KASPERSKY SECURITY BULLETIN 2013 / 2014

KASPERSKY LAB
GLOBAL RESEARCH
AND ANALYSIS TEAM
(GREAT)

DEUTSCHE VERSION

KASPERSKY lab

INHALT

KASPERSKY SECURITY BULLETIN 2013/2014

Costin Raiu (@craiu), David Emm (@emm_david)

JAHRESRÜCKBLICK VON KASPERSKY LAB AUF 2013

Es ist wieder einmal Zeit für den traditionellen Jahresrückblick von Kaspersky Lab. In diesem Jahr stehen Ereignisse im Fokus, die die Bedrohungslandschaft im Jahr 2013 geprägt haben.

Zu Beginn überprüfen wir die Überschriften der Voraussagen, die das Kaspersky-Team aufgrund der im Jahr 2012 beobachteten Trends Ende letzten Jahres getroffen hat:

> Zielgerichtete Attacken und Cyberspionage

> Vormarsch des Hacktivismus

> Staatlich gesponserte Cyberattacken

> Verwendung legaler Überwachungstools

> Wolkige Aussichten, mit Malware-Wahrscheinlichkeit

> Alter, wo ist meine Privatsphäre?!

> Wem trauen wir?

> Cyber-Erpressung

> Mac OS-Malware

> Mobile Malware

> Sicherheitslücken und Exploits

Urteilen Sie selbst, wie richtig wir mit unseren Vorhersagen lagen und werfen Sie einen Blick auf unsere Top 10 der Security-Stories 2013!

DIE ZEHN ULTIMATIVEN SECURITY-STORIES DES JAHRES 2013

QUICK-INFO

- Die üblichen Verdächtigen: Roter Oktober, MiniDuke, TeamSpy, NetTraveler, Winnti, Icefog
- Motive für Hackerangriffe
- Mobile Malware und App-Store-(Un)sicherheit
- Wasserloch-Attacken
- Der Mensch als Schwachstelle
- Verlust der Privatsphäre und des Vertrauens
- Sicherheitslücken
- Virtuelle Währungen
- Was 2014 für uns bereithält

Top security stories of 2013 - the expert opinion (Englisch)

1. NEUE „ALTE" CYBERSPIONAGE-KAMPAGNEN

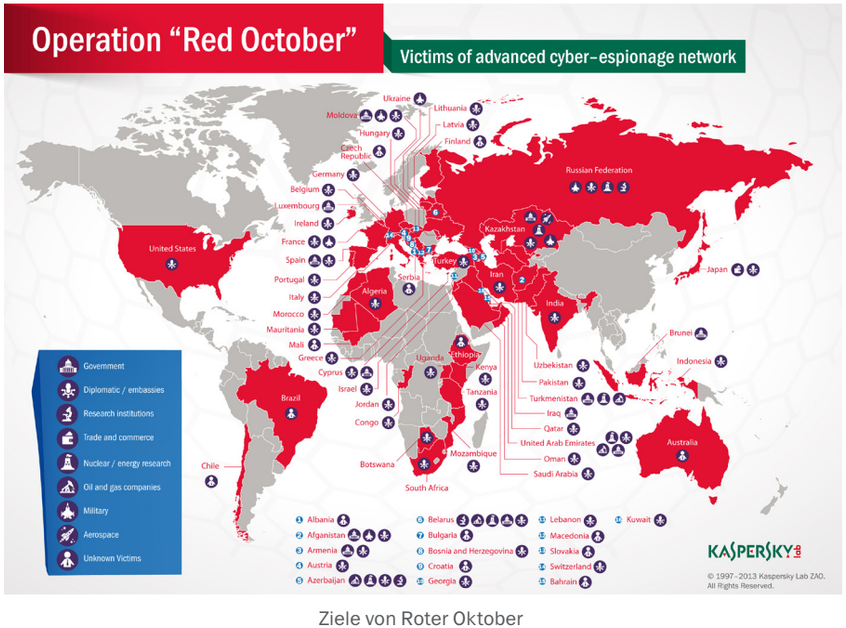
In einer Retrospektive auf das Jahr 2013 mag man Geschichten erwarten, die sich auch in diesem Jahr zugetragen haben.

Doch wenn es um zielgerichtete Attacken geht, ist es nicht ganz so einfach. Oftmals liegen die Ursprünge der Kampagnen weit vor der Zeit, zu der sie bekannt, analysiert und öffentlich gemacht werden. Sie werden sich vielleicht daran erinnern, dass es auch bei Stuxnet so war – je gründlicher wir den Schädling analysierten, desto weiter in die Vergangenheit mussten wir seinen Ursprung

datieren. Dasselbe gilt für einige der großen Cyberspionage-Kampagnen, mit denen es das Kaspersky-Team in diesem Jahr zu tun hatte.

Roter Oktober ist eine Cyberspionage-Kampagne, die hunderte Opfer weltweit betraf, darunter Regierungsorganisationen, diplomatische Einrichtungen und Forschungsinstitutionen, Energiekonzerne sowie Handels- und Weltraumorganisationen. Die Malware ist überaus hoch entwickelt – unter anderem verfügt sie über einen „Wiederbelebungsmodus", der es dem Schädling ermöglicht, Computer immer wieder zu infizieren. Der Code ist sehr modular, wodurch ihn die Angreifer problemlos auf jedes einzelne Ziel passend zuschneiden können.

Interessanterweise sammelte Roter Oktober nicht nur Informationen von traditionellen Endgeräten, sondern auch von mobilen Geräten, die mit den Netzwerken der Opfer verbunden waren – ein klares Eingeständnis der Cyberkriminellen, dass mobile Geräte eine Kernkomponente des heutigen Geschäftslebens sind und wertvolle Informationen enthalten. Kaspersky Lab veröffentlichte die Ergebnisse seiner Analyse im Januar 2013, doch es steht fest, dass die Kampagne auf das Jahr 2008 zurückdatiert.



Ziele von Roter Oktober

Im Februar veröffentlichte Kaspersky Lab die Analyse von MiniDuke, einem Schädling, der entwickelt wurde, um Daten von Regierungsorganisationen und Forschungsinstitutionen zu stehlen. Unsere Analyse deckte 59 prominente, vom Schädling angegriffene Organisationen in 23 Ländern auf, darunter in der Ukraine, Belgien, Portugal, Rumänien, der Tschechischen Republik, Irland, Ungarn und den USA. Wie viele zielgerichtete Attacken kombinierte auch MiniDuke den Einsatz von althergebrachten Social-Engineering-Tricks mit raffinierten Techniken. So enthielt MiniDuke beispielsweise das erste Exploit, das in der Lage ist, die Sandbox im Adobe Acrobat Reader zu umgehen. Zusätzlich erhielten die kompromittierten Endgeräte über eigens eingerichtete Twitter-Accounts Anweisungen vom Command-and-Control-Server (und der Schädling nutzte zudem die Google-Suche als Reservefunktion).

Im März erfuhren die Kaspersky-Experten von einer Angriffswelle, die sich gegen hochrangige Politiker und Menschenrechtsaktivisten in den GUS-Staaten und Osteuropa richtete. Die Angreifer nutzen das Remote-Administrationstool TeamViewer, um die Computer ihrer Opfer zu kontrollieren, daher wurde die Operation unter der Bezeichnung „TeamSpy" bekannt. Der Sinn und Zweck dieser Angriffe war das Sammeln von Informationen auf den kompromittierten Computern. Wenn auch nicht so ausgefeilt und hochentwickelt wie Roter Oktober, NetTraveler und andere Attacken, war diese Kampagne doch erfolgreich – was wiederum beweist, dass nicht alle erfolgreichen zielgerichteten Attacken auf komplett neuem Code basieren müssen.

NetTraveler (auch bekannt als „NetFile"), über den wir im Juni berichteten, ist eine weitere Bedrohung, die zum Zeitpunkt ihrer Entdeckung schon seit langer Zeit aktiv war – in diesem Fall seit 2004.

Diese Kampagne diente dem Diebstahl von Daten, die mit Weltraumforschung, Nanotechnologie, Energiegewinnung, Atomkraft, Lasertechnik, Medizin und Telekommunikation zu tun haben. NetTraveler wurde erfolgreich eingesetzt, um mehr als 350 Organisationen in 40 Ländern zu kompromittieren, unter anderem in Russland, der Mongolei, Indien, Kasachstan, Kirgisien, China, Tadschikistan, Südkorea, Spanien und Deutschland. Die Ziele waren sowohl staatliche als auch

private Organisationen, einschließlich Regierungsbehörden, Botschaften, Öl- und Gasunternehmen, Forschungszentren, Militärlieferanten sowie einzelne Aktivisten.

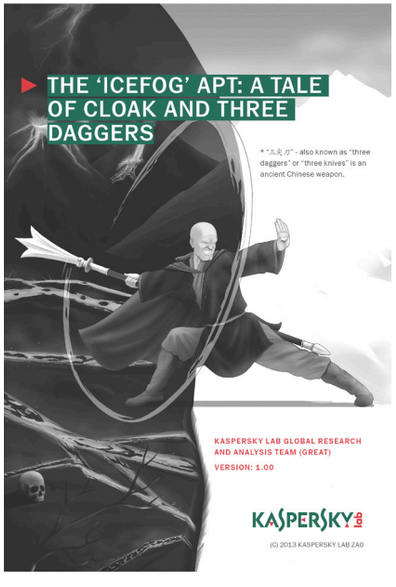
Wenn Ihre Organisation nie Ziel einer Attacke war, ist es einfach, sich einzureden, dass einem so etwas nie passieren wird, oder dass das meiste, was man über Malware hört, reine Übertreibung ist. Es ist einfach, die Schlagzeilen zu lesen und zu dem Schluss zu kommen, dass zielgerichtete Angriffe ausschließlich ein Problem großer Organisationen sind. Aber nicht alle Angriffe richten sich gegen prominente Ziele oder gegen solche, die mit „kritischer Infrastruktur“ in Verbindung stehen. Die Wahrheit ist, dass jede Organisation Opfer einer Attacke werden kann. Jede Organisation, die Daten besitzt, die für Cyberkriminelle von Wert sein oder die als Sprungbrett in andere Unternehmen genutzt werden könnten. Dieser Punkt wurde von den Winnti- und Icefog-Attacken anschaulich demonstriert.

Im April veröffentlichten wir einen Bericht über die Cyberkriminellen-Bande „Winnti“. Diese Gruppe ist seit 2009 aktiv und hat sich auf den Diebstahl von digitalen Zertifikaten spezialisiert, die von legitimen Softwareanbietern signiert wurden, sowie auf den Diebstahl von geistigem Eigentum (unter anderem Quellcode für Online-Gaming-Projekte). Der von dieser Bande verwendete Trojaner ist eine für 64-Bit-Umgebungen kompilierte DLL-Bibliothek. Sie nutzt einen ordnungsgemäß signierten Treiber und fungiert als voll funktionsfähiges Remote-Administration-Tool, das den Angreifern die vollständige Kontrolle über einen kompromittierten Computer verschafft. Insgesamt haben wir mehr als 30 Unternehmen aus der Online-Gaming-Branche identifiziert, die von der Aktivität der Gruppe in Mitleidenschaft gezogen wurden. Die meisten befinden sich in Südostasien, aber auch Firmen in Deutschland, den USA, Japan, China, Russland, Brasilien, Peru, Weißrussland und Großbritannien waren betroffen. Die „Winnti“-Gruppe ist noch immer aktiv.

Die Icefog-Attacken, die Kaspersky Lab im September öffentlich bekannt machte (und die im folgenden Abschnitt besprochen werden), richteten sich gegen Lieferketten sowie gegen sensible Daten innerhalb des angegriffenen Netzwerks. Es wurden aber auch Anmeldedaten für E-Mail-Accounts und Netzwerke von Ressourcen außerhalb des angegriffenen Netzwerks zusammengetragen.

2. CYBER-SÖLDNER - EIN NEUER TREND

Auf den ersten Blick scheint Icefog wie alle anderen auch eine zielgerichtete Attacke zu sein. Es handelt sich hierbei um eine seit 2011 aktive Cyberspionage-Kampagne, die sich hauptsächlich gegen Ziele in Südkorea, Taiwan und Japan, aber auch gegen solche in den USA, Europa und China richtet. So setzen die Angreifer typischerweise Spear-Phishing-Mails ein, die entweder Anhänge oder Links auf schädliche Webseiten enthalten, um so die Malware an die Nutzer zu bringen. Wie bei allen derartigen Attacken ist es schwer, mit Sicherheit zu sagen, wie viele Anwender betroffen sind, doch das Kaspersky-Team konnte mehrere Dutzend betroffene Windows-PCs und mehr als 350 Rechner unter Mac OSX identifizieren (die meisten der letztgenannten in China).



Allerdings gibt es einige herausragende Merkmale, die diese Attacke von denen unterscheidet, über die wir eingangs berichteten. Erstens ist Icefog Teil eines aufkommenden Trends – Angriffe kleiner Gruppen von Cybersöldnern, die schnell zuschlagen und danach sofort wieder verschwinden. Zweitens greifen die Verbrecher ganz gezielt die Lieferkette an: Unter den Opfern waren Regierungsinstitutionen, Militärlieferanten, Reedereien, Telekommunikationsanbieter, Satellitenbetreiber, Industrie- und Hightech-Unternehmen sowie Massenmedien. Drittens stützen sich ihre Kampagnen auf maßgeschneiderte Cyberspionage-Tools für Windows und Mac OS X, und sie kontrollieren die kompromittierten Computer direkt. Zudem hat Kaspersky Lab beobachtet, dass die Cyberkriminellen neben Icefog auch Backdoors und andere schädliche Werkzeuge als Quereinstieg innerhalb der Zielorganisationen und zum Ausschleusen von Daten nutzen.

Die chinesische Gruppe „Hidden Lynx“, über deren Aktivität die Experten von Symantec im September berichteten, fallen in dieselbe Kategorie – „Söldner“, die Angriffe mit Hilfe von innovativen maßgeschneiderten Tools durchführen. Diese Gruppe war unter anderem für eine Attacke auf Bit9 in diesem Jahr verantwortlich. Wir nehmen an, dass die Zahl solcher Gruppen künftig steigen wird, da sich nach und nach ein Schwarzmarkt für „APT“-Dienstleistungen bildet.

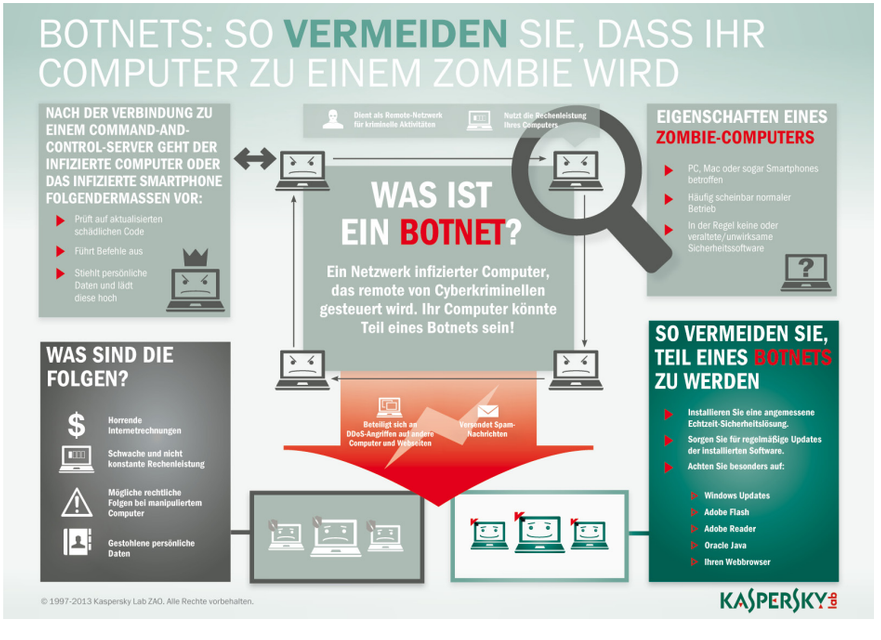
3. HACKTIVISMUS UND LECKS

Der Diebstahl von Geld – entweder direkt über den Zugriff auf Bankkonten oder indirekt durch den Diebstahl von vertraulichen Daten – ist nicht das einzige Motiv für Hackerangriffe. Sie können auch eine Form des politischen oder sozialen Protests sein oder den Sinn haben, die Reputation des angegriffenen Unternehmens zu untergraben. Tatsache ist, dass das Internet heute nahezu jeden Aspekt des Lebens durchdringt. Für jemanden mit den entsprechenden Fähigkeiten ist es unter Umständen einfacher, eine Attacke auf eine kommerzielle Webseite oder die Online-Ressource einer Regierung durchzuführen, als eine Protestaktion oder Demonstration in der realen Welt zu koordinieren.

Eine Art dieser Angriffe sind DDoS-Attacken (Distributed Denial of Service). Eine der größten derartigen Angriffe in der Geschichte (einige würden behaupten, es war DIE größte schlechthin) richtete sich im März gegen Spamhaus. Es wird geschätzt, dass die Attacke in der Spitze einen Datendurchsatz von 300 GB pro Sekunde erreichte. Eine der Organisationen, die verdächtigt wurde, hinter dem Angriff zu stecken, hieß Cyberbunker. Der Konflikt zwischen dieser Organisation und Spamhaus geht zurück bis in das Jahr 2011, erreichte jedoch seinen Höhepunkt, als Cyberbunker einige Wochen vor dem Vorfall von Spamhaus auf die Schwarze Liste gesetzt wurde. Die Besitzer von Cyberbunker wiesen die Vorwürfe zurück, traten jedoch als Sprecher für die für den Angriff verantwortlichen Hacker auf. Die Attacke wurde eindeutig von jemandem durchgeführt, der in der

Lage ist, Unmengen von Traffic zu generieren. Um die Auswirkungen der Attacke abzumildern, war Spamhaus gezwungen, zu CloudFlare zu wechseln, einem Hosting- und Serviceprovider, der dafür bekannt ist, groß angelegte DDoS-Attacken abzuwehren. Während einige der Schlagzeilen mit dem Tenor „Die Welt wird nie wieder so sein, wie sie einmal war“ die Folgen dieses Ereignisses sicherlich überbewerteten, hat der Vorfall dennoch gezeigt, was für einen Einfluss ein fest entschlossener Angreifer haben kann.

