARCH
AND ANALYSIS TEAM
(GReAT)

DEUTSCHE VERSION

KASPERSKY lab

INHALT

KASPERSKY SECURITY BULLETIN 2014/2015

Autor: Stefan Rojacher

JAHRESANALYSE VON KASPERSKY LAB FÜR 2014 UND 2015

Mit dem Kaspersky Security Bulletin 2014/2015 veröffentlicht Kaspersky Lab seine Analyse der Cybergefahren und deren Entwicklungen für das Jahr 2014 sowie eine Prognose für zukünftige Internetgefahren und Angriffsszenarien.

Die Malware-Statistiken für das Jahr 2014 bieten einen Überblick über Bedrohungen aus dem mobilen Bereich, speziellen Gefährdungen im Bankensektor, für Mac-Anwender und unterschiedlichen Gefahrenpotenziale nach Online- und Offline-Angriffen. Die Geografie des Malware- und Infizierungsniveaus liefert daneben Aufschlüsse hinsichtlich regionaler Gefährdungen.

Der Rückblick auf das Jahr 2014 wird durch die ultimativen Security-Stories abgeschlossen. Neben den großen Malware-Kampagnen bleiben uns hauptsächlich das Internet der (un)sicheren Dinge, Angriffe auf Bankautomaten oder die Diskussion um die Privatsphäre der Internetnutzer im Gedächtnis.

Für das Jahr 2015 werfen die Experten von Kaspersky Lab einen Blick in die APT-Kristallkugel und sagen u.a. eine Fusion von Cyberkriminalität und APT sowie die Kommerzialisierung von APT voraus. Einen weiteren sicherheitsrelevanten Bereich werden virtuelle Bezahlsysteme wie Apple Pay darstellen. Natürlich bleibt im Jahr 2015 auch das Internet der Dinge unter Beobachtung der Sicherheitsexperten von Kaspersky Lab.

Hacking 2014: Der Cyberkampf um Geld und private Daten

STATISTIK FÜR DAS JAHR 2014

Autor(en): Maria Garnaeva, Viktor Chebyshev, Denis Makrushin, Roman Unuchek, Anton Ivanov

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

Die Daten stammen aus dem Zeitraum von November 2013 bis Oktober 2014.

QUICK INFO

- Das Jahr in Zahlen
- Mobile Bedrohungen
- Geografie der mobilen Trojaner
- Top 20 der mobilen Bedrohungen 2014
- SMS-Trojaner: Ruckgang der Attacken
- Mobile Bank-Trojaner
- Bedrohungen fur Mac OS X
- Geografie der Bedrohungen
- Von Cyberkriminellen ausgenutzte angreifbare Anwendungen
- Schadprogramme im Internet (Attacken uber das Web)
- Online-Bedrohungen im Bankensektor
- Top 20 der Schadprogramme im Internet
- Top 10 der Lander, auf deren Ressourcen Schadprogramme untergebracht sind
- Lander, mit dem hochsten Infektionsrisiko uber das Internet
- Lokale Bedrohungen
- Lander, mit dem hochsten lokalen Infektionsrisiko

DAS JAHR IN ZAHLEN

- Laut den Daten des KSN blockierten die Produkte von Kaspersky Lab im Jahr 2014 insgesamt **6.167.233.068** schädliche Attacken auf den Computern und mobilen Geräten der Anwender.
- Es wurden **3.693.936** Versuche blockiert, Mac-OS-X-Rechner zu infizieren.
- **1.363.549** Attacken auf Android-Geräte wurden abgewehrt.
- Die Lösungen von Kaspersky Lab wehrten **1.432.660.467** Attacken ab, die von Internet-Ressourcen aus verschiedenen Ländern der Welt kommen.
- Zur Durchführung von Angriffen über das Netz nutzten die Cyberverbrecher **9.766.119** individuelle Hosts.
- **44 Prozent** der von Kaspersky-Produkten blockierten Webattacken wurden unter Verwendung schädlicher Webressourcen durchgeführt, die sich in den USA und in Deutschland befinden.
- Im Laufe des Jahres waren **38,3 Prozent** der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt.
- Auf den Computern von **1.910.520** Anwendern wurden Versuche abgewehrt, Banken-Malware zu starten.
- Kaspersky Lab Anti-Virus erkannte **123.054.503** individuelle Objekte (Skripte, Exploits, ausführbare Dateien und andere).
- Auf den Computern der Anwender detektierte Kaspersky Lab Anti-Virus **1.849.949** schädliche und potenziell unerwünschte Programme.

MOBILE BEDROHUNGEN

Innerhalb des Berichtszeitraums wurden entdeckt:

- **4.643.582** schädliche Installationspakete
- **295.539** neue mobile Schadprogramme
- **12.100** mobile Bank-Trojaner

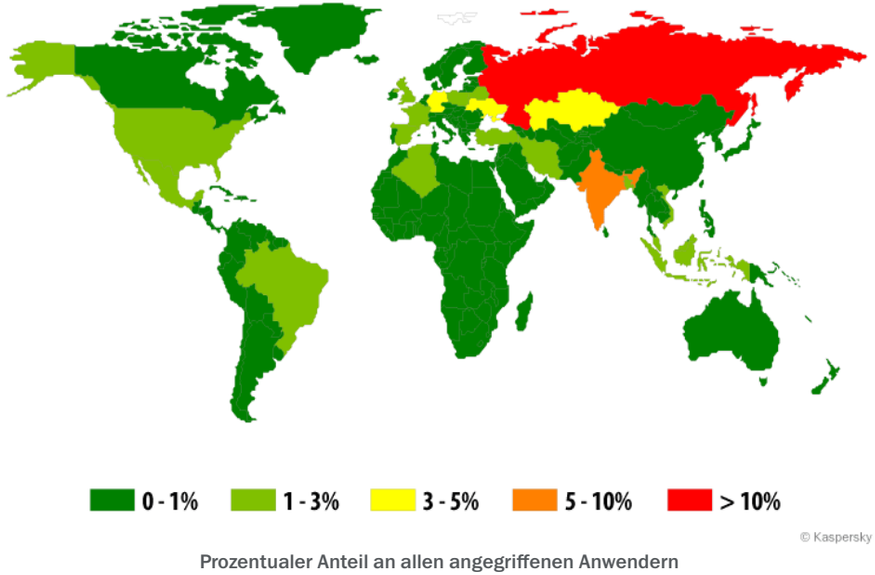
Die Lösungen von Kaspersky Lab wehrten in der Zeit von November 2013 bis Ende Oktober 2014 insgesamt **1.363.549** individuelle Attacken ab. In dem entsprechenden Zeitraum der Jahre 2012 und 2013 wurden **335.000** individuelle Attacken abgewehrt. Somit hat sich die Zahl der Angriffe auf Android-Geräte vervierfacht.

Im Laufe des Jahres wurden **19 Prozent** der Android-User zumindest einmal mit mobilen Bedrohungen konfrontiert – das ist praktisch jeder Fünfte.

Bei **53 Prozent** der Android Attacken wurden mobile Trojaner verwendet, die auf den Diebstahl von finanziellen Mitteln der Anwender spezialisiert sind (SMS-Trojaner, Bank-Trojaner).

GEOGRAFIE DER MOBILEN TROJANER

Angriffe durch mobile Malware wurden in mehr als 200 Ländern der Welt registriert.



Prozentualer Anteil an allen angegriffenen Anwendern

TOP 10 DER LÄNDER NACH ZAHL DER ANGEGRIFFENEN ANWENDER

	LAND	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER*
1	**Russland**	45,7 %
2	**Indien**	6,8 %
3	**Kasachstan**	4,1 %
4	**Deutschland**	4,0 %
5	**Ukraine**	3,0 %
6	**Vietnam**	2,7 %
7	**Iran**	2,3 %
8	**Großbritannien**	2,2 %
9	**Malaysia**	1,8 %
10	**Brasilien**	1,6 %

*Prozentualer Anteil der im jeweiligen Land angegriffenen Anwender an allen angegriffenen Anwendern.

Russland behauptet sich auf der Spitzenposition nach Anzahl der angegriffenen Anwender.

Die Zahl der registrierten Attacken hängt zum großen Teil von der Gesamtzahl der Anwender im jeweiligen Land ab. Um die Gefahr einer Infektion durch mobile Schädlinge in den verschiedenen Ländern einschätzen zu können, haben wir berechnet, wie viel Prozent die Schadprogramme an allen Programmen ausmachen, die die Anwender zu installieren versuchen. Das Länder-Rating nach diesem Wert unterscheidet sich von dem oben aufgeführten Rating.

TOP 10 DER LÄNDER NACH INFEKTIONSRISIKO

	LAND*	PROZENTUALER ANTEIL DER SCHÄDLICHEN ANWENDUNGEN
1	**Vietnam**	2,34 %
2	**Polen**	1,88 %
3	**Griechenland**	1,70 %
4	**Kasachstan**	1,62 %
5	**Usbekistan**	1,29 %
6	**Serbien**	1,23 %
7	**Armenien**	1,21 %
8	**Tschechien**	1,02 %
9	**Marokko**	0,97 %
10	**Malaysia**	0,93 %

*Aus unseren Berechnungen haben wir die Länder ausgeschlossen, in denen die Zahl der Programm-Downloads unter 100.000 lag.

An der Spitze dieses Ratings steht Vietnam: Von allen Anwendungen, die die Nutzer zu installieren versuchten, entfielen in diesem Land **2,34 Prozent** auf Schadprogramme.

Russland, das nach Anzahl der Angriffe mit großem Abstand vor allen anderen Ländern an der Spitze steht, liegt in dem Rating nach Infektionsrisiko auf **Position 22**, mit einem Wert von **0,69** Prozent.

In Spanien beträgt das Infektionsrisiko **0,54** Prozent, in Deutschland **0,18 Prozent**, in Großbritannien **0,16** Prozent, in Italien **0,09** Prozent und in den USA sind es **0,07 Prozent**. Am besten ist diesbezüglich die Situation in Japan, wo die schädlichen Anwendungen einen Anteil von nur **0,01** Prozent an allen Anwendungen haben, die die Nutzer zu installieren versuchten.

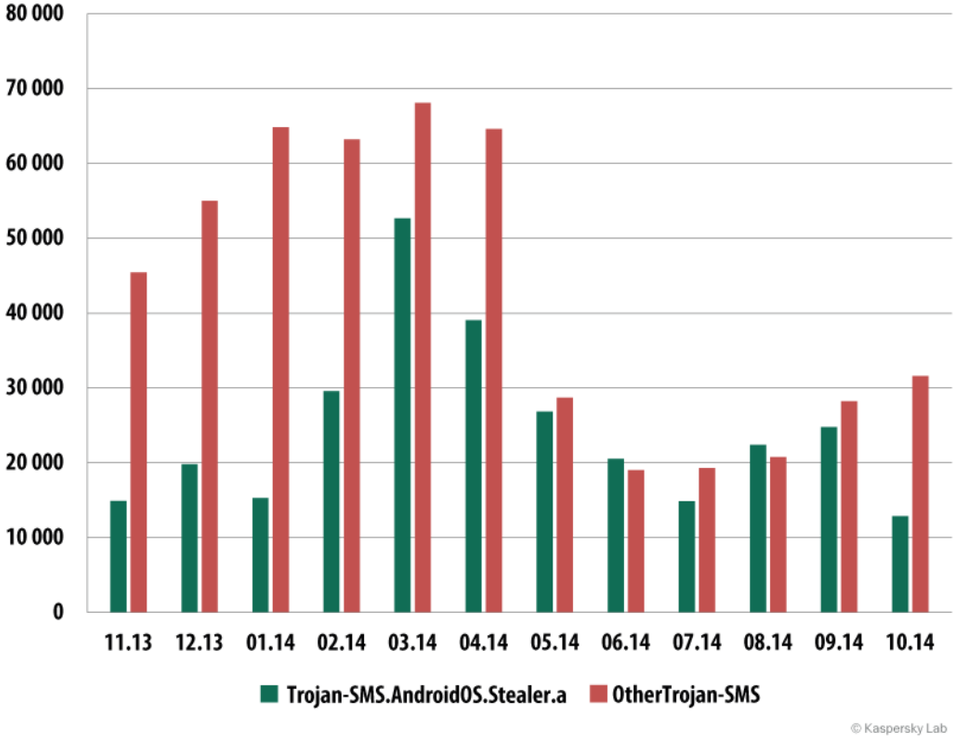
TOP 20 DER MOBILEN BEDROHUNGEN 2014

	NAME	PROZENTUALER ANTEIL AN DEN ATTACKEN
1	**Trojan-SMS.AndroidOS.Stealer.a**	18,0 %
2	**RiskTool.AndroidOS.MimobSMS.a**	7,1 %
3	**DangerousObject.Multi.Generic**	6,9 %
4	**RiskTool.AndroidOS.SMSreg.gc**	6,7 %
5	**Trojan-SMS.AndroidOS.OpFake.bo**	6,4 %
6	**AdWare.AndroidOS.Viser.a**	5,9 %
7	**Trojan-SMS.AndroidOS.FakeInst.a**	5,4 %
8	**Trojan-SMS.AndroidOS.OpFake.a**	5,1 %
9	**Trojan-SMS.AndroidOS.FakeInst.fb**	4,6 %
10	**Trojan-SMS.AndroidOS.Erop.a**	4,0 %
11	**AdWare.AndroidOS.Ganlet.a**	3,8 %
12	**Trojan-SMS.AndroidOS.Agent.u**	3,4 %
13	**Trojan-SMS.AndroidOS.FakeInst.ff**	3,0 %
14	**RiskTool.AndroidOS.Mobogen.a**	3,0 %
15	**RiskTool.AndroidOS.CallPay.a**	2,9 %
16	**Trojan-SMS.AndroidOS.Agent.ao**	2,5 %
17	**Exploit.AndroidOS.Lotoor.be**	2,5 %
18	**Trojan-SMS.AndroidOS.FakeInst.ei**	2,4 %
19	**Backdoor.AndroidOS.Fobus.a**	1,9 %
20	**Trojan-Banker.AndroidOS.Faketoken.a**	1,7 %

Bei zehn von 20 Programmen aus diesem Rating handelt es sich um SMS-Trojaner der Familien Stealer, OpFake, FakeInst, Agent und Erop.

Im Verlauf des gesamten Jahres belegte Trojan-SMS.AndroidOS.Stealer.a die Führungsposition unter allen mobilen Schadprogramm-Familien. Auch nach den Ergebnissen des Jahres steht dieser Trojaner an der Spitze des Ratings.

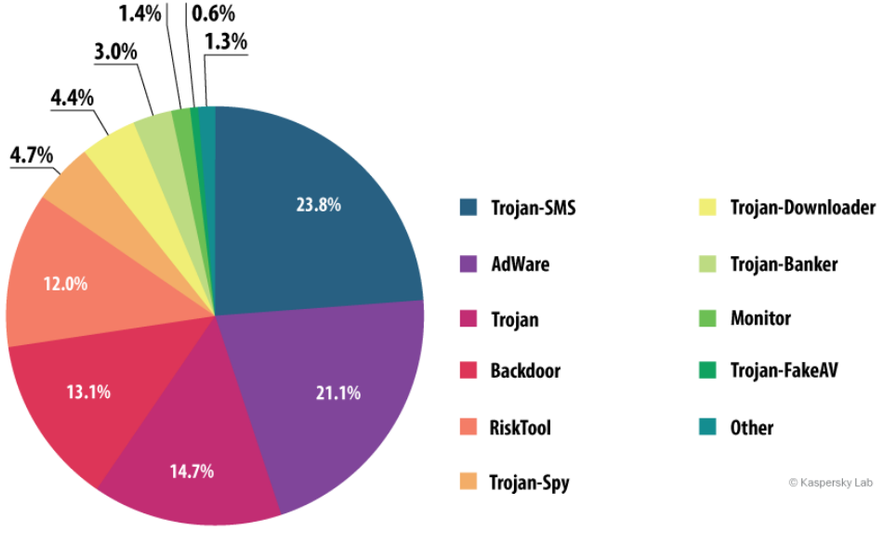
Dieser SMS-Trojaner hat sich überaus aktiv verbreitet. Seit Mai 2014 ist die Zahl der Stealer-Attacken ähnlich hoch wie die Zahl aller anderen Attacken unter Verwendung anderer verbreiteter SMS-Trojaner.



Anzahl der Anwender, die von Trojan-SMS.AndroidOS.Stealer.a angegriffen wurden, gegenüber den von allen anderen SMS-Trojanern angegriffenen Nutzern (November 2013 bis Oktober 2014)

SMS-TROJANER: RÜCKGANG DER ATTACKEN

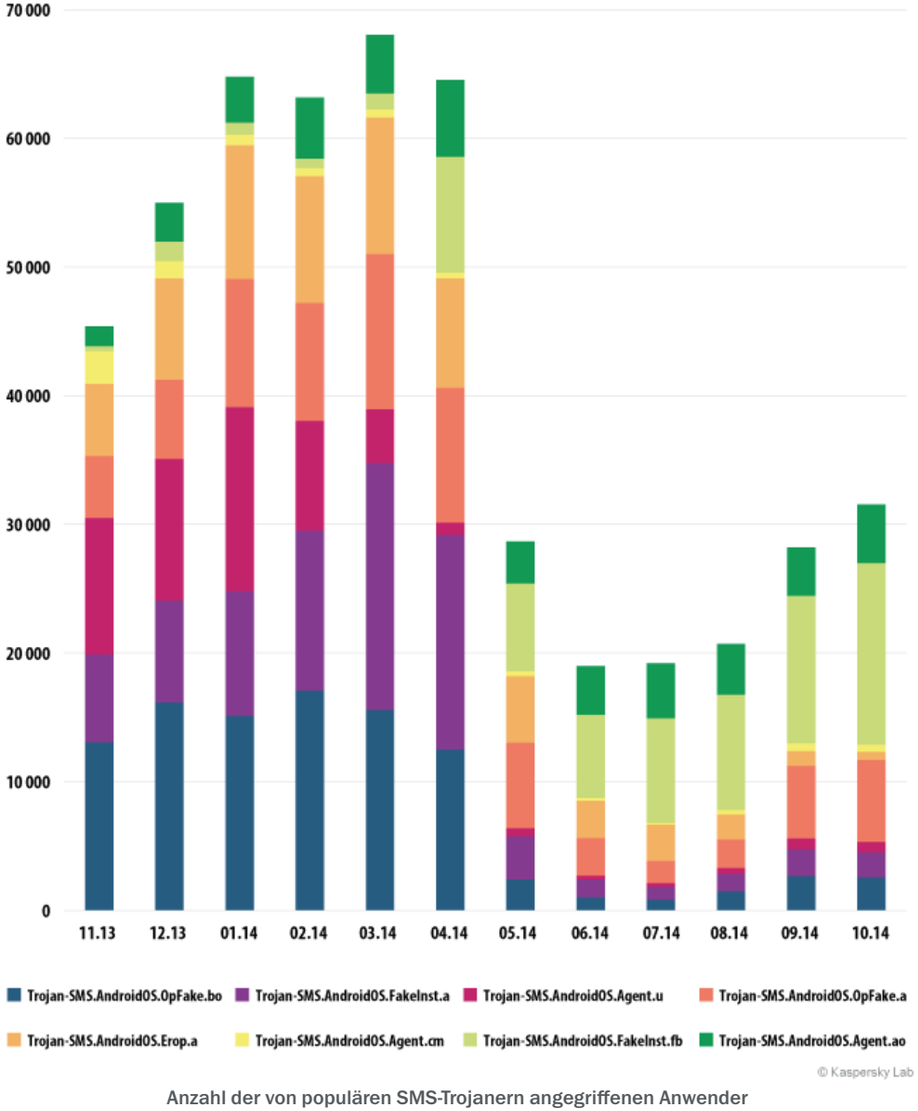
Die SMS-Trojaner dominieren nach wie vor den allgemeinen Strom der mobilen Malware – in unserer Kollektion entfallen darauf **23,8 Prozent**.



Verteilung mobiler Bedrohungen nach Typen (Malware-Kollektion Kaspersky Lab)

Wie auf dem oben stehenden Diagramm zur Angriffsdynamik allerdings zu erkennen ist, ging die Zahl der Angriffe unter Verwendung von SMS-Trojanern im zweiten Halbjahr 2014 insgesamt zurück. Das hatte zur Folge, dass der Wert dieser Kategorie um **12,3 Prozentpunkte** abnahm.

Werfen wir nun einen genaueren Blick auf die Verbreitungsdynamik der unter Cyberkriminellen beliebtesten SMS-Trojaner (mit Ausnahme von Stealer.a).



