SOPHOS
Security made simple.

So verhindern Sie, dass Sie Teil eines Botnets werden

Botnets sind verborgene Gruppen kompromittierter Netzwerk-Computer und -Geräte (sogenannte Bots), die von Malware infiltriert wurden, um eine externe Kontrolle durch Cyberkriminelle zu ermöglichen. Botnets werden von Hackern aufgebaut und gesteuert: Das Ergebnis sind leistungsstarke Dark-Cloud-Computing-Netzwerke, über die kriminelle Cyberangriffe ausgeführt werden – so z. B. der kürzliche DDoS-Angriff auf den beliebten Domain Name Service (DNS) Provider Dyn. Dieser Angriff legte mehere Stunden lang eine Reihe viel besuchter Websites sowie weite Teile des gesamten Internets lahm. Tatsächlich ist es relativ einfach, Computer und Geräte vor Botnet-Angriffen abzuschirmen. In diesem Whitepaper erklären wir, wie Sie sich vor Botnet-Infektionen schützen und Bots in Ihrem Netzwerk einfach aufspüren und diese beseitigen, bevor sie Teil des nächsten Cyberangriffs werden.

Botnets und das Internet der Dinge

Die wachsende Zahl mobiler und Netzwerkgeräte ist zweifellos mit vielen Vorteilen verbunden. Wir sind heutzutage in der Lage, nicht nur auf unsere Computer, sondern auch auf unsere Sicherheitssysteme, Kameras, Haushaltsgeräte und immer mehr andere Geräte remote über das Internet remote zuzugreifen und diese unabhängig von unserem Aufenthaltsort zu steuern. Diese Geräte werden unter dem Sammelbegriff „Internet der Dinge" (IoT, Internet of Things) zusammengefasst und eröffnen uns bei der Steuerung und Effizienz unseres Alltags ganz neue Möglichkeiten. Allerdings stellt diese riesige Zahl untereinander verbundener Geräte auch eine erstklassige Gelegenheit für Hacker dar, neue Systeme zu infiltrieren und in ihre Botnets einzubinden.

Besonders beunruhigend in Hinblick auf die Zunahme Internet-fähiger Geräte ist das Fehlen grundlegender Sicherheitsmaßnahmen. Dass fast jedes IoT-Gerät ab Werk mit Standard-Zugangsdaten (die die Besitzer fast nie ändern) ausgeliefert wird, ist schon schlimm genug, denn so kann sich Malware in vielen Fällen problemlos Zugriff verschaffen. Aktuellen Schätzungen zufolge sind derzeit etwa 500.000 IoT-Geräte mit Standard-Zugangsdaten im Umlauf.

Noch gefährlicher ist jedoch, dass viele dieser Geräte auch über Backdoor-Support oder Diagnose-Zugangsdaten (Telnet oder SSH) verfügen, von denen die Besitzer gar nichts wissen. So können die Geräte selbst dann kompromittiert werden, wenn ihre Besitzer richtig gehandelt und komplexe Zugangsdaten eingerichtet haben. Außerdem nutzt fast jedes IoT-Gerät eine Variante von Linux, weshalb es für Hacker ein Leichtes ist, Exploits aufzuspüren oder Malware auf den Geräten zu installieren.

Mit dieser Flut neuer IoT-Geräte und bereits kompromittierter Computer steht Cyberkriminellen eine noch nie da gewesene Rechenleistung zur Verfügung – Rechenleistung, die bei unsachgemäßem Gebrauch verheerende Folgen haben kann. Ein aktuelles Beispiel ist das Mirai-Botnet, dessen jüngster DDoS-Angriff einen Tag lang weite Teile des Internets zum Erliegen brachte und geschätzte 1 TBit/s generierte.