Während der Angriff auf Spamhaus ein isolierter Vorfall zu sein scheint, haben sich laufende Hacktivisten-Aktionen von Gruppen, die schon seit längerem aktiv sind, auch in diesem Jahr fortgesetzt. Dazu gehört auch „Anonymous“. Im Jahr 2013 hat diese Gruppe die Verantwortung für Attacken auf das US-Justizministerium, das MIT (Massachusetts Institute of Technology) sowie auf die Webseiten von diversen Regierungen übernommen, unter anderem von Polen, Griechenland, Singapur, Indonesien und Australien (die letzten zwei Vorfälle schließen einen Austausch der Anonymous-Gruppen in den jeweiligen Ländern ein). Die Gruppe behauptet zudem, das WLAN-Netz des britischen Parlaments während der Proteste auf dem Parliament Square in der ersten Novemberwoche gehackt zu haben.



Auch die so genannte „Syrian Electronic Army“ (Unterstützer des syrischen Präsidenten Bashar-al-Assad) waren über das Jahr aktiv. Im April übernahmen sie die Verantwortung für den Hack des Twitter-Accounts der Nachrichtenagentur Associated Press und für das Senden eines gefälschten Tweets über eine Explosion im Weißen Haus – wodurch der US-amerikanische Aktienindex DOW vorübergehend 136 Milliarden Dollar an Wert verlor. Im Juli kompromittierte die Gruppe die Gmail-Accounts dreier Mitarbeiter des Weißen Hauses und den Twitter-Account von Thomson Reuters.

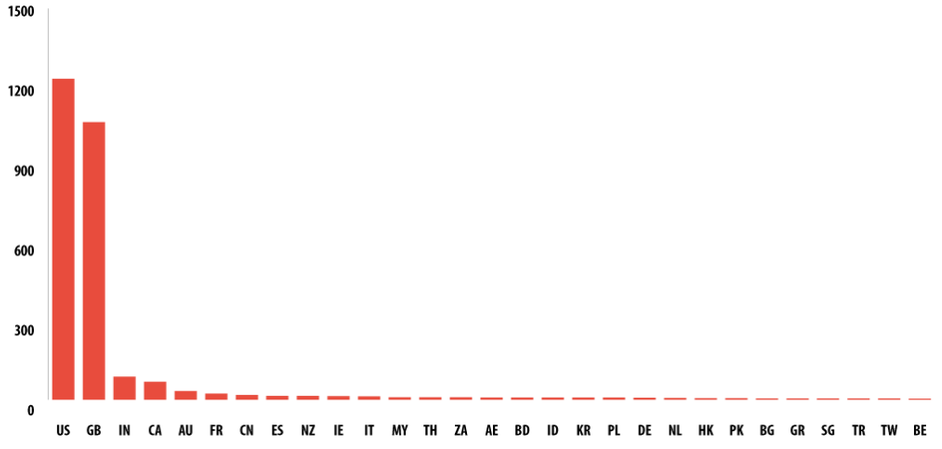
Es ist klar, dass unsere Abhängigkeit von der Technik kombiniert mit den enormen Rechenleistungen heutiger Computer bedeutet, dass wir potenziell durch Personengruppen mit den unterschiedlichsten Motiven angreifbar sind. Daher ist es unwahrscheinlich, dass Hacktivisten und alle anderen, die Organisationen aller Art angreifen, ihre Aktivitäten in nächster Zeit einstellen werden.

4. RANSOMWARE

Die Methoden, mit deren Hilfe Cyberkriminelle ihre Opfer um ihr Geld bringen, sind keineswegs immer subtil. Programme des Typs „Ransomware“ lösen so etwas wie eine Computer-spezifische „Denial-of-Service“-Attacke aus – sie blockieren den Zugriff auf das Dateisystem eines Computers oder verschlüsseln die auf dem Rechner gespeicherten Daten. Der Modus Operandi kann dabei variieren. In Regionen, in denen Software-Piraterie verbreitet ist, würden die Erpresser-Trojaner, also Ransomware, vielleicht behaupten, dass sie unlizenzierte Software auf dem Computer gefunden haben und Geld für die Wiederherstellung des Zugriffs auf den Computer verlangen. An anderen Orten zeigen diese Schädlinge Pop-up-Benachrichtigungen an, die angeblich von der Polizei stammen und in denen behauptet wird, dass auf dem Computer Kinderpornografie oder andere illegale Inhalte gefunden wurden, und verlangen die Zahlung einer Strafe. Manchmal verzichten die Cyberkriminellen aber auf jegliche List – die Daten werden einfach verschlüsselt und für die Dechiffrierung wird Geld verlangt. So geschehen im Fall des Trojaners Cryptolocker, den Kaspersky Lab im Oktober analysierte.

Cryptolocker lädt einen öffentlichen RSA-Schlüssel von seinem Command-and-Control-Server (C2). Für jedes neue Opfer wird ein individueller Schlüssel erstellt, und nur die Autoren haben Zugriff auf die Dechiffrierungsschlüssel. Zur Verbindung mit dem C2-Server verwendet Cryptolocker einen Domain-Erzeugungsalgorithmus, der täglich 1.000 potenziell einzigartige Domain-Namen generiert. Die Cyberkriminellen geben ihren Opfern nur drei Tage Zeit, um sich freizukaufen – dabei erschrecken sie ihre Opfer mit furchteinflößenden Mitteilungen, die besagen, dass ihre Daten für

immer verloren seien, wenn sie nicht rechtzeitig bezahlen.



Opfer pro Land – TOP 30

Die Cyberkriminellen akzeptieren unterschiedliche Zahlungsarten, darunter auch Bitcoins. Am stärksten von dieser Bedrohung betroffen waren Großbritannien und die USA, mit einigem Abstand gefolgt von Indien, Kanada und Australien.

In diesem Fall ist es nicht schwer, die Malware zu entfernen oder das infizierte System wiederherzustellen, aber die Daten können für immer verloren sein. In der Vergangenheit hat es das Kaspersky-Team manchmal geschafft, die gekaperten Daten zu entschlüsseln. Aber das ist nicht immer möglich, insbesondere, wenn die Verschlüsselung besonders stark ist, wie im Fall von einigen Gpcode-Varianten. Das gilt auch für Cryptolocker. Daher ist es wichtig, dass Heimanwender und Unternehmen regelmäßig Backups erstellen. Gehen dann Daten – aus welchem Grund auch immer – verloren, wird dann aus einer Unannehmlichkeit nicht automatisch ein Desaster.

Cryptolocker war nicht das einzige Erpresser-Programm, das dieses Jahr Schlagzeilen machte. Im Juni hatten es die Kaspersky-Experten mit einer Android-App namens „Free Calls Update“ zu tun – einem gefälschten Antiviren-Programm, das seine Opfer dazu bringen soll, Geld für das Entfernen nicht existierender Malware zu zahlen. Einmal auf dem Gerät installiert, versucht die App Administratoren-Rechte zu erhalten. Dadurch ist sie in der Lage, die WiFi- und 3G-Module ein- und auszuschalten und

kann das Opfer daran hindern, die App einfach zu entfernen. Die Installationsdatei wird hinterher gelöscht, um so zu vermeiden, dass eventuell auf dem Gerät installierte echte Antiviren-Programme das Schadprogramm entdecken. Die App gibt vor, Malware zu identifizieren und fordert das Opfer auf, eine Lizenz für die Vollversion zu kaufen, um die Schadsoftware zu entfernen. Während die App läuft, informiert sie den Nutzer darüber, dass Malware versucht, pornografische Inhalte vom Telefon zu stehlen.

5. MOBILE MALWARE UND APP-STORE-(UN)SICHERHEIT

Die explosive Zunahme der mobilen Malware, die im Jahr 2011 einsetzte, hat sich auch dieses Jahr fortgesetzt. Es gibt nun über 148.427 mobile Malware-Modifikationen in 777 Familien. Die überwiegende Mehrheit von ihnen richtet sich wie auch schon in den letzten Jahren gegen Android – 98,05 Prozent der mobilen Schadprogramme greifen diese Plattform an. Das ist auch nicht verwunderlich, denn sie ist für Cyberkriminelle wie geschaffen: Android ist weit verbreitet, es lassen sich problemlos Programme dafür entwickeln, und Leute, die Android-Geräte verwenden, können Programme (inklusive Malware) von wo auch immer herunterladen. Dieser letzte Punkt ist sehr wichtig: Cyberkriminelle nutzen die Tatsache aus, dass Nutzer Apps von Google Play, von anderen Marktplätzen oder von anderen Webseiten downloaden. Das ermöglicht es Cyberkriminellen auch, ihre eigenen Fake-Webseiten zu erstellen, die als legitime App Stores getarnt sind. Daher ist es überaus unwahrscheinlich, dass in Zukunft weniger schädliche Android-Apps entwickelt werden.

Schadprogramme, die mobile Geräte angreifen, sind ein Spiegel der Malware, die normalerweise auf infizierten Desktop-Rechnern und in Backdoors gefunden wird: Trojaner und Spionage-Trojaner. Die einzige Ausnahme sind trojanische SMS-Programme – eine exklusive Smartphone-Kategorie.

Die Bedrohung nimmt nicht nur mengenmäßig zu. Die Kaspersky-Experten beobachten zudem eine wachsende Komplexität. Im Juni analysierten wir den raffiniertesten mobilen Trojaner, den

wir je gesehen haben, das trojanische Programm Obad. Dessen Bedrohung ist multifunktional: Obad schickt Nachrichten an Premium-Nummern, lädt und installiert andere Schadprogramme, nutzt Bluetooth, um sich selbst an andere Geräte zu senden und führt Befehle an der Konsole aus. Der Code ist stark verschleiert und nutzt drei vorher unbekannte Sicherheitslücken aus, darunter eine, die es dem Trojaner erlaubt, die erweiterten Rechte eines Geräteadministrators zu erhalten – allerdings ohne dabei in der Liste der Programme zu erscheinen, die diese Rechte haben. So wird es dem Opfer unmöglich, die Malware einfach von seinem Gerät zu entfernen. Außerdem ist der Trojaner dadurch in der Lage, den Bildschirm zu blockieren. Er macht das für nicht länger als 10 Sekunden, doch das reicht dem Schädling aus, sich selbst (und andere Malware) an die umliegenden Geräte zu senden – ein Trick, der verhindern soll, dass das Opfer die Aktivität des Trojaners registriert.

Obad setzt außerdem mehrere Verbreitungsmethoden ein. Auf die Nutzung von Bluetooth haben wir bereits hingewiesen. Zusätzlich verbreitet er sich über einen gefälschten Google Play-Store mittels Spam-SMS und durch die Umleitung auf gehackte Webseiten. Zu allem Überfluss wird Obad auch noch von einem weiteren mobilen Trojaner ausgeliefert, und zwar Opfake.

Die Cyberkriminellen hinter Obad können den Trojaner so steuern, dass er vordefinierte Text-Strings in den Kurzmitteilungen benutzt. Der Schädling kann verschiedene Aktionen ausführen, unter anderem SMS versenden, einen Ping an eine bestimmte Ressource schicken, als Proxy-Server agieren, sich mit einer speziellen Adresse verbinden, eine bestimmte Datei herunterladen und installieren, eine Liste der auf dem Gerät installierten Apps senden, Informationen über eine bestimmte App verschicken, die Kontakte des Opfers an den Server schicken und Befehle vom Server ausführen.

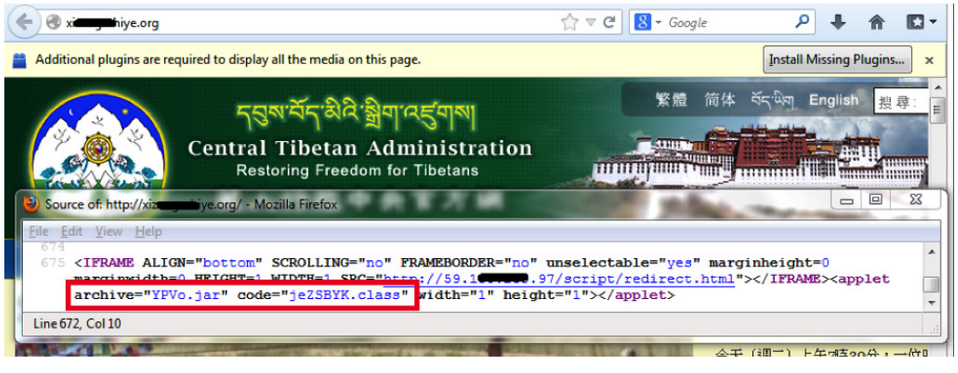
Der Trojaner sammelt Daten über das Gerät und schickt sie an den Command-und-Control-Server. Dazu zählen unter anderem die MAC-Adresse des Gerätes, der Gerätename, die IMEI, das Kontoguthaben, die lokale Zeit sowie Informationen darüber, ob der Trojaner die Rechte eines Geräteadministrators erhalten hat oder nicht. Alle diese Daten werden auf den C2 von Obad hochgeladen: Der Trojaner versucht zuerst, eine aktive Internetverbindung zu nutzen. Ist keine verfügbar, sucht er nach der nächstgelegenen WLAN-Verbindung, die keine Authentifizierung erfordert.

Meet the Experts: Das mobile Internet sicher erleben

6. WASSERLOCH-ATTACKEN

Sicher sind Ihnen die Begriffe „Drive-by-Download“ und Spear-Phishing vertraut. Im erstgenannten Fall suchen Cyberkriminelle nach unsicheren Webseiten und pflanzen ein schädliches Skript in deren HTTP- oder PHP-Code. Dieses Skript kann Schadsoftware auf dem Computer eines Nutzers installieren, der die Webseite besucht, oder es kann ein IFrame verwenden, um den Computer auf eine schädliche Webseite umzuleiten, die von Cyberkriminellen kontrolliert wird. Spear-Phishing ist eine zielgerichtete Form des Phishings, die Cyberkriminelle häufig als Einfallstor für zielgerichtete Attacken einsetzen. Dazu wird eine E-Mail an eine spezielle Person in einer Zielorganisation gesendet, in der Hoffnung, dass diese auf einen in der E-Mail enthaltenen Link klickt oder einen Anhang öffnet, der den Code der Angreifer ausführt und ihnen hilft, einen Fuß in die Tür des Unternehmens zu bekommen.

Kombiniert man diese beiden Ansätze (also Drive-by-Downloads und Spear-Phishing), ergibt das eine „Watering-Hole“- oder auch „Wasserloch“-Attacke. Die Angreifer studieren das Verhalten der Mitarbeiter einer bestimmten Firma oder Organisation, um etwas über deren Surfeigenschaften zu erfahren. Daraufhin kompromittieren sie eine Webseite, die von den entsprechenden Mitarbeitern regelmäßig frequentiert wird – möglichst eine, die von einer vertrauenswürdigen Organisation betrieben wird und eine wertvolle Informationsquelle darstellt. Idealerweise verwenden die Angreifer ein Zero-Day-Exploit. Besucht also ein Mitarbeiter eine solche Webseite, wird sein Computer infiziert, typischerweise mit einer Backdoor, die den Angreifern Zugriff auf das interne Netzwerk des Unternehmens verschafft. Anstatt das Opfer also zu jagen, legen sich die Cyberkriminellen in diesem Fall an einem Ort auf die Lauer, den das Opfer mit hoher Wahrscheinlichkeit besuchen wird – daher die Bezeichnung Wasserloch.



Diese Methode hat sich in diesem Jahr für Cyberkriminelle als erfolgreich erwiesen. Kurz nach Veröffentlichung ihres Berichts über die Winnti-Attacken entdeckten die Kaspersky-Experten ein Flash-Player-Exploit auf der Webseite der „Tibetan Homes Foundation“, einer wohltätigen Institution, die tibetanische Flüchtlingskinder unterstützt. Es zeigte sich, dass diese Webseite kompromittiert wurde, um Backdoors zu verbreiten, die mit gestohlenen Zertifikaten aus dem Winnti-Fall signiert waren. Ein Beispiel für eine Wasserloch-Attacke wie aus dem Lehrbuch: die Cyberkriminellen hatten die von ihren Opfern bevorzugten Webseiten ausgekundschaftet und diese gehackt, um deren Computer zu infizieren. Im August hatte es das Kaspersky-Team erneut mit dieser Technik zu tun, als Code auf der Webseite der „Central Tibetan Administration“ die Computer chinesischsprachiger Besucher auf ein Java-Exploit umleitete, das wiederum eine Backdoor installierte, die Teil einer zielgerichteten Attacke war.

Im September waren dann Wasserloch-Attacken gegen eben diese Gruppen Teil der NetTraveler-Kampagne. Wichtig ist darauf hinzuweisen, dass Wasserloch-Attacken nur eine von Cyberkriminellen eingesetzte Methode ist, und kein Ersatz für das Spear-Phishing und andere Methoden. Zudem sind die oben erwähnten Attacken nur ein Teil einer Angriffsserie auf Webseiten von Tibetanern und Uiguren, die sich über mindestens zwei Jahre erstreckt.

Alle diese Attacken sind ein weiterer Beleg für die Tatsache, dass nicht nur multinationale Konzerne oder prominente Organisationen zielgerichteten Angriffen zum Opfer fallen können.