Anzahl der von populären SMS-Trojanern angegriffenen Anwender
(November 2013 bis Oktober 2014)

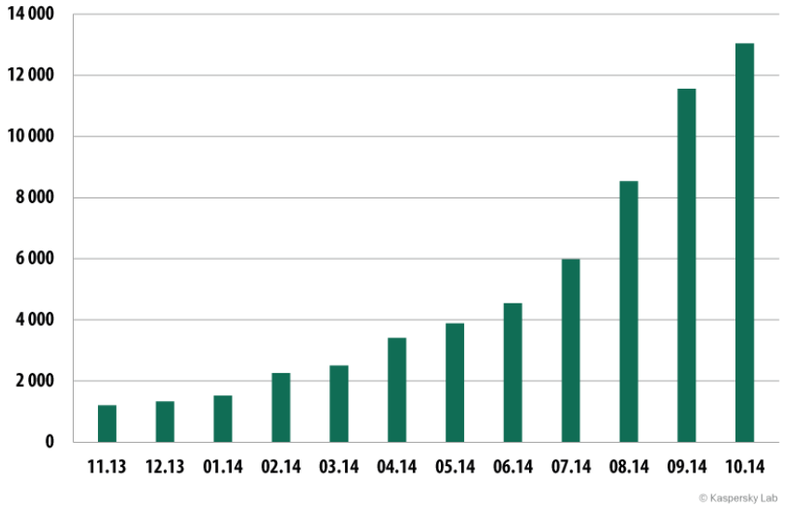
Die auffallende Abnahme der Zahl der SMS-Trojaner im Mai hängt mit der veränderten Situation bezüglich kostenpflichtiger Nachrichten in Russland zusammen, wo Attacken unter Einsatz von SMS-Trojanern bei Online-Kriminellen besonders beliebt sind. Seit Mai 2014 sind die Mobilfunkbetreiber in Russland verpflichtet, das Leistungsmerkmal Advice of Charge (AoC) zu nutzen: Wenn jetzt von einem mobilen Gerät eine Mitteilung an eine kostenpflichtige Nummer geschickt wird, muss der Betreiber den Inhaber des Geräts über die dafür anfallenden Kosten informieren, der dann die Zahlung bestätigen muss.

Das hat zur Folge, dass das Geschäft mit den SMS-Trojanern nun weniger gewinnträchtig und zudem eindeutig kriminell ist. Um nun noch einen Gewinn zu erzielen, müssen die Cyberkriminellen Trojaner verwenden, die SMS an kostenpflichtige Nummern senden. Die Trojaner fangen die Mitteilung des Mobilfunkbetreibers ab und senden im Namen des Nutzers eine Bestätigung an den Betreiber. Als Konsequenz haben sich einige halblegale Partnerprogramme aus diesem Geschäft zurückgezogen, die vorher dort mit der Funktionalität von SMS-Trojanern präparierte Anwendungen verbreitet haben. Bei Programmen sind die Bedingungen für das Ablehnen kostenpflichtiger Dienstleistungen nur schwach festgeschrieben oder die Preise für ein Abonnement oder eine Dienstleistung werden überhaupt nicht genannt.

Es ist anzunehmen, dass die somit beschäftigungslos gewordenen russischen Entwickler von SMS-Trojanern nun gezwungen sind, sich neue Betätigungsfelder und Einnahmequellen zu suchen. Einige von ihnen könnten sich auf Cyberangriffe auf Anwender in anderen Ländern verlegen, andere auf ernsthaftere Schadprogramme wie etwa mobile Bank-Trojaner. Bleibt zu hoffen, dass es auch solche Entwickler gibt, die kein Risiko mehr eingehen wollen und sich einer legalen Tätigkeit zuwenden.
Die Veränderungen in der Verbreitungsdynamik sind sehr schön zu erkennen an dem Beispiel der (unter Cyberkriminellen) so populären SMS-Trojaner wie OpFake.bo, FakeInst.a und OpFake.a. Ihre Werte gingen von **10.000 bis 20.000** angegriffenen Nutzern im Monat auf **1.000 bis 2.000** zurück.

MOBILE BANK-TROJANER

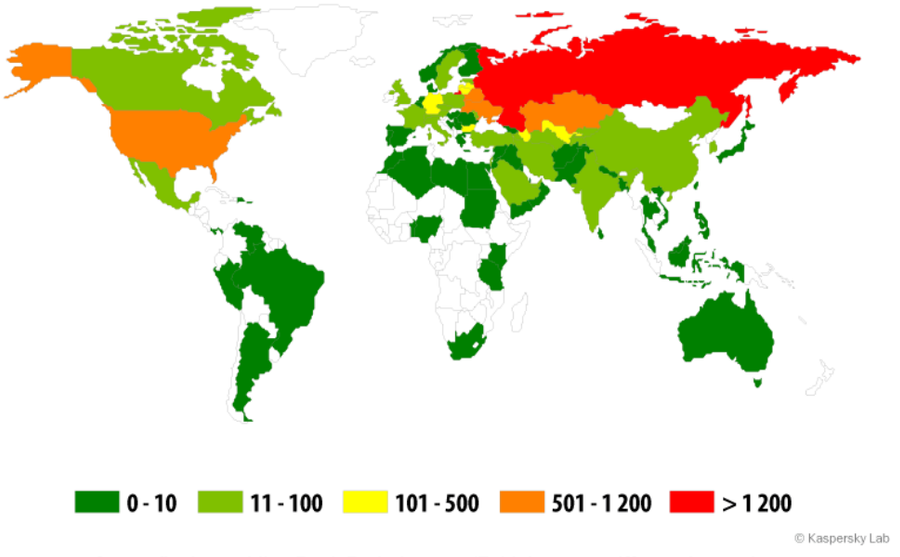
Im Berichtszeitraum entdeckte Kaspersky Lab **12.100** mobile Bank-Trojaner. Das sind neunmal mehr als im Jahr 2013.



Zahl mobiler Bank-Trojaner in der Malware-Kollektion von Kaspersky Lab (November 2013 bis Oktober 2014)

Im Laufe des Jahres wurden **45.032** Anwender mindestens einmal von mobilen Trojanern angegriffen.

Die Zahl der angegriffenen Länder nimmt zu: Attacken mobiler Bank-Trojaner wurden im Laufe eines Jahres mindestens einmal in **90** Ländern der Welt registriert.



Geografie der mobilen Bank-Bedrohungen (Zahl der angegriffenen Anwender in der Zeit von November 2013 bis Oktober 2014)

TOP 10 DER VON BANK-TROJANERN ANGEGRIFFENEN LÄNDER

	LAND	ZAHL DER ANGEGRIFFENEN ANWENDER	PROZENTUALER ANTEIL AN ALLEN ATTACKEN*
1	**Russland**	39 561	87,85 %
2	**Kasachstan**	1 195	2,65 %
3	**Ukraine**	902	2,00 %
4	**USA**	831	1,85 %
5	**Weißrussland**	567	1,26 %
6	**Deutschland**	203	0,45 %
7	**Litauen**	201	0,45 %
8	**Aserbaidschan**	194	0,43 %
9	**Bulgarien**	178	0,40 %
10	**Usbekistan**	125	0,28 %

*Prozentualer Anteil der im jeweiligen Land angegriffenen Anwender an allen angegriffenen Anwendern.

Traditioneller Spitzenreiter in diesem Rating ist und bleibt Russland.

BEDROHUNGEN FÜR MAC OS X

Im Jahr 2014 blockierten die Lösungen von Kaspersky Lab insgesamt **3.693.936** Infektionsversuche unter Mac OS X.
Die Experten von Kaspersky Lab entdeckten **1.499** neue Schadprogramme für Mac OS X, das sind **200** Schädlinge weniger als im entsprechenden Vorjahreszeitraum.

Jeder zweite Anwender von Apple-Produkten war einem Angriff ausgesetzt.
Im Laufe des Jahres war jeder Mac-OS-X-User durchschnittlich **neunmal** mit einer Cyberbedrohung für sein Betriebssystem konfrontiert.

TOP 20 DER BEDROHUNGEN FÜR MAC OS X

	NAME	PROZENTUALER ANTEIL DER ATTACKEN*
1	**AdWare.OSX.Geonei.b**	9,04 %
2	**Trojan.Script.Generic**	5,85 %
3	**Trojan.OSX.Vsrch.a**	4,42 %
4	**Trojan.Script.Iframer**	3,77 %
5	**AdWare.OSX.Geonei.d**	3,43 %
6	**DangerousObject.Multi.Generic**	2,40 %
7	**AdWare.OSX.Vsrch.a**	2,18 %
8	**Trojan.Win32.Generic**	2,09 %
9	**AdWare.OSX.FkCodec.b**	1,35 %
10	**Trojan.OSX.Yontoo.i**	1,29 %
11	**Trojan-PSW.Win32.LdPinch.ex**	0,84 %
12	**AdWare.Win32.Yotoon.heur**	0,82 %
13	**Trojan.OSX.Yontoo.j**	0,80 %
14	**Exploit.Script.Generic**	0,76 %
15	**AdWare.OSX.Bnodlero.a**	0,58 %
16	**AdWare.JS.Agent.an**	0,57 %
17	**Trojan.OSX.Yontoo.h**	0,52 %
18	**Exploit.PDF.Generic**	0,51%
19	**AdWare.Win32.MegaSearch.am**	0,50 %
20	**Trojan.Win32.AutoRun.gen**	0,43 %

*Prozentualer Anteil der von dem jeweiligen Schädling angegriffenen Anwender an allen angegriffenen Anwendern.

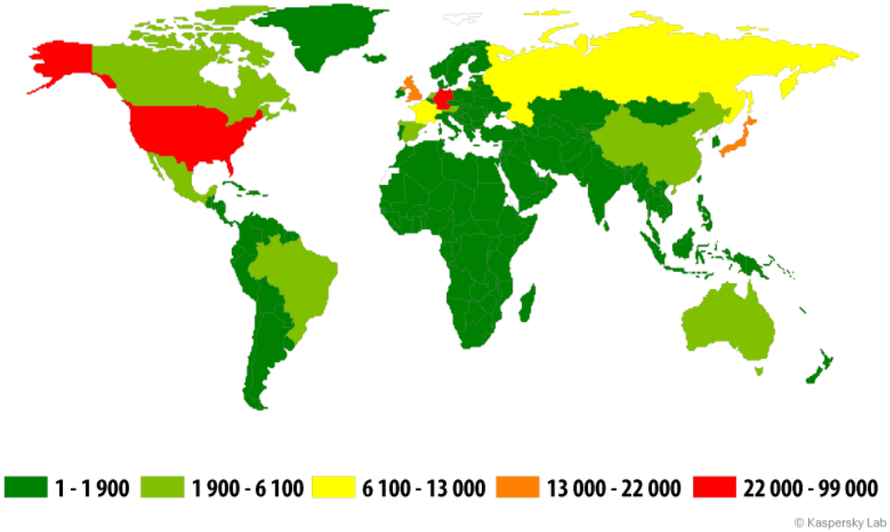
Praktisch die Hälfte aller Positionen in unseren Top 20, Platz eins eingeschlossen, werden von Werbeprogrammen besetzt (AdWare). In der Regel gelangen solche Schädlinge zusammen mit einem legalen Programm auf den Computer des Anwenders, wenn dieses nicht von der offiziellen Webseite des Herstellers, sondern von einer Drittanbieter-Webseite geladen wurde. Zusammen mit dem Programm wird ein AdWare-Modul auf dem Rechner installiert, das unter anderem Werbelinks und Browser-Tabs hinzufügen, das standardmäßig eingestellte Suchsysteme verändern sowie Kontextwerbung anzeigen kann.

Interessant ist, dass sich auf dem achten Platz der Schädling Trojan.Win32.Generic platzierte, der auf Windows-Betriebssystemen läuft. Vermutlich geht es hier um das Eindringen in die virtuelle Maschine, auf der Windows installiert ist.

Im Laufe des Jahres 2014 entdeckten die Experten von Kaspersky Lab verschiedene interessante Schädlinge für Mac OS X, über die es sich lohnt, gesondert zu berichten.

- **Backdoor.OSX.Callme.** Die Backdoor stellt Cyberkriminellen entfernten Zugriff auf das System zur Verfügung und stiehlt gleichzeitig die Kontaktliste des Anwenders, vermutlich zur Suche neuer Opfer. Der Schädling wird über ein speziell konstruiertes Word-Dokument verbreitet, das beim Start die Backdoor über eine Sicherheitslücke im System installiert.
- **Backdoor.OSX.Laoshu.** Der Schädling erstellt im Minutentakt Screenshots des Bildschirms. Diese Backdoor ist mit einem vertrauenswürdigen Zertifikat signiert, daher ist anzunehmen, dass sie die Entwickler im Apple App Store unterbringen wollten.
- **Backdoor.OSX.Ventir.** Ein multimodularer Spionage-Trojaner mit der Funktion zur verborgenen Fernsteuerung. Backdoor.OSX.Ventir enthält den Treiber „logkext" zum Abfangen der Tastatureingaben, dessen Quellcode öffentlich zugänglich ist.
- **Trojan.OSX.IOSinfector.** Ein Installer der mobilen Version Trojan-Spy.IPhoneOS.Mekir (OSX/Crisis).
- **Trojan-Ransom.OSX.FileCoder.** Der erste Dateiverschlüsseler unter Mac OS X. Ein bedingt funktionierender Prototyp, dessen Autor aus irgendwelchen Gründen beschlossen hat, den Schädling nicht weiterzuentwickeln.
- **Trojan-Spy.OSX.CoinStealer.** Der erste Bitcoin-Dieb für Mac OS X, der sich als verschiedene Bitcoin-Tools mit offenem Quellcode tarnt. Tatsächlich installiert er eine schädliche Browsererweiterung und/oder die gepatchte Variante bitcoin-qt.
- **Trojan-Downloader.OSX.WireLurker.** Ungewöhnlicher Schädling, der Daten stiehlt. Er greift nicht nur Mac-Computer an, sondern auch daran angeschlossene iOS-Geräte. Es gibt auch eine Windows-Version des Schädlings. Der Trojaner wird über einen bekannten chinesischen App-Shop für Mac OS X und iOS verbreitet.

GEOGRAFIE DER BEDROHUNGEN



Geografie der Angriffe auf Nutzer von Mac OS X im Jahr 2014
(nach Anzahl der angegriffenen Anwender)

Cyberthreat-Map

TOP 10 DER ANGEGRIFFENEN LÄNDER

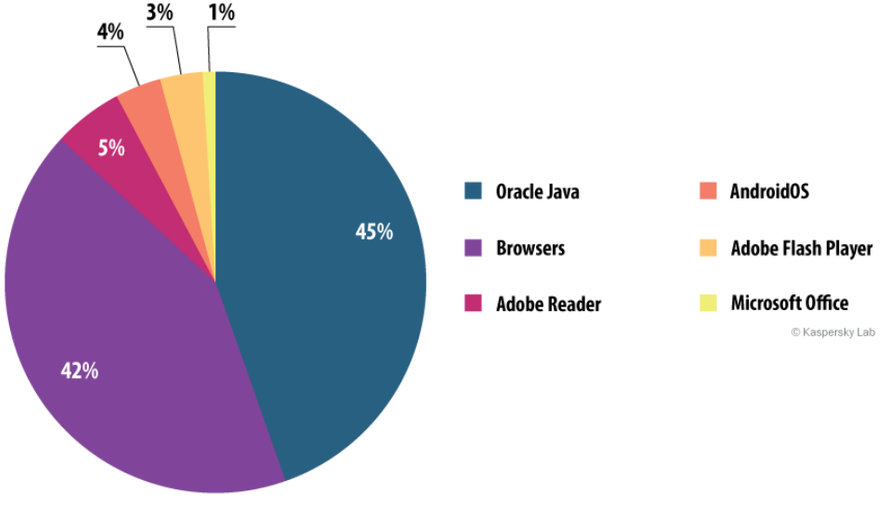
	LAND	ZAHL DER ANGEGRIFFENEN ANWENDER	PROZENTUALER ANTEIL DER ATTACKEN*
1	**USA**	98.077	39,14 %
2	**Deutschland**	31.466	12,56 %
3	**Japan**	13.808	5,51 %
4	**Großbritannien**	13.763	5,49 %
5	**Russische Föderation**	12.207	4,87 %
6	**Frankreich**	9.239	3,69 %
7	**Schweiz**	6.548	2,61 %
8	**Kanada**	5.841	2,33 %
9	**Brasilien**	5.558	2,22 %
10	**Italien**	5.334	2,13 %

* Prozentualer Anteil der im jeweiligen Land angegriffenen Anwender an allen angegriffenen Anwendern.

Auf Platz eins unseres Ratings positionierten sich die **USA** (39,14 Prozent), wobei sich ein Großteil der Angriffe auf die Einwohner dieses Landes mit der großen Popularität von Apple in den Vereinigten Staaten erklären lässt. Den zweiten Platz besetzt **Deutschland** (12,56 Prozent), den dritten **Japan** (5,51 Prozent).

VON CYBERKRIMINELLEN AUSGENUTZTE ANGREIFBARE ANWENDUNGEN

Das unten aufgeführte 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.



Verteilung der in Attacken von Cyberkriminellen verwendeten Exploits nach Typen der angegriffenen Anwendungen, Jahr 2014

Am häufigsten versuchten Cyberkriminelle im Jahr 2014, Sicherheitslücken in Oracle Java auszunutzen. Im Vergleich zum Vorjahr hat sich der Anteil dieser Anwendung allerdings halbiert, und zwar von **90,5** auf **45 Prozent**. Wir registrierten einen Rückgang der Popularität von Java-Sicherheitslücken über das gesamte Jahr 2014. Vermutlich hat das mit dem Schließen alter Sicherheitslücken und dem Mangel an Informationen über neue Schwachstellen in dieser Anwendung zu tun.

Den zweiten Platz in unserem Rating belegte die Kategorie „Browser“ (**42 Prozent**). Sie umfasst Exploits für den Internet Explorer, Google Chrome, Mozilla Firefox und andere. Im Jahr 2014 belegte diese Kategorie nach der Summe der Werte der letzten drei Quartale die Führungsposition, konnte den Spitzenreiter für den gesamten Berichtszeitraum allerdings nicht einholen, da es Ende 2013 bis Anfang 2014 sehr viele Java-Exploits gab.

Auf dem dritten Platz positionierten sich Exploits für Sicherheitslücken im Adobe Reader (5 Prozent). Solche Sicherheitslücken werden im Rahmen von Drive-by-Attacken über das Internet ausgenutzt, und PDF-Exploits gehören zur Grundausstattung einer Vielzahl von Exploit-Packs.

Im Laufe des Jahres beobachteten wir einen Rückgang der Angriffe unter Verwendung von Exploit-Packs. Dafür könnte es gleich mehrere Gründe geben, insbesondere die Verhaftungen mehrerer Entwickler von Exploit-Packs. Außerdem haben viele Exploit-Packs die Angriffe auf Computer eingestellt, die von Kaspersky-Lab-Produkten geschützt werden (die Exploit-Packs überprüfen den zu attackierenden Computer und brechen den Angriff ab, wenn auf ihm eine Kaspersky-Lab-Lösung läuft). Trotz der hier aufgezählten Faktoren ist und bleibt die Ausnutzung von Sicherheitslücken eine der wichtigsten Methoden, Malware auf den Computer des Anwenders zu transportieren.

SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)

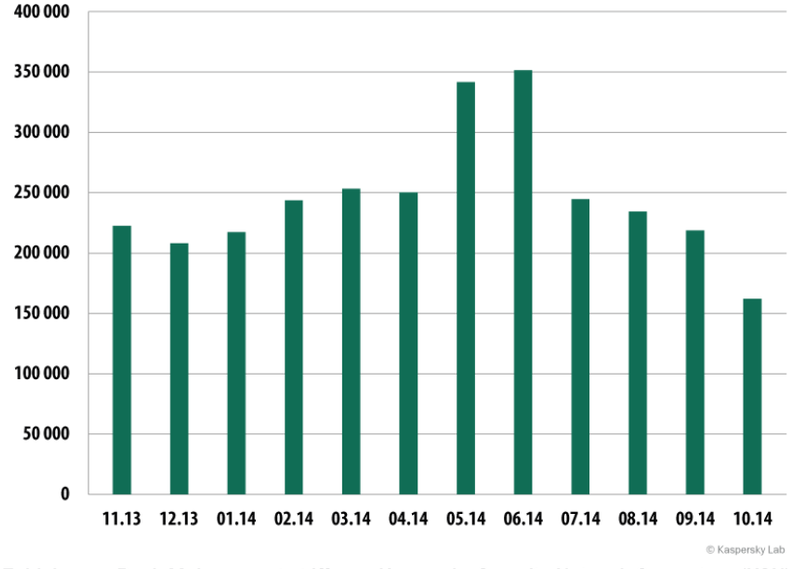
Die statistischen Daten in diesem Abschnitt basieren auf dem Modul Kaspersky Anti-Virus, das Windows-Nutzer in dem Moment schützt, in dem Schadcode von einer schädlichen oder infizierten Webseite geladen wird. Schädliche Webseiten werden von Cyberkriminellen speziell zu diesem Zweck erstellt. Infiziert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

Im Jahr 2014 betrug die Zahl der Attacken, die von Internet-Ressourcen in verschiedenen Ländern der Welt ausgingen, insgesamt **1.432.660.467**. Das heißt, die Produkte von Kaspersky Lab schützten die Anwender beim Surfen im Netz durchschnittlich **3.925.097-Mal** pro Tag.

Die wichtigste Angriffsmethode ist die mit Hilfe von Exploit-Packs. Sie gibt Cyberkriminellen praktisch die Garantie, Computer infizieren zu können, auf denen kein Schutzprogramm läuft und zumindest eine populäre und angreifbare (nicht aktualisierte) Anwendung installiert ist.