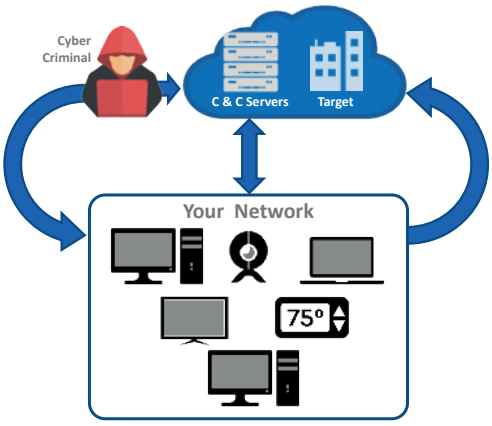
Wie Botnets funktionieren und was Sie dagegen tun können

Um zu verstehen, wie Sie Botnets identifizieren und stoppen können, müssen Sie sich zunächst mit dem Funktionsprinzip vertraut machen – wie nehmen Botnets ihren Anfang, wie breiten sie sich aus und wie operieren sie?

Wie jede andere Malware nehmen auch Botnets ihren Anfang, indem sie sich über eine Reihe konventioneller Methoden Zugang zu Ihrem Netzwerk verschaffen:

- **E-Mail-Anhänge:** Malware wird oft im Rahmen einer Spam- oder Phishing-Kampagne als E-Mail-Anhang in Umlauf gebracht. Dieser Anhang soll vom Benutzer ausgeführt werden, um den Exploit zu starten.
- **Websites:** Kompromittierte Websites enthalten häufig Malware, die unentdeckt vom Browser ausgeführt werden kann. Auf diese Weise wird eine Kette von Ereignissen ausgelöst, die zur Ausnutzung einer Schwachstelle auf dem System führt und dieses infiziert.

- **Remote-Zugriff:** IoT-Geräte mit Internet-Zugang, auf die über Standard-Zugangsdaten direkt zugegriffen werden kann, sind die schlimmsten Übeltäter. Hacker sind jedoch nach wie vor durchaus bereit, Passwörter auch per Brute-Force-Methode zu hacken oder bekannte Schwachstellen in Web-Oberflächen auszunutzen, um sich Kontrolle über ein Gerät zu verschaffen.
- **USB-Sticks:** Diese Infektionsmethode ist seit langem als Klassiker bekannt. Dennoch besteht nach wie vor die Gefahr, dass Benutzer aus Leichtsinn einen USB-Stick unbekannter Herkunft an ihren Computer anschließen, um herauszufinden, was auf diesem gespeichert ist – mit dem Ergebnis, dass das System mit Malware infiziert wird.



Die zur Infiltration Ihres Unternehmens eingesetzte Malware kann extrem raffiniert und evasiv sein. Bei Sophos beobachten wir, dass 70 % aller bei uns eingehenden Malware-Samples speziell für ein bestimmtes Unternehmen entwickelt wurden. Außerdem wird solche hochentwickelte Malware ständig modifiziert. Diese neue Generation gezielter Malware stellt den Schutz auf eine neue Probe und erfordert neben herkömmlichen Signaturen auch Verhaltensanalysen.

In anderen Fällen kann Malware zur Ausnutzung von IoT-Geräten auch ganz simpel sein und einfach großangelegte Port-Scans weiter Teile des Internets durchführen – auf der Suche nach Zugriffsmöglichkeiten und unter Ausnutzung von Standard-Zugangsdaten oder Brute-Force-Hacking, um sich Zugang zu verschaffen. Solche Malware lässt sich viel einfacher abwehren, da hierfür lediglich eine geeignete Firewall-Konfiguration und entsprechende Schutzmaßnahmen erforderlich sind.

Sobald Malware in Ihrem Unternehmen Fuß gefasst hat, baut sie in der Regel eine Call-Home-Kommunikationsverbindung zum „Command-and-Control"-Server (C&C) des Hackers auf, um ihren Erfolg zu melden und weitere Anweisungen entgegenzunehmen. In manchen Fällen wird die Malware angewiesen, sich unauffällig zu verhalten und abzuwarten, sich seitwärts im Netzwerk fortzubewegen, um weitere Geräte zu infizieren, oder sich an einem Angriff zu beteiligen. Diese Call-Home-Versuche sind eine ideale Gelegenheit, infizierte Systeme in Ihrem Netzwerk zu erkennen, die in ein Botnet eingebunden sind. Um diese Erkennung jedoch effektiv zu gestalten, ist die richtige Technologie erforderlich.

Abgesehen von der Call-Home-Kommunikation kann es sehr schwer sein, Bots in Ihrem Netzwerk zu erkennen. In den meisten Fällen läuft das Gerät ganz normal weiter. Eventuell wird die Performance leicht beeinträchtigt, was aber auch an vielen anderen Faktoren liegen kann und deshalb nicht verdächtig erscheint.