7. DIE NOTWENDIGKEIT, DAS SCHWÄCHSTE GLIED IN DER KETTE NEU ZU SCHMIEDEN

Viele der heutigen Bedrohungen sind absolut hochentwickelt. Das gilt insbesondere für zielgerichtete Attacken, wenn Cyberkriminelle Exploit-Code entwickeln, um noch nicht geschlossene Programmschwachstellen auszunutzen oder maßgeschneiderte Module erstellen, die ihnen den Datendiebstahl erleichtern. Trotzdem ist und bleibt die von Angreifern ausgenutzte Schwachstelle Nummer eins der Mensch. Die Verbrecher setzen Social-Engineering-Tricks ein, um Mitarbeiter einer bestimmten Organisation dazu zu bringen, etwas zu tun, was die Unternehmenssicherheit untergräbt. Menschen sind aus unterschiedlichen Gründen für solche Ansätze anfällig. Manchmal erkennen sie die Gefahr schlichtweg nicht. Manchmal ist es die Hoffnung, irgendetwas umsonst zu bekommen. Manchmal ist es einfach Bequemlichkeit, weil sie beispielsweise ein und dasselbe Passwort für alles Mögliche benutzen.

Viele der prominenten zielgerichteten Attacken, die Kaspersky Lab in diesem Jahr analysiert hat, begannen mit einem „Hack des Menschen“. Roter Oktober, die Angriffsserie auf tibetanische und uigurische Aktivisten, MiniDuke, NetTraveler und Icefog haben sich alle mittels Spear-Phishing Zutritt zu den angegriffenen Organisationen verschafft. Die Cybergangster nähern sich den betreffenden Mitarbeitern mit Hilfe von Informationen, die sie an unterschiedlichen Orten zusammengetragen haben: auf der Webseite des Unternehmens, in öffentlichen Foren und beim Durchsieben der verschiedenen Info-Schnipsel, die Leute heutzutage in Sozialen Netzwerken hinterlassen. Dadurch sind die Cyberkriminellen in der Lage, E-Mails zu erstellen, die einen legitimen Eindruck machen und die Mitarbeiter unvorbereitet erwischen.

Sicherlich verfolgen auch solche Cybergangster diesen Ansatz, die hinter der Masse von willkürlichen, spekulativen Attacken stecken, welche die Mehrheit der cyberkriminellen Aktivität ausmachen – Phishing-Mails, die en Gros an eine Unmenge von Empfängern gesendet werden.

Social Engineering kann zudem in der realen Welt angewandt werden, und diese Dimension wird manchmal einfach übersehen. Das wurde im Jahr 2013 besonders deutlich, als Verbrecher versuchten, KVM-Switches in den Filialen zweier britischer Banken zu installieren. In beiden Fällen tarnten sich die Angreifer als Monteure, um physischen Zugriff auf die Bank zu erhalten und das Equipment zu installieren. Das hätte es ihnen ermöglicht, die Netzwerkaktivität zu verfolgen. Mehr über diese Vorfälle finden Sie hier und hier.

Das Social-Engineering-Problem wurde im September auch von unserem Kollegen David Jacoby näher beleuchtet: in Stockholm führte er ein kleines Experiment durch, um festzustellen, wie leicht es ist, Zugriff auf Geschäftssysteme zu erlangen, indem man die Bereitschaft der Mitarbeiter ausnutzt, um einem Fremden in Not zu helfen. Davids Bericht dazu finden Sie hier.

Leider ignorieren Unternehmen bei Sicherheitsfragen häufig den menschlichen Faktor. Selbst wenn die Notwendigkeit der Mitarbeiteraufklärung erkannt wird, sind die Umsetzungsmethoden meist ineffektiv. Denn wir ignorieren den menschlichen Faktor in der Unternehmenssicherheit auf eigene Gefahr, obwohl es nur allzu klar ist, dass Technologie allein keine Sicherheit garantieren kann. Daher ist es für alle Organisationen überaus wichtig, das Sicherheitsbewusstsein zu einem Kernstück ihrer Sicherheitsstrategie zu machen.

DIE ZEHN ULTIMATIVEN SECURITY-STORIES DES JAHRES 2013

8. VERLUST DER PRIVATSPHÄRE: LAVABIT, SILENT CIRCLE, NSA UND DER VERTRAUENSVERLUST

Kein Rückblick auf die Ereignisse des Jahres 2013 im Bereich IT-Sicherheit wäre vollständig ohne die Erwähnung des Namens Edward Snowden und der weitreichenden Auswirkungen, die die Veröffentlichung der Geschichten über Prism, XKeyscore und Tempora sowie über andere Überwachungsprogramme auf den Datenschutz hat.

Eine der ersten sichtbaren Folgen war die Schließung des verschlüsselten E-Mail-Dienstes Lavabit, über die Kaspersky Lab bereits hier berichtet hat. Silent Circle, ein anderer verschlüsselter E-Mail-Anbieter, hat seinen Service ebenfalls eingestellt und nur sehr wenige Optionen für den privaten und sicheren E-Mail-Verkehr offen gelassen. Der Grund, warum diese beiden Anbieter ihre Tätigkeit eingestellt haben, lag in der Unmöglichkeit, derartige Dienste unter dem Druck der Strafverfolgungs- und Regierungsbehörden anzubieten.

Eine andere Geschichte, die Auswirkungen auf den Datenschutz hat, ist die NSA-Sabotage der vom NIST herausgegebenen Algorithmen der elliptischen Kurvenkryptografie. Anscheinend hat die NSA eine Art Backdoor in den „Dual Elliptic Curve Deterministic Random Bit Generation“-Algorithmus (oder auch Dual EC DRBG) eingeschleust. Die Backdoor ermöglicht es bestimmten Parteien, leichte Attacken gegen ein spezielles Verschlüsselungsprotokoll durchzuführen und so vermutlich die sichere Kommunikation zu unterlaufen. RSA, einer der größten Verschlüsselungsprovider weltweit, wies darauf hin, dass dieser Algorithmus grundlegender Bestandteil seines Verschlüsselungs-Toolkits war und empfahl allen Kunden, es nicht mehr zu nutzen. Der fragliche Algorithmus wurde im Jahr 2006 vom NIST angenommen, nachdem er seit spätestens 2004 verfügbar war und in

großem Maßstab verwendet wurde.

Interessanterweise hatte einer der Aufsehen erregenden Vorfälle direkte Auswirkungen auf die Antiviren-Industrie. Im September erklärte Belgacom, ein belgischer Telekommunikationsanbieter, dass er gehackt wurde. Während einer Routineuntersuchung hatten die Mitarbeiter des Unternehmens einen unbekannten Virus auf mehreren Servern und Computern der Mitarbeiter entdeckt. Später kamen Spekulationen über die Herkunft des Virus und der Attacke auf, die in Richtung GCHQ und NSA gingen. Wenngleich Samples des Schadprogramms der Sicherheitsbranche noch nicht zugänglich gemacht wurden, tauchten weitere Details auf, die darauf hindeuteten, dass die Attacke über eine „verseuchte“ LinkedIn-Seite umgesetzt wurde, die wiederum mittels Man-in-the-Middle-Techniken, mit Links auf CNE-Server (Computer Network Exploitation), vermint worden war.

Alle diese Überwachungsgeschichten haben auch Fragen über die Zusammenarbeit zwischen Sicherheitsunternehmen und Regierungen aufgeworfen. Die Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) hat zusammen mit anderen Gruppen am 25. Oktober einen offenen Brief geschrieben, in dem Sicherheitsanbietern eine Reihe von Fragen bezüglich der Erkennung und Blockierung von staatlich geförderter Malware gestellt wird.

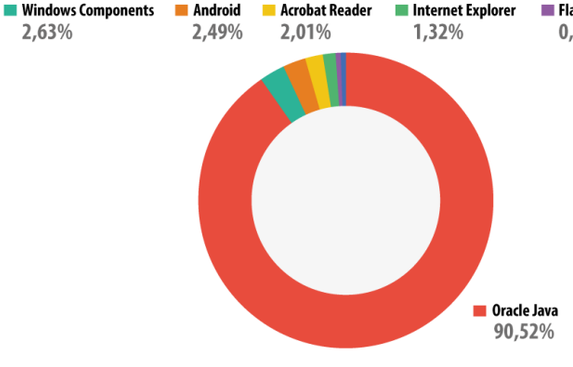
Bei Kaspersky Lab verfolgen wir eine einfache und schnörkellose Politik hinsichtlich der Erkennung von Malware: Wir erkennen und wehren jede Art von Schädlingsangriff ab, ungeachtet seines Ursprungs oder Zwecks. Für uns gibt es keine „richtige“ oder „falsche“ Malware. Unser Forschungsteam war an der Entdeckung und Aufklärung mehrerer Malware-Attacken mit Verbindungen zu Nationalstaaten und Regierungen beteiligt. Im Jahr 2012 veröffentlichten wir detaillierte Analysen über Flame und Gauss, zwei der umfassendsten staatlichen Massenüberwachungsaktionen überhaupt. Kaspersky Lab hat zudem öffentlich vor den Risiken der so genannten „legalen“ Überwachungstools gewarnt, genauso wie etwa DaVinci von HackingTeam und FinFisher von Gamma. Es kommt darauf an, dass die Überwachungstools nicht in die falschen Hände geraten, daher kann

die IT-Sicherheitsbranche keine Ausnahmen machen, wenn Malware erkannt wird. In der Realität ist es äußerst unwahrscheinlich, dass irgendeine kompetente und bewanderte Regierungsorganisation einen (oder mehrere) Antiviren-Hersteller darum bitten wird, bei bestimmter staatlich gesponserter Malware ein Auge zuzudrücken. Denn es kann überaus leicht passieren, dass die „unentdeckten“ Schadprogramme dann in die falschen Hände geraten und schließlich gegen dieselben Leute eingesetzt werden, die sie entwickelt haben.

9. SICHERHEITSLÜCKEN UND ZERO-DAY-EXPLOITS

Cyberkriminelle nutzen nach wie vor im großen Stil Sicherheitslücken in legitimer Software aus, um Malware-Attacken zu starten. Zu diesem Zweck verwenden sie Exploits – Codefragmente, die geschrieben werden, um einen Programmfehler zur Installation von Schadprogrammen auf einem Computer auszunutzen, ohne dass dessen Besitzer dabei aktiv werden muss. Dieser Exploit-Code kann in einen eigens dafür erstellten E-Mail-Anhang integriert sein oder kann eine Schwachstelle im Browser angreifen. Das Exploit fungiert als Ladeprogramm für die Schadprogramme, die die Cyberkriminellen installieren wollen.

Wenn ein Angreifer eine Sicherheitslücke ausnutzt, die nur ihm bekannt ist – eine so genannte „Zero-Day“-Sicherheitslücke – ist jeder, der die angreifbare Anwendung nutzt, so lange ungeschützt, bis der Hersteller einen Patch entwickelt hat, der die Lücke schließt. Doch in vielen Fällen machen sich Online-Verbrecher auch wohlbekannte Schwachstellen zunutze, für die schon ein Patch veröffentlicht wurde. Das gilt für viele der großen zielgerichteten Attacken des Jahres 2013, eingeschlossen Red October, MiniDuke, TeamSpy und NetTraveler. Das gilt ebenfalls für viele der willkürlichen, spekulativen Angriffe, die den Großteil der Fälle von Cyberkriminalität ausmachen.



Verteilung von Zero-Day-Exploits auf Anwendungen

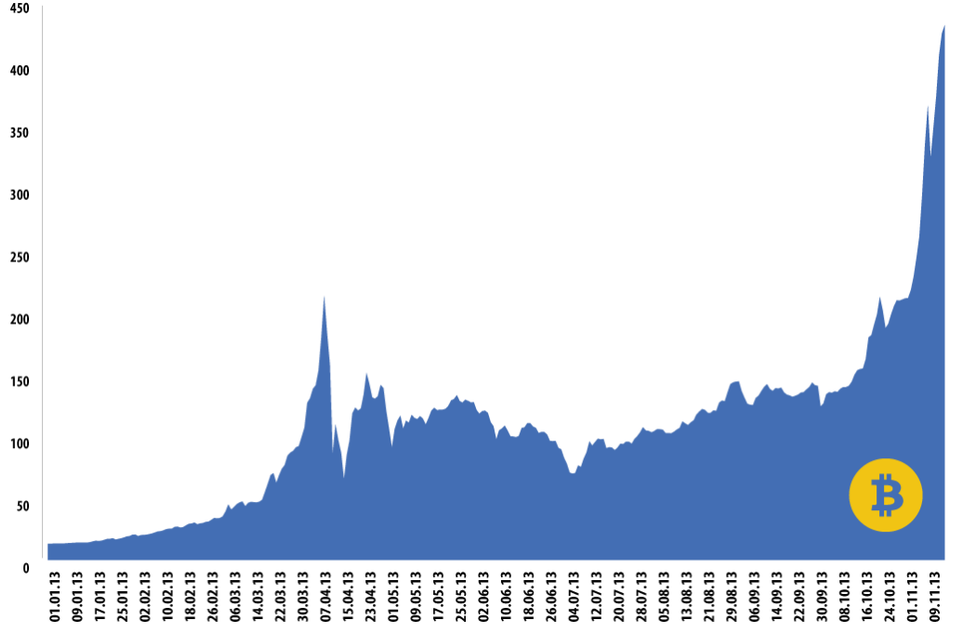
Online-Gangster konzentrieren sich auf Anwendungen, die weit verbreitet sind und vermutlich für eine lange Zeit ungepatcht bleiben, so dass ihnen ein großes Zeitfenster zur Verfügung steht, um ihre Ziele zu erreichen. Im Jahr 2013 waren Java-Schwachstellen für etwa 90,52 Prozent der Attacken verantwortlich, während auf Adobe Acrobat Reader 2,01 Prozent entfielen. Das folgt einem bewährten Trend und ist nicht weiter überraschend. Java ist nicht nur auf einer Unmenge von Computern installiert (drei Milliarden laut Oracle), auch die Updates werden nicht automatisch installiert. Adobe Reader wird weiterhin von Cyberkriminellen ausgenutzt, doch die Zahl der Exploits für diese Anwendung ist im Laufe der letzten zwölf Monate deutlich zurückgegangen, und zwar dank der regelmäßigeren (und in den neusten Versionen automatischen) Veröffentlichungen von Patches.

Um ihre Angriffsfläche zu verringern, sollten Unternehmen stets die neusten Versionen aller der in ihrem Betrieb verwendeten Programme verwenden, Sicherheitsupdates installieren, sobald sie verfügbar sind, und Software entfernen, die in der Organisation nicht länger gebraucht wird. Risiken können auch durch den Einsatz eines Sicherheitslücken-Scanners reduziert werden, der ungepatchte Anwendungen erkennt, sowie durch die Verwendung einer Anti-Malware-Lösung, die die Nutzung von Exploits in nicht aktualisierten Programmen verhindert.

10. DIE HOCHS UND TIEFS DER VIRTUELLEN WÄHRUNGEN – WIE DIE BITCOINS DIE WELT REGIEREN

Im Jahr 2009 veröffentlichte ein Mann namens Satoshi Nakamoto einen Aufsatz, der die Welt der elektronischen Währungen revolutionieren sollte. In der Publikation mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“ werden die Grundlagen für ein distributives, dezentralisiertes Finanz-Bezahlsystem ohne Transaktionsgebühren definiert. Das Bitcoin-System wurde eingeführt und die Menschen begannen es zu nutzen. Welche Art von Menschen? Zunächst waren es in erster Linie nur Liebhaber dieser Technologie und Mathematiker. Bald aber gesellten sich andere zu ihnen – ganz normale Leute, aber auch Cyberkriminelle und Terroristen.

Noch im Januar 2013 lag der Bitcoin-Kurs bei 13 US-Dollar. Als immer mehr Dienstleister Bitcoin als Zahlungsmittel anerkannten, stieg der Preis. Am 9. April 2013 erreichte er 260 US-Dollar (der Durchschnittspreis lag bei 214 US-Dollar), bevor der Kurs am nächsten Tag einbrach, als Unternehmen mit vielen Bitcoins im Geldbeutel damit begannen, die virtuelle Währung gegen echtes Geld einzutauschen.



Täglicher Bitcoin-Durchschnittspreis (MT. Gox)

Im November 2013 nahm der Bitcoin-Kurs wieder Fahrt auf und überschritt die 400-Dollar-Marke auf dem Weg zu 450 US-Dollar und vielleicht auch mehr.

Was macht Bitcoins so beliebt? Erstens sind sie ein fast anonymes und sicheres Zahlungsmittel für Waren. Zum einen ist es in Folge der Überwachungsstorys von 2013 kaum überraschend, dass sich die Menschen nach alternativen Zahlungsmitteln umsehen. Zweitens gibt es wohl wenig Zweifel daran, dass die virtuelle Währung auch unter Cyberkriminellen beliebt ist, die nach Möglichkeiten suchen, das Gesetz zu umgehen.

Im Mai haben die Kaspersky-Experten über brasilianische Cyberkriminelle berichtet, die angebliche Bitcoin-Wechselstuben betrieben. Botnetze traten auf den Plan, die Bitcoins schürften, und Schadprogramme zum Diebstahl von Bitcoin-Geldbörsen wurden entwickelt.

Am Freitag, dem 25. Oktober, wurde im Rahmen einer gemeinsamen Operation von FBI und DEA die berüchtigte Plattform Silk Road beschlagnahmt. Silk Road war laut Pressemitteilung der US-

Staatanwaltschaft „ein versteckter Service, der Nutzern die Möglichkeit geben sollte, illegal Drogen und andere ungesetzliche Waren und Dienstleistungen anonym und außerhalb der Reichweite von Strafverfolgungsbehörden zu kaufen und zu verkaufen“. Dieser Service basierte auf Bitcoins, wodurch Verkäufer und Kunden gleichermaßen unerkannt blieben. FBI und DEA konfiszierten etwa 140.000 Bitcoins (zum heutigem Kurs etwa 56 US-Millionen Dollar) von „Dread Pirate Roberts“, dem Betreiber von Silk Road. Gegründet im Jahr 2011, wurde Silk Road über das TOR Onion-Netzwerk betrieben und scheffelte über 9,5 Millionen Bitcoins an Einnahmen.