ONLINE-BEDROHUNGEN IM BANKENSEKTOR

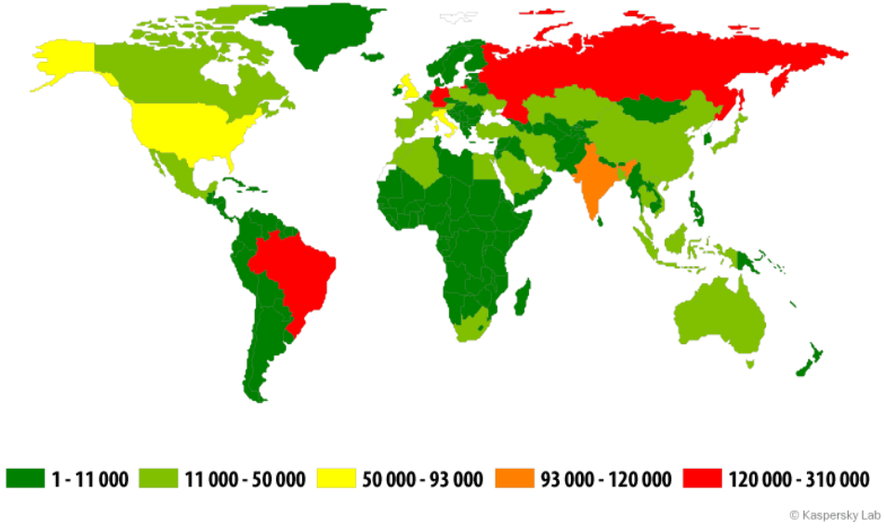
Innerhalb des Berichtszeitraums wehrten die Lösungen von Kaspersky Lab auf den Computern von **1.910.520** Anwendern Versuche ab, schädliche Software zu starten, die auf den Diebstahl von Geld via Online-Zugriff auf Bankkonten spezialisiert ist.



Zahl der von Bank-Malware angegriffenen Kaspersky-Security-Network-Computern (KSN), November 2013 bis Oktober 2014

Auffallend ist die extreme Zunahme der Angriffe im Mai und Juni 2014. Diese Tatsache hängt mit dem Beginn der Urlaubssaison zusammen, wenn die finanzielle Aktivität der Online-Banking-Nutzer steigt, sowie mit dem wichtigsten Sportereignis des Jahres 2014 – der Fußball-Weltmeisterschaft in Brasilien. Während der WM setzten Cyberkriminelle Finanz-Malware ein, um die Finanzmittel der Touristen zu stehlen.

Insgesamt erfassten die Schutzlösungen von Kaspersky Lab **16.552.498** Benachrichtigungen über Infektionsversuche durch Schadprogramme, die für den Diebstahl von Finanzmitteln via Online-Zugriff auf Bankkonten vorgesehen sind.



Geografie der Angriffe von Bank-Malware im Jahr 2014

TOP 10 DER LÄNDER NACH ZAHL DER ANGEGRIFFENEN ANWENDER

	LAND	ZAHL DER ANGEGRIFFENEN ANWENDER
1	**Brasilien**	299.830
2	**Russische Föderation**	251.917
3	**Deutschland**	155.773
4	**Indien**	98.344
5	**USA**	92.224
6	**Italien**	88.756
7	**Großbritannien**	54.618
8	**Vietnam**	50.040
9	**Österreich**	44.445
10	**Algerien**	33.640

TOP 10 DER FINANZ-MALWARE-FAMILIEN

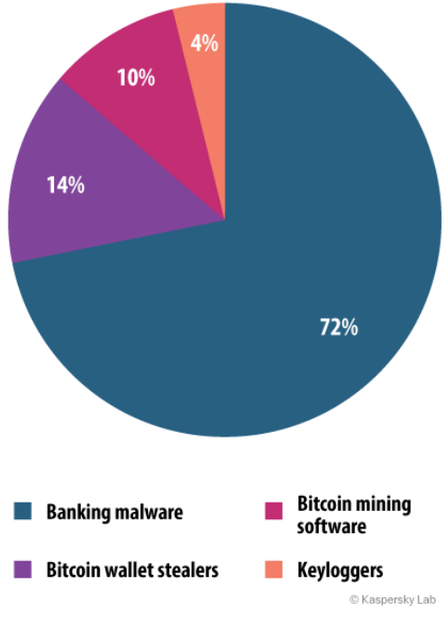
	NAME	ANZAHL DER ANGEGRIFFENEN ANWENDER
1	**Trojan-Spy.Win32.Zbot**	742.794
2	**Trojan-Banker.Win32.ChePro**	192.229
3	**Trojan-Banker.Win32.Lohmys**	121.439
4	**Trojan-Banker.Win32.Shiotob**	95.236
5	**Trojan-Banker.Win32.Agent**	83.243
6	**Trojan-Banker.AndroidOS.Faketoken**	50.334
7	**Trojan-Banker.Win32.Banker**	41.665
8	**Trojan-Banker.Win32.Banbra**	40.836
9	**Trojan-Spy.Win32.SpyEyes**	36.065
10	**Trojan-Banker.HTML.Agent**	19.770

Der am weitesten verbreitete Bank-Trojaner bleibt ZeuS (Trojan-Spy.Win32.Zbot). Im Laufe des Jahres führte der Schädling die Quartalsstatistiken an. Daher ist es nicht verwunderlich, dass er auf das gesamte Jahr gesehen ebenfalls den ersten Platz in unseren Top 10 einnimmt. Position zwei belegt Trojan-Banker.Win32.ChePro und Position drei Trojan-Banker.Win32.Lohmys. Beide Familien verfügen über dieselbe Funktionalität und werden mittels Spam-Mails verbreitet, deren Betreff sich immer auf das Online-Banking bezieht (beispielsweise „Online-Banking-Konto“). In der E-Mail befindet sich ein Word-Dokument mit integriertem Bild, das – wenn man darauf klickt – schädlichen Code ausführt.

Der Bank-Trojaner Trojan-Banker.Win32.Shiotob belegt den vierten Platz. Er überwacht den Traffic mit dem Ziel, Bezahldaten abzufangen und verbreitet sich – wie viele andere Schädlinge auch – in erster Linie mittels Spam-Mitteilungen.

Die überwiegende Mehrheit der Schädlinge aus den Top 10 schleust willkürlichen HTML-Code in die im Browser dargestellte Webseite ein und fängt die Bezahldaten ab, die der Anwender in originale und gefälschte Webformulare eingibt.

Obwohl im Jahr 2014 fast drei Viertel der Angriffe, die es auf das Geld der Anwender abgesehen hatten, mit Hilfe von Bank-Malware umgesetzt wurden, sind die finanziellen Bedrohungen nicht allein darauf beschränkt.



Verteilung der Schädlinge, die es im Jahr 2014 auf das Geld der Anwender abgesehen haben, sortiert nach Malware-Typen

Das unter Cyberkriminellen zweitbeliebteste Online-Delikt ist der Diebstahl von Bitcoin-Wallets (14 Prozent). Es folgt eine weitere Bedrohung, die mit Kryptowährung in Zusammenhang steht, und zwar die Infektion eines Computers mit dem Ziel, ihn zur Generierung von Bitcoins zu verwenden, sprich Bitcoin-Mining (10 Prozent).

TOP 20 DER SCHADPROGRAMME IM INTERNET

Im Laufe des gesamten Jahres erkannte Kaspersky Anti-Virus **123.054.503** individuelle schädliche Bedrohungen (zum Beispiel Skripte, Exploits und ausführbare Dateien).

Von allen Schadprogrammen, die an Internet-Attacken beteiligt waren, hat das Kaspersky-Team nachfolgend die 20 aktivsten aufgeführt. Auf sie entfielen **95,8 Prozent** aller Web-Attacken.

	NAME*	PROZENTUALER ANTEIL AN ALLEN ATTACKEN**
1	**Malicious URL**	73,70 %
2	**Trojan.Script.Generic**	9,10 %
3	**AdWare.Script.Generic**	4,75 %
4	**Trojan.Script.Iframer**	2,12 %
5	**Trojan-Downloader.Script.Generic**	2,10 %
6	**AdWare.Win32.BetterSurf.b**	0,60 %
7	**AdWare.Win32.Agent.fflm**	0,41 %
8	**AdWare.Win32.Agent.aiyc**	0,38 %
9	**AdWare.Win32.Agent.allm**	0,34 %
10	**Adware.Win32.Amonetize.heur**	0,32 %
11	**Trojan.Win32.Generic**	0,27 %
12	**AdWare.Win32.MegaSearch.am**	0,26 %
13	**Trojan.Win32.AntiFW.b**	0,24 %
14	**AdWare.JS.Agent.an**	0,23 %
15	**AdWare.Win32.Agent.ahbx**	0,19 %
16	**AdWare.Win32.Yotoon.heur**	0,19 %
17	**AdWare.JS.Agent.ao**	0,18 %
18	**Trojan-Downloader.Win32.Generic**	0,16 %
19	**Trojan-Clicker.JS.Agent.im**	0,14 %
20	**AdWare.Win32.OutBrowse.g**	0,11 %

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

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

Wie gehabt sind in den Top 20 schädliche Objekte vertreten, die bei Drive-by-Attacken eingesetzt werden, sowie Werbeprogramme und Links aus der Schwarzen Liste (erster Platz mit **73,7 Prozent**). Gegenüber dem Vorjahr ist die Zahl der Positionen im Ranking gestiegen, die von Werbeprogrammen belegt werden, und zwar von fünf auf zwölf. Auf die Werbeprogramme in den Top 20 entfielen **8,2 Prozent**, das sind 7,01 Prozentpunkte mehr als im Jahr 2013. Die Zunahme der Werbeprogramme, ihre aggressive Verbreitungsart und ihre Mechanismen zur Abwehr der Erkennung durch Antivirenprogramme definieren den Trend des Jahres 2014.

Trojan-Clicker.JS.Agent.im steht ebenfalls im Zusammenhang mit Werbung und allerlei anderen „potenziell unerwünschten" Aktivitäten. So fand das Kaspersky-Team beispielsweise Skript-Redirectoren auf den Amazon-Dienst Cloudfront, welche die Anwender auch auf Seiten mit Werbung umleiten. Links auf diese Skripte werden von Werbeprogrammen und unterschiedlichen Browser-Erweiterungen meistens auf Seiten platziert, auf denen Anwender Suchanfragen eingeben. Die Skripte können die Anwender auch auf schädliche Seiten umleiten, auf denen Empfehlungen platziert sind, Adobe Flash und Java zu aktualisieren – das ist eine unter Cyberkriminellen beliebte Methode, Schadprogramme zu verbreiten.

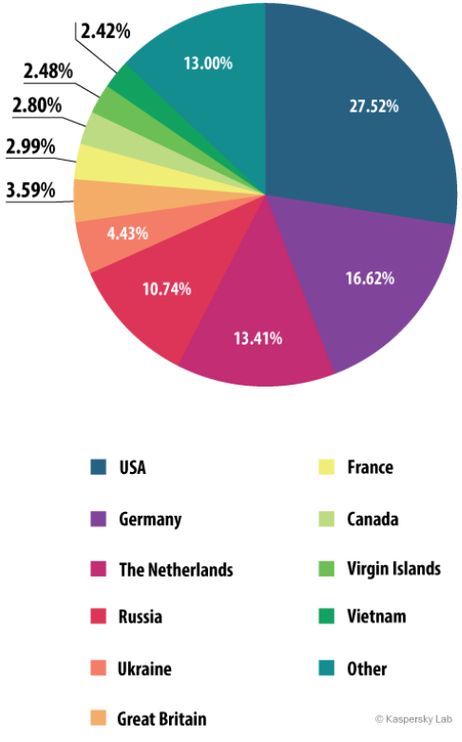
TOP 10 DER LÄNDER, AUF DEREN RESSOURCEN SCHADPROGRAMME UNTERGEBRACHT SIND

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.

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 **1.432.660.467** Attacken über das Internet verwendeten die Cyberkriminellen **9.766.119** individuelle Hosts, das sind **838.154** (rund acht Prozentpunkte) weniger als im Jahr 2013.

Insgesamt **87 Prozent** der Benachrichtigungen über die Blockierung von Attacken entfielen auf Angriffe von Webressourcen, die sich in insgesamt zehn Ländern der Welt befinden – das sind fünf Prozentpunkte mehr als im Jahr 2013.



Verteilung der Quellen von Webattacken nach Ländern

Die Zusammensetzung der Länder-Top-10 hat sich gegenüber 2013 nicht geändert, die Verteilung innerhalb des Ratings aber schon. Russland rutschte von dem zweiten auf den vierten Platz ab, Deutschland stieg umgekehrt von Position vier auf Rang zwei auf. Die Ukraine kletterte eine Position nach oben, von sechs auf fünf, und ließ damit Großbritannien hinter sich, das auf Platz sechs des Ratings landete.

44 Prozent der Web-Attacken wurden von Web-Ressourcen durchgeführt, die sich in den USA und in Deutschland befinden.

LÄNDER, MIT DEM HÖCHSTEN INFEKTIONSRISIKO ÜBER DAS INTERNET

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**	53,81 %
2	**Kasachstan**	53,04 %
3	**Aserbaidschan**	49,64 %
4	**Vietnam**	49,13 %
5	**Armenien**	48,66 %
6	**Ukraine**	46,70 %
7	**Mongolei**	45,18 %
8	**Weißrussland**	43,81 %
9	**Moldawien**	42,41 %
10	**Kirgisien**	40,06 %
11	**Deutschland**	39,56 %
12	**Algerien**	39,05 %
13	**Katar**	38,77 %
14	**Tadschikistan**	38,49 %
15	**Georgien**	37,67 %
16	**Saudi-Arabien**	36,01 %
17	**Österreich**	35,58 %
18	**Litauen**	35,44 %
19	**Sri Lanka**	35,42 %
20	**Türkei**	35,40 %

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.

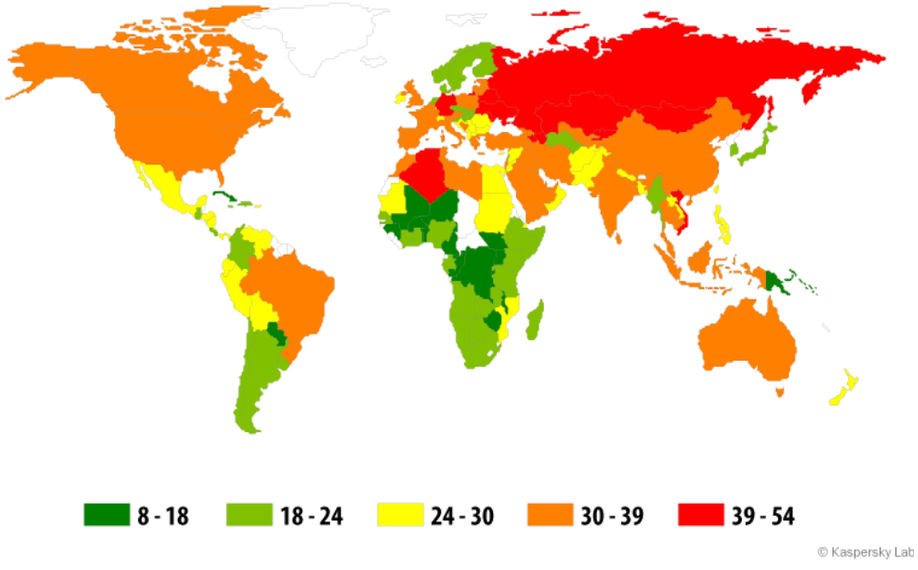
** Prozentualer Anteil individueller Anwender-PCs, die Web-Attacken ausgesetzt waren, an allen Nutzern von Kaspersky-Produkten in diesem Land.

Im Jahr 2014 wurde die Spitzenposition neu besetzt: Dem größten Risiko einer Infektion über das Internet ist man in Russland ausgesetzt, wo **53,81 Prozent** der Anwender Webattacken ausgesetzt waren.

Der Spitzenreiter des Vorjahres, Aserbaidschan, fiel auf den dritten Platz zurück (49,64 %).
Nicht mehr in den Top 20 vertreten sind Indien, Usbekistan, Malaysia, Griechenland und Italien. Neu eingestiegen sind die Mongolei, Katar, Saudi Arabien, Litauen und die Türkei.

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

1. Gruppe mit erhöhtem Risiko: Zu dieser Gruppe mit Werten über 41 Prozent gehören neun Länder aus den Top 20, die gegenüber dem Vorjahr also zahlenmäßig abgenommen hat: Im Jahr 2013 gehörten ihr noch 15 Länder an.
2. Risikogruppe: In dieser Gruppe mit Werten zwischen 21 und 40,9 Prozent sind 111 Länder vertreten, unter anderem: Kirgisien (40,1 Prozent), Deutschland (39,6 Prozent), Katar (38,8 Prozent), Tadschikistan (38,5 Prozent), Georgien (37,7 Prozent), Saudi-Arabien (36 Prozent), die Türkei (35,4 Prozent), Frankreich (34,9 Prozent), Indien (34,8 Prozent), Spanien (34,4 Prozent), die USA (33,8 Prozent), Kanada (33,4 Prozent), Australien (32,5 Prozent), Brasilien (32,1 Prozent), Polen (31,7 Prozent), Italien (31,5 Prozent), Israel (30,2 Prozent), China (30,1 Prozent), Großbritannien (30 Prozent), Ägypten (27,8 Prozent), Mexiko (27,5 Prozent), die Philippinen (27,2 Prozent), Kroatien (26,2 Prozent), Pakistan (26,1 Prozent), Rumänien (25,7 Prozent), Japan (21,2 Prozent) und Argentinien (21,1 Prozent).
3. Gruppe der beim Surfen im Internet sichersten Länder (0 bis 20,9 Prozent): Zu dieser Gruppe zählen 39 Länder. Dazu gehören auch Schweden (19,5 Prozent), Dänemark (19,2 Prozent), Uruguay (19,5 Prozent) und eine Reihe afrikanischer Länder.



Im Jahr 2014 waren weltweit **38,3 Prozent** der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt.

Die Gefahrenstufe ist innerhalb des Jahres durchschnittlich um 3,3 Prozentpunkte gesunken. 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 überprüfen viele Exploit-Packs jetzt, ob auf einem Computer eines unserer Produkte läuft. Finden sie ein Kaspersky-Produkt, so versuchen sie gar nicht erst, den Computer anzugreifen.
- Drittens bevorzugen immer mehr Anwender mobile Geräte und Tablets zum Surfen im Netz.

Außerdem hat auch die Zahl der Angriffe unter Verwendung von Exploit-Packs leicht abgenommen – die Verhaftungen von Exploit-Pack-Entwicklern waren nicht umsonst. Allerdings braucht man diesbezüglich nicht auf eine grundlegende Veränderung der Situation zu hoffen. Exploits bleiben das wichtigste Mittel zur Zustellung von Schadprogrammen, unter anderem auch im Rahmen zielgerichteter Attacken. Das Internet ist in den meisten Ländern der Welt nach wie vor die Hauptquelle von schädlichen Objekten.

LOKALE BEDROHUNGEN

Ein überaus wichtiger Indikator ist die Statistik der lokalen Infektionen der Computer. Zu diesen Daten gehören Objekte, die nicht über das Internet, E-Mails oder Portzugriffe in die Computer von Windows-Nutzern eindringen. 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).

TOP 20 DER AUF DEN COMPUTERN DER ANWENDER ENTDECKTEN SCHÄDLICHEN OBJEKTE

Im Jahr 2014 spürte Kaspersky Anti-Virus **1.849.949** schädliche und potenziell unerwünschte Programme auf.

	NAME	PROZENTUALER ANTEIL DER ANGEGRIFFENEN ANWENDER*
1	**DangerousObject.Multi.Generic**	26,04 %
2	**Trojan.Win32.Generic**	25,32 %
3	**AdWare.Win32.Agent.ahbx**	12,78 %
4	**Trojan.Win32.AutoRun.gen**	8,24 %
5	**Adware.Win32.Amonetize.heur**	7,25 %
6	**Virus.Win32.Sality.gen**	6,69 %
7	**Worm.VBS.Dinihou.r**	5,77 %
8	**AdWare.MSIL.Kranet.heur**	5,46 %
9	**AdWare.Win32.Yotoon.heur**	4,67 %
10	**Worm.Win32.Debris.a**	4,05 %
11	**AdWare.Win32.BetterSurf.b**	3,97 %
12	**Trojan.Win32.Starter.lgb**	3,69 %
13	**Exploit.Java.Generic**	3,66 %
14	**Trojan.Script.Generic**	3,52 %
15	**Virus.Win32.Nimnul.a**	2,80%
16	**Trojan-Dropper.Win32.Agent.jkcd**	2,78%
17	**Worm.Script.Generic**	2,61%
18	**AdWare.Win32.Agent.aljt**	2,53%
19	**AdWare.Win32.Kranet.heur**	2,52%
20	**Trojan.WinLNK.Runner.ea**	2,49%

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.

Schädliche Programme des Typs DangerousObject.Multi.Generic, die mit Hilfe von Cloud-Technologien aufgespürt werden, belegen den ersten Platz (26,04 Prozent). 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.