Wenn ein Bot in Ihrem Netzwerk aufgefordert wird, sich an einem Angriff zu beteiligen, kommuniziert er in der Regel mit dem C&C-Server, um Anweisungen entgegenzunehmen (z. B. welches Ziel mit welcher Attacke angegriffen wird). Dies ist eine weitere ideale Gelegenheit, Botnet-Hosts in Ihrem Netzwerk zu identifizieren. Sobald ein Angriff jedoch im Gange ist, kann der Angriff selbst sehr schwer zu erkennen sein. Von der Perspektive des Netzwerkverkehrs betrachtet, sendet das Gerät lediglich E-Mails (Spam), überträgt Daten (Datendiebstahl oder Bitcoin-Mining) oder DNS-Lookups bzw. führt diverse andere alltägliche Traffic-Anfragen aus (bei DDoS-Anfragen). Keine dieser Aktivitäten ist für sich genommen besonders erwähnenswert oder alarmierend. Und genau das ist für ein Botnet charakteristisch: Ein Bot allein ist für sich genommen relativ harmlos. Es ist die Koordination großer Mengen von Botnet-Geräten,

die alle gleichzeitig dasselbe Ziel angreifen, was den Angriff so verheerend macht.

Ein weiterer beunruhigender Aspekt von Botnets ist die Tatsache, dass sie mittlerweile im Dark Web günstig zum Kauf oder zur Miete angeboten werden – nicht selten mit technischem Rund-um-die-Uhr-Support. So wird eine neue Generation unqualifizierter Cyberkrimineller herangezogen, die zu einem Bruchteil eines Bitcoins und mit wenig oder keiner Erfahrung Botnet-Angriffe starten können.

Standort	Preis
Botnet – Kanada	270 $ für 1.000 Computer
Botnet – Frankreich	200 $ für 1.000 Computer
Botnet – Russland	200 $ für 1.000 Computer
Botnet – Vereinigtes Königreich	240 $ für 1.000 Computer
Botnet – Vereinigte Staaten	180 $ für 1.000 Computer
Botnet – weltweit	35 $ für 1.000 Computer

Quelle: http://www.havocscope.com/black-market-prices/hackers/

Die Auswirkungen von Botnets

Botnets stellen nicht nur eine massive Gefahr für das Internet als Ganzes dar, wie wir erst kürzlich bei einer Reihe von extrem schädlichen DDoS-Angriffen beobachten konnten. Botnets können auch verheerende Folgen für Ihr Unternehmen haben, insbesondere wenn sensible Daten gestohlen werden. Denken Sie daran, welchen Schaden ein Botnet beim US-Einzelhändler Target im Jahr 2013 angerichtet hat: Über Monate hinweg wurden von Kassensystemen mehrere Millionen Kreditkartendaten abgeschöpft. Und selbst wenn das in Ihrem Netzwerk operierende Botnet es nicht auf Ihre Daten abgesehen hat, könnte es Ihre Geräte und Netzwerkressourcen für kriminelle Zwecke nutzen und in einem anderen Unternehmen massiven Schaden anrichten – vielleicht in einem Unternehmen, das Ihr Geschäftspartner ist. Sie dürfen also nicht zulassen, dass Ihr Netzwerk in einen Botnet-Angriff involviert wird.

Wie Sie Ihr Unternehmen schützen können

Für den effektiven Schutz vor Botnets spielt Ihre Netzwerk-Firewall eine Schlüsselrolle. Damit Sie bestmöglichen Schutz erhalten, achten Sie bei der Wahl einer Next-Gen-Firewall unbedingt auf die folgenden Komponenten:

- **Advanced Threat Protection:** Advanced Threat Protection kann Botnets identifizieren, die bereits in Ihrem Netzwerk aktiv sind. Stellen Sie sicher, dass Ihre Firewall über Malicious Traffic Detection, Botnet Detection und Command and Control (C&C) Call-Home Traffic Detection verfügt. Die Firewall sollte ein mehrschichtiges Konzept nutzen, das IPS, DNS und Web kombiniert, um Call-Home-Datenverkehr zu erkennen und nicht nur den infizierten Host, sondern auch den Benutzer und Prozess sofort zu identifizieren. Im Idealfall sollte die Firewall das infizierte System auch blockieren oder isolieren, bis es überprüft werden kann.
- **Intrusion Prevention:** IPS kann Hacker erkennen, die versuchen, Ihre Netzwerkressourcen zu veruntreuen. Stellen Sie sicher, dass Ihre Firewall über ein Next-Gen Intrusion Prevention System (IPS) verfügt, das in der Lage ist, komplexe Angriffsmuster in Ihrem Netzwerkverkehr zu identifizieren. So können Sie Hacking-Versuche und Malware, die sich seitwärts über Netzwerksegmente fortbewegt,

erkennen. Ziehen Sie außerdem in Betracht, ganze Geo-IP-Bereiche für Regionen zu blockieren, in denen Ihr Unternehmen nicht tätig ist. So können Sie Ihre Angriffsfläche weiter verringern.

- **Sandboxing:** Sandboxing kann selbst neueste evasive Malware stoppen, bevor diese auf Ihre Computer gelangt. Stellen Sie sicher, dass Ihre Firewall über eine leistungsstarke Sandboxing-Funktion verfügt, die verdächtige Web- oder E-Mail-Dateien identifizieren und diese in einer sicheren Sandbox-Umgebung ausführen kann. So können Sie das Verhalten von Dateien analysieren, bevor sie Zugriff auf Ihr Netzwerk erhalten.
- **Web und Email Protection:** Effektive Web und Email Protection können bereits im Vorfeld verhindern, dass Botnet-Malware überhaupt in Ihr Netzwerk gelangt. Stellen Sie sicher, dass Ihre Firewall über eine verhaltensbasierte Web Protection verfügt. Diese sollte in der Lage sein, JavaScript-Code in Web-Inhalten zu emulieren bzw. zu simulieren, um festzustellen, welche Absichten und Verhaltensweisen vorliegen, bevor die Inhalte an den Browser übermittelt werden. Sorgen Sie außerdem dafür, dass Ihre Firewall oder E-Mail-Filter-Lösung über leistungsstarke Anti-Spam- und Antivirus-Technologien verfügt, damit Sie neueste Malware in E-Mail-Anhängen erkennen können.
- **Web Application Firewall:** Eine WAF kann Ihre Server, Geräte und Geschäftsanwendungen vor Hacks schützen. Stellen Sie sicher, dass Ihre Firewall WAF-Schutz für alle Systeme in Ihrem Netzwerk bereitstellt, die Remote-Zugang vom Internet benötigen. Eine Web Application Firewall bietet einen Reverseproxy und Offload-Authentifizierung und härtet die Systeme außerdem gegen Hacking-Versuche.

Best Practices, die Sie berücksichtigen sollten (sowohl für Ihr Unternehmen als auch zu Hause):

- Ändern Sie die Standard-Passwörter für alle Netzwerkgeräte immer sofort in individuelle komplexe Passwörter und nutzen Sie bei Bedarf einen Passwort-Manager.
- Beschränken Sie den Einsatz von IoT-Geräten auf das Notwendigste und halten Sie die unverzichtbaren Geräte immer auf dem aktuellen Stand. Trennen Sie die Verbindung aller nicht notwendigen Geräte, ersetzen Sie ältere Geräte durch neuere und sicherere Modelle und halten Sie alle Geräte mit den aktuellen Firmware-Updates auf dem neuesten Stand.
- Vermeiden Sie IoT-Geräte, bei denen für Remote-Zugriff Ports auf Ihrer Firewall oder Ihrem Router geöffnet werden müssen. Verwenden Sie stattdessen cloudbasierte Geräte, die sich nur mit den Servern des Cloud-Anbieters verbinden, und bieten Sie keinen direkten Remote-Zugriff an.
- Aktivieren Sie auf Ihrer Firewall oder Ihrem Router kein UPnP. Dieses Protokoll erlaubt Geräten, bei Bedarf ohne Ihr Wissen Ports auf Ihrer Firewall zu öffnen, wodurch sich Ihre Angriffsfläche vergrößert.
- Nutzen Sie sichere VPN-Technolgien, um Geräte remote zu verwalten.

Der Sophos-