Auch wenn es auf der Hand liegt, dass Cyberkriminelle in der virtuellen Währung einen sicheren Hafen gefunden haben, so gibt es auch viele andere Bitcoin-Nutzer, die keine üblen Absichten hegen. Da Bitcoins immer populärer werden, wird es interessant sein zu sehen, ob sich irgendeine Regierung zu einem harten Durchgreifen entschließen wird, in der Absicht, die illegale Verwendung dieser Währung zu unterbinden.

Sollten Sie Bitcoins besitzen, so ist die wichtigste Frage, die sich stellt, wahrscheinlich die, wie man sie sicher verwahren kann. Dazu geben Ihnen die Kaspersky-Experten Stefan Tanase und Sergey Lozhkin in diesem Artikel einige Tipps.

FAZIT UND AUSBLICK: „2014, DAS JAHR DES VERTRAUENS“

Das Jahr 2011 nannten wir in der Jahresrückschau explosiv. Wir sagten für das Jahr 2012 viele Enthüllungen voraus und über 2013 behaupteten wir, es würde uns die Augen öffnen.

Tatsächlich haben uns einige Enthüllungen des Jahres 2013 die Augen geöffnet und Fragen über die Art und Weise aufgeworfen, wie wir das Internet heutzutage nutzen, sowie über die Art der Risiken, denen wir gegenüberstehen. Im Jahr 2013 haben fortschrittliche Angreifer weiterhin groß angelegte Kampagnen entwickelt, wie zum Beispiel Roter Oktober oder NetTraveler. Neue Techniken wie etwa Wasserloch-Attacken haben sich durchgesetzt, während Zero-Day-Schwachstellen unter technisch versierten Akteuren nach wie vor beliebt sind. Kaspersky Lab hat zudem das Aufkommen von Cyber-Söldnern beobachtet, die für APT-Attacken angeheuert werden, schnell zuschlagen und dann wieder verschwinden. Hacktivisten waren in den Nachrichten allgegenwärtig, immer im Zusammenhang mit dem Begriff „Leak“, was jeden seriösen Systemadministrator in Angst versetzen sollte. In der Zwischenzeit waren die Cyberkriminellen damit beschäftigt, neue Methoden zu entwickeln, um Geld oder Bitcoins zu stehlen. Ransomware ist beinahe schon omnipräsent, und Malware ist und bleibt ein ernsthaftes Problem, für das es keine einfache Lösung gibt.

Natürlich möchte jeder wissen, wie alle diese Geschichten das Jahr 2014 beeinflussen werden. Unserer Meinung nach wird sich 2014 alles um die Wiederherstellung des Vertrauens drehen.

Datenschutz wird ein wichtiges Thema sein, mit allen seinen Höhen und Tiefen. Verschlüsselung kommt wieder in Mode und wir glauben, dass unzählige neue Services auftauchen werden, die behaupten, die Nutzer vor neugierigen Augen zu schützen. Die Cloud, das Wunderkind der letzten Jahre, gerät nun in Vergessenheit, da die Menschen das Vertrauen verloren haben und Länder und Regierungen sich nun ernsthaftere Gedanken über den Datenschutz zu machen beginnen. Im Jahr 2014 werden die Finanzmärkte vermutlich das Schwanken des Bitcoin spüren, wenn Unmengen von Geld von China und anderen Ländern hineingepumpt wird. Vielleicht erreicht der Bitcoin die 10.000-Dollar-Marke oder vielleicht bricht der Kurs auch ein und die Menschen schauen sich nach vertrauenswürdigeren Alternativen um.

BEDROHUNGEN FÜR UNTERNEHMEN

Vitaly Kamluk (@vkamluk), Sergey Lozhkin (@61ack1ynx)

QUICK-INFO

- Angriffe auf Unternehmen
- Gründe
- Vorgehensweisen
- Technologien
- Auswirkungen

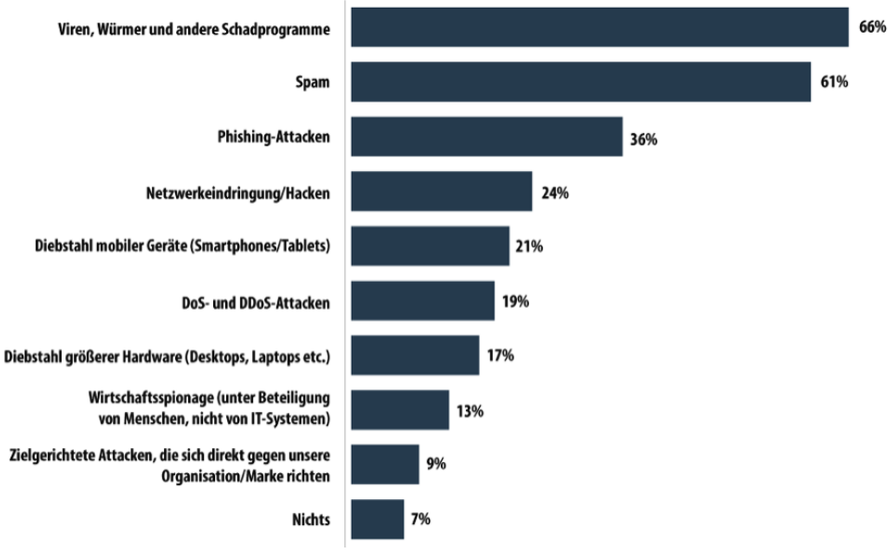
Corporate threats in 2013 - the expert opinion (Englisch)

Innerhalb der letzten zwei Jahre ist die Zahl der erkannten ernstzunehmenden Cyberattacken derart angestiegen, dass ein neuer Angriff nur noch selten Verwunderung auslöst. Berichte von Antiviren-Unternehmen über die Entdeckung eines neuen Botnetzes oder einer hyperraffinierten Software, die Daten stiehlt, erscheinen mit schöner Regelmäßigkeit.

Immer häufiger fallen kommerzielle Unternehmen Cyberattacken zum Opfer. Laut einer von Kaspersky Lab und dem Marktforschungsunternehmen B2B International durchgeführten Umfrage waren 91 Prozent der befragten Unternehmen mindestens einmal pro Jahr einer Cyberattacke ausgesetzt. Neun Prozent der Unternehmen gerieten ins Visier zielgerichteter Attacken.

Die Verwendung von Computern und anderen digitalen Geräten in allen Geschäftsprozessen hat die Grundlage für die erfolgreiche Anwendung von Schadsoftware gelegt, die auf Industriespionage und den Diebstahl von Unternehmensdaten spezialisiert ist. Das Potenzial dieses Ansatzes hat sich als so groß erwiesen, dass der Einsatz von Schadprogrammen in naher Zukunft die Insiderspionage möglicherweise vollständig ablösen wird. Doch die Risiken für den Unternehmenssektor beschränken

sich nicht allein darauf. Die Abhängigkeit der heutigen Geschäftswelt vom zuverlässigen Funktionieren der Computer und der Übertragungskanäle zwischen den Rechnern gibt Cyberkriminellen die Möglichkeit, verschiedene Programme destruktiver Art einzusetzen – von Verschlüsselungs- und "Lösch"-Programmen, die sich wie eine Krankheit in der Unternehmensumgebung ausbreiten, bis zur Armee gehorsamer Zombies, die alle freien Ressourcen der Unternehmens-Webserver und Datenübertragungsnetze verschlingen.



GRÜNDE FÜR ATTACKEN

> **Datendiebstahl.** Der Raub von Unternehmensdaten, Geschäftsgeheimnissen oder persönlichen Daten von Unternehmensmitarbeitern und -kunden oder das Überwachen der Tätigkeit eines Unternehmens ist das Ziel vieler – von Organisationen, die die Dienstleistungen Cyberkrimineller in Anspruch nehmen, damit diese in das Unternehmensnetzwerk von Konkurrenten eindringen, bis hin zu den Geheimdiensten verschiedener Länder.

> **Datenvernichtung und Blockierung der Infrastruktur.** Einige Schadprogramme werden zu einer bestimmten Spionageart eingesetzt. Ihre Aufgabe besteht in der Zerstörung wichtiger Daten oder der Störung des reibungslosen Geschäftsablaufs. Die trojanischen Programme

Wiper und Shamoon löschen beispielsweise Systemdaten der Workstations und Server, ohne dass es eine Möglichkeit zur Wiederherstellung gibt.

> **Gelddiebstahl.** Die Infektion mit trojanischen Programmen, die auf den Diebstahl von Finanzmitteln über Online-Banking-Systeme und auf zielgerichtete Attacken auf interne Ressourcen von Rechen- und Finanzzentren spezialisiert sind, führen für die angegriffenen Unternehmen zu finanziellen Verlusten.

> **Reputationsschädigung.** Der Erfolg eines Geschäfts sowie hohe Besucherzahlen der offiziellen Webseiten von Unternehmen, die im Bereich Internet-Dienstleistungen tätig sind, locken Cyberkriminelle an. Der Hack einer Unternehmenswebseite mit anschließender Einschleusung von schädlichen Links, die die Besucher auf schädliche Ressourcen umleiten, und das Platzieren von schädlichen Werbebannern oder von politisch motivierten Nachrichten auf der gehackten Ressource fügen dem Verhältnis zwischen Kunden und Unternehmen einen erheblichen Schaden zu.

Ein weiteres beachtliches Risiko, das den guten Ruf bedroht, liegt im Diebstahl von digitalen Zertifikaten von IT-Unternehmen. In einzelnen Fällen, beispielsweise für Unternehmen, die eigene öffentliche Zertifizierungszentren unterhalten, kann der Verlust von Zertifikaten oder das Eindringen in die Infrastruktur zum vollständigen Vertrauensverlust gegenüber dem entsprechenden Unternehmen und sogar zur anschließenden Geschäftsaufgabe führen.

> **Finanzieller Schaden.** DDoS-Attacken sind eine der beliebtesten Methoden, wenn es darum geht, Unternehmen und Organisationen direkten Schaden zuzufügen. Cyberkriminelle entwickeln neue Ansätze zur Durchführung solcher Attacken. So können DDoS-Attacken die externen Webressourcen eines Unternehmens gleich mehrere Tage außer Gefecht setzen. In solchen Fällen ist es den Kunden nicht nur unmöglich, die Dienste der angegriffenen Unternehmen zu nutzen – was direkte finanzielle Verluste für die attackierte Organisation nach sich zieht –, sondern es erweckt bei den Besuchern der Webseiten auch den Wunsch, sich an ein vertrauenswürdigeres Unternehmen zu wenden. Das wiederum führt zu einer Verringerung des Kundenstamms und somit zu langfristigen finanziellen Verlusten.

Im Jahr 2013 nahm die Beliebtheit von DNS-Amplification-Attacken zu, wobei Cyberkriminelle mit Hilfe von Botnetzen rekursive Anfragen an DNS-Server versenden und die Antworten auf

die angegriffenen Systeme leiten. Auf diese Art und Weise wurde eine der leistungsstärksten DDoS-Attacken des Jahres 2013 umgesetzt – der Angriff auf die Spamhaus-Webseite.

ZIELORGANISATIONEN

Bei der massenhaften Verbreitung von Schadprogrammen kann jedes beliebige Unternehmen zum Opfer werden, dessen Computer angreifbar sind. So kann sich auch eine kleine Firma mit einem der bekannten Banktrojaner infizieren (ZeuS, SpyEye und andere) und als Folge sowohl Geld als auch geistiges Eigentum verlieren.

Objekte zielgerichteter Attacken (also sorgfältig geplanter Aktionen zur Infektion der Netzinfrastruktur einer bestimmten Organisation oder einer Privatperson) waren gemäß den Ergebnissen einer Untersuchung von Kaspersky Lab im Jahr 2013 Konzerne und Organisationen aus den folgenden Bereichen: Erdölindustrie, Telekommunikation, Weltraumforschung, Schiffsbau und andere Industriebranchen, die mit Hightech-Entwicklungen zusammenhängen.

VORBEREITUNG DER ANGRIFFE

Cyberkriminellen steht ein großes Arsenal komplexer Werkzeuge zum Eindringen in die Computernetzwerke von Unternehmen zur Verfügung. Die Planung einer zielgerichteten Attacke auf ein Unternehmen kann mehrere Monate in Anspruch nehmen, bei der alle nur möglichen Techniken angewandt werden – vom Social Engineering bis zur Ausnutzung unbekannter Software-Sicherheitslücken.

Die Angreifer studieren akribisch das kommerzielle Profil des Unternehmens, öffentliche Ressourcen, von denen sich alle möglichen nützlichen Informationen abschöpfen lassen, Webseiten und Webportale des Unternehmens, Profile der Mitarbeiter in Sozialen Netzwerken, Anzeigen und Bilanzen, Präsentationen auf Messen und ähnliches. Die Verbrecher können die Netzinfrastruktur von Unternehmen sowie die Netzressourcen und die Kommunikationsknoten studieren und ausgehend davon ihre Strategie zum Eindringen und Stehlen von Informationen planen.

Online-Gangster können bei der Planung von Attacken gefälschte Webseiten erstellen, die äußere Aufmachung der Webseiten von Kunden oder Partnern der angegriffenen Organisationen kopieren und dabei ähnlich lautende Domain-Namen registrieren. Im Folgenden werden diese Webseiten benutzt, um Opfer in die Irre zu führen und Rechner zu infizieren.

EINDRINGUNGSMETHODEN

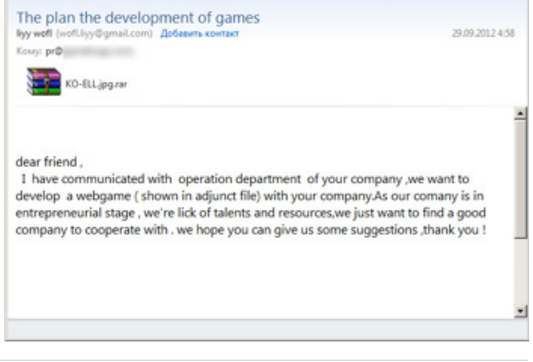
Im Jahr 2013 bestand eine der beliebtesten Methoden, die Cyberkriminelle anwandten, um Schadcode in ein Unternehmensnetzwerk einzuschleusen, darin, den Mitarbeitern des angegriffenen Unternehmens E-Mails mit schädlichen Anhängen zu schicken. Der häufigste Anhang war ein Dokument in einem für Büroangestellte gewohnten Format, wie zum Beispiel Word, Excel oder PDF. Beim Öffnen der angehängten Datei wird eine Sicherheitslücke in der Software ausgenutzt und das System wird mit einem Schadprogramm infiziert.

DAS SCHWÄCHSTE GLIED

Oftmals sind die Empfänger schädlicher E-Mails Mitarbeiter, die aufgrund ihrer Tätigkeit häufig mit Adressaten außerhalb der Unternehmensstruktur kommunizieren. Am häufigsten erhalten Mitarbeiter aus der PR schädliche Korrespondenz. Auch Personalabteilungen erhalten viele E-Mails von externen Absendern. Ein Verbrecher kann sich als Bewerber auf eine ausgeschriebene Stelle ausgeben, Kontakt aufnehmen und seinen Lebenslauf als schädliche PDF-Datei mitschicken. Ohne Zweifel wird ein Mitarbeiter der Personalabteilung eine solche Datei öffnen. Findet der schädliche Anhang eine Sicherheitslücke, wird der Computer infiziert. An die Finanzabteilungen von Unternehmen schicken Cyberkriminelle schädliche E-Mails im Namen von Steuerbehörden, getarnt als Anfragen, Forderungen und Anträge aller Art. Die juristischen Abteilungen erhalten schädliche Schreiben, die angeblich von Gerichten, Polizeidezernaten und anderen staatlichen Stellen stammen.

SOCIAL ENGINEERING

Der Inhalt eines Schreibens ist normalerweise von Interesse für den Mitarbeiter, an den es gerichtet ist – es hat entweder mit seinem Aufgabenbereich oder mit dem Tätigkeitsfeld des Unternehmens zu tun. So schickte die Hackergruppe Winnti beispielsweise im Rahmen einer zielgerichteten Attacke einem Privatunternehmen aus dem Bereich


The plan the development of games

lyy wofl (wofl.lyy@gmail.com) Добавить контакт 29.09.2012 4:58

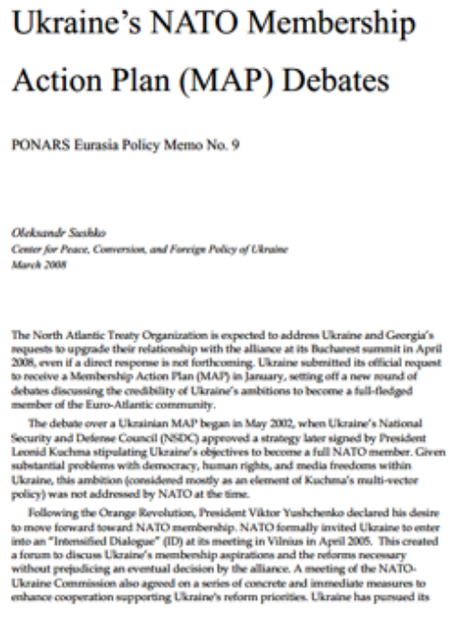
Кому: pr@

KO-ELL.jpg.rar

dear friend ,
I have communicated with operation department of your company ,we want to develop a webgame (shown in adjunct file) with your company.As our comany is in entrepreneurial stage , we're lick of talents and resources,we just want to find a good company to cooperate with . we hope you can give us some suggestions ,thank you !

Videogames eine E-Mail, die eine mögliche Zusammenarbeit zum Thema hatte.

Die Spyware MiniDuke wurde mit Hilfe eines Schreibens verbreitet, das ein Interesse an der ukrainischen Außenpolitik wecken sollte, insbesondere an den Beziehungen zwischen der Ukraine und der NATO:


Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

SICHERHEITSLÜCKEN UND EXPLOITS

Cyberkriminelle nutzen aktiv Exploits zu bekannten Software-Sicherheitslücken aus.