Nicht mehr unter den ersten Zwanzig ist der berühmt-berüchtigte Wurm Net-Worm.Win32.Kido. Auch der Anteil der Viren nimmt weiter ab: Während es im vergangenen Jahr noch **13,4 Prozent** der Anwender mit dem Schädling Virus.Win32.Sality.gen zu tun hatten, waren es im Jahr 2014 nur noch **6,69 Prozent**.

Werbeprogramme finden immer weitreichendere Verbreitung, was sich sowohl in diesem Rating als auch im Rating der Web-Detektionen widerspiegelt. Die Zahl der Anwender, die sich mit Werbeprogrammen konfrontiert sahen, hat sich im Vergleich zum Vorjahr fast verdoppelt und betrug **25.406.107** Personen. Dabei wird die Adware nicht nur immer lästiger, sondern auch immer gefährlicher. Einige Programme dieser Art überschreiten die Grenze der Kategorie „potenziell unerwünscht“ und werden nun einer „härteren“ Rubrik zugeordnet. Ein Beispiel für ein solches Programm ist Trojan-Dropper.Win32.Agent.jkcd (16. Platz): Diese Adware belästigt den Nutzer nicht nur mit nerviger Werbung und ändert die Suchergebnisse, sondern ist auch in der Lage, ein Schadprogramm auf seinen Computer zu laden.

LÄNDER, MIT DEM HÖCHSTEN LOKALEN INFEKTIONSRISIKO

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 Schadprogramme, die direkt auf den Computern gefunden wurden oder auf Wechseldatenträgern, die an die Computer angeschlossen waren, zum Beispiel USB-Sticks, Speicherkarten aus Fotoapparaten und Telefonen 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**	69,58 %
2	**Mongolei**	64,24 %
3	**Nepal**	61,03 %
4	**Bangladesch**	60,54 %
5	**Jemen**	59,51 %
6	**Algerien**	58,84 %
7	**Irak**	57,62 %
8	**Laos**	56,32 %
9	**Indien**	56,05 %
10	**Kambodscha**	55,98 %
11	**Afghanistan**	55,69 %
12	**Ägypten**	54,54 %
13	**Saudi-Arabien**	54,37 %
14	**Kasachstan**	54,27 %
15	**Pakistan**	54,00 %
16	**Syrien**	53,91 %
17	**Sudan**	53,88 %
18	**Sri Lanka**	53,77 %
19	**Myanmar**	53,34 %
20	**Türkei**	52,94 %

Die Statistik basiert auf Daten von Kaspersky Anti-Virus, dessen Anwender zugestimmt haben, dass die Software statistische Informationen zu Auswertungszwecken sammeln darf.

* 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.

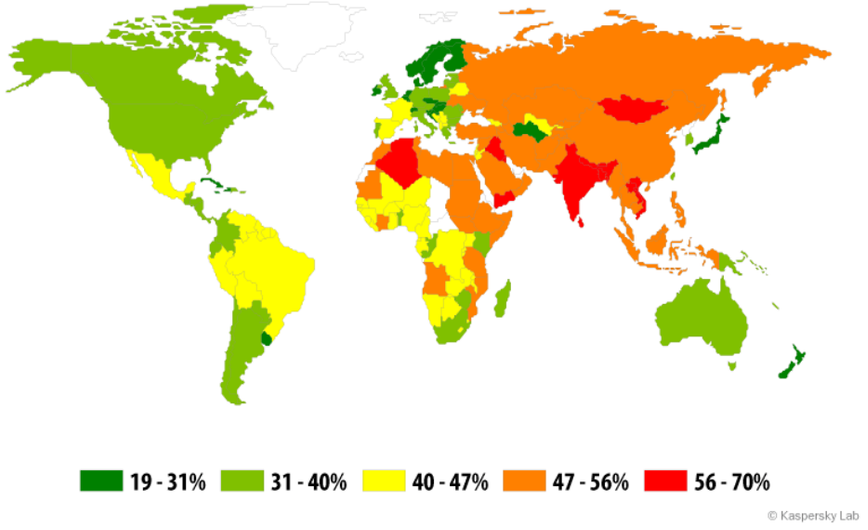
Die Zusammensetzung der ersten vier Positionen blieb gegenüber dem Vorjahr unverändert: Den ersten Platz besetzt nach wie vor Vietnam; während die Mongolei und Bangladesch die Plätze getauscht haben. Bangladesch ist von Position zwei auf den vierten Platz abgerutscht, Mongolei hingegen vom vierten auf den zweiten Platz aufgestiegen.

Nicht mehr in den Top 20 vertreten sind Dschibuti, die Malediven, Mauretanien, Indonesien, Ruanda und Angola. Neu hinzugekommen sind der Jemen, Saudi-Arabien, Kasachstan, Syrien, Myanmar und die Türkei.

Durchschnittlich wurde in den Ländern aus den Top 20 bei **58,7 Prozent** der KSN-Anwender, die uns Informationen zur Verfügung stellen, mindestens einmal ein schädliches Objekt auf dem Computer gefunden – auf der Festplatte oder auf angeschlossenen mobilen Datenträgern –, gegenüber **60,1 Prozent** im Jahr 2013.

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

1. **Maximales Infektionsniveau** (über 60 Prozent)
   Hier sind die vier ersten Länder des Ratings vertreten – Vietnam (69,6 Prozent), die Mongolei (64,2 Prozent), Nepal (61,0 Prozent) und Bangladesch (60, 5Prozent).
2. **Hohes Infektionsniveau** (41 bis 60 Prozent)
   83 Länder, darunter Indien (56,0 Prozent), Kasachstan (54,3 Prozent), die Türkei (52,9 Prozent), Russland (52,0 Prozent), China (49,7 Prozent), Brasilien (46,5 Prozent), Weißrussland (45,3 Prozent), Mexiko (41,6 Prozent) und die Philippinen (48,4 Prozent).
3. **Mittleres Infektionsniveau** (21 bis 40,9 Prozent)
   70 Länder, darunter Spanien (40,9 Prozent), Frankreich (40,3 Prozent), Polen (39,5 Prozent), Litauen (39,1 Prozent), Griechenland (37,8 Prozent), Portugal (37,7 Prozent), Südkorea (37,4 Prozent), Argentinien (37,2 Prozent), Italien (36,6 Prozent), Österreich (36,5 Prozent), Australien (35,3 Prozent), Kanada (34,8 Prozent), Rumänien (34,5 Prozent), die USA (34,4 Prozent), Großbritannien (33,8 Prozent), Schweiz (30,8 Prozent), Hongkong (30,4 Prozent), Irland (29,7 Prozent), Uruguay (27,8 Prozent), Niederlande (26,4 Prozent), Norwegen (25,1 Prozent), Singapur (23,5 Prozent), Japan (22,9 Prozent), Schweden (23 Prozent) und Dänemark (21,3 Prozent).
4. **Niedriges Infektionsniveau** (0 bis 20,9 Prozent)
   Drei Länder: Finnland (20 Prozent), Kuba (19,1 Prozent) und die Seychellen (19 Prozent).



TOP 10 DER LÄNDER MIT MINIMALEN COMPUTER-INFEKTIONSRATEN

	LAND	ANTEIL DER ANGEGRIFFENEN ANWENDER*
1	**Seychellen**	19,03 Prozent
2	**Kuba**	19,08 Prozent
3	**Finnland**	20,03 Prozent
4	**Dänemark**	21,34 Prozent
5	**Japan**	22,89 Prozent
6	**Schweden**	22,98 Prozent
7	**Tschechien**	23,13 Prozent
8	**Singapur**	23,54 Prozent
9	**Martinique**	25,04 Prozent
10	**Norwegen**	25,13 Prozent

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

Gegenüber dem Jahr 2013 gab es in dieser Liste einige Veränderungen. Neu hinzugekommen sind Martinique, Singapur und Schweden, nicht mehr vertreten sind die Slowakei, Slowenien und Malta. Durchschnittlich wurden **23 Prozent** der Computer in den zehn sichersten Ländern mindestens einmal im Laufe des Jahres angegriffen. Im Vergleich zum Vorjahr ist dieser Wert um 4,2 Prozentpunkte gestiegen.

DIE 10 ULTIMATIVEN SECURITY-STORIES DES JAHRES 2014

Autor: David Emm

QUICK INFO

- Zielgerichtete Attacken und Malware-Kampagnen
- Unser Heim und andere Schwachstellen
- Das fortgesetzte exponentielle Wachstum mobiler Malware
- Geld oder Datei(en)!
- Malware für Überfälle auf Bankautomaten
- Windows XP: vergessen, aber nicht vergangen?
- Unter der Zwiebelschale
- Gute Malware, schlechte Malware!?
- Privatsphäre und Sicherheit
- Internationale Strafverfolgung: Zusammenarbeit zeigt Ergebnisse

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 2014 geprägt haben.

Game Of Cyberthrones: Attacken gegen Unternehmen und Führungskräfte in 2014

1. 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. Die komplexe Cyberspionage-Kampagne mit der Bezeichnung **„Careto“** oder „The Mask“ (Careto ist ein spanischer Slangausdruck für „hässliches Gesicht“ oder „Maske“) dient dazu, bei bestimmten Organisationen Daten zu stehlen. Zu den Opfern dieser Attacke gehören Regierungsagenturen, Botschaften, Energieunternehmen, Forschungsinstitutionen, private Immobilienfirmen und Aktivisten aus 31 Ländern rund um den Globus.

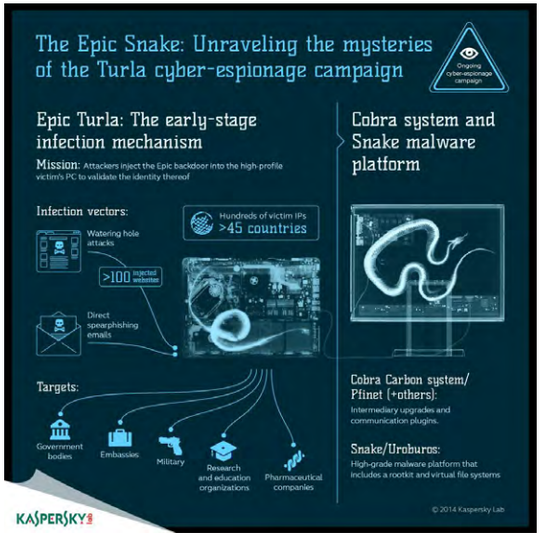
Careto umfasst eine raffinierte trojanische Backdoor, die in der Lage ist, alle Kommunikationskanäle abzufangen und Daten aller Art von infizierten Computern abzuernten. Dazu gehören Chiffrierungsschlüssel, VPN-Konfigurationen, SSH-Schlüssel, RDP-Dateien und einige unbekannte Dateitypen, die mit maßgeschneiderten Verschlüsselungstools des Militärs und der Regierung in Verbindung stehen könnten. Der Code von Careto war hochgradig modular, was es den Angreifern ermöglichte, nach Belieben neue Funktionalitäten hinzuzufügen. Es gibt Versionen der Backdoor für Windows und Mac OS X. Das Kaspersky-Team hat zudem Indizien in einigen Modulen gefunden, die darauf hinweisen, dass es auch Versionen für Linux, iOS und Android geben könnte. Wie bei jeder ausgeklügelten Kampagne dieser Art ist es auch in diesem Fall sehr schwer, sie zuzuordnen. Die Tatsache, dass im Code die spanische Sprache benutzt wird, hilft da nicht weiter, da in vielen Teilen der Welt spanisch gesprochen wird. Möglicherweise soll der Gebrauch des Spanischen sogar bewusst in die Irre führen. Das hohe Maß an Professionalität der Gruppe hinter dieser Attacke ist indessen ungewöhnlich für cyberkriminelle Banden – ein Indikator dafür, dass Careto eine staatlich gesponserte Kampagne sein könnte. Ebenso wie bei früheren zielgerichteten Angriffskampagnen reichen auch die Wurzeln von Careto weit vor die Zeit zurück, in der diese Kampagne ans Licht kam: Wir glauben, dass die Angreifer bereits seit 2007 aktiv sind.

Anfang März wurde eine Cyberspionage Kampagne mit dem Namen „Epic Turla“ unter Sicherheitsexperten heiß diskutiert. Die Spezialisten von G-DATA waren der Meinung, die Malware könnte von russischen Fachdiensten entwickelt worden sein. Eine von BAE Systems durchgeführte Studie hingegen brachte die Kampagne mit einem Schadprogramm in Verbindung, das als „Agent.btz“ identifiziert wurde. Es war auf das Jahr 2007 zurückdatiert und wurde im Jahr 2008 benutzt, um die lokalen Netzwerke der USA zu infizieren, die sie für ihre Militäroperationen im Mittleren Osten verwendeten. **Unsere Erstanalyse von Epic Turla** konzentrierte sich auf die Benutzung von USB-Massenspeichern durch die Malware, die gestohlene Daten darauf ablegte, die nicht direkt über das Internet zum Command-and-Control-Server (C2) der Angreifer geschickt werden konnten.

Der Wurm schreibt eine Datei namens „thumb.dll“ auf alle USB-Sticks, die mit einem infizierten Computer verbunden sind. Wird der USB-Stick daraufhin mit einen anderen Computer verbunden, wird die Datei „thumb.dll“ auf diesen kopiert. Es handelt sich dabei um eine der Dateien aus dem „USB Stealer-Modul“ von Roter Oktober. Schaut man noch weiter zurück, so hatten auch Gauss und miniFlame die Datei „thumb.dll“ im Visier und suchten auf USB-Sticks nach ihr. Eine Grafik mit den Verbindungen der Schädlinge zueinander finden Sie **hier**. Wir halten es durchaus für möglich, dass es weltweit zehntausende von USB-Massen-speichern gibt, die „thumb.dll“-Dateien enthalten, die von dieser Malware erstellt wurden.

In unserer nächsten **Analyse der Epic-Turla-Kampagne** erklärten wir, wie die Angreifer Social Engineering einsetzen, um die Malware zu verbreiten, und haben gleichzeitig die Gesamtstruktur der Kampagne dargestellt. Die Angreifer benutzen Spear-Phishing-Mails, um ihre Opfer dazu zu bringen, eine Backdoor auf ihrem Computer zu installieren. Einige davon enthalten Zero-Day-Exploits – eins davon betrifft den Adobe Acrobat Reader und das andere eine Privilegien-Eskalation in Windows XP und Windows Server 2003. Die Verbrecher hinter der Kampagne setzen zudem Wasserloch-Attacken ein, die entweder ein Java-Exploit sowie Exploits für den Adobe Flash Player und den Internet Explorer installieren. Oder sie bringen ihre Opfer dazu, einen gefälschten „Flash Player“ auszuführen, der Malware installiert. In Abhängigkeit von der IP-Adresse des Opfers liefern die Angreifer Java- oder Browser-Exploits, signierte gefälschte Adobe-Flash-Player-Software oder eine gefälschte Version von Microsoft Security Essentials. Es überrascht nicht, dass die Auswahl der Webseiten die spezifischen Interessen der Angreifer widerspiegelt (wie auch die Interessen der Opfer). Die Analyse von Kaspersky Lab hat allerdings gezeigt, dass die Epic-Turla-Backdoor nur die erste Stufe der Infektion ist. Sie wird benutzt, um eine noch raffiniertere Backdoor einzuschleusen, die unter dem Namen „Cobra/Carbon system“ bekannt ist (einige Anti-Malware-Produkte nennen sie auch „Pfinet“). Das spezifische Wissen, das zum betreiben dieser beiden Backdoors erforderlich ist, weist auf eine eindeutige und direkte Verbindung zwischen ihnen hin: Eine wird benutzt, um einen Fuß in die Tür zu bekommen und um das jeweils im Fokus stehende Opfer zu bewerten. Erweist es sich als interessant für die Angreifer, erhält der infizierte Computer ein Update auf das vollständige Carbon-System.

Folgende Grafik zeigt die Epic-Turla-Kampagne im Überblick:



Im Juni berichteten wir über unsere Untersuchung eines Angriffs auf die Kunden einer großen europäischen Bank, die im Diebstahl einer halben Million Euro innerhalb nur einer Woche mündete. Wir tauften den Angriff **„Luuuk“**, nach dem Pfad, den die Administratorkonsole im C2-Server verwendet. Obwohl wir nicht in der Lage waren, an den Schadcode zu gelangen, der gegen die Opfer eingesetzt wurde, sind wir überzeugt davon, dass die Kriminellen einen Bank-Trojaner verwendeten, der Man-in-the-Browser-Operationen durchführte, um über eine schädliche Webeinschleusung an deren Anmeldedaten zu gelangen. Den Informationen aus einigen Logdateien zufolge stahl die Malware in Echtzeit Benutzernamen, Passwörter und Einmalkennwörter (OTP). Die Angreifer verwendeten die gestohlenen Anmeldedaten, um den Kontostand der Opfer zu überprüfen und automatisch verschiedene bösartige Transaktionen durchzuführen, vermutlich indem sie im Hintergrund einer legitimen Online-Banking-Sitzung operierten. Das gestohlene Geld wurde dann automatisch auf vordefinierte Geldesel-Konten transferiert. Die von den Anwendern verwendete Klassifikation der Geldkuriere war überaus interessant. Es gab vier verschiedene Geldkurier-Gruppen, wobei jede über die Geldmenge definiert wurde, die die Kuriere aus dieser Gruppe akzeptieren durften – vermutlich ein Indikator für den Grad des Vertrauens untereinander. Das Kaspersky-Team hat insgesamt 190 Opfer identifiziert, von denen sich die meisten in Italien und der Türkei befinden. Die von jedem Opfer gestohlenen Summen lagen zwischen 1.700 Euro und 39.000 Euro; die Gesamtsumme betrug 500.000 Euro.

Auch wenn die Angreifer kurz nach dem Beginn unserer Untersuchungen alle sensitiven Daten entfernt haben, glauben wir, dass es sich hierbei eher um einen Umbau der Infrastruktur als um einen generellen Abbruch der Operation handelt. Die Cyberkriminellen, die hinter dieser Kampagne stecken, sind höchst professionell und sehr aktiv. Sie haben außerdem eine proaktive operative Sicherheitsaktivität an den Tag gelegt, wobei sie ihre Taktik ändern und ihre Spuren verwischen, sobald sie entdeckt werden. Die Untersuchungen dieser Kampagne, über die wir die betroffene Bank und die zuständigen Strafverfolgungsbehörden informiert haben, dauern an.

Der Juni brachte die Reaktivierung der zielgerichteten Angriffskampagne „MiniDuke“ aus dem frühen Jahr 2013 mit sich. Die **ursprüngliche Kampagne** hob sich aus verschiedenen Gründen von anderen ab. Sie beinhaltete eine maßgeschneiderte Backdoor, die nach alter Schule in der Programmiersprache Assembler geschrieben war. Die Attacke wurde mit Hilfe einer ungewöhnlichen Command-and-Control-Infrastruktur (C2) verwaltet: Sie machte sich zahlreiche redundante Pfade zunutze, unter anderem auch Twitter-Accounts. Die Entwickler transportierten ihre aktualisierten ausführbaren Dateien versteckt in GIF-Dateien.

Die Ziele der neuen Operation, bekannt unter dem Namen **„CosmicDuke“** oder „TinyBaron“, umfassen die Bereiche Regierung, Diplomatie, Energie, Militär und Telekommunikation. Ungewöhnlich ist aber, dass die Liste der Opfer auch Personen enthält, die mit Schwarzhandel und dem Verkauf illegaler Substanzen wie Steroide und Hormone in Verbindung gebracht werden. Es ist nicht klar, warum. Vielleicht wurde die anpassbare Backdoor als so genannte „legale Spyware“ verfügbar gemacht, oder sie war auf dem Schwarzmarkt verfügbar und wurde von verschiedenen Konkurrenten aus der Pharmazie-Branche erworben, die sich gegenseitig ausspionieren wollten.

Geografische Verteilung der Opfer von Miniduke und CosmicDuke

Die Malware imitiert populäre Anwendungen, die im Hintergrund laufen, Dateiinformationen, Icons und sogar Dateigröße eingeschlossen. Die Backdoor selbst wurde mit Hilfe von „BotGenStudio“ kompiliert, einem flexiblen Framework, das es dem Angreifer ermöglicht, Komponenten zu aktivieren und zu deaktivieren, wenn der Bot eingerichtet wird. Die Malware stiehlt nicht nur Dateien, die bestimmte Erweiterungen besitzen, sondern greift auch Passwörter ab, sowie den Verlauf, Netzwerkinformationen, Adressbücher, auf dem Bildschirm dargestellte Informationen (alle fünf Minuten werden Screenshots erstellt) und andere sensitive Daten. Jedes der Opfer erhält eine eindeutige ID und kann so individuell und gezielt mit Updates versorgt werden.

Die Malware wird von einem maßgeschneiderten obfuskierten Ladeprogramm geschützt, das drei bis fünf Minuten, bevor es die Payload ausführt, sehr viele CPU-Ressourcen verbraucht. Dadurch ist das Schadprogramm schwer zu analysieren. Doch es zehrt auch die Ressourcen auf, die die Sicherheitssoftware benötigt, um die Ausführung der Malware zu emulieren. Neben dieser Verschleierungstaktik macht die Malware auch regen Gebrauch von Verschlüsselung und Kompression, basierend auf den Algorithmen RC4 und LZRW. Ihre Umsetzung unterscheidet sich leicht von den Standardversionen. Wir sind der Meinung, dass Absicht dahinter steckt und so die Sicherheitsforscher in die Irre geführt werden sollen. Die interne Konfiguration des Schädlings ist verschlüsselt, komprimiert und angeordnet als eine komplizierte Registry-artige Struktur, die verschiedene Eintragstypen hat, unter anderem Zeichenketten (Strings), ganze Zahlen (Integer) und interne Referenzen. Die gestohlenen Daten zerteilt der Schädling in kleine Stückchen (von etwa 3 KB), komprimiert und verschlüsselt sie und lädt sie anschließend in einem Container verpackt auf den C2-Server hoch. Handelt es sich um eine große Datei, kann sie auf mehrere hundert Container verteilt sein, die alle unabhängig voneinander hochgeladen werden. Es ist wahrscheinlich, dass diese Daten-Häppchen auf Angreifer-Seite geparst, entschlüsselt, entpackt, extrahiert und wieder zusammengesetzt werden. Auch wenn diese Methode einen Mehraufwand beinhaltet, so gewährleisten die Schichten zusätzlicher Verarbeitung doch, dass nur sehr wenige Forscher an die Originaldaten gelangen. Diese Methode bietet zudem eine höhere Ausfallsicherheit gegenüber Netzwerk-Fehlern.

Im Juli veröffentlichte Kaspersky Lab eine Tiefenanalyse einer zielgerichteten Attacke, die wir auf den Namen **„Crouching Yeti“** tauften – auch bekannt als „Energetic Bear“, da die Experten von CrowdStrike annahmen, die Angreifer stammten aus Russland: Wir glauben nicht, dass es ausreichend Beweise gibt, um diese Annahme zu bestätigen oder zu widerlegen. Die Kampagne ist seit dem Spätjahr 2010 aktiv und hat bisher die folgenden Branchen ins Visier genommen: Industrie und Industrieanlagen, Produktion, Pharmazie, Bau, Bildung und Informationstechnologie. Bis jetzt wissen wir von über 2.800 Opfern weltweit und wir konnten 101 verschiedene Organisationen identifizieren, die sich größtenteils in den USA, in Spanien, Japan, Deutschland, Frankreich, Italien, der Türkei, Irland, Polen und China befinden.

Die Hacker hinter Crouching Yeti verwenden verschiedene Arten von Malware (zur Infektion von Windows-Systemen), um in Rechner einzubrechen, weiter in die angegriffenen Organisationen einzudringen und vertrauliche Daten zu stehlen – inklusive intellektuellem Eigentum und anderen strategischen Informationen. Die verwendete Malware umfasst spezielle Module zum Sammeln von Daten von bestimmten industriellen IT-Umgebungen. Infizierte Computer verbinden sich mit einem großen Netzwerk von gehackten Webseiten, die Malware-Module beherbergen, Informationen über Opfer speichern und Befehle an die infizierten Systeme senden. Die Angreifer infizieren die Computer auf drei verschiedene Arten: Sie nutzen einen legitimen Software-Installer, der neu gepackt wird, um eine schädliche DLL-Datei zu integrieren; daneben kommen Spear-Phishing-Mails und Wasserloch-Attacken zum Einsatz.

Technologie ist heute ein wesentlicher Bestandteil unseres Lebens. Daher ist es alles andere als überraschend, dass Konflikte rund um den Erdball nun auch eine Cyberdimension erhalten. Dies gilt insbesondere für den Mittleren Osten, wo sich die geopolitischen Konflikte in den letzten Jahren immer weiter zugespitzt haben. Im August berichteten wir über eine **Zunahme der Malware-Aktivität in Syrien** seit Anfang des Jahres 2013. Die Opfer dieser Attacken befinden sich nicht nur in Syrien. Derartige Angriffe wurden ebenfalls in der Türkei, in Saudi-Arabien, im Libanon, in Palästina, den Vereinigten Arabischen Emiraten, Israel, Marokko, Frankreich und den USA beobachtet. Wir konnten die C2-Server der Angreifer zu IP-Adressen in Syrien, Russland, dem Libanon, den USA und Brasilien zurückverfolgen. Insgesamt fanden wir 110 Dateien, 20 Domains und 47 IP-Adressen, die mit den Attacken in Verbindung stehen.

Es ist klar, dass die Gruppen, die hinter diesen Attacken stehen, äußerst gut organisiert sind. Bisher haben die Angreifer bewährte Malware-Tools benutzt und keine eigenen Werkzeuge entwickelt (obwohl sie ein breites Spektrum von Obfuskationsmethoden einsetzen, um die simple Signatur-basierte Erkennung zu verhindern). Wir sind der Meinung, dass die in dieser Region eingesetzte Schadsoftware sowohl an Quantität als auch an Qualität zunehmen wird.

Im November veröffentlichten wir unsere Analyse der **„Darkhotel“**-APT, eine Kampagne, die seit fast einem Jahrzehnt aktiv ist und Opfer rund um den Globus angreift. Etwa 90 Prozent der Infektionen erfolgten in Japan, Taiwan, China, Russland und Hong Kong, doch es gab sie ebenfalls in Deutschland, den USA, Indonesien, Indien und Irland.

Im Rahmen der Kampagne werden wechselnde Angriffsschemata verwendet. Erstens setzen die Online-Verbrecher Spear-Phishing-Mails und Zero-Day-Exploits ein, um in Organisationen aus unterschiedlichen Bereichen einzudringen, unter anderem Rüstungsindustrie, Regierung und Nicht-Regierungsorganisationen (NGOs). Zweitens verbreiten sie völlig willkürlich Malware über japanische P2P-Filesharing-Sites. Drittens greifen sie gezielt Führungskräfte an, die nach Übersee reisen und in Hotels in verschiedenen Ländern absteigen: In einem zweistufigen Infektionsprozess identifizieren die Angreifer zunächst ihre Opfer und laden dann weitere Malware, die entwickelt wurde, um vertrauliche Daten von befallenen Rechnern zu stehlen, auf die Computer von bedeutungsvolleren Zielen.

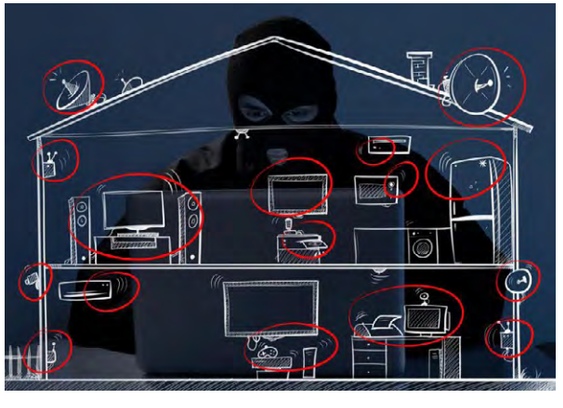
2. UNSER HEIM UND ANDERE SCHWACHSTELLEN

Die Ausnutzung von Sicherheitslücken ist und bleibt einer der wichtigsten Mechanismen zur Installation von Schadcode auf den Computern von Opfern Cyberkrimineller. Dieser Mechanismus funktioniert also nur, wenn Sicherheitslücken in weit verbreiteter Software vorhanden sind, und wenn einzelne Anwender und Unternehmen es versäumen, die entsprechenden Patches zu installieren.

In diesem Jahr wurden in zwei stark genutzten Open-Source-Protokollen Sicherheitslücken gefunden, die als „Heartbleed“ und „Shellshock“ bekannt wurden. **Heartbleed,** ein Fehler im Verschlüsselungsprotokoll **OpenSSL**, ermöglicht es einem Angreifer, die Speicherinhalte zu lesen und persönliche Daten auf Systemen abzufangen, die angreifbare Versionen des Protokolls benutzen. OpenSSL wird häufig benutzt, um Internet-basierte Kommunikation abzusichern, wie etwa den Webtraffic, E-Mail, Instant Messaging und Virtual Private Networks (VPN), sodass die potenziellen Auswirkungen dieser Schwachstelle sehr groß waren. Wie es häufig der Fall ist, wenn persönliche Daten abgeflossen sein könnten, gab es eindringliche Aufrufe, die Passwörter zu ändern. Das ergibt selbstverständlich nur dann einen Sinn, wenn die Online-Anbieter vorher die notwendigen Schritte unternommen haben, um OpenSSL zu patchen und dadurch ihre Systeme zu sichern – andernfalls wäre jedes neue Passwort ebenso in Gefahr, Angreifern in die Hände zu fallen, die versuchen, die Schwachstelle auszunutzen. Zwei Monate nach ihrer Entdeckung haben wir diese **Schwachstelle aus verschiedenen Blickwinkeln beleuchtet**.

Im September läuteten in der IT-Sicherheitsbranche alle Alarmglocken, nachdem die **Shellshock-Sicherheitslücke** (auch bekannt als „Bash“) entdeckt worden war. Der Fehler ermöglicht es Angreifern aus der Ferne, eine schädliche Datei an eine Variable anzuhängen, die ausgeführt wird, wenn der Bash-Kommandointerpreter aufgerufen wird. (Bash ist die Standard-Shell in Linux und Mac OS X). Die extremen Auswirkungen dieser Sicherheitslücke in Kombination mit der unproblematischen Ausnutzung gaben Anlass zu beträchtlichen Sorgen. Von einigen wird diese Schwachstelle mit der „Heartbleed”-Sicherheitslücke verglichen. Doch Bash ist viel einfacher auszunutzen als Heartbleed, und während Heartbleed es einem Angreifer nur ermöglichte, Daten aus dem Speicher eines angreifbaren Computers zu stehlen, kann Shellshock die Kontrolle über das gesamte System bereitstellen.

Die Angreifer brauchten nicht lange, um die Sicherheitslücke zu testen und ihren Nutzen daraus zu ziehen – bereits kurz nach ihrem Erscheinen haben wir einige **frühe Beispiele** besprochen. In den meisten Fällen griffen Hacker entfernt Webserver an, die **CGI-Skripte** (Common Gateway Interface) beherbergen, die in Bash geschrieben wurden oder Werte an Shell-Skripte weitergeben. Wie auch immer – es ist möglich, dass die **Sicherheitslücke Auswirkungen auf eine Windows-basierte Infrastruktur** hat. Das Problem beschränkt sich leider auch nicht allein auf Webserver. Bash ist auch in der Firmware von Geräten verbreitet, die heute Teil unseres alltäglichen Lebens sind. Dazu gehören Router, Haushaltsgeräte und drahtlose Zugriffspunkte. Einige dieser Geräte sind nur schwer oder gar unmöglich zu patchen.



Das Internet durchdringt unser alltägliches Leben immer stärker, und zwar wortwörtlich, da immer mehr Alltagsgeräte mit dem World Wide Web verbunden werden können. Diese Tendenz, bekannt als das „Internet der Dinge“, zieht immer mehr Aufmerksamkeit auf sich. Es mag vielleicht futuristisch erscheinen, aber das Internet der Dinge ist in Wahrheit näher als man denkt. In einem modernen Heim können sich heute eine Handvoll Geräte befinden, die mit dem lokalen Netzwerk verbunden sind, und bei denen es sich nicht um klassische Computer handelt – Geräte wie Smart-TV, Drucker, Spielkonsolen, Netzwerkspeichergeräte oder irgendeine Art von Media Player oder Satellitenreceiver.

Einer unserer Sicherheitsexperten **untersuchte sein eigenes Zuhause**, um festzustellen, ob es wirklich cybersicher ist. Er nahm verschiedene Geräte unter die Lupe, unter anderem Netzwerkspeichergeräte (NAS), einen Smart-TV, einen Router und einen Satellitenreceiver, um zu sehen, ob sie angreifbar sind. Das Ergebnis war erschreckend. Er fand 14 Sicherheitslücken in den Netzwerkspeichergeräten, eine in dem Smart-TV und mehrere potenziell verborgene Funktionen zur entfernten Kontrolle in seinem Router. Den vollständigen Bericht lesen Sie **hier**. Es ist sehr wichtig, dass wir uns alle der möglichen Sicherheitsrisiken bewusst sind, die mit dem Gebrauch von Netzwerkgeräten einhergehen – das gilt für Heimanwender und Unternehmen gleichermaßen. Wir müssen zudem einsehen, dass unsere Informationen nicht sicher sind, nur weil wir starke Passwörter verwenden und eine Software zum Schutz vor Schadcode laufen lassen. Es gibt so viele Dinge, über die wir keine Kontrolle haben, und wir befinden uns bis zu einem gewissen Grad in den Händen von Software- und Hardware-Anbietern. So sind beispielsweise automatisierte Update-Checks nicht in alle Geräte integriert – manchmal sind die Verbraucher selbst aufgefordert, eine neue Firmware herunterzuladen und zu installieren. Das ist nicht immer ganz einfach. Schlimmer noch: Es ist gar nicht immer möglich, ein Gerät zu aktualisieren (die meisten im Rahmen dieser Analyse untersuchten Geräte waren schon über ein Jahr lang Auslaufmodelle).

3. DAS FORTGESETZTE EXPONENTIELLE WACHSTUM MOBILER MALWARE

In den letzten Jahren hat die Zahl der mobilen Schadprogramme dramatisch zugenommen. In der Zeit von 2004 bis 2013 haben die Kaspersky-Experten fast 200.000 mobile Schadcode-Samples analysiert. Allein im Jahr 2014 analysierten wir weitere 295.539 Samples. Doch diese Zahlen spiegeln noch nicht das gesamte Bild wider. Die Code-Samples werden recycelt und neu verpackt: Im Jahr 2014 stießen wir auf 4.643.582 Installationspakete für mobile Malware (zusätzlich zu den 10.000.000 Installationspaketen aus den Jahren 2004 bis 2013). Die Zahl der Attacken durch mobile Malware ist um das Zehnfache gestiegen – von 69.000 pro Monat im August 2013 auf 644.000 im März 2014 (siehe **Mobile Cyber Threats, Kaspersky Lab and INTERPOL Joint Report, Oktober 2014**).

Bei 53 Prozent aller Detektionen von mobiler Malware handelt es sich jetzt um Schadprogramme, die in der Lage sind, Geld zu stehlen. Eines der auffallendsten Beispiele ist Spveng, der entwickelt wurde, um das Geld der Kunden der drei größten russischen Banken zu rauben. Der Trojaner wartet, bis ein Kunde eine Online-Banking-App öffnet, ersetzt sie dann durch seine eigene und versucht so

an die Anmeldedaten des Kunden zu gelangen. Er versucht zudem, die Kreditkartendaten seiner Opfer zu stehlen, indem er sein eigenes Fenster über der Google-Play-App anzeigt und nach den Kreditkartendetails fragt. Ein weiterer Schädling ist **Waller**, der sich nicht nur wie ein typischer SMS-Trojaner benimmt, sondern auf infizierten Geräten obendrein auch Geld aus QIWI-Wallets stiehlt.

Online-Verbrecher haben ihre Bemühungen, Geld aus ihren Opfern zu pressen, nun breiter gestreut und verwenden auch Methoden, die sich auf Desktop-Rechnern und Laptops bereits bewährt haben. Das schließt unter anderem Erpresser-Trojaner ein, so genannte Ransomware. **Gefälschte Antiviren-Apps** sind ein weiteres Beispiel für einen bewährten Ansatz, der nun auch auf mobile Geräte angewandt wird. Schließlich erschien dieses Jahr auch erstmals ein Trojaner, der über einen C2-Server verwaltet wird, welcher im Netzwerk Tor beherbergt ist. Die **Torec**-Backdoor ist eine Modifikation des gebräuchlichen Tor-Clients Orbot. Der Vorteil liegt selbstverständlich darin, dass der C2-Server nicht offline genommen werden kann.

Bis vor kurzem war jegliche iOS-Malware auf die Ausnutzung von „Jailbreak“-Geräten ausgerichtet.

Doch das Erscheinen von **„WireLurker“** hat gezeigt, dass iOS nicht gegen Angriffe immun ist.

Mobile Geräte sind heute etwas alltägliches, und es ist daher nicht überraschend, dass der Entwicklung mobiler Malware ein cyberkriminelles Geschäftskonstrukt zugrunde liegt, zu dem Schadprogramm-Autoren, Tester, App-Designer, Web-Entwickler und Botnet-Manager gehören.

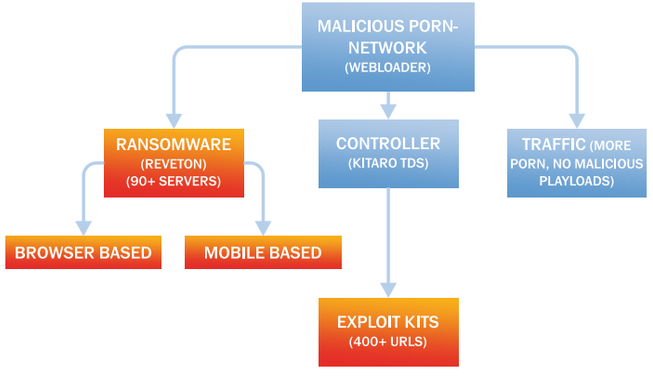
4. GELD ODER DATEI(EN)!

Die Zahl der Erpresser-Programme (Ransomware) ist in den letzten Jahren gestiegen. Einige blockieren einfach den Zugriff auf den infizierten Computer und fordern vom Nutzer ein Lösegeld für die Entsperrung. Doch viele Ransomware-Programme gehen noch weiter, indem sie die Daten auf dem Computer verschlüsseln. Ein jüngeres Beispiel hierfür ist **„ZeroLocker“**. Diese Ransomware verschlüsselt nahezu alle Dateien auf dem infizierten Rechner und fügt den chiffrierten Dateien die Erweiterung „encrypt“ („verschlüsselt“) an (obwohl sie keine Dateien in Verzeichnissen verschlüsselt, die die Wörter „Windows“, „WINDOWS“, „Program Files“, „ZeroLocker“ oder „Destroy“ enthalten, und auch keine Dateien, die größer als 20 MB sind). Der Trojaner verwendet zur Chiffrierung der Dateien einen AES-Schlüssel mit einer Länge von 160 Bit. Nachdem er die Dateien verschlüsselt hat, führt der Schädling das Tool „cipher.exe“ aus, um alle ungenutzten Daten von dem Laufwerk zu entfernen. Durch diese beiden Faktoren wird die Dateiwiederherstellung wesentlich erschwert. Die Cyberkriminellen hinter ZeroLocker verlangen zunächst eine Zahlung von 300 US-Dollar in Bitcoins für die Entschlüsselung der Dateien. Zahlt das Opfer nicht umgehend, so erhöht sich die Gebühr zunächst auf 500 und mit der Zeit dann auf 1.000 US-Dollar.

Ein weiteres Ransomware-Programm, das wir dieses Jahr analysiert haben, ist **Onion**. Dieser Trojaner nutzt nicht nur das Netzwerk Tor, um seine C2 Server zu verbergen, sondern unterstützt auch die vollständige Interaktion mit Tor, ohne jeglichen Input durch das Opfer. Andere Programme dieser Art kommunizieren mit dem Tor-Netzwerk, indem sie die legitime Datei „tor.exe“ starten (manchmal durch die Einschleusung von Code in andere Prozesse). Onion hingegen setzt diese Kommunikation als Teil des Malware-Codes selbst um. Onion verwendet zudem einen unorthodoxen kryptographischen Algorithmus, der die Dateientschlüsselung unmöglich macht, selbst wenn der Datenverkehr zwischen dem Trojaner und dem C2-Server abgefangen wird. Dieser Trojaner setzt nicht nur asymmetrische Verschlüsselung ein, sondern er verwendet auch ein als ECDH (Elliptic Curve Diffie-Hellman) bekanntes kryptografisches Protokoll. Dadurch wird eine Entschlüsselung ohne den privaten Master-Key unmöglich, der wiederum niemals den von den Cyberkriminellen kontrollierten Server verlässt.

Dieses Jahr wurde der Einsatz von Ransomware-Programmen auf Geräte unter Android ausgeweitet. Beispielsweise blockiert die erste Version von **Svpeng**, die Anfang des Jahres 2014 entdeckt wurde, das Telefon unter dem Vorwand, sein Besitzer habe angeblich kinderpornografische Inhalte angesehen, und verlangt eine „Strafe“ von 500 US-Dollar, nach deren Zahlung das Mobiltelefon wieder entsperrt würde. Eine spätere Modifikation dieser Malware, die im Juni 2014 entdeckt wurde, blockiert das Gerät vollständig, so dass es nur noch ausgeschaltet werden kann, indem man den Power-Knopf lange gedrückt hält.