Im Rahmen der berüchtigten Kampagne Roter Oktober wurden beispielsweise mindestens drei verschiedene Exploits für bereits bekannte Sicherheitslücken in Microsoft Office eingesetzt – CVE-2009-3129 (Microsoft Excel), CVE-2010-3333 (Microsoft Word) und CVE-2012-0158 (Microsoft Word). Der Schädling NetTraveler verwendete ein Exploit für CVE-2013-2465 – eine Schwachstelle in Java der Versionen 5, 6 und 7, die von Oracle erst im Juni 2013 geschlossen wurde.

Doch am gefährlichsten sind Sicherheitslücken, die den Entwicklern der Software noch nicht bekannt

sind, so genannte Zero-Day-Sicherheitslücken. Cyberkriminelle suchen in populären Programmen aktiv nach bisher noch unbekannten „Löchern“ und entwickeln Exploits dafür. Werden sie bei ihrer Suche fündig, so ist die Wahrscheinlichkeit sehr hoch, dass eine solche Sicherheitslücke auch ausgenutzt wird. Eine derartige Schwachstelle (CVE-2013-0640) im Adobe Reader der Versionen 9, 10, 11, die zur Zeit der Attacke noch unbekannt war, machte sich MiniDuke zunutze.

TECHNOLOGIEN

Cyberkriminelle perfektionieren kontinuierlich ihre Software, und sie verwenden ungewöhnliche Ansätze und Lösungen, um Informationen abzuschöpfen.

Roter Oktober arbeitete nach dem Eindringen in ein System wie eine multifunktionale modulare Plattform und fügte dem infizierten System in Abhängigkeit von seinem Ziel verschiedene Module hinzu, von denen jedes eine bestimmte Auswahl von Aktionen ausführte: erstes Sammeln von Informationen über den infizierten Rechner und die Netzinfrastruktur, Diebstahl von Passwörtern für verschiedene Dienste, Tastaturspionage, Selbstverbreitung, Übertragung der gestohlenen Informationen und so weiter.

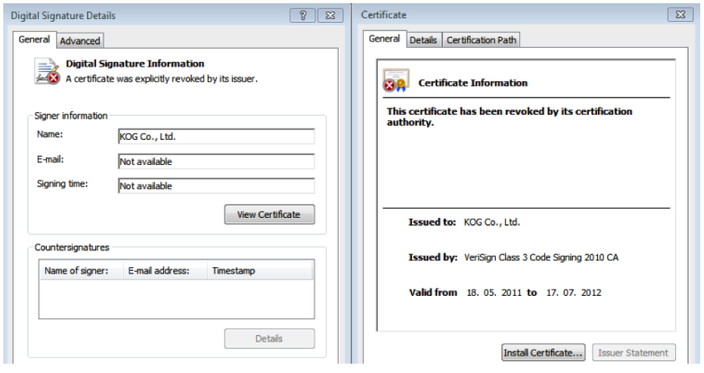
Außerdem ist es erwähnenswert, dass die Entwicklung mobiler Technologien und die Verbreitung mobiler Geräte in der Unternehmensumgebung nicht an den Cyberkriminellen vorbeigegangen sind. Ein modernes Smartphone oder ein Tablet ist praktisch eine voll funktionsfähige Workstation, auf der eine Vielzahl von Daten gespeichert ist, die ein klares Ziel für Online-Kriminelle darstellen. Die Autoren von Roter Oktober entwickelten spezielle Module, die feststellen können, wann sich Smartphones der Plattformen Apple iOS und Windows Mobile sowie Handys des Herstellers Nokia mit dem infizierten Computer verbinden. Die Module kopieren daraufhin die Daten und schicken sie an den Steuerungsserver.

Die Entwickler von Kimsuky integrierten in ihren Schädling ein vollständiges Modul zur entfernten Steuerung der infizierten Systeme, und zwar auf der Basis des vollkommen legitimen Remote-Administration-Tools TeamViewer, wobei sie dessen Code nur geringfügig modifizierten. Daraufhin verbanden sich mehrere Kimsuky-Betreiber manuell mit den infizierten Computern und kopierten Daten, die für sie von Interesse waren.

Die Hackergruppe Winnti stahl in den Unternehmensnetzwerken von Online-Gaming-Entwicklern

digitale Zertifikate, signierte damit ihre schädlichen Treiber und infizierte im Folgenden andere Unternehmen. Beispielsweise wurde das digitale Zertifikat des südkoreanischen Unternehmens KOG gestohlen. Nachdem die Kaspersky-Experten die Firma über den Diebstahl informiert hatten, wurde das Zertifikat zurückgerufen.

Zurückgerufenes Zertifikat:



Darüber hinaus war eines der Module des 64-Bit-Trojaners eine multifunktionale Backdoor – das ist der erste uns bekannte Fall der Verwendung eines 64-Bit-Schadprogramms, das über eine gültige digitale Signatur eines legalen Unternehmens verfügt.

Das Spionage-Schadprogramm MiniDuke nutzte Twitter, um Informationen über die Steuerungsserver zu erhalten: die Betreiber von MiniDuke veröffentlichten mit Hilfe eines speziell erstellten Accounts auf bestimmte Weise aufgemachte Tweets, die die verschlüsselte Adresse des Steuerungsservers enthielten.

Der Trojaner las die Tweets vom infizierten Rechner aus und verband sich mit den Kontrollsystemen.

WAS WIRD GESTOHLEN?

Cyberkriminelle sind an Informationen unterschiedlichster Art interessiert. Das können die neuesten technischen Entwicklungen von Unternehmen und wissenschaftlichen Forschungsinstituten sein oder Quellcode von Software-Produkten, finanzielle und juristische Dokumente, persönliche Mitarbeiter- und Kundendaten und alle beliebigen anderen Informationen, die ein Betriebsgeheimnis darstellen könnten. Häufig sind solche Informationen unverschlüsselt in den Unternehmensnetzwerken zum Beispiel in Form von elektronischen Dokumenten, Pflichtenheften, Berichten, Zeichnungen oder Präsentationen gespeichert.

Wie bereits erläutert, nutzen Cyberkriminelle unterschiedlichste Ansätze zum Sammeln von Informationen. Einige Schädlinge tragen praktisch alle Arten von elektronischen Dokumenten zusammen. So interessierte sich etwa Roter Oktober unter anderem für Dokumente der Formate txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps und iau, die der Schädling dann an den Steuerungsserver weiterschickte.

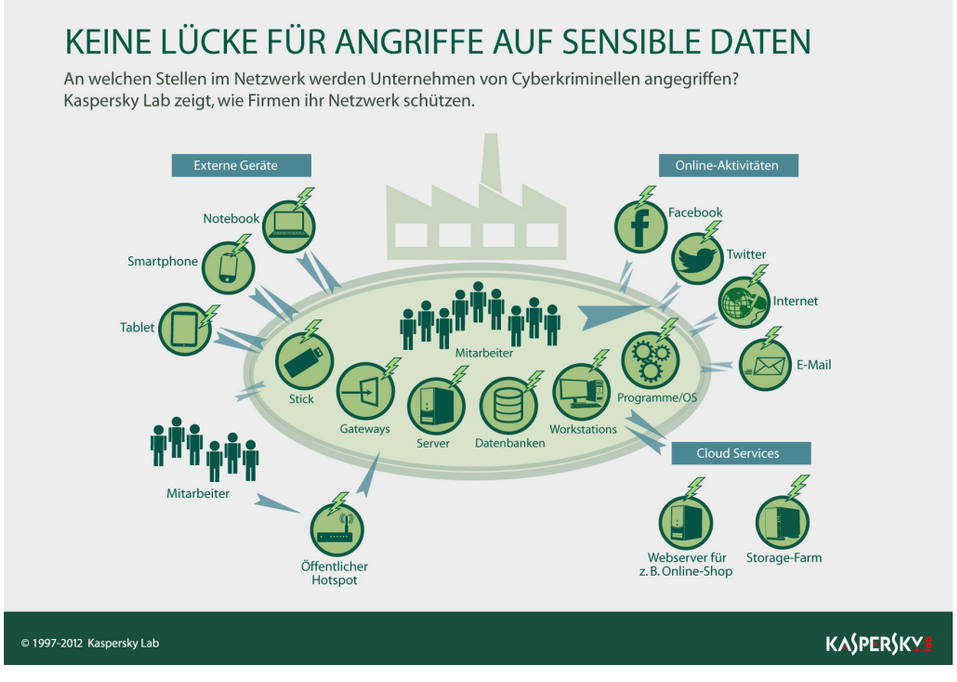
Eine weitere Methode, die Kaspersky Lab in Kimsuky und Icefog feststellte, ist die quasi manuelle Analyse der in Unternehmensnetzwerken gespeicherten Daten (mit Hilfe von in den Schädling integrierten Technologien für den Remote-Zugriff auf infizierte Workstations) und das anschließende Kopieren nur entsprechender Dokumente, die für die Verbrecher von Interesse sind. Dabei bedenken die Cyberkriminellen alle Besonderheiten des angegriffenen Unternehmens und vollziehen sehr genau nach, welche Datenformate dort verwendet und welche Art von Informationen dort gespeichert werden. Auch im Fall von Kimsuky und Icefog wurden für die betroffenen Unternehmen absolut spezifische Dokumente im Format hwp gestohlen, das in Südkorea weit verbreitet ist.

NEUE TENDENZ: CYBERSÖLDNER

Bei der Analyse der zielgerichteten Attacken von Kimsuky und Icefog kam das Kaspersky-Team zu dem Schluss, dass eine neue Kategorie von Angreifern auf der Bühne der Cyberkriminalität erschienen ist, die wir „Cybersöldner“ nennen. Dabei handelt es sich um organisierte Gruppen von hochqualifizierten Hackern, die von Regierungen und Privatunternehmen zur Organisation und Durchführung von komplexen, effektiven, zielgerichteten Attacken auf Unternehmen angeheuert werden können, um Informationen zu stehlen oder um Daten oder Infrastruktur zu zerstören.

Cybersöldner erhalten einen Vertrag, in dem die Ziele des Hackerauftrags definiert werden, woraufhin sie mit der sorgfältigen Vorbereitung und der Umsetzung der Attacke beginnen. Während bei zielgerichteten Attacken früher massenhaft unterschiedliche Informationen gestohlen wurden, so versuchen Cybersöldner absolut konkrete Dokumente oder Kontakte von Personen zu ergaunern, die über wertvolle Informationen verfügen könnten.

Im Jahr 2013 untersuchten wir die Tätigkeit der Cybersöldnergruppe Icefog, die mit dem gleichnamigen Schädling zielgerichtete Attacken durchgeführt hatten. Im Laufe der Ermittlungen fiel uns das Aktivitätsprotokoll der Icefog-Betreiber in die Hände, in dem alle Aktionen der Angreifer genau beschrieben werden. Aufgrund dieser Aufzeichnungen wurde klar, dass die Cyberkriminellen wussten, in welchen Verzeichnissen sich die Informationen befinden, die für sie von Interesse sind.



DIE FOLGEN AUFSEHENERREGENDER ENTHÜLLUNGEN

Im Jahr 2013 wurden viele Angriffe von Spionage-Programmen aufgedeckt, die direkt oder indirekt mit der Tätigkeit verschiedener Staaten in Verbindung standen. Die Folge solcher Enthüllungen kann der Verlust des Vertrauens in globale Dienste und Organisationen sein, aber auch der Wunsch nach der Entwicklung ähnlicher nationalstaatlicher Strukturen. Das wiederum kann zu einer eigentümlichen De-Globalisierung und zu einer steigenden Nachfrage nach lokalen IT-Produkten und -Diensten führen. Schon heute gibt es in vielen Ländern lokale Varianten der globalen Dienste, wie etwa nationale Suchsysteme, E-Mail-Anbieter, nationale IM-Clients und sogar lokale Soziale Netzwerke.

Dabei sorgen nationale Entwicklungsunternehmen für eine steigende Zahl von Software-Produkten und Services. In der Regel sind das Unternehmen, deren Größe und Budget geringer ist als die der führenden internationalen Entwickler. Dementsprechend wird auch die Qualitätskontrolle in diesen Unternehmen nicht so gründlich durchgeführt werden können. Nach den Erfahrungen von Kaspersky Lab bei der Untersuchung von Cyberattacken weist der Code von Softwareprodukten umso mehr Sicherheitslücken auf, je kleiner und unerfahrener der Hersteller ist. Dieser Umstand erleichtert es Cyberkriminellen ungemein, zielgerichtete Attacken durchzuführen.

Zudem könnten einige Staaten, nachdem sie die Kontrolle über Informationen und Hardware-ressourcen gewonnen haben, lokale Unternehmen dazu verpflichten, nationale Software-produkte oder Internet-Dienste zu nutzen, was sich schließlich wiederum negativ auf die Sicherheit im Unternehmenssektor auswirken könnte.

STATISTIK FÜR DAS JAHR 2013

Maria Garnaeva, Christian Funk

QUICK-INFO

- Bedeutsame Ereignisse
- Statistik
- Top 20 der Schadprogramme im Internet
- Top 10 der Länder, auf deren Ressourcen Schadprogramme untergebracht sind
- Länder, in denen Computer dem höchsten Risiko einer Infektion über das Internet ausgesetzt sind
- Top 20 der auf den Computern entdeckten schädlichen Objekte
- Top 20 der Länder nach Infektionsniveau der Computer
- Top 10 der Länder mit minimalen Computer-Infektionsraten

Die vorliegende Statistik ist Teil des Kaspersky Security Bulletin 2013/2014 und beruht auf Daten, die mit Hilfe des Kaspersky Security Network (KSN) gesammelt und ausgewertet wurden. Das KSN verwendet eine Cloud-Architektur in den Kaspersky-Produkten für Heimanwender und Unternehmen und zählt zu den wichtigsten Technologien von Kaspersky Lab.

Die Statistiken im Jahresbericht basieren auf Daten von Kaspersky-Lab-Produkten, deren Anwender ihre Zustimmung zur Übermittlung von statistischen Informationen gegeben haben.

DAS JAHR IN ZAHLEN

> Laut den Daten des KSN blockierten die Produkte von Kaspersky Lab im Jahr 2013 insgesamt **5.188.740.554** schädliche Attacken auf die Computer und mobilen Geräte der Anwender.

> Es wurden **104.427** neue Modifikationen von Schadprogrammen für mobile Geräte gefunden.

> Die Lösungen von Kaspersky Lab wehrten **1.700.870.654** Attacken von Internet-Ressourcen aus verschiedenen Ländern der Welt ab.

> Unsere Antiviren-Lösungen detektierten fast **drei Milliarden** Virenangriffe auf die Rechner der KSN-Nutzer. Im Rahmen dieser Vorfälle wurden insgesamt **1,8 Millionen** schädliche und potenziell unerwünschte Programme registriert.

> 45 Prozent der von Kaspersky-Produkten blockierten Webattacken wurden unter Verwendung schädlicher Webressourcen durchgeführt, die sich in den USA und in Russland befinden.

MOBILE BEDROHUNGEN

Im Jahr 2013 wurde die Sicherheit mobiler Geräte zu einem immer dringenderen Problem, was sowohl mit der quantitativen als auch mit der qualitativen Zunahme mobiler Bedrohungen zusammenhängt. Wenn 2011 das Jahr der Entstehung mobiler Schädlinge war, insbesondere für Android-Geräte, und wenn sich im Jahr 2012 eine Vielfalt dieser Schadprogramme entwickelt hat, so war 2013 das Jahr, in dem die mobile Malware erwachsen wurde. Es ist nicht erstaunlich, dass die Welt der mobilen Schädlinge der Welt der Bedrohungen für PCs hinsichtlich der von Cyberkriminellen angewandten Methoden und Technologien immer ähnlicher wird. Das Entwicklungstempo in diesem Bereich ist jedoch wirklich beeindruckend.

Obad steht wohl für das bedeutendste Ereignis im Bereich der mobilen Schädlinge. Dieser mobile Trojaner verbreitet sich auf verschiedene Arten, darunter über ein bereits existierendes mobiles Botnetz: Smartphones, die mit der Malware Trojan-SMS.AndroidOS.Opfake.a infiziert sind, werden als zusätzliche Infektionsquelle eingesetzt. Von ihnen versendet die Malware Mitteilungen mit schädlichen Links an alle Nummern aus der Kontaktliste. Diese Praxis ist bei den Bedrohungen für PCs weit verbreitet und wird von Botmastern auf dem cyberkriminellen Schwarzmarkt als

Dienstleistung angeboten.

Tatsache ist, dass mobile Botnetze gegenüber traditionellen Zombie-Netzwerken entscheidende Vorteile haben. Ein mobiles Botnetz ist viel stabiler: Smartphones werden selten abgeschaltet, daher sind sämtliche Botnetz-Knoten immer erreichbar und bereit, neue Befehle auszuführen. Die Aufgaben, die mit Hilfe von traditionellen Botnetzen am häufigsten ausgeführt werden, sind der massenhafte Spam-Versand, die Durchführung von DDoS-Attacken und das massenhafte Ausspionieren von persönlichen Daten. Alle diese Aufgaben stellen keine großen Ansprüche an die Rechenleistung der Geräte und sind daher auch problemlos auf Smartphones umzusetzen. Das Botnetz MTK, das Anfang des Jahres 2013 in Erscheinung trat, sowie das Botnetz Opfake und viele andere bestätigen die Tatsache, dass mobile Botnetze für Cyberkriminelle mittlerweile mehr sind als nur ein „Spielplatz“ und sie bereits aktiv zur Erreichung des Hauptziels eingesetzt werden: den Cyberkriminellen dazu zu verhelfen, Geld zu verdienen.

BEDEUTSAME EREIGNISSE

> **Mobile Bankentrojaner.** Dazu gehören mobiles Phishing, Diebstahl von Kreditkarteninformationen, Überweisung von Geldern von Kreditkarten auf das Konto des Mobiltelefons und von dort aus in QIWI-Wallets. Im Jahr 2013 erschienen zudem mobile Trojaner, die in der Lage sind, den Kontostand des Opfers zu überprüfen, um so die „Rendite“ zu maximieren.