Der Trojaner wird sofort wieder geladen, sobald das Gerät erneut eingeschaltet wird. Diese Version richtete sich in erster Linie gegen Nutzer in den USA, doch wir konnten auch Opfer in Großbritannien, der Schweiz, Deutschland, Indien und Russland identifizieren. Diese Version fordert eine Zahlung von 200 US-Dollar, um das Telefon zu entsperren, die mittels MoneyPak-Vouchers erfolgen soll. Auf dem Bildschirm mit der Lösegeldforderung ist ein Foto des Nutzers zu sehen, das mit der Webkamera aufgenommen wurde. Ein anderer Trojaner mit dem Namen **„Koler“**, der im Mai 2014 entdeckt wurde, verwendet denselben Ansatz: Er blockiert den Zugriff auf das Gerät und verlangt eine Lösegeldzahlung in Höhe von 100 bis 300 US-Dollar, damit das Telefon entsperrt wird. Wie Svpeng tut auch dieser Trojaner dabei so, als stamme diese Nachricht von der Polizei. Er greift Opfer in mehr als 30 Ländern rund um den Globus an und verwendet dabei lokalisierte „Polizei“-Mitteilungen.



Verbreitungsinfrastruktur von Koler

Der erste Trojaner, der Daten verschlüsselt und **„Pletor“** genannt wird, erschien im Mai 2014. Dieser Schädling verwendet den AES-Verschlüsselungsalgorithmus, um die Inhalte auf der Speicherkarte des Telefons zu chiffrieren und zeigt dann eine Lösegeldforderung auf dem Bildschirm an, die mittels der QIWI Visa Wallet des Opfers, mittels MoneXy oder über eine Standardüberweisung an eine Telefonnummer beglichen werden soll. Dieser Trojaner greift in erster Linie Opfer in Russland und der Ukraine an (obwohl wir auch Betroffene in anderen Ländern der ehemaligen Sowjetunion identifiziert haben) und verlangt einen Betrag in Rubel oder in Griwna, der in etwa 300 US-Dollar entspricht.

Die Einträglichkeit von Ransomware hängt davon ab, ob das Opfer zahlt oder nicht. Tun Sie es nicht! Machen Sie stattdessen regelmäßige Backups von Ihren Daten. Wenn Sie jemals Opfer eines Ransomware-Programms werden sollten (oder ein Hardwareproblem haben sollten, das den Zugriff auf Ihre Daten unmöglich macht), verlieren Sie auf diese Weise keine Ihrer Daten.

5. MALWARE FÜR ÜBERFÄLLE AUF BANKAUTOMATEN

Schadprogramme für Bankautomaten sind nichts Neues. Die erste Malware dieser Art, genannt **„Skimer“**, wurde im Jahr 2009 entdeckt. Sie griff Geldautomaten in Osteuropa an, auf denen ein Windows-basiertes Betriebssystem lief. Dieser Schädling nutzte nicht dokumentierte Funktionen, um Details der in einen infizierten Automaten eingeführten Kreditkarten zu drucken und Kassetten mittels eines Mastercard-Befehls zu öffnen. Im Jahr 2010 stieß das Kaspersky-Team in Brasilien auf weitere Geldautomaten-Malware (**„SPSniffer“**): Dieses Schadprogramm sammelte PINs auf veralteten Bankautomaten unter Verwendung von PIN-Pads mit nur schwachem kryptografischen Schutz. Im letzten Jahr registrierten wir schließlich eine weitere Familie von ATM-Schädlingen („Atmer“), die entwickelt wurden, um Geld von Geldautomaten in Mexiko zu stehlen.

In diesem Jahr führten wir nun auf Anfrage einer Finanzinstitution forensische Ermittlungen einer cyberkriminellen Attacke auf zahlreiche Geldautomaten in Asien, Europa und Lateinamerika durch. Der Angriff läuft in zwei Schritten ab. Die Cyberkriminellen verschaffen sich physischen Zugriff auf die Bankautomaten und verwenden eine bootfähige CD, um eine Malware mit dem Namen **„Tyupkin“** darauf zu installieren. Daraufhin booten sie die Maschine neu, um die Malware zu laden und sich selbst die Kontrolle über den Geldautomaten zu verschaffen. Das Schadprogramm läuft dann in einer Endlosschleife und wartet auf Befehle.

Damit der Betrug nicht auffliegt, nimmt die Malware nur sonntags und montags nachts zu bestimmten Uhrzeiten Befehle entgegen. Die Angreifer geben dann eine Ziffernkombination auf der Tastatur des Bankautomaten ein, rufen die Malwarebetreiber an, geben eine weitere Ziffernkombination ein und sammeln dann das von dem Automaten ausgespuckte Geld ein.

Video-Material von Überwachungskameras bei den infizierten Geldautomaten gab Aufschluss über die Methode, mittels derer die Verbrecher an das Geld gelangten. Ein zufälliger Schlüssel wird für jede Sitzung neu generiert: So stellen die Gangster sicher, dass niemand aus Versehen von dem Betrug profitiert.

Der Betreiber der Schadsoftware enthält dann via Telefon Instruktionen von einem anderen Bandenmitglied, das den Algorithmus kennt und in der Lage ist, aufgrund der angezeigten Zahlen einen Sitzungsschlüssel zu generieren: Dadurch wiederum wird sichergestellt, dass die Kuriere, die das Geld einsammeln, keine Alleingänge unternehmen. Nach Eingabe des korrekten Schlüssels zeigt der Automat an, wie viel Geld in jeder Kassette verfügbar ist, und fordert den Verbrecher auf, die Kassette auszuwählen, die geplündert werden soll. Daraufhin gibt sie aus der ausgewählten Kassette 40 Banknoten auf einmal aus.

Die Zunahme von Angriffen auf Geldautomaten in den letzten Jahren ist eine natürliche Weiterentwicklung der bereits etablierten Methoden unter Verwendung von physischen Geräten, die dazu dienen, Daten von Karten abzugreifen, die in manipulierte Geldautomaten eingeführt werden. Leider laufen auf vielen Geldautomaten Betriebssysteme mit bekannten Sicherheitsschwachstellen. Dadurch wird physikalische Sicherheit noch wichtiger. Wir möchten deshalb alle Banken dringend dazu aufrufen, die physische Sicherheit ihrer Bankautomaten zu überprüfen.

6. WINDOWS XP: VERGESSEN, ABER NICHT VERGANGEN?

Der Support für Windows XP lief am 8. April 2014 aus. Das bedeutet, es gibt keine neuen Sicherheitsupdates mehr, keine Sicherheits-Hotfixes, keine technischen Content-Updates online und auch keine kostenlosen oder bezahlpflichtigen Supportoptionen. Leider gibt es aber noch viele Nutzer, auf deren Rechnern Windows XP läuft. Unseren Daten zufolge entfallen etwa 18 Prozent aller Infektionen auf Windows XP. Das heißt, eine Menge Leute haben Angriffen Tür und Tor geöffnet, nachdem keine Sicherheitspatches mehr verfügbar sind. Denn effektiv ist jede Sicherheitslücke, die seit April entdeckt wurde, eine Zero-Day-Schwachstelle – also eine Schwachstelle, für die keine Chance auf einen Patch besteht. Dieses Problem wird sich noch verschärfen, wenn die Anbieter von Apps keine Updates mehr für Windows XP entwickeln. Jede ungepatchte Anwendung bietet dann eine weitere potenzielle Schwachstelle, was die Angriffsfläche wiederum vergrößert. Tatsächlich ist es schon jetzt so weit: Die **neueste Java-Version** unterstützt Windows XP nicht mehr.

Es mag nun so erscheinen, als sei die leichteste und offensichtlichste Lösung dieses Problems ein Upgrade auf ein neueres Betriebssystem. Doch obwohl Microsoft immer wieder auf das Ende des Supports aufmerksam gemacht hat, lässt sich leicht erklären, aus welchen Gründen die Migration zu einem neuen Betriebssystem für einige Unternehmen schwierig sein könnte. Neben den Kosten, die durch die Umstellung entstehen, könnten auch Investitionen für neue Hardware fällig werden, oder es könnte sich als notwendig erweisen, eine eigens für das Unternehmen entwickelte Anwendung zu ersetzen, da diese nicht mehr auf einem neueren Betriebssystem läuft. Daher überrascht es nicht, dass einige Organisationen bereit sind, **für einen verlängerten XP-Support zu zahlen**.

Sicherlich bietet ein Antiviren-Produkt Schutz. Doch das gilt nur, wenn wir unter „Antiviren-Produkt“ eine umfassende Internet-Security-Lösung verstehen, die proaktive Technologien zur Abwehr neuer, unbekannter Bedrohungen verwendet und über eine Funktionalität verfügt, die den Einsatz von Exploits verhindert. Ein Basis-AV-Produkt, das im Wesentlichen auf einer Signatur-basierten Suche nach bekannter Schadsoftware fußt, ist hier unzureichend. Man darf auch nicht vergessen, dass Anbieter von Sicherheitslösungen mit der Zeit ebenfalls neue Schutztechnologien auf den Markt bringen werden, die nicht mehr mit Windows XP kompatibel sind.

Jeder, der jetzt noch Windows XP laufen hat, sollte das als eine Übergangslösung ansehen, für die Zeit, in der die Migrationsstrategie ausgearbeitet wird. Malware-Autoren werden ohne Zweifel Windows XP angreifen, solange eine nennenswerte Zahl von Menschen es weiterhin benutzt, da ein ungepatchtes Betriebssystem ihnen ein viel breiteres Spektrum an Möglichkeiten bietet. Jeder Windows-XP-Computer in einem Netzwerk bietet eine Schwachstelle, die im Rahmen von zielgerichteten Angriffen auf das Unternehmen ausgenutzt werden kann und die dann als Trittbrett in das weitere Netzwerk fungieren könnte.

Keine Frage, dass die Umstellung auf ein neueres Betriebssystem unbequem und mit Kosten verbunden ist – sowohl für Heimanwender als auch für Unternehmen. Aber die Vermeidung des potenziellen Risikos, das die Verwendung eines zunehmend unsicheren Betriebssystems mit sich bringt, sollten die Mühen und Kosten auf jeden Fall wieder wettmachen.

7. UNTER DER ZWIEBELSCHALE

Tor (kurz für „The Onion Router“) ist eine Software, die es ermöglicht, sich im Internet anonym zu bewegen. Es gibt sie schon seit einiger Zeit, sie wurde jedoch hauptsächlich von Experten und Enthusiasten benutzt. Der Gebrauch des Tor-Netzwerks hat in diesem Jahr allerdings stark zugenommen, hauptsächlich wegen der zunehmenden Sorge um die Privatsphäre. Tor ist zu einer hilfreichen Lösung für all jene geworden, die – aus welchen Gründen auch immer – eine Überwachung und das Abfließen ihrer vertraulichen Daten fürchten. Doch von Kaspersky Lab durchgeführte **Untersuchungen** haben gezeigt, dass Tor auch für Cyberkriminelle attraktiv ist. Sie wissen die Anonymität, die diese Software bietet, ebenfalls zu schätzen.

Im Jahr 2013 beobachteten wir erstmals, dass Cyberkriminelle aktiv Tor nutzen, um ihre schädliche Malware-Infrastruktur zu hosten. Die Experten von Kaspersky Lab haben verschiedene Schadprogramme gefunden, die gezielt Tor verwenden. Untersuchungen des Tor-Netzwerks offenbarten, dass viele Ressourcen mit Schadprogrammen in Verbindung stehen, inklusive C2-Servern, Administrationskonsolen und vielem mehr. Indem sie ihre Server im Tor-Netzwerk hosten, sorgen Cyberkriminelle dafür, dass diese schwerer zu identifizieren, zu klassifizieren und zu löschen sind. Es hat sich zudem ein Tor-basierter Untergrundmarkt etabliert, auf dem Malware und gestohlene persönliche Daten gehandelt werden, die meist mit der Krypto-Währung Bitcoin bezahlt werden, wodurch die Spuren der Cyberkriminellen nicht zurückverfolgt werden können. Tor bietet Online-Verbrechern die Möglichkeit, die Operationen der von ihnen benutzten Malware zu verbergen, bei Cybercrime-Services Handel zu treiben und ihre illegalen Einnahmen zu waschen.

Im Juli veröffentlichten wir unsere Analyse eines Erpresser-Trojaners mit dem Namen „Onion“, der neue Wege in der Nutzung des Tor-Netzwerkes beschritt.

Die Entwickler von Android-basierter Schadsoftware haben ebenfalls Tor für sich entdeckt. Der Trojaner **Torec**, eine schädliche Variante des populären Tor-Clients Orbot, verwendet eine Domain in der Pseudo-Zone „.onion“ als C2-Server. Einige Modifikationen des Erpresser-Trojaners **Pletor** nutzen ebenfalls das Netzwerk Tor um mit den Cyberkriminellen zu kommunizieren, die hinter dem Betrug stecken.

Online-Verbrecher können nicht immer auf Straffreiheit hoffen, selbst wenn sie Tor für ihre Machenschaften verwenden, wie eine kürzlich durchgeführte weltweite Strafverfolgungsaktion gegen eine Reihe von Tor-basierten Cybercrime-Services (**„Operation Onymous“**) gezeigt hat.

Das wiederum wirft die Frage auf, wie die daran beteiligen Polizeibehörden in der Lage sein konnten, ein mutmaßlich „undurchdringbares“ Netzwerk zu kompromittieren. Denn zumindest in der Theorie gibt es keine Möglichkeit, den physischen Standort eines Webservers herauszufinden, der hinter einem verborgenen Service steckt, den jemand besucht. Doch es gibt Wege, einen verborgenen Service zu kompromittieren, ohne dabei die Tor-Architektur selbst anzugreifen, wie wir **an dieser Stelle** gezeigt haben. Ein Tor-basierter Service kann nur sicher bleiben, wenn er sorgfältig konfiguriert wurde, wenn er frei von Sicherheitslücken oder Konfigurationsfehlern ist und die Webanwendungen keinerlei Fehler aufweisen.

8. GUTE MALWARE, SCHLECHTE MALWARE!?

Leider ist Software nicht strikt in gute und in schlechte Programme unterteilt. Es besteht immer das Risiko, dass Software, die zu legitimen Zwecken entwickelt wurde, von Cyberkriminellen missbraucht wird. Auf dem Kaspersky Security Analyst Summit 2014 im Februar erläuterten wir, wie eine unsauber in die Firmware von gängigen Laptops und einigen Desktop-Computern implementierte Anti-Diebstahl-Technologie in den Händen von Cyberkriminellen zu einer mächtigen Waffe werden kann. Wir begannen unsere Nachforschungen, nachdem auf einem der privaten Laptops eines Kaspersky-Lab-Mitarbeiters wiederholt Systemprozesse abgestürzt waren, und zwar in Folge einer Instabilität in Modulen, die zu der Software Computrace des Unternehmens Absolute Software gehören. Unser Kollege hatte diese Software niemals installiert und wusste noch nicht einmal, dass sie auf seinem Laptop läuft. Das wiederum bereitete uns Sorgen, da die Installation laut einem Whitepaper von Absolute Software vom Besitzer des Computers oder der IT-Abteilung des Unternehmens durchgeführt werden müsse. Und während die meiste vorinstallierte Software vom Besitzer des Computers entfernt oder deaktiviert werden kann, kann Computrace sogar eine professionelle System-Reinigung und selbst den Austausch der Festplatte überleben. Wir konnten diesen Fall nicht einfach als einmalige Angelegenheit abtun, da wir Hinweise darauf fanden, dass die Computrace-Software auch auf den PCs einiger unserer Experten sowie auf einigen Unternehmensrechnern läuft. Das hatte zur Folge, dass wir eine Tiefenanalyse durchführten.

Bei unserem ersten Blick auf Computrace hielten wir die Software irrtümlicherweise für schädlich, da das Programm mit so vielen Tricks arbeitet, die auch in aktueller Malware zum Einsatz kommen. Aus diesem Grunde wurde diese Software tatsächlich früher als Malware eingestuft, doch aktuell stehen die ausführbaren Dateien von Computrace bei den meisten Antiviren-Anbietern auf der Weißen Liste.

Wir sind der Meinung, dass Computrace in guter Absicht entwickelt wurde. Unsere Untersuchungen zeigen allerdings, dass Sicherheitslücken in der Software Cyberkriminellen die Möglichkeit geben könnten, das Programm zu missbrauchen. Unserer Ansicht nach sollte eine starke Authentifizierung und Verschlüsselung in ein solch leistungsstarkes Tool integriert sein. Wir haben keine Beweise dafür gefunden, dass Computrace-Module heimlich auf den Computern, die wir analysiert haben, aktiviert wurden. Aber es liegt auf der Hand, dass es viele Computer mit aktivierten Computrace-Agents gibt. Wir sind der Meinung, dass es in der Verantwortung der Hersteller und bei Absolute Software liegt, die entsprechenden Nutzer zu identifizieren und ihnen zu erklären, wie sie die Software deaktivieren können, wenn sie sie nicht verwenden möchten. Andernfalls werden diese verwaisten Agents weiter unbemerkt laufen und Gelegenheit zur entfernten Ausnutzung bieten.

Im Juni veröffentlichte Kaspersky Lab die Ergebnisse seiner **jüngsten Untersuchung** der „legalen“ Software Remote Control System (RCS), die von dem italienischen Unternehmen HackingTeam entwickelt wurde.

Wir entdeckten ein Feature, mit dem die RCS-Kontrollserver mit einem Fingerabdruck ausgestattet werden können. Wir konnten diese Methode verwenden, um den gesamten IPv4-Raum zu scannen. Dadurch wurde es uns möglich, alle IP-Adressen der RCS-C2-Server auf der ganzen Welt zu finden. Insgesamt machten wir 326 Server ausfindig, von denen sich die meisten in den USA, Kasachstan und Ecuador befanden. Mehrere IP-Adressen wurden aufgrund ihrer WHOIS-Informationen als regierungszugehörig identifiziert. Natürlich können wir nicht sicher sein, dass die Server, die sich in einem bestimmten Land befinden, auch von den Strafverfolgungsbehörden dieses Landes verwendet werden. Allerdings würde es schon Sinn ergeben: Am Ende würde es grenzübergreifende rechtliche Probleme vermeiden sowie das Risiko minimieren, dass die Server von anderen beschlagnahmt werden. Wir entdeckten zudem eine Reihe von mobilen Schadmodulen für Android, iOS, Windows Mobile und BlackBerry, die von HackingTeam stammen. Sie werden alle unter Verwendung desselben Konfigurationstyps kontrolliert – ein zuverlässiges Zeichen dafür, dass sie miteinander in Verbindung stehen und zur selben Produktfamilie gehören. Da Android und iOS besonders populär sind, waren wir natürlich besonders an den Modulen für diese Plattformen interessiert.

Auf Windows- oder Mac-OS-Rechnern werden die Module mit Hilfe von Infektoren installiert – speziellen ausführbaren Dateien, die auf bereits infizierten Computern laufen. Das iOS-Modul unterstützt ausschließlich Geräte mit Jailbreak. Dadurch werden seine Ausbreitungsmöglichkeiten eingeschränkt, doch die von RCS verwendete Infektionsmethode beinhaltet, dass ein Angreifer ein Jailbreaking-Tool (wie etwa Evasi0n) von einem infizierten Computer aus laufen lassen kann, mit dem das Telefon verbunden ist – solange das Gerät nicht gesperrt ist. Das iOS-Modul ermöglicht es einem Angreifer, die auf dem Gerät gespeicherten Daten einzusehen (inklusive E-Mails, Kontakte, Anruflisten und Webseiten im Cache), unbemerkt das Mikrophon zu aktivieren und in regelmäßigen Abständen Kameraaufnahmen zu machen. Dadurch erhält das Schadmodul die komplette Kontrolle über das Mobilgerät und kann die gesamte Umgebung überwachen.

Das Android-Modul wird von dem Optimiser/Obfuskator DexGuard geschützt, daher war es schwer zu analysieren. Doch wir konnten trotzdem feststellen, dass es über dieselbe Funktionalität wie das iOS-Modul verfügt und zudem von den folgenden Apps Informationen stehlen kann: „com.tencent.mm“, „com,google,android,gm“, „android,calendar“, „com,facebook“, „jp,naver,line,android“ und „com,google.android,talk“.

Diese neuen Daten unterstreichen einmal mehr die Raffinesse solcher Überwachungstools. Die Haltung von Kaspersky Lab gegenüber solchen Tools ist absolut klar: Wir versuchen jegliche Malware aufzuspüren und unschädlich zu machen, ungeachtet ihres Ursprungs und ihrer Bestimmung. Für uns gibt es keine „richtigen“ oder „falschen“ Schadprogramme, und wir haben bereits in der Vergangenheit öffentlich vor den Risiken so genannter „legaler“ Spyware gewarnt. Es ist von zwingender Wichtigkeit, dass diese Überwachungstools nicht in die falschen Hände geraten. Daher kann die IT-Sicherheitsindustrie auch keine Ausnahmen machen, wenn es um die Detektion von Malware geht.

9. PRIVATSPHÄRE UND SICHERHEIT

Die anhaltenden Spannungen zwischen Privatsphäre und Sicherheit sorgten im Jahr 2014 weiterhin für Schlagzeilen.

Es ist wenig überraschend, dass unter den üblichen Datenlecks in diesem Jahr derjenige Sicherheitsvorfall die größte Aufmerksamkeit auf sich gezogen hat, infolge dessen **unzweideutige Fotos verschiedener Hollywood Sternchen gestohlen und daraufhin veröffentlicht wurden**. Diese Geschichte unterstreicht die zweifache Verantwortung, die Provider und Individuen bei der Sicherung online gespeicherter Daten gleichermaßen tragen. Es sieht so aus, als wäre der Diebstahl durch ein Schlupfloch in der Sicherheit der iCloud möglich geworden: Der „Find My iPhone"-Oberfläche fehlte es an jeglicher Beschränkung bei der Anzahl der Passworteingabeversuche, so dass Angreifer in der Lage waren, die Kennwörter ihrer Opfer mit der Brute-Force-Methode zu knacken. Apple hat dieses Leck bald darauf gestopft. Trotzdem wäre dieser Angriff nicht durchführbar gewesen, wenn die Anwender keine so schwachen Passwörter verwendet hätten. Wir leben unsere Leben zunehmend online. Aber viele von uns bedenken nicht, welche Auswirkungen das Online-Speichern von persönlichen Daten haben kann. Die Sicherheit eines Cloud-Services liegt in den Händen des Providers. In dem Moment, in dem wir unsere Daten Dritten anvertrauen, verlieren wir einen Teil der Kontrolle darüber. Es ist wichtig, die Daten sorgfältig auszuwählen, die wir in der Cloud speichern, und gewissenhaft zu entscheiden, welche Daten automatisch von unseren Geräten in die Cloud verschoben werden sollen.

Das Problem mit den Passwörtern verliert nicht an Aktualität. Wählen wir ein Passwort, das leicht zu erraten ist, öffnen wir dem Identitätsdiebstahl Tür und Tor. Das Problem wird potenziert, wenn wir dieses eine Passwort dann immer wieder für alle möglichen Online-Accounts benutzen – denn wird einer dieser Accounts kompromittiert, so sind alle anderen auch gefährdet! Daher bieten viele Provider, Apple, Google und Microsoft eingeschlossen, nun eine Zwei-Faktoren-Authentifizierung an. Das heißt, der Kunde muss einen von einem Hardware-Token generierten oder einen auf ein mobiles Gerät gesendeten Code eingeben, um auf eine Webseite zugreifen zu können, oder zumindest um die Einstellungen seines Accounts zu ändern. Die Zwei-Faktoren-Authentifizierung verstärkt die Sicherheit zweifellos, jedoch nur, wenn sie auch obligatorisch ist und nicht nur als Option angeboten wird.

Zwischen Sicherheit und Benutzerfreundlichkeit muss immer ein Kompromiss gefunden werden. In einem Versuch, diesbezüglich ein Gleichgewicht herzustellen, startete Twitter kürzlich seinen **Digits-Service**. Die Kunden müssen nun nicht länger eine Kombination aus Nutzername und Passwort angeben, um sich bei der App zu registrieren. Stattdessen geben sie einfach ihre Telefonnummer ein. Sie erhalten dann ein Einmalpasswort zur Bestätigung jeder Transaktion – dieser Code wird dann automatisch von der App gelesen. Twitter macht sich hier im Grunde zum Mittelsmann, indem es die Identität des Kunden für den App-Provider überprüft. Das hat mehrere Vorteile. Die Nutzer müssen sich nicht länger mit dem Erstellen einer Kombination aus Nutzername und Passwort herumplagen, um einen Account bei einem App-Provider einzurichten; und sie müssen keine E-Mail-Adresse besitzen. App-Entwickler müssen wiederum kein eigenes Framework bereitstellen, um die Logins zu überprüfen, und sie verlieren keine potenziellen Kunden, die keine Mail-Adresse haben. Twitter bekommt eine bessere Sicht auf das, was die Kunden tatsächlich interessiert. Die Tatsache, dass keine Passwörter mehr auf dem Server des App-Providers gespeichert werden, ist ein zusätzliches Plus: Ein Leck in dessen Server führt also nicht zu dem Verlust von persönlichen Daten der Kunden. Doch wenn jemand sein Gerät verliert oder es gestohlen wird, funktioniert die Überprüfung der Telefonnummer noch immer, und jeder, der Zugriff auf das Gerät hat, kann ebenso wie der legitime Besitzer auf eine App zugreifen. Abgesehen davon ist dieser Ansatz aber kein Rückschritt in der Sicherheit verglichen mit der traditionellen Methode unter Verwendung von Nutzername und Passwort. Aktuell verlangen mobile Apps auch nicht jedes Mal ein Login, wenn sie ausgeführt werden. Wenn also jemand ein Gerät stiehlt und der Besitzer kein Passwort oder keine Fingerabdruck-Erkennung nutzt, so hat der Dieb Zugriff auf alles – E-Mail, Soziale Netzwerke und Apps. Mit anderen Worten: Die Sicherheit hängt ab von einem Single Point of Failure – der PIN, dem Passcode oder dem Fingerabdruck, der für den Zugriff auf das Gerät selbst verwendet wird.

Als Reaktion auf die zunehmenden Sorgen um die Privatsphäre haben die Entwickler der Webseite „pwnedlist.com" ein einfach zu bedienendes Interface entwickelt, auf dem die Nutzer überprüfen können, ob ihre E-Mail-Adressen und Passwörter gestohlen und online veröffentlicht wurden. **Dieses Jahr wurde dieser Service kostenpflichtig**.

Apple und Google haben auf die wachsenden Ängste vor dem Verlust der Privatsphäre mit der Aktivierung der **Standardverschlüsselung von Daten auf iOS- und Android-Geräten** reagiert. Einige Strafverfolgungsbehörden sind der Meinung, das spiele Cyberkriminellen in die Hände, denn sie hätten es damit leichter, die Detektion von Schadprogrammen zu verhindern.

10. INTERNATIONALE STRAFVERFOLGUNG: ZUSAMMENARBEIT ZEIGT ERGEBNISSE

Cyberkriminalität ist ein Teil des Lebens geworden, im Kielwasser unserer immer weiter zunehmenden Online-Aktivitäten. Man könnte meinen, Cyberkriminelle können nach Belieben agieren und kommen ungestraft davon, doch Aktionen von Strafverfolgungsbehörden können einen starken Einfluss auf die Aktivitäten der Online-Gangster haben. Internationale Zusammenarbeit ist dabei aufgrund der globalen Natur von Cyberkriminalität von besonderer Bedeutung. In diesem Jahr hatte die Polizei einige bemerkenswerte Erfolge zu verbuchen.

Im Juni 2014 gelang es den Strafverfolgungsbehörden verschiedener Länder, darunter der britischen **NCA** (National Crime Agency) und dem FBI, das weltumspannende Netz von Computern zu zerschlagen, die für das Funktionieren des Botnetzes **„GameoverZeus“** verantwortlich waren. Die Polizeioperation („Operation Tovar“) unterbrach die Kommunikation, die dem Botnetz zugrunde lag, und entzog den Cyberkriminellen so die Kontrolle über das Zombie-Netzwerk. GameoverZeus war eines der größten aktiven Botnetze, das auf dem Code des Bank-Trojaners Zeus basierte. Das Botnetz infizierte die Computer nicht nur mit dem Trojaner Zeus und stahl Login-Daten für E-Mail-Accounts, Soziale Netzwerke, Online-Banking-Systeme und andere Finanzdienste, sondern das Botnetz verbreitete auch das Erpresser-Programm **„Cryptolocker“.** Durch die Polizeiaktion erhielten die Opfer eine Atempause, in der sie Gelegenheit hatten, ihre Computer zu säubern.

Früher im laufenden Jahr war Kaspersky Lab Teil einer Allianz aus Strafverfolgungs- und Industrieorganisationen, die von der britischen National Crime Agency (NCA) koordiniert wurde und zu dem Zweck gegründet worden war, die **Infrastruktur hinter dem Shylock-Trojaner** zu zerschlagen. Der Bank-Trojaner Shylock, der seinen Namen erhielt, weil sein Code Auszüge aus Shakespeares „Der Kaufmann von Venedig“ enthält, wurde erstmals im Jahr 2011 entdeckt. Wie andere wohl bekannte Bank-Trojaner auch ist **Shylock** eine Man-in-the-Browser-Attacke, die darauf spezialisiert ist, die Login-Daten für Online-Banking-Systeme von den Computern der Bankkunden zu stehlen. Der Trojaner benutzt eine vorkonfigurierte Liste der Zielbanken, die sich in verschiedenen Ländern rund um den Globus befinden.

Im November mündete die **Operation Onymous** in der Zerschlagung zweier grauer Märkte im Netzwerk Tor.

Kaspersky Lab hat im Oktober 2014 ein Abkommen mit INTERPOL unterzeichnet, um die Zusammenarbeit mit der internationalen Strafverfolgungsbehörde im gemeinsamen Kampf gegen Cyberkriminalität auszuweiten.

EIN BLICK IN DIE APT-KRISTALLKUGEL

Autor: Costin Raiu (@craiu)

QUICK INFO

- Fusion von Cyberkriminalität und APT
- Aufspaltung größerer APT-Gruppen
- Sich entwickelnde Malware-Techniken
- Neue Methoden des Datendiebstahls
- Neue APTs von ungewöhnlichen Quellen
- Attacken unter falscher Flagge
- Bedrohungsakteure fügen ihrem Arsenal mobile Attacken hinzu
- APT + Botnetze = Präzise Attacken + massenhafte Überwachung
- Angriffe auf Hotel-Netzwerke
- Kommerzialisierung von APT und die Privatwirtschaft
- Fazit

In den letzten Jahren hat das Global Research and Analysis Team (GReAT) von Kaspersky Lab Licht ins Dunkel einiger der größten APT-Kampagnen gebracht, unter anderem bei RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/Mask und anderen. Bei den Untersuchungen dieser Kampagnen identifizierten wir auch einige Zero-Day-Exploits, unter anderem die erst vor kurzem entdeckte Schwachstelle **CVE-2014-0546**. Wir gehörten außerdem zu den Ersten, die über die aufkommenden Tendenzen in der APT-Welt berichteten, wie zum Beispiel über **Cyber-Söldner,** die Blitzangriffe durchführen, oder – erst kürzlich – über ungewöhnliche Angriffsziele **wie WLAN-Netze in Hotels**. Im Laufe der letzten Jahre hat das Global Research and Analysis Team (GReAT) von Kaspersky über 60 Bedrohungsakteure beobachtet, die weltweit für Cyberangriffe verantwortlich sind. Das sind Organisationen, die anscheinend viele Sprachen fließend beherrschen, wie etwa Russisch, Chinesisch, Deutsch, Spanisch, Arabisch, Persisch und andere.

Logbook

Durch eine genaue Beobachtung dieser Akteure konnten wir eine Liste der Bedrohungen erstellen, die unserer Meinung nach zu den künftigen Trends in der APT-Welt gehören. Wir meinen, diese Bedrohungen werden im Jahr 2015 eine wichtige Rolle spielen und unsere besondere Aufmerksamkeit verdienen – nicht nur von einem geheimdienstlichen Standpunkt aus betrachtet, sondern auch bezüglich der Technologien, die dazu dienen, diese Bedrohungen aufzuhalten.

FUSION VON CYBERKRIMINALITÄT UND APT

Viele Jahre lang waren cyberkriminelle Gangs ausschließlich darauf fokussiert, den Endnutzern Geld zu stehlen. Eine Explosion bei den Kreditkartendiebstählen, unzählige Fälle von „Entführungen" elektronischer Bezahlkonten oder das Abfangen von Online-Banking-Verbindungen haben zu Verlusten der Verbraucher in Höhe vieler hundert Millionen US-Dollar geführt. Vielleicht ist dieser Markt nicht mehr so lukrativ oder einfach gesättigt. In jedem Fall sieht es nun so aus, als gäbe es einen „Überlebenskampf", und dieser Kampf führt wie immer zu einer Evolution.

WAS ZU ERWARTEN IST: In einem Fall, den wir kürzlich **untersucht haben**, kompromittierten die Angreifer den Computer eines Buchhalters und benutzten ihn, um eine große Überweisung bei ihrer Bank zu tätigen. Obwohl es so scheinen mag, als wäre das nicht sehr ungewöhnlich, sehen wir hierin vielmehr einen interessanten Trend: **Zielgerichtete Attacken direkt gegen Banken und nicht gegen deren Kunden.**

In verschiedenen Fällen, die die Experten aus dem Global Research and Analysis Team von Kaspersky Lab untersucht haben, wurden mehrere Banken unter Verwendung von Methoden attackiert, die direkt aus dem APT-Lehrbuch stammen. Waren die Angreifer erst einmal in die Netzwerke einer Bank eingedrungen, konnten sie ausreichend Informationen sammeln, die es ihnen ermöglichten, auf verschiedene Arten das Geld direkt von der Bank zu stehlen:

- Entfernte Steuerung von Geldautomaten, die dann auf Befehl Bargeld ausgeben.
- Durchführung von SWIFT-Überweisungen von verschiedenen Kundenkonten.
- Manipulation von Online-Banking-Systemen zur Durchführung von Überweisungen im Hintergrund.

Diese Angriffe sind Anzeichen für einen neuen Trend, der die APT-artigen Attacken in der Cybercrime-Welt erfasst. Wie immer machen es sich die Online-Verbrecher so einfach wie möglich: Sie greifen nun die Banken direkt an, weil dort das Geld ist. Wir sind der Meinung, dass wir es mit einem Trend zu tun haben, der unsere Aufmerksamkeit verdient und sich im Jahr 2015 noch weiter ausbreiten wird.

AUFSPALTUNG GRÖSSERER APT-GRUPPEN

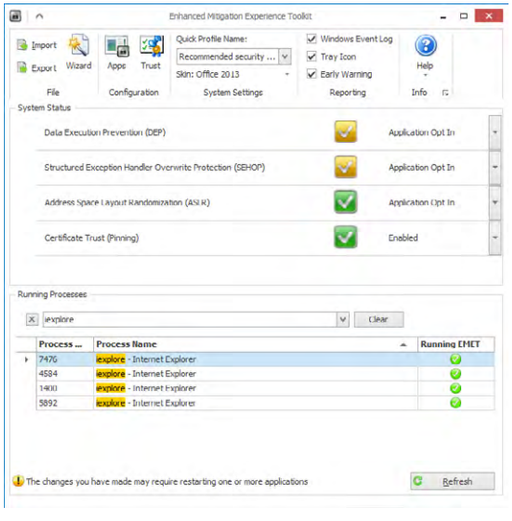
Im Jahr 2014 waren verschiedene Quellen dafür verantwortlich, dass APT-Gruppen an das Licht der Öffentlichkeit gezerrt wurden. Der vermutlich bekannteste Fall dieser Art ist die **FBI-Anklage** von fünf Hackern wegen unterschiedlicher Computerdelikte:

Aufgrund dieses öffentlichen „an-den-Pranger-Stellens“ ist zu erwarten, dass einige der größeren und auffälligeren APT-Banden auseinanderbrechen und in kleinere Gruppen zerfallen werden, die unabhängig voneinander agieren.

WAS ZU ERWARTEN IST: Die Folge wird eine breiter gestreute Angriffsbasis sein, was wiederum bedeutet, dass mehr Unternehmen betroffen sein werden, da kleinere Gruppen enger spezialisierte Attacken durchführen werden. Gleichzeitig bedeutet es, dass größere Unternehmen, die vorher von zwei oder drei der großen APT-Gruppen kompromittiert wurden (zum Beispiel von Comments Crew und Wekby), mannigfaltigeren Angriffen von einer größeren Auswahl an Quellen ausgesetzt sein werden.

SICH ENTWICKELNDE MALWARE-TECHNIKEN

Während Computer immer leistungsstärker und komplexer werden, stehen ihnen diesbezüglich auch die Betriebssysteme in nichts nach. Sowohl Apple als auch Microsoft haben eine Menge Zeit investiert, um die Sicherheitsvorkehrungen ihrer jeweiligen Betriebssysteme zu verbessern. Zusätzlich sind nun spezielle Tools wie etwa Microsofts EMET verfügbar, die helfen können, zielgerichtete Attacken auf Sicherheitslücken zu verhindern.



Da Windows x64 und Apple Yosemite immer populärer werden, erwarten wir, dass die APT-Banden ihre Toolsets mit leistungsstärkeren Backdoors und fortschrittlicheren Technologien zur Umgehung von Sicherheitslösungen ausstatten werden.

WAS ZU ERWARTEN IST: Schon jetzt stellen APT-Banden laufend Schadprogramme für 64-Bit-Systeme bereit, Rookits eingeschlossen. Für das Jahr 2015 erwarten wir raffiniertere Malware-Implantate, verbesserte Umgehungstechniken und den Einsatz von Dateisystemen (wie auch bei **Turla** und **Regin**), um wertvolle Tools und gestohlene Daten zu verstecken.

Zwar beobachten wir einerseits diese Zunahme fortschrittlicher Techniken, doch andererseits schlagen einige Angreifer genau den entgegengesetzten Weg ein. Während sie die Zahl der Exploits und den Umfang von kompiliertem Code minimieren, die sie insgesamt in kompromittierte Netzwerke einschleusen, verlangt ihre Arbeit weiterhin, dass raffinierter Code oder Exploits über einen dauerhaften Zugang ins Unternehmen eingeschleust werden. Diese Tätigkeit macht Skript-Tools und Privilegien-Eskalationen aller Art erforderlich sowie gestohlene Zugangsdaten zu den Opferorganisationen.

Wie wir es bei **BlackEnergy 2** (BE2) beobachten konnten, verteidigen Angreifer ihre eigene Präsenz und Identität innerhalb der Netzwerke ihrer Opfer, nachdem sie entdeckt wurden. Die Techniken zur Verlängerung der Lebensdauer ihrer Machwerke in Netzwerken werden immer fortschrittlicher und breiten sich immer weiter aus. Dieselben Gruppen werden den Umfang und die Aggressivität der zerstörerischen Komponenten steigern, die verwendet werden, um ihre Spuren zu verwischen, und sie werden weiteren *nix-Support, Netzwerk-Equipment und eingebetteten Betriebssystem-Support integrieren. Wir konnten bereits eine gewisse Expansion von BE2-, Yeti- und Winnti-Akteuren beobachten.

NEUE METHODEN DES DATENDIEBSTAHLS

Die Zeiten, in denen Angreifer einfach eine Backdoor in einem Unternehmensnetzwerk aktiviert und dann Terabytes von Daten auf FTP-Server rund um den Erdball abgeleitet haben, sind schon lange vorbei. Raffiniertere Gruppen verwenden heutzutage neben maßgeschneiderten Kommunikationsprotokollen regelmäßig SSL.

Einige wegweisende Gruppen verlegen sich darauf, Netzwerkgeräte mit Backdoors auszustatten und den Traffic direkt für Befehle abzufangen. Andere Techniken, die wir beobachten konnten, beinhalten das Umleiten gestohlener Daten in Cloud-Services, beispielsweise über das Protokoll WebDAV (erleichtert die Zusammenarbeit zwischen Nutzern beim Bearbeiten und Verwalten von auf Webservern gespeicherten Dokumenten und Dateien).

Das wiederum hatte zur Folge, dass viele Unternehmen öffentliche Cloud-Services wie Dropbox aus ihren Netzwerken verbannt haben. Doch es ist und bleibt eine effektive Methode, die Intrusion-Detection-Systeme und DNS-Blacklists zu umgehen.

WAS ZU ERWARTEN IST: Im Jahr 2015 werden mehr cyberkriminelle Gruppen Cloud-Services nutzen, um den Datendiebstahl noch besser zu verheimlichen und ihn schwerer durchschaubar zu machen.

NEUE APTS VON UNGEWÖHNLICHEN QUELLEN, DA SICH IMMER MEHR LÄNDER AM CYBER-WETTRÜSTEN BETEILIGEN

Im Februar 2014 veröffentlichten wir eine Studie über **Careto/Mask**, einen extrem hochentwickelten Bedrohungsakteur, der anscheinend fehlerfrei Spanisch beherrscht, eine Sprache, die im Rahmen zielgerichteter Attacken nur selten anzutreffen ist. Im August brachten wir außerdem einen Bericht über **Machete** heraus – ein weiterer Schädling, der sich der spanischen Sprache bedient.

Bis dahin hatten wir es in erster Linie mit APT-Akteuren zu tun, die nur einige wenige Sprachen fließend beherrschten. Hinzu kommt, dass viele Profis nicht ihre Muttersprache verwenden, sondern es vorziehen, perfektes Englisch zu schreiben.

Im Jahr 2014 konnten wir beobachten, dass viele Nationen rund um den Globus öffentlich ihr Interesse bekundet haben, APT-Kapazitäten zu entwickeln:

WAS ZU ERWARTEN IST: Obwohl wir bisher noch keine APT-Attacke beobachten konnten, die sich der schwedischen Sprache bedient, sagen wir voraus, dass sich immer mehr Länder am Cyber-Wettrüsten beteiligen und ihre Cyberspionage-Ressourcen ausbauen werden.

ATTACKEN UNTER FALSCHER FLAGGE

Angreifer machen Fehler. In der überwiegenden Mehrheit der Fälle, die wir analysieren, finden wir Artefakte, die Aufschluss über die von den Angreifern gesprochene Sprache geben. Beispielsweise schlussfolgerten wir im Fall von **Roter Oktober** und **Epic Turla**, dass die Angreifer vermutlich fließend Russisch sprechen. Im Fall von **NetTraveler** kamen wir zu dem Schluss, dass die Cyberverbrecher die chinesische Sprache perfekt beherrschen.