> **Mobile Botnetze.** Wie bereits oben erwähnt, bieten Botnetze mehr Möglichkeiten und eine größere Flexibilität, wenn es um illegale Verdienstschemata geht. Diese Erscheinung hat nun auch die mobilen Geräte erfasst. Den Einschätzungen des Kaspersky-Teams zufolge handelt es sich bei etwa 60 Prozent der mobilen Schadprogramme um Bestandteile großer oder kleiner mobiler Botnetze.

> **Backdoor.AndroidOS.Obad.** Dieser Schädling ist wohl universeller als alle anderen uns heute bekannten Schadprogramme. Er umfasst drei Exploits, eine Backdoor, einen SMS-Trojaner und verfügt über die funktionellen Möglichkeiten eines Bots und anderer Programme. Er ist wie ein Schweizer Messer, ausgestattet mit den unterschiedlichsten Werkzeugen.

> **Botnetz-Kontrolle über Google Cloud Messaging.** Cyberkriminelle haben einen Weg gefunden, den Service Google Cloud Messaging (GCM) für die Kontrolle der Zombie-Geräte in einem Botnetz auszunutzen. Diese Methode wird in relativ wenigen Schadprogrammen umgesetzt, doch einige von ihnen sind dafür recht weit verbreitet. Die über GCM empfangenen Befehle werden auch von GCM ausgeführt und lassen sich so nicht mehr direkt auf dem infizierten Gerät löschen.

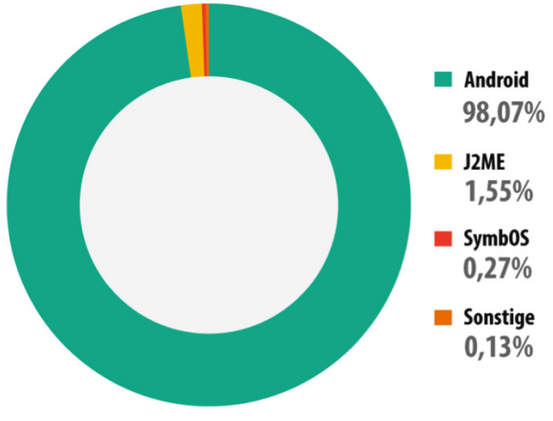
> **APT-Attacken gegen uigurische Aktivisten.** Kaspersky Lab hat beobachtet, wie in zielgerichteten Attacken gegen uigurische Aktivisten Schädlinge verwendet werden, die unter Windows und unter Mac OS X laufen. In der Vergangenheit erfolgten Attacken auch über PDF-, XLS-, DOC- und ZIP-Dateien, die via E-Mail verschickt werden. Jetzt haben die Cyberkriminellen ihrem Arsenal APK-Dateien hinzugefügt, die nach persönlichen Informationen suchen, die auf dem angegriffenen Computer gespeichert sind, und die zudem Daten über den Standort weiterleiten.

> **Sicherheitslücken in Android.** Im Jahr 2013 beobachteten wir Exploits, die sich gegen Android richten und drei verschiedene Ziele verfolgen: Umgehen der Überprüfung der Codeintegrität der Anwendung während der Installation (auch bekannt als Master-Key-Sicherheitslücke), Erhöhung der Privilegien und schließlich Erschweren der Analyse der Applikation. Die letzten zwei Funktionen sind auch in Obad umgesetzt.

> **Angriffe auf PCs mit Hilfe eines Android-Gerätes.** Es gibt Bedrohungen für PCs, die auch Smartphones infizieren können. Doch die Kaspersky-Experten entdeckten jetzt einen Schädling unter Android, der auch PCs ansteckt. Wenn sich ein Android-Gerät mit einem Computer als ‚USB-Laufwerk' verbindet, werden schädliche Inhalte gestartet.

STATISTIK

Hinsichtlich der von Schadprogrammen attackierten mobilen Betriebssysteme gab es im Jahr 2013 keine wesentlichen Veränderungen. Android ist und bleibt das Hauptziel von Schadprogramm-Attacken. Gegen diese Plattform richten sich bereits 98,05 Prozent aller bekannten Schädlinge. Wie auf dem untenstehenden Diagramm zu sehen ist, kann es hinsichtlich der „Popularität" kein anderes Betriebssystem mit Android aufnehmen. Die Gründe dafür liegen in der Führungsposition von Android auf dem Markt, dem Vorherrschen von Android-App-Stores von Drittanbietern und in der äußerst offenen Architektur dieser Plattform, dank derer man sowohl als Programmentwickler als auch als Virenautor problemlos Anwendungen für Android schreiben kann. Wir gehen nicht davon aus, dass sich diese Tendenz in näherer Zukunft ändern wird.

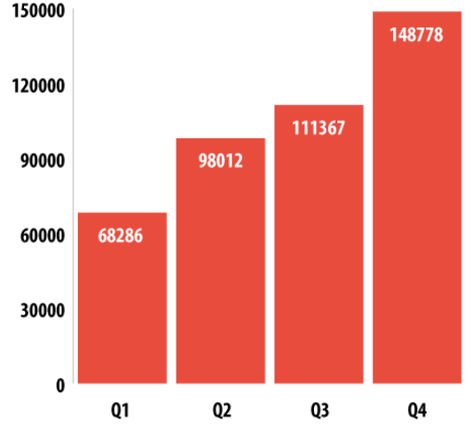


Verteilung der mobilen Schadprogramme nach Plattformen

Bis zum heutigen Tag konnte das Kaspersky-Team 8.260.509 individuelle schädliche Installationspakete zusammentragen. Man sollte dabei bedenken, dass verschiedene Installationspakete Programme mit ein und derselben Funktionalität installieren können, wobei der Unterschied dann nur in der Benutzeroberfläche der Schadanwendung und beispielsweise im Inhalt der von ihnen versendeten SMS liegt.

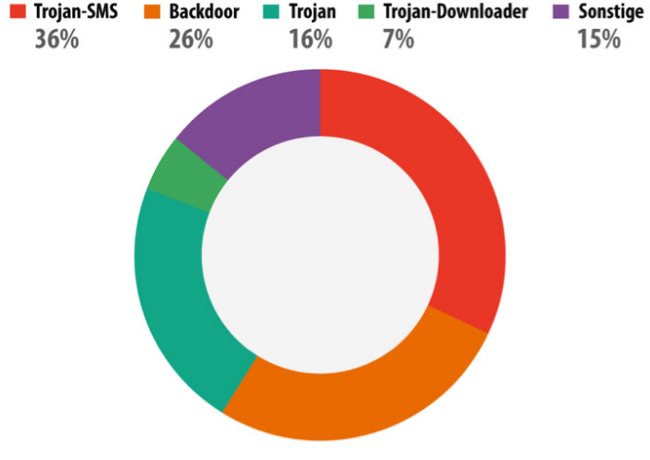
Die Gesamtzahl der Samples von mobilen Schädlingen in unserer Sammlung beträgt 148.778, von denen 104.427 im Jahr 2013 entdeckt wurden. Allein im Oktober erschienen 19.966 Modifikationen

– halb so viele Modifikationen wie Kaspersky Lab innerhalb des ganzen Jahres 2012 entdeckt hat. Glücklicherweise unterscheidet sich diese Situation stark von der in der Welt der PC-Schädlinge beobachteten Lage – hier verarbeiten wir über 315.000 Samples pro Tag. Trotzdem ist die Tendenz zu einem intensiven Wachstum unübersehbar:



Zahl der Samples mobiler Schädlinge in der Sammlung von Kaspersky Lab

Bei den mobilen Schädlingen stehen nach wie vor die SMS-Trojaner an der Spitze:



Verteilung der mobilen Schadprogramme nach Typen

Allerdings haben sich die Schädlinge der Kategorie Trojan-SMS bis auf sehr wenige Ausnahmen zu Bots entwickelt. Daher lassen sich die zwei größten Schädlingsvertreter aus dem Diagramm zu einer Kategorie zusammenfassen, und zwar zur Kategorie Backdoor. Deshalb kann man sagen, dass 62 Prozent der schädlichen Anwendungen Teile mobiler Botnetze sind.

FAZIT

> Alle Techniken und Mechanismen zur Infektion und Verschleierung von schädlicher Aktivität werden sehr schnell vom PC auf die mobile Plattform Android übertragen. Offenheit und Popularität dieses Betriebssystems begünstigen diese Tendenz.

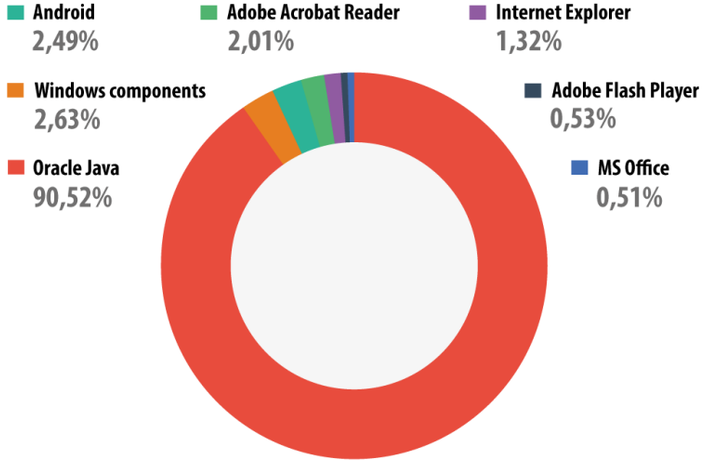
> Die meisten mobilen schädlichen Anwendungen sind auf den Diebstahl von Geld und erst in zweiter Linie auf den Diebstahl von persönlichen Informationen ausgerichtet.

> Bei der Mehrheit der mobilen Schadprogramme handelt es sich um Bots mit umfassender Funktionalität. In nächster Zeit wird ein Handel mit mobilen Botnetzen einsetzen.

> Ganz eindeutig ist eine „Bankenausrichtung“ in der Entwicklung mobiler Schadprogramme zu beobachten. Die Virenautoren verfolgen die Entwicklung der Online-Banking-Dienste sehr genau. Bei erfolgreicher Infektion eines Smartphones wird sofort überprüft, ob das Telefon mit einer Kreditkarte in Verbindung steht.

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.

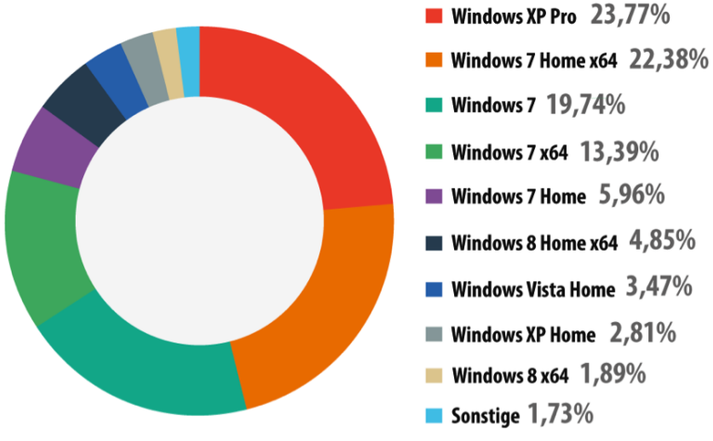


Verteilung der in Attacken von Cyberkriminellen verwendeten Exploits nach Typen der angegriffenen Anwendungen

Von allen von Kaspersky Lab registrierten versuchten Ausnutzungen von Sicherheitslücken entfielen 90,52 Prozent auf Schwachstellen in Oracle Java. Derartige Sicherheitslücken werden im Zuge von Drive-by-Attacken über das Internet ausgenutzt. Neue Java-Exploits sind heute in den meisten Exploit-Packs zu finden. Näheres zu Java-Exploits finden Sie auf unserer Webseite.

Auf dem zweiten Platz positionierte sich die Kategorie „Windows-Komponenten“, die angreifbare Dateien der Windows-Familien enthält, die nicht zum Internet Explorer und Microsoft-Office-Programmen gehören – diese haben wir einzeln betrachtet. In dieser Kategorie entfällt die Mehrzahl der Attacken auf die in win32k.sys gefundene Sicherheitslücke CVE-2011-3402, die erstmals von Duqu ausgenutzt wurde.

Position drei belegen mit einem Wert von 2,5 Prozent die Exploits für Android OS. Die Sicherheitslücken in Android verwenden Cyberkriminelle (und manchmal auch die Anwender selbst), um Root-Privilegien zu erhalten, die praktisch unbegrenzte Möglichkeiten zur Manipulation des Systems eröffnen. Diese Sicherheitslücken werden nicht bei Drive-by-Attacken eingesetzt. Die entsprechenden Exploits erkennt Kaspersky Anti-Virus entweder schon bei der Installation oder wenn der Anwender versucht, eine mit einem Exploit verseuchte Anwendung zu laden. Erwähnenswert ist an dieser Stelle, dass vor Kurzem über die Entdeckung einer Sicherheitslücke im Browser Chrome auf den Smartphones Google Nexus 4 und Samsung Galaxy S4 berichtet wurde, die zur späteren Ausnutzung von Android-Sicherheitslücken in Drive-by-Attacken eingesetzt werden kann.



Bei den KSN-Teilnehmern im Jahr 2013 installierte Windows-Versionen

Von den Nutzern der Produkte von Kaspersky Lab, die ihre Zustimmung zur Teilnahme am KSN erteilt haben, verwenden insgesamt 61,5 Prozent verschiedene Versionen des Betriebssystems Windows 7 (rund fünf Prozentpunkte mehr als im vergangenen Jahr); 6,3 Prozent nutzen Windows XP (etwa 7,75 Prozentpunkte weniger als 2012).

SCHADPROGRAMME IM INTERNET (ATTACKEN ÜBER DAS WEB)

Die statistischen Daten in diesem Abschnitt basieren auf dem Modul Kaspersky Anti-Virus, das einen Computer in dem Moment schützt, in dem Schadcode von einer schädlichen Webseite geladen wird. Infiziert sein können Seiten, die Cyberkriminelle speziell zu diesem Zweck erstellt haben, sowie Webressourcen, deren Inhalt von den Nutzern selbst generiert wird (zum Beispiel Foren) und gehackte legitime Ressourcen.

Die Zahl der Attacken, die von Internet-Ressourcen in verschiedenen Ländern der Welt ausgehen, stieg innerhalb eines Jahres von 1.595.587.670 auf **1.700.870.654.** Das heißt, die Kaspersky-Produkte schützten die Anwender beim Surfen im Netz durchschnittlich 4.659.920 Mal pro Tag.

Verglichen mit dem Vorjahr ist die Geschwindigkeit zurückgegangen, mit der die Attacken über den Browser zunehmen. Die Zahl der im Jahr 2013 abgewehrten Internet-Attacken übersteigt den entsprechenden Vorjahreswert um das 1,07-Fache, während wir im Jahr 2012 eine Zuwachsrate von 1,7 registrierten. Die Hauptangriffsmethode mit Hilfe von Exploit-Packs garantiert Cyberkriminellen praktisch die Infektion von Computern, auf denen kein Schutz installiert ist und auf denen zumindest eine gängige und angreifbare (nicht aktualisierte) Anwendung installiert ist.

TOP 20 DER SCHADPROGRAMME IM INTERNET

Von allen Schadprogrammen, die an Internet-Attacken beteiligt waren, hat das Kaspersky-Team nachfolgend die 20 aktivsten aufgeführt. Auf sie entfielen 99,9 Prozent aller Web-Attacken.

	NAME*	ANTEIL IN %**
1	**Malicious URL**	93.01%
2	**Trojan.Script.Generic**	3.37%
3	**AdWare.Win32.MegaSearch.am**	0.91%
4	**Trojan.Script.Iframer**	0.88%
5	**Exploit.Script.Blocker**	0.49%
6	**Trojan.Win32.Generic**	0.28%
7	**Trojan-Downloader.Script.Generic**	0.22%
8	**Trojan-Downloader.Win32.Generic**	0.10%
9	**Hoax.SWF.FakeAntivirus.i**	0.09%
10	**Exploit.Java.Generic**	0.08%
11	**Exploit.Script.Blocker.u**	0.08%
12	**Exploit.Script.Generic**	0.07%
13	**Trojan.JS.Iframe.aeq**	0.06%
14	**Packed.Multi.MultiPacked.gen**	0.05%
15	**AdWare.Win32.Agent.aece**	0.04%
16	**WebToolbar.Win32.MyWebSearch.rh**	0.04%
17	**AdWare.Win32.Agent.aeph**	0.03%
18	**Hoax.HTML.FraudLoad.i**	0.02%
19	**AdWare.Win32.IBryte.heur**	0.02%
20	**Trojan-Downloader.HTML.Iframe.ahs**	0.02%

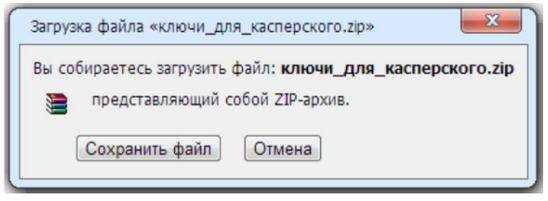
* Von Kaspersky Anti-Virus erkannte Objekte. Die Informationen stammen von KSN-Teilnehmern, die der Übermittlung der Daten zu statistischen Zwecken zugestimmt haben.
** Anteil an allen Web-Attacken, die auf den Computern einzelner KSN-Teilnehmer registriert wurden.

Im Vergleich zum Jahr 2012 stieg der Anteil der Objekte, die mit dem Blockieren schädlicher Links aus der Schwarzen Liste von Kaspersky Anti-Virus zusammenhängen (1. Platz – Malicious URL). Die Entwicklung neuer, auf den Möglichkeiten des KSN basierender Erkennungstechnologien hat dazu geführt, dass der Anteil der mittels KSN entdeckten Bedrohungen von 87 auf 93 Prozent angestiegen ist. Ein bedeutender Teil der Detektionen von gefährlichen URL-Adressen entfällt auf Webseiten mit Exploits und auf Webseiten, die auf Exploits umleiten.

Sieben von 20 Positionen aus unserem Rating belegen schädliche Objekte, die bei Drive-by-Attacken eingesetzt werden – eine der heute wichtigsten Infektionsmethoden über das Internet. Dazu gehören auch schädliche Webseiten, die sowohl nicht-heuristisch als auch mit Hilfe heuristischer Methoden erkannt werden, wie Trojan.Script.Generic, Trojan.Script.Iframer, Exploit.Script.Blocker, Trojan-Downloader.Script.Generic und Exploit.Java.Generic, Exploit.Script.Generic. Solche Schädlinge erhalten Skripte, die auf Exploits umleiten, wie auch Exploits selbst.

Den neunten Platz besetzt Hoax.SWF.FakeAntivirus.i. Unter diese Bezeichnung fallen Flash-Dateien mit Animationen, die die Funktion einer Antiviren-Software imitieren. Gemäß den Ergebnissen des „Scans“ ist der Computer des Users mit einer Unmenge von Schadprogrammen „infiziert“. Um diese wieder loszuwerden, bieten die Cyberkriminellen eine spezielle Schutzlösung an. Das Betrugsopfer muss lediglich eine SMS an eine Kurznummer senden und erhält im Gegenzug einen Link, über den er angeblich das Antiviren-Programm herunterladen kann. Derartige Flash-Dateien können auch auf Webseiten gezeigt werden, auf denen Banner eines Werbenetzwerks platziert sind, deren Teilnehmer nicht davor zurückschrecken, von Zeit zu Zeit eine Umleitung auf unerwünschte Inhalte einzurichten.

Auf Position achtzehn liegt Hoax.HTML.FraudLoad.i. Bei diesen Schädlingen handelt es sich um HTML-Seiten, die ein Standard-Downloadfenster imitieren:



Auf eine derartige Seite leiten verschiedene russischsprachige Webseiten um, auf denen der Download bestimmter Inhalte angeboten wird: Spiele, Anwendungen und Filme. Meist sind solche Webseiten auf kostenlosen Hostings untergebracht. Klickt der Anwender auf die Schaltfläche „Datei speichern“, wird sein Browser auf einen Datei-Hoster umgeleitet, wo ihm der Download der Datei angeboten wird, nachdem er sich kostenpflichtig per SMS registriert hat. Doch hat er alle Forderungen erfüllt, enthält er im Gegenzug entweder nur eine Textdatei mit Instruktionen zur Nutzung von Suchsystemen oder – und das ist noch schlimmer – ein Schadprogramm.

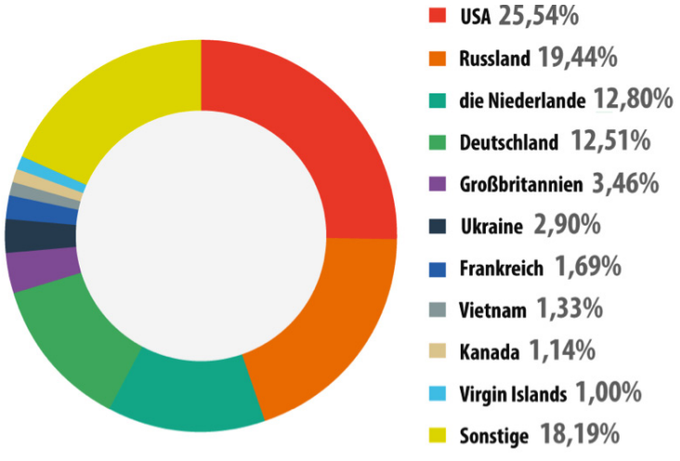
Verglichen mit 2012 sind im Rating nun mehr Werbeprogramme vertreten, deren Gesamtanteil in den Top 20 somit von 0,3 auf 1,04 Prozent angestiegen ist.

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 **1.700.870.654** Attacken über das Internet verwendeten die Cyberkriminellen 10.604.273 individuelle Hosts, das sind rund vier Millionen mehr als im Jahr 2012. Insgesamt 82 Prozent der Benachrichtigungen über die Blockierung von Attacken entfielen auf Angriffe von Webressourcen, die sich in insgesamt zehn Ländern der Welt befinden – das sind rund 14,1 Prozentpunkte weniger als im Jahr 2012.



Verteilung der Quellen von Webattacken nach Ländern

Die Top 10 der Länder für das Jahr 2013 haben sich gegenüber dem Vorjahr praktisch nicht verändert. Nicht mehr unter den ersten Zehn ist China, das Land, das dieses Rating bis 2010 angeführt hat. Dafür kam Vietnam auf Platz acht hinzu. Im Jahr 2010 gelang es den chinesischen Behörden, eine Vielzahl von schädlichen Hostings aus dem lokalen Cyberraum zu verbannen, während gleichzeitig die Bedingungen für die Registrierung von Domains in der Zone .cn verschärft wurden. Daraufhin ging der Anteil der schädlichen Hostings in China drastisch zurück. Im Jahr 2010 belegte China noch den dritten Platz, 2011 den sechsten und im Jahr 2012 den achten Platz. 2013 kam dieses Land nicht mehr über den 21. Platz hinaus.

LÄNDER, IN DENEN COMPUTER DEM HÖCHSTEN RISIKO EINER INFEKTION ÜBER DAS INTERNET AUSGESETZT SIND

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

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

NUMMER	LAND*	% INDIVIDUELLER KSN TEILNEHMER**
1	Aserbaidschan	56.29%
2	Kasachstan	55.62%
3	Armenien	54.92%
4	Russland	54.50%
5	Tadschikistan	53.54%
6	Vietnam	50.34%
7	Moldawien	47.20%
8	Weißrussland	47.08%
9	Ukraine	45.66%
10	Kirgisien	44.04%
11	Sri Lanka	43.66%
12	Österreich	42.05%
13	Deutschland	41.95%
14	Indien	41.90%
15	Usbekistan	41.49%
16	Georgien	40.96%
17	Malaysia	40.22%
18	Algerien	39.98%
19	Griechenland	39.92%
20	Italien	39.61%

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 2013 gab es in diesem Rating einen neuen Spitzenreiter: den ersten Platz belegte Aserbaidschan, wo 56,3 Prozent der Anwender Web-Attacken ausgesetzt waren. Russland, das dieses Rating zwei Jahre in Folge anführte, rutschte mit einem Wert von 54,5 Prozent auf den vierten Platz ab (das sind 4,1 Prozentpunkte weniger als im Vorjahr).

Nicht mehr in den Top 20 vertreten sind die USA, Spanien, Oman, Sudan, Bangladesch, die Malediven und Turkmenistan. Neu hinzugekommen sind Österreich, Deutschland, Griechenland, Georgien, Kirgisien, Vietnam und Algerien.

Die USA rutschten von Position 19 auf den 25. Platz. Der Wert dieses Landes ging um sieben Prozentpunkte zurück und betrug 38,1 Prozent. Wir erinnern daran, dass sich dieses Land nach dem Grad der Web-Bedrohungen noch vor zwei Jahren auf dem dritten Platz befand. Der Rückgang des Infektionsrisikos für Computer über das Internet in den USA könnte unter anderem damit zusammenhängen, dass die Nutzer dort zunehmend mit mobilen Geräten im Netz surfen. Spanien, das die Top 20 im letzten Jahr abschloss, landete 2013 auf dem 31. Platz (36,7 Prozent, etwa 8 Prozentpunkte weniger als im Vorjahr).

Österreich (plus acht Prozentpunkte) landete bei seiner Premiere sofort auf dem 12. Platz der Top 20, Deutschland (plus 9,3 Prozentpunkte) auf dem 13. Platz und Griechenland (minus 1,6 Prozentpunkte) auf Position 19. Das Schlusslicht der Top 20 bildet mit Italien (minus sechs Prozentpunkte) ein weiteres westeuropäisches Land.

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

> **Gruppe mit erhöhtem Risiko:** Zu dieser Gruppe mit Werten zwischen 41 und 60 Prozent gehören die ersten 15 Länder aus den Top 20, und zwar Russland, Österreich, Deutschland, die meisten Länder aus dem postsowjetischen Raum und asiatische Länder. Diese Gruppe ist um mehr als die Hälfte geschrumpft – im Jahr 2012 waren hier noch 31 Länder vertreten.

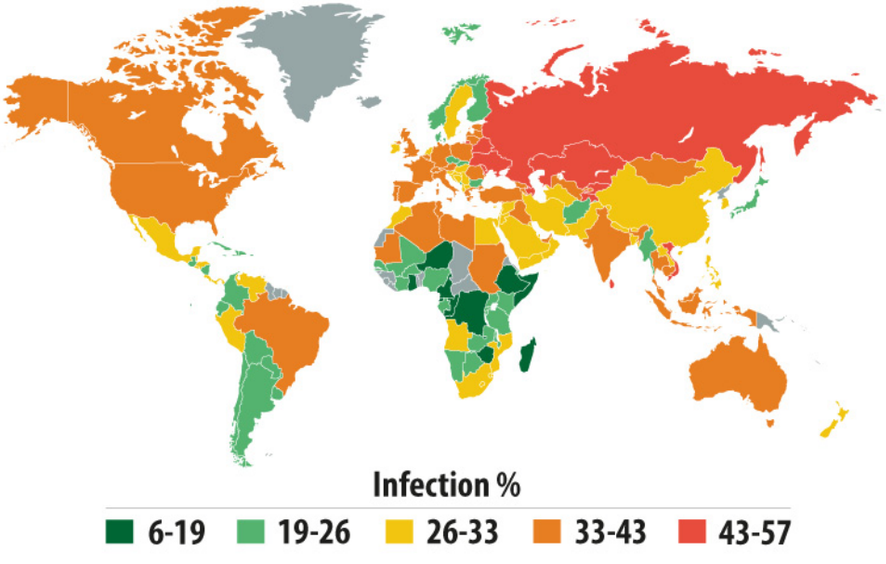
> **Risikogruppe:** In dieser Gruppe mit Werten zwischen 21 und 40,99 Prozent gehören 118 Länder, darunter Australien (38,9 %), die USA (38,1 %), Kanada (36,5 %), Italien (39,6 %), Frankreich (38,1 %), Spanien (36,7 %), Großbritannien (36,7 %), die Niederlande (27,3 %), Finnland (23,6 %), Dänemark (21,8 %), Polen (37,6 %), Rumänien (33,2 %), Bulgarien (24,1 %), Brasilien (34,6 %), Mexiko (29,5 %), Argentinien (25 %), China (32,3 %) und Japan (25,3 %).

> **Gruppe der beim Surfen im Internet sichersten Länder** (Null Prozent bis 20,99 %): Im Jahr 2013 zählten zu dieser Gruppe insgesamt 25 Länder. Dazu gehören Tschechien (20,3 %), die Slowakei (19,7 %), Singapur (18,5 %) und eine Reihe afrikanischer Länder.

Die afrikanischen Länder aus der Gruppe der beim Surfen im Netz sichersten Länder landeten

bei den lokalen Bedrohungen in den Gruppen „mittleres“ oder „hohes Infektionsniveau“ (siehe unten). In diesen Ländern ist das Internet bisher noch nicht besonders weit entwickelt, daher verwenden die User verschiedene mobile Datenträger für den Austausch von Dateien. So sind die User hier nur wenigen Web-Bedrohungen ausgesetzt, während Schadprogramme, die auf mobilen Speichermedien verbreitet werden, häufig auf den Computern detektiert werden.

Durchschnittlich stieg das Gefahrenniveau des Internets um 6,9 Prozentpunkte: Im Jahr 2013 waren weltweit 41,6 Prozent der Computer von Internetnutzern mindestens einmal einer Webattacke ausgesetzt. 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 Systeme 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).

Im Jahr 2013 entdeckten und blockierten unsere Antiviren-Lösungen fast **drei Milliarden** Versuche einer lokalen Infektion auf den Computern der KSN-Teilnehmer. Bei diesen Vorfällen wurden **1,8 Millionen** schädliche und potenziell unerwünschte Programme registriert.

TOP 20 DER AUF DEN COMPUTERN ENTDECKTEN SCHÄDLICHEN OBJEKTE:

	NAME	% INDIVIDUELLER KSN TEILNEHMER*
1	**DangerousObject.Multi.Generic**	39.1%
2	**Trojan.Win32.Generic**	38.0%
3	**Trojan.Win32.AutoRun.gen**	20.1%
4	**Virus.Win32.Sality.gen**	13.4%
5	**Exploit.Win32.CVE-2010-2568.gen**	10.6%
6	**AdWare.Win32.DelBar.a**	8.0%
7	**Trojan.Win32.Starter.lgb**	6.6%
8	**Virus.Win32.Nimnul.a**	5.5%
9	**Worm.Win32.Debris.a**	5.4%
10	**Virus.Win32.Generic**	5.4%
11	**Trojan.Script.Generic**	5.4%
12	**Net-Worm.Win32.Kido.ih**	5.1%
13	**AdWare.Win32.Bromngr.i**	4.6%
14	**Net-Worm.Win32.Kido.ir**	4.4%
15	**Trojan.Win32.Starter.yy**	3.9%
16	**DangerousPattern.Multi.Generic**	3.8%
17	**HiddenObject.Multi.Generic**	3.8%

18	**Trojan.Win32.Hosts2.gen**	3.7%
19	**AdWare.Win32.Agent.aeph**	3.6%
20	**Trojan.WinLNK.Runner.ea**	3.6%

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

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

Schädliche Programme des Typs DangerousObject.Multi.Generic, die mit Hilfe von Cloud-Technologien aufgespürt werden, stiegen im Jahr 2013 vom zweiten auf den ersten Platz. 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. Mit Hilfe der in das KSN integrierten Technologie UDS (Urgent Detection System) wurden über 11 Millionen Computer in Echtzeit geschützt.

Den zweiten Platz belegt Trojan.Win32.Generic, das Kaspersky-Produkte mittels heuristischer Analysefunktionen aufspüren und das im Vorjahr den ersten Platz belegte.

Exploit.Win32.CVE-2010-2568.gen (fünfter Platz) und Trojan.WinLNK.Runner.ea (20. Platz) sind schädliche lnk-Dateien (Verknüpfungen). In den lnk-Dateien dieser Familien wird der Start einer anderen schädlichen ausführbaren Datei umgesetzt. Sie werden häufig von Würmern zur Verbreitung über USB-Speicher eingesetzt.

Acht Programme aus den Top 20 verfügen entweder über einen Selbstverbreitungsmechanismus oder werden als ein Element im Verbreitungsschema von Würmern eingesetzt. Das sind Virus.Win32.Sality.gen (vierter Platz), Trojan.Win32.Starter.lgb (siebter Platz), Virus.Win32.Nimnul.a (achter Platz), Worm.Win32.Debris.a (neunter Platz), Virus.Win32.Generic (zehnter Platz), Net-Worm.Win32.Kido.ih (zwölfter Platz), Net-Worm.Win32.Kido.ir (14. Platz) und Trojan.Win32.Starter.yy (15. Platz).

Der Anteil der berühmten Würmer Net-Worm.Win32.Kido (zwölfter und 14. Platz), die erstmals bereits im Jahr 2008 in Erscheinung traten, geht von Jahr zu Jahr in dem Maße zurück, in dem die Anwender ihre Systeme aktualisieren.

Nicht in den Top 20 des Jahres vertreten ist dieses Mal die Familie Virus.Win32.Virut, obwohl der Anteil anderer Vertreter des Schädlingstyps Viren – Sality (vierter Platz) und Nimnul (achter Platz) – um jeweils 8,5 Prozent beziehungsweise um 1,4 Prozent gestiegen ist.

Ein Neueinsteiger im Rating des Jahres 2013 ist die Familie Worm.Win32.Debris.a auf Platz neun. Der Wurm wird über mobile Datenträger mittels lnk-Dateien verbreitet. Die Payload dieses Wurms besteht aus dem Schadprogramm Andromeda, das für den Download von Drittdateien verwendet wird. Dieses Programm ist auf dem Virenschreiber-Schwarzmarkt bereits seit 2011 bekannt. Seine neue Installations- und Verbreitungsmethode haben die Kaspersky-Experten allerdings in eine separate Familie eingeteilt.

Auf Rang 18 positionierte sich Trojan.Win32.Hosts2.gen. Die gleichnamige Ereignismeldung gibt Kaspersky Anti-Virus bei der Detektion von Schadprogrammen aus, die versuchen, die Hosts-Datei zu ändern, indem sie die Anfragen der User auf bestimmte Domains auf von ihnen kontrollierte Hosts umleiten.

LÄNDER, IN DENEN DIE COMPUTER DEM HÖCHSTEN RISIKO EINER LOKALEN INFEKTION AUSGESETZT WAREN

Um zu bewerten, in welchen Ländern es die Anwender am häufigsten mit Cyberbedrohungen zu tun hatten, haben wir für jedes Land berechnet, wie häufig unsere Antiviren-Lösung im Laufe des Jahres bei den Anwendern Alarm geschlagen hat. Berücksichtigt wurden dabei 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*	%**
Vietnam	68.14%
Bangladesch	64.93%
Nepal	62.39%
Mongolei	60.18%

Indien	59.26%
Sudan	58.35%
Afghanistan	57.46%
Algerien	56.65%
Laos	56.29%
Kambodscha	55.57%
Irak	54.91%
Dschibuti	54.36%
Malediven	54.34%
Pakistan	54.12%
Sri Lanka	53.36%
Mauretanien	53.02%
Indonesien	52.03%
Ruanda	51.68%
Angola	50.91%
Ägypten	50.67%

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.

Schon seit mehr als einem Jahr setzen sich die Top 20 der Länder nach Infektionsniveau aus Ländern Afrikas, des Nahen Ostens und Südostasiens zusammen. Allerdings hat sich die Situation innerhalb des letzten Jahres insgesamt zum Besseren gewendet. Während im Jahr 2012 der Wert des Spitzenreiters bei über 99 Prozent lag, so kommt der Höchstwert im Jahr 2013 nicht an die 70- Prozent-Marke heran.