In einigen Fällen beobachten Experten andere Metamerkmale, die auf die Angreifer hinweisen könnten. Eine Analyse der Zeitstempel der in der Attacke verwendeten Dateien kann etwa Rückschlüsse darauf zulassen, in welchem Teil der Welt die meisten Samples kompiliert wurden.

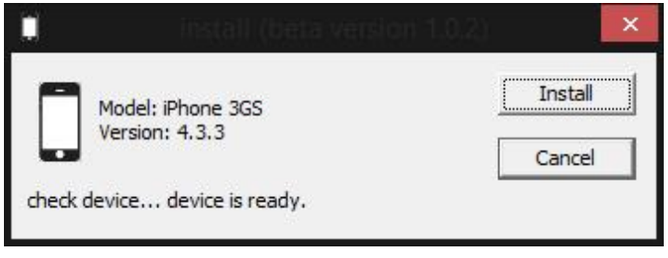
Doch die Angreifer beginnen, auf diese Situation zu reagieren. Im Jahr 2014 hatten wir es mehrfach mit Operationen „unter falscher Flagge“ zu tun, bei denen Angreifer „inaktive“ Malware aufboten, die normalerweise von anderen APT-Gruppen verwendet wird. So kann man sich beispielsweise einen Akteur westlicher Herkunft vorstellen, der ein Schadprogramm in Umlauf bringt, das normalerweise von der „Comment Crew”, einem bekannten chinesischen Akteur, verwendet wird. Während jeder die von „Comment Crew” eingeschleuste Malware kennt, waren nur wenige Opfer in der Lage, die hochentwickelten neuen Einschleusungen zu analysieren. Das könnte leicht zu der falschen Schlussfolgerung führen, dass der chinesische Bedrohungsakteur hinter dieser Attacke steckt.

WAS ZU ERWARTEN IST: Da immer mehr Regierungen geneigt sind, die Angreifer öffentlich an den Pranger zu stellen, sind wir der Meinung, dass die APT-Gruppen im Jahr 2015 größere Vorsicht walten lassen und häufiger unter falscher Flagge operieren werden.

BEDROHUNGSAKTEURE FÜGEN IHREM ARSENAL MOBILE ATTACKEN HINZU

Obwohl schon beobachtet wurde, dass APT-Gruppen Mobiltelefone infiziert haben, war das bisher noch kein wegweisender Trend. Vielleicht sind die Angreifer auf Daten aus, die normalerweise nicht auf Smartphones verfügbar sind, oder sie haben nicht alle Zugriff auf Technologien, die Geräte unter Android und iOS infizieren können.

Im Jahr 2014 erschienen einige neue APT-Tools, die für die Infektion mobiler Geräte entwickelt wurden, so zum Beispiel das **Remote Control System von Hacking Team**.



Außerdem wurden während der Hongkonger Proteste im Oktober 2014 Attacken auf Android- und iOS-Nutzer registriert. Die Angriffe stehen anscheinend mit APT-Operationen in Verbindung.

Auch wenn auf Mobiltelefonen keine wertvollen Dokumente, Schaltbilder oder geopolitischen Expansionspläne für die nächsten zehn Jahre gespeichert sind, so können sie doch eine wertvolle Quelle für Kontakte und auch eine gute Abhörstation sein. Wir haben das bei der Gruppe hinter Roter Oktober beobachtet, die in der Lage war, Mobiltelefone zu infizieren und sie in mobile Wanzen zu verwandeln.

WAS ZU ERWARTEN IST: Für das Jahr 2015 erwarten wir mehr mobil-spezifische Malware, mit einem Fokus auf Android und iOS mit Jailbreak.

APT + BOTNETZE = PRÄZISE ATTACKEN + MASSENHAFTE ÜBERWACHUNG

Im Allgemeinen gehen APT-Gruppen bei ihren Operationen vorsichtig vor, um unnötiges Aufsehen zu vermeiden. Daher ist bei APT-Attacken verwendete Malware sehr viel weniger weit verbreitet als gewöhnliche Malware, wie etwa Zeus, SpyEye und Cryptolocker.

Im Jahr 2014 beobachteten wir zwei APT-Gruppen (Animal Farm und Darkhotel), die zusätzlich zu ihren regulären zielgerichteten Operationen auch Botnetze einsetzten. Sicherlich können sich Botnetze im Cyberkrieg von schätzbarem Wert erweisen und sie können bei DDoS-Attacken auf feindliche Länder eingesetzt werden; das ist in der Vergangenheit bereits der Fall gewesen. Daher ist es nachvollziehbar, warum einige APT-Banden zusätzlich zu ihren zielgerichteten Operationen auch bestrebt sind, Botnetze aufzubauen.

Neben den DDoS-Attacken bieten Botnetze auch noch einen anderen Vorteil – sie können einem „armen Land“ als massenhaftes Abhör-Instrument dienen. Flame und Gauss beispielsweise, die Kaspersky Lab im Jahr 2012 entdeckte, wurden als Massenüberwachungs-Tools konzipiert, die automatisch Informationen von zehntausenden Opfern sammelten. Diese Informationen sollten dann von einem Supercomputer analysiert, indexiert und nach Schlüsselwörtern und Themen zusammengefasst werden; die meisten davon sind vermutlich nutzlos. Doch unter diesen hunderttausenden gestohlenen Dokumenten liefert vielleicht eines die entscheidenden geheimdienstlichen Informationen, die in bestimmten Situationen den Unterschied ausmachen.

WAS ZU ERWARTEN IST: im Jahr 2015 werden mehr APT-Gruppen diesem Trend folgen und zielgerichtete, lautlose Attacken durchführen und daneben lärmende Operationen initiieren, um ihre eigenen Zombie-Netzwerke zu errichten.

ANGRIFFE AUF HOTEL-NETZWERKE

Die **Darkhotel-Bande** ist ein APT-Akteur, von dem bekannt ist, dass er in gewissen Ländern bestimmte Besucher während ihrer Aufenthalte in Hotels angreift. Tatsächlich bieten Hotels hervorragende Möglichkeiten, eine bestimmte Kategorie von Menschen anzugreifen, wie etwa Führungskräfte. Angriffe auf Hotels sind überaus lukrativ, da sie Daten über die Bewegungen von wichtigen Individuen rund um den Erdball liefern.

Der Angriff auf ein Hotel-Reservierungssystem ist eine gute Methode, ein bestimmtes Ziel auszuspionieren. Die Cyberkriminellen erfahren so, in welchem Zimmer das Opfer abgestiegen ist, was wiederum sowohl physische als auch virtuelle Angriffe möglich macht.

Es ist nicht immer einfach, ein Hotel anzugreifen. Das ist auch der Grund dafür, dass es in der Vergangenheit nur einige wenige Gruppen getan haben, sozusagen die Crème de la Crème der APT-Akteure, bei denen diese Attacken zum Angriffs-Repertoire gehören.

WAS ZU ERWARTEN IST: Einige wenige andere Gruppen werden diese Techniken im Jahr 2015 aufgreifen, aber sie werden für die meisten APT-Akteure außerhalb ihrer Reichweite bleiben.

KOMMERZIALISIERUNG VON APT UND DIE PRIVATWIRTSCHAFT

In den letzten Jahren haben wir ausführliche Analysen über Schadprogramme veröffentlicht, die von Unternehmen wie HackingTeam oder Gamma International entwickelt wurden, zwei der bekanntesten Anbieter „legaler Spionagesoftware“. Obwohl die Unternehmen behaupten, ihre Programme nur an „vertrauenswürdige Regierungsinstitutionen“ zu verkaufen, haben öffentliche Berichte von verschiedenen Quellen, unter anderem Citizen Lab, wiederholt gezeigt, dass der Verkauf von Spyware nicht kontrolliert werden kann. Irgendwann landen diese gefährlichen Softwareprodukte in den Händen von weniger vertrauenswürdigen Individuen oder Nationen, die sie dann für die Cyberspionage gegen andere Länder oder gegen das eigene Volk einsetzen.

Tatsache ist, dass solche Aktivitäten für Unternehmen, die Cyberspionage-Software entwickeln, höchst profitabel sind. Das Risiko ist für sie zudem gering, da uns nicht bekannt ist, dass eines dieser Unternehmen in einem Fall von Cyberspionage verurteilt wurde. Die Entwickler dieser Tools befinden sich normalerweise außerhalb der Reichweite des Gesetzes, da der Nutzer des Tools zur Verantwortung gezogen wird, und nicht das Unternehmen, das die Spionage überhaupt möglich macht.

WAS ZU ERWARTEN IST: Dieses einträgliche und risikoarme Geschäft wird zur vermehrten Gründung von Softwarefirmen führen, die auf dem Markt der „legalen Überwachungstools“ mitmischen. Das wiederum bedeutet, dass diese Tools in Spionageoperationen zwischen Nationen, zur internen Spionage und vielleicht sogar zur Sabotage eingesetzt werden.

FAZIT

Die APT-Vorfälle im Jahr 2014 kann man unter dem Strich als raffiniert und mannigfaltig bezeichnen. Wir haben mehrere Zero-Day-Sicherheitslücken entdeckt, zum Beispiel **CVE-2014-0515**, die von einer Gruppe ausgenutzt wurde, die wir „Animal Farm” nennen. CVE-2014-0487, eine weitere von uns entdeckte Zero-Day-Sicherheitslücke, wurde von der **DarkHotel-Bande** missbraucht. Neben diesen Zero-Day-Sicherheitslücken konnten wir verschiedene neue Nachhaltigkeits- und Verbergungstechniken beobachten, die wiederum in der Entwicklung und Bereitstellung verschiedener Abwehrmechanismen für unsere Nutzer resultierten.

Wenn wir das Jahr 2014 als „raffiniert“ bezeichnen, muss die Charakterisierung für das Jahr 2015 „schwer fassbar“ lauten. Wir meinen, dass sich mehr APT-Gruppen Sorgen um ihre Entdeckung machen und noch fortschrittlichere Maßnahmen ergreifen werden, um sich davor zu schützen.

Schließlich werden einige von ihnen Operationen „unter falscher Flagge“ durchführen. Wir sagen diese Entwicklungen voraus und werden sie wie immer sorgfältig in unseren Berichten dokumentieren.

Protecting Your World Against Cyber Security Threats

VORSCHAU AUF 2015

Autor(en): Global Research & Analysis Team (GReAT), Kaspersky Lab

QUICK INFO

- Cyberkriminelle entdecken APTs
- APT-Gruppen spalten sich auf und streuen Angriffe
- Alter Code, neue (gefährliche) Sicherheitslücken
- Eskalation der Angriffe auf Geldautomaten und Kassen-Systeme
- Mac-Angriffe: OS-X-Botnetze
- Angriffe auf Ticketautomaten
- Apple Pay
- Angriffe auf virtuelle Zahlungssysteme
- Missbrauch des Internet der Dinge

CYBERKRIMINELLE ENTDECKEN APTS

Im Jahr 2015 erwartet Kaspersky Lab eine neue Stufe in der Evolution cyberkrimineller Aktivitäten. Vor allem gehen wir davon aus, dass APT-Taktiken (Advanced Persistent Threats) und -Techniken stärker in finanziell motivierten, kriminellen Aktivitäten genutzt werden.

Während einer aktuellen **Untersuchung** haben wir eine Attacke entdeckt, bei der der Computer eines Buchhalters kompromittiert und dazu missbraucht worden war, eine große finanzielle Transaktion über eine Bank zu starten. Das zeigt das Aufkommen eines interessanten Trends: zielgerichtete Angriffe direkt auf Banken.
Wir registrieren immer mehr Vorfälle mit Schadprogrammen, die in Banken eindringen und dabei Methoden nutzen, die aus einem APT-Lehrbuch stammen könnten. Sind die Angreifer einmal im Netzwerk der Bank, ziehen sie genug Informationen ab, um Geld auf mehrere Arten direkt von der Bank stehlen zu können:

- sie befehlen Geldautomaten per Fernbedienung, Geld auszuspucken
- sie führen SWIFT-Überweisungen von verschiedenen Kundenkonten aus durch
- sie manipulieren Online-Banking-Systeme, um im Hintergrund Überweisungen durchführen zu können

Solche Angriffe sind ein Zeichen für den neuen Trend, dass Cyberkriminelle jetzt auch APT-ähnliche Attacken durchführen.

APT-GRUPPEN SPALTEN SICH AUF UND STREUEN ANGRIFFE

Die Aufdeckung von APT-Gruppen im Jahr 2014 führte zur Anklage einer Hackergruppe, die Cyberspionage-Aktionen gegen US-Firmen durchgeführt haben soll.

Da Sicherheitsforscher weiterhin die Aktivitäten regierungsgestützter APT-Gruppen aufdecken, erwarten wir im Jahr 2015 eine Aufspaltung größerer APT-Gruppen in kleinere Einheiten, die unabhängig voneinander operieren. Das wird wiederum eine breiter gestreute Angriffsbasis nach sich ziehen, was bedeutet, dass mehr Firmen betroffen sein werden, da die kleineren Gruppen ihre Angriffe variieren und streuen werden. Gleichzeitig bedeutet das, dass größere Unternehmen, die bisher von zwei oder drei großen APT-Gruppen (zum Beispiel Comment Crew und Webky) angegriffen worden sind, unterschiedlicheren Angriffen ausgesetzt sein werden, die aus verschiedenen Quellen kommen.

ALTER CODE, NEUE (GEFÄHRLICHE) SICHERHEITSLÜCKEN

Wegen mutwillig oder unabsichtlich implementierten Fehlern in Verschlüsselungsalgorithmen („goto fail") oder kritischen Sicherheitslücken in Programmen (Shellshock, Heartbleed, OpenSSL) kommt nicht auditierte Software vielen Anwendern mittlerweile verdächtig vor. Als Reaktion darauf wurden entweder unabhängige Prüfungen bei wichtigen Programmen durchgeführt oder Sicherheitsforscher engagiert, um kritische Sicherheitslücken zu suchen (was so viel wie ein inoffizielles Audit ist). Das bedeutet, dass im Jahr 2015 erneut neue, gefährliche Sicherheitslücken in altem Code auftauchen und Internetnutzer gefährlichen Angriffen ausgesetzt sein werden.

ESKALATION DER ANGRIFFE AUF GELDAUTOMATEN UND KASSEN-SYSTEME

Angriffe auf Geldautomaten scheinen im vergangenen Jahr explosionsartig angestiegen zu sein: Es gab einige große Vorfälle, und die Strafverfolgungsbehörden beeilten sich, auf diese Krise zu reagieren. Eine Konsequenz ist die Erkenntnis, dass Geldautomaten reif sind, angegriffen zu werden, und Cyberkriminelle werden diese Schwäche sicher bemerken. Da die meisten dieser Systeme unter Windows XP laufen und physikalisch schlecht gesichert sind, macht sie das automatisch sehr angreifbar und zum begehrenswerten Ziel für Cyberkriminelle.

Im Jahr 2015 erwartet Kaspersky Lab eine Weiterentwicklung der APT-Angriffe auf Geldautomaten. Mit diesen verfeinerten Techniken wollen die Cyberkriminellen besser an das „Gehirn" der Automaten herankommen. In der folgenden Phase werden die Angreifer dann die Netzwerke der Banken kompromittieren und diesen Zugriff nutzen, um Geldautomaten in Echtzeit zu manipulieren.

MAC-ANGRIFFE: OS-X-BOTNETZE

Trotz aller Bemühungen von Apple, das Mac-Betriebssystem abzusichern, sehen wir laufend, dass schädliche Apple-Programme über Torrent-Netze und als Raubkopien verteilt werden. Die stetig wachsende Popularität von OS-X-Geräten lässt auch Cyberkriminelle aufhorchen, und es wird für sie immer attraktiver, Schadsoftware für diese Plattform zu entwickeln. Das standardmäßig geschlossene Mac-Ökosystem macht es schwerer für Schadprogramme, Apple-Computer erfolgreich zu kompromittieren. Es gibt jedoch viele Nutzer, die nur zu gerne die Sicherheitsmaßnahmen von Mac OS X ausschalten – vor allem, wenn sie dort Raubkopien verwenden.

Das bedeutet, dass Kriminelle, die aus verschiedensten Gründen OS-X-Systeme infizieren wollen, wissen, dass sie ihre schädlichen Machwerke nur mit beliebter Software verknüpfen müssen (wahrscheinlich in Form von Key-Generatoren), um die Schädlinge erfolgreich verbreiten zu können. Dank dem immer noch weit verbreiteten Glauben über die Sicherheit der OS-X-Plattform ist auf diesen Systeme oft auch keine Antivirus-Software installiert, die eine Infizierung verhindern könnte. Schädlinge bleiben auf den Macs damit sehr lange unentdeckt und können unbehelligt ihren Aktivitäten nachgehen.

ANGRIFFE AUF TICKETAUTOMATEN

Vorfälle wie der **Hack des chilenischen öffentlichen Verkehrssystems** zeigen ein Interesse am Missbrauch öffentlicher Ressourcen, etwa von Transportsystemen. Manche Hacker wollen daraus nicht einmal großen Gewinn schlagen. Sie freuen sich schon, wenn sie ein paarmal kostenlos mit der Bahn fahren und diese Möglichkeit mit anderen teilen können, um es den „Firmen so richtig zu zeigen". Gerade Ticketsysteme sind anfällig (da viele unter Windows XP laufen), und verarbeiten Kreditkartendaten direkt. Wir erwarten daher mutigere Angriffe auf diese Systeme, um sie entweder zu kompromittieren oder um Kreditkartendaten zu stehlen.

APPLE PAY

Bisherige Angriffe haben sich auf NFC-Zahlungssysteme konzentriert, doch da diese nur wenig genutzt werden, brachte das kaum illegale Gewinne für die Angreifer. Apple Pay könnte das ändern. Der Enthusiasmus für diese neue Zahlungsmöglichkeit wird deren Nutzung in die Höhe treiben und unvermeidlich auch viele Cyberkriminelle anziehen, die aus den über Apple Pay getätigten Zahlungen Gewinn schlagen wollen. Apple Pay ist sehr stark auf Sicherheit ausgelegt (zum Beispiel virtualisierte Transaktionsdaten), doch wir sind schon gespannt darauf, wie Hacker die Funktionen dieser Implementation ausnutzen werden.

ANGRIFFE AUF VIRTUELLE ZAHLUNGSSYSTEME

Die Erfahrung zeigt uns, dass Cyberkriminelle versuchen, ihre Taten so einfach und effektiv wie möglich in Geld umzumünzen. Was wäre also ein besseres Ziel als virtuelle Zahlungssysteme, die noch in den Kinderschuhen stecken? Da die Beliebtheit virtueller Zahlungssysteme in Ländern wie Ecuador rasant steigt, erwarten wir, dass Cyberkriminelle sich darauf stürzen und sie missbrauchen werden. Egal ob sie die Anwender mit Social-Engineering-Tricks hereinlegen, die Endpunkte (meist Handys) angreifen oder die Banken direkt hacken – Cyberkriminelle werden sich auf direkt monetarisierbare Angriffe verlegen und virtuelle Zahlungssysteme werden die Hauptleidtragenden sein.

Dies kann auch auf Apple Pay ausgeweitet werden, das NFC (Near Field Communication) für drahtlose Transaktionen nutzt. Dieser Bereich ist eine Fundgrube für Sicherheitsforscher. Wir erwarten die ersten Warnungen vor Sicherheitslücken in Apple Pay, Virtual Wallets und anderen virtuellen Zahlungssystemen.

MISSBRAUCH DES INTERNET DER DINGE

Angriffe auf das Internet der Dinge beschränken sich bisher auf manchmal etwas zu reißerische Nachweise der Machbarkeit (Proof-of-Concept). Sie sollen davor warnen, dass Smart-TVs und Kühlschränke von Hackern angegriffen werden können, um Botnetze aufzubauen oder um Angriffe zu starten.

Da es immer mehr solcher verbundenen Geräte gibt, erwarten wir vor allem bei Firmen aus diesem Bereich mehr Diskussionen über die Sicherheit der Produkte und über die Privatsphäre ihrer Anwender. Im Jahr 2015 wird es sicher echte (In-The-Wild-)Angriffe auf Netzwerkdrucker und andere verbundene Geräte geben, die den Angreifern helfen können, ihren Zugriff auf Firmennetzwerke zu gewährleisten. Wir erwarten, dass Geräte aus dem Internet der Dinge zum Ziel von APT-Angriffen werden, vor allem bei ‚attraktiven' Opfern, bei denen eine Konnektivität in Herstellungs- und industrielle Prozesse besteht.

Auf Heimanwenderseite werden solche Angriffe auf die Demonstration von Sicherheitsmängeln in Protokoll-Implementierungen und die Möglichkeit eingebundener Werbung (Adware/Spyware) in das Smart-TV-Programm beschränkt bleiben.

KASPERSKY lab

www.kaspersky.de

DEUTSCHE VERSION

| viruslist.com/de | 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

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 Lab GmbH, Ingolstadt, Deutschland
www.kaspersky.de

Informationen zur Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in Ihrer Nähe finden Sie hier:
www.kaspersky.de/buyoffline

KASPERSKY lab