Durchschnittlich wurde in den Ländern aus den Top 20 bei 60,1 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 73,8 Prozent im Jahr 2012.

Auch bei den lokalen Bedrohungen lassen sich alle Länder in verschiedene Kategorien einteilen. Angesichts des allgemeinen Rückgangs des Infektionsniveaus – der allem Anschein nach damit

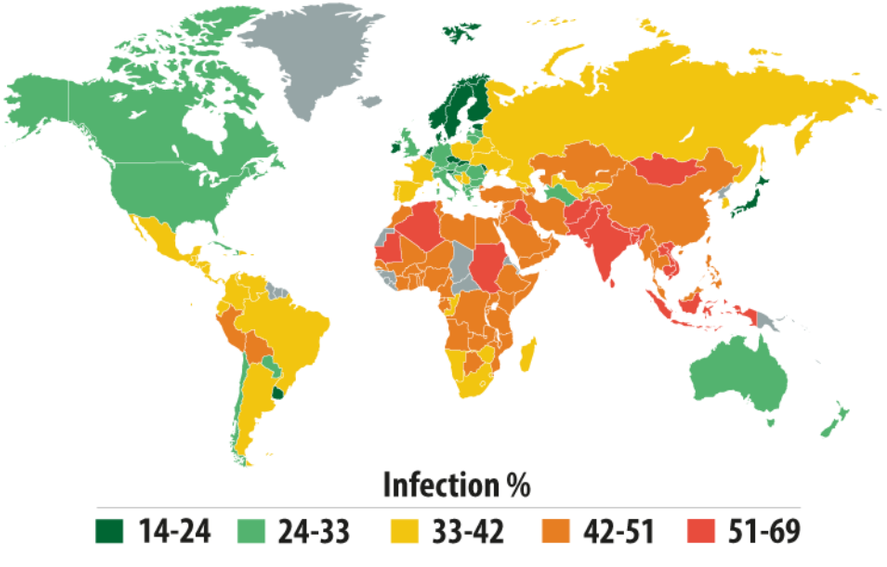
zu erklären ist, dass zum Austausch von Informationen immer seltener USB-Speichermedien benutzt werden – haben wir die Grenzwerte der Gruppen (im Vergleich zur Statistik für das Jahr 2012) gesenkt.

> **Maximales Infektionsniveau** (über 60 Prozent): hier sind die ersten vier Länder im Rating vertreten – Vietnam (68,1 %), Bangladesch (64,9 %), Nepal (62,4 %) und die Mongolei (60,2 %).

> **Hohes Infektionsniveau** (41 bis 60 Prozent): 67 Länder, darunter Indien (59,2 %), China (46,7 %), Kasachstan (46 %), Aserbaidschan (44,1 %), Russland (41,5 %) sowie die meisten Länder Afrikas.

> **Mittleres Infektionsniveau** (21 bis 40,99 Prozent): 78 Länder, darunter Spanien (36 %), Frankreich (33,9 %), Portugal (33,1 %), Italien (32,9 %), Deutschland (30,2 %), die USA (29 %), Großbritannien (28,5 %), die Schweiz (24,6 %), Schweden (21,4 %), die Ukraine (37,3 %), Brasilien (40,2 %), Argentinien (35,2 %), Chile (28,9 %), Südkorea (35,2 %) und Singapur (22,8 %).

> **Niedriges Infektionsniveau** (Null Prozent bis 20,99 Prozent): neun Länder.



TOP 10 DER LÄNDER MIT MINIMALEN COMPUTER-INFEKTIONSRATEN:

POS.	LAND	%
1	**Dänemark**	14.74%
2	**Tschechien**	15.584%
3	**Finnland**	15.93%
4	**Kuba**	17.18%
5	**Japan**	18.93%
6	**Slowakei**	19.24%
7	**Slowenien**	19.32%
8	**Norwegen**	19.36%
9	**Seychellen**	19.90%
10	**Malta**	21.28%

Gegenüber dem Jahr 2012 gab es in dieser Liste eine Veränderung – die Niederlande wurden durch den Neueinsteiger Seychellen ersetzt.

Durchschnittlich wurden 18,8 Prozent der Computer in den zehn sichersten Ländern mindestens einmal im Laufe des Jahres angegriffen. Im Vergleich zum Vorjahr ist dieser Wert um 6,6 Prozentpunkte zurückgegangen.

PROGNOSEN

Alexander Gostev (@codelancer)

QUICK-INFO

- Attacken auf Bitcoin
- Probleme beim Schutz des Privatlebens
- Angriffe auf Cloud-Speicher
- Attacken auf Software-Entwickler
- Cybersöldner
- Fragmentierung des Internets
- Die Pyramide der Cyberbedrohungen

Forecasts for 2014 - expert opinion (Englisch)

MOBILE BEDROHUNGEN

„Erpresser“-Malware nahm vor vielen Jahren mit dem Trojaner Gpcode ihren Anfang. Mittlerweile haben sich daraus zwei Grundtypen entwickelt. Zum einen Trojaner, die die Funktionen des Computers blockieren und Geld für dessen Entsperrung fordern, und zum anderen Trojaner, die Daten auf dem Computer verschlüsseln und wesentlich höhere Summen für die Dechiffrierung fordern.

Im Jahr 2014 wird die Cyberkriminalität den nächsten logischen Schritt in der Entwicklung dieser zwei Arten von trojanischen Programmen gehen und sich nun den mobilen Geräten zuwenden. In erster Linie natürlich Geräten mit dem Betriebssystem Android. Die Verschlüsselung von Anwenderdaten auf dem Smartphone – Fotos, Kontakte, Korrespondenz – ist für einen Trojaner ein Kinderspiel, wenn er über Administratorenrechte verfügt. Auch die Verbreitung derartiger tro-

janischer Programme – unter anderem über den legalen Service Google Play – macht Cyberkriminellen keine großen Umstände.

Im Jahr 2014 wird sich die Tendenz zu immer komplexer werdender mobiler Malware, die wir bereits im Jahr 2013 beobachtet haben, ohne Zweifel fortsetzen. Wie auch schon früher werden Cyberkriminelle versuchen, mit Hilfe mobiler Trojaner Geld von den Anwendern zu ergaunern. Auch die Entwicklung von Methoden und Technologien, die den Zugriff auf Bankkonten von Inhabern mobiler Geräte ermöglichen, wird sich fortsetzen (mobiles Phishing, „Banking"-Trojaner). Ein Handel mit mobilen Botnetzen wird einsetzen; diese wird man aktiv zur Verbreitung von Dritt-Malware einsetzen. Sicherheitslücken im Betriebssystem Android werden wie gehabt bei der Infektion mobiler Geräte und möglicherweise auch bei Drive-by-Attacken auf Smartphones ausgenutzt werden.

ATTACKEN AUF BITCOIN

Attacken auf Bitcoin-Pools, Börsen und Nutzer von Bitcoins werden zu einem der brennendsten Themen des Jahres 2014 werden.

Attacken auf Börsen werden sich dabei der größten Beliebtheit unter Cyberkriminellen erfreuen, da bei der Durchführung solcher Angriffe ein maximaler Ertrag einem geringen Einsatz gegenübersteht.

Was die Angriffe auf die Nutzer von Bitcoins betrifft, so wird das Risiko von Attacken, die den Diebstahl der Wallets zum Ziel haben, im Jahr 2014 deutlich ansteigen. Wir erinnern daran, dass Cyberkriminelle in der Vergangenheit die Computer der Anwender infizierten und sie zum Mining nutzten. Die Effizienz dieser Methode ist nun allerdings erheblich zurückgegangen, während der Diebstahl von Bitcoins den Angreifern enorme Gewinne bei vollständiger Anonymität verspricht.

PROBLEME BEIM SCHUTZ DES PRIVATLEBENS

Die Menschen möchten ihr Privatleben vor den Geheimdiensten verschiedenster Länder dieser Welt schützen. Dieser Schutz kann nicht gewährleistet werden, wenn Internet-Dienste, die Anwender in Anspruch nehmen, nicht die entsprechenden Maßnahmen ergreifen. Gemeint sind unter anderem Soziale Netzwerke, E-Mail-Provider und Cloud-Speicher. Allerdings sind auch die heute verfügbaren Schutzmethoden nicht ausreichend. Eine Reihe solcher Internetdienste hat bereits die Einführung zusätzlicher Maßnahmen zum Schutz der Anwenderdaten verkündet, wie

etwa die Verschlüsselung der Daten, die zwischen den eigenen Servern übertragen werden. Die Integration von Schutztechnologien wird fortgesetzt, da die Anwender sie fordern werden, und das Vorhandensein solcher Technologien kann eine wesentliche Rolle bei der Auswahl des einen oder anderen Internetdienstes spielen.

Doch es gibt auch Herausforderungen für den Endanwender. Er muss die Informationen sichern, die er auf seinem Computer und seinen mobilen Geräten speichert, und ebenso selbstständig für die Geheimhaltung seiner Aktivitäten im Netz sorgen. Das wird eine zunehmende Nutzung von VPN-Services und Tor-Anonymisierern zur Folge haben, ebenso wie eine steigende Nachfrage nach lokalen Verschlüsselungswerkzeugen.

ANGRIFFE AUF CLOUD-SPEICHER

Für die Cloud brechen harte Zeiten an. Einerseits wankt das Vertrauen in Cloud-Speicherdienste auf Grund der von Edward Snowden enthüllten Fakten über die Datensammlung durch verschiedene nationale Geheimdienste. Andererseits werden die dort gespeicherten Daten, ihr Umfang und – was noch wichtiger ist – ihr Inhalt ein zunehmend attraktives Ziel für Hacker. Schon vor drei Jahren hat Kaspersky Lab davon gesprochen, dass es für Cybergangster mit der Zeit leichter sein würde, einen Cloud-Provider zu hacken und dort die Daten irgendeines Unternehmens zu stehlen, als das Unternehmen selbst zu hacken. Es sieht so aus, als wäre diese Zeit nun angebrochen. Hacker werden zielgerichtet das schwächste Glied in der Kette angreifen – die Mitarbeiter von Cloud-Services. Ein Angriff auf sie könnte der Schlüssel zum Zugriff auf gigantische Datenmengen sein. Neben dem Diebstahl von Informationen könnten sich die Angreifer auch für das Entfernen oder Modifizieren der Daten interessieren – was für die Auftraggeber der Attacken in verschiedenen Fällen durchaus noch vorteilhafter sein könnte.

ATTACKEN AUF SOFTWARE-ENTWICKLER

Mit dem oben beschriebenen Problem wird vermutlich eine Zunahme der Angriffe auf Software-Entwickler einhergehen. Im Jahr 2013 deckten wir eine Angriffsserie der Cyberkriminellengruppe Winnti auf. Die Opfer dieser Attacken waren Spiele-Entwickler, denen serverseitige Quellcodes von Online-Games gestohlen wurden. Opfer einer anderen Attacke wurde das Unternehmen Adobe – hier wurden unter anderem die Quellcodes von Adobe Acrobat und ColdFusion gestohlen. Von früheren Beispielen derartiger Vorfälle ist die Attacke auf RSA im Jahr 2011 besonders erwähnenswert, als

die Angreifer sich Quellcodes von SecureID verschafften und diese Daten daraufhin in einer Attacke auf Lockheed Martin benutzt wurden.

Der Diebstahl von Quellcodes gängiger Produkte eröffnet Angreifern wunderbare Möglichkeiten bei der Suche nach Sicherheitslücken in eben diesen Produkten – welche dann später ausgenutzt werden. Haben Angreifer Zugriff auf das Projektarchiv des Opfers, so können sie den Quellcode zudem modifizieren, beispielsweise indem sie Backdoors hinzufügen.

Wieder sind es die Entwickler von mobilen Anwendungen, die einem besonders hohen Risiko ausgesetzt sind – und es gibt tausende von ihnen, die wiederum tausende Apps entwickeln, welche dann auf Millionen Geräten installiert werden.

CYBERSÖLDNER

Die Enthüllungen Snowdens haben gezeigt, dass der Staat unter anderem darum Cyberspionage betreibt, um „seinen" Unternehmen Hilfestellung zu leisten. Diese Tatsache zeigt, welche drastischen Mittel im Konkurrenzkampf der Geschäftswelt eingesetzt werden. Unter Berücksichtigung der neuen Realitäten sehen sich Organisationen nun mit der Einführung entsprechender Aktivitäten konfrontiert.

Unternehmen werden gewissermaßen gezwungen sein, Cyberspionage zu betreiben, wenn sie konkurrenzfähig bleiben wollen – denn andere spionieren bereits, um sich einen Wettbewerbsvorteil zu verschaffen. Es ist nicht ausgeschlossen, dass Unternehmen in einigen Ländern Regierungsstrukturen im Cyberspace ausspionieren werden, ebenso wie ihre eigenen Mitarbeiter, Partner und Lieferanten.

Umsetzen kann die Geschäftswelt derlei Aktivität allerdings nur mit Hilfe von Cybersöldnern – organisierte Gruppen von qualifizierten Hackern, die Unternehmen kommerzielle Dienste bei der Durchführung von Cyberspionage-Tätigkeiten anbieten. Diese Hacker werden sich selbst allerdings eher „Cyberdetektive" nennen.

Ein Beispiel für den Einsatz von angeheuerten Hackern zur Umsetzung kommerzieller Cyberspionage lieferte die Attacke Icefog, die das Kaspersky-Team im Jahr 2013 aufdecken konnte.

FRAGMENTIERUNG DES INTERNETS

Verdächtige Dinge gehen im Netz vor sich. Viele Experten, insbesondere Eugene Kaspersky, sprechen von der Notwendigkeit, ein paralleles, „sicheres Internet" zu schaffen, das keine Möglichkeiten bietet, dort anonym Straftaten zu begehen. Die Cyberkriminellen erschaffen bereits ihr eigenes separates Darknet, das auf den Technologien Tor und I2P basiert, die es ihnen ermöglichen, anonym zu handeln, zu kommunizieren und illegalen Tätigkeiten nachzugehen.

Gleichzeitig hat ein Fragmentierungsprozess des Internets in nationale Segmente eingesetzt. Bis vor kurzem tat sich diesbezüglich nur China mit seiner „Great Firewall of China" hervor. Allerdings steht China mit seinem Bestreben, einen wesentlichen Teil seiner Ressourcen abzuspalten und diese selbstständig zu kontrollieren, nicht allein da. Eine Reihe von Ländern, darunter Russland, hat Gesetze verabschiedet oder beabsichtigt, solche Gesetze zu verabschieden, die die Nutzung ausländischer Services verbieten. Diese Tendenzen haben sich besonders nach den Veröffentlichungen von Edward Snowden verstärkt. So erklärte Deutschland im November, dass es plane, die gesamte interne Kommunikation zwischen deutschen Behörden vollständig innerhalb des Landes abzuwickeln. Brasilien gab seine Absicht bekannt, einen alternativen Hauptinternetkanal zu legen, um nicht den Kanal benutzen zu müssen, der durch das US-amerikanische Florida führt.

Das World Wide Web zerfällt in Einzelteile. Die Länder möchten nicht ein einziges Byte an Informationen über die Grenzen ihrer Netze hinaus durchsickern lassen. Diese Bestrebungen werden immer stärker werden, und von juristischen Einschränkungen bis zu technischen Verboten ist der Weg nicht weit. Der Schritt, der wahrscheinlich darauf folgen wird, ist der Versuch, ausländischen Zugriff auf die Daten innerhalb des eigenen Landes einzuschränken.

Schreiten derartige Tendenzen weiter voran, so könnten wir schon sehr bald ohne einheitliches Internet dastehen, dafür aber mit Dutzenden nationaler Netze. Es ist nicht ausgeschlossen, dass einige Netze nicht einmal die Möglichkeit haben werden, miteinander zu interagieren. Dabei wird das Untergrund-Darknet das einzige Nationen übergreifende Netz sein.

DIE PYRAMIDE DER CYBERBEDROHUNGEN

Alle von uns erwarteten Ereignisse und Tendenzen für das Jahr 2014 lassen sich am einfachsten grafisch in Form einer Pyramide der Cyberbedrohungen darstellen, wie wir sie im Jahr zuvor bereits beschrieben haben.

Diese Pyramide besteht aus drei Elementen. Die untere Ebene bilden die Bedrohungen, die bei Attacken auf durchschnittliche Nutzer durch traditionelle Cyberkriminelle eingesetzt werden, die ausschließlich von eigenen finanziellen Interessen angetrieben werden. Die mittlere Ebene besteht aus Bedrohungen, die in zielgerichteten Attacken im Rahmen von Wirtschaftsspionage zum Einsatz kommen, sowie aus sogenannten Polizei-Spionageprogrammen, die Regierungen benutzen, um ihre Bürger und Unternehmen auszuspionieren. Die Spitze der Pyramide bilden Cyberbedrohungen, die von Staaten zur Durchführung von Cyberattacken auf andere Staaten entwickelt werden.

Die meisten der oben beschriebenen Entwicklungsszenarien von Cyberbedrohungen sind in die mittlere Ebene der Pyramide einzuordnen. Daher erwartet Kaspersky Lab im Jahr 2014 eine rasantere Zunahme von Bedrohungen, die mit wirtschaftlicher und innerstaatlicher Cyberspionage zusammenhängen.

Ermöglicht wird die Zunahme derartiger Angriffe durch die Umorientierung von Cyberkriminellen, die derzeit noch mit Attacken auf Heimanwender beschäftigt sind und sich künftig als Cybersöldner/ Cyberdetektive verdingen werden. Zudem ist es durchaus möglich, dass auch solche IT-Spezialisten ihre Dienste als Cybersöldner anbieten werden, die noch nie illegal tätig waren. Dazu trägt auch der Anstrich der Legitimität bei, den die Aufträge von soliden Unternehmen der Arbeit der Cyberdetektive verleihen.

KASPERSKY lab

www.kaspersky.com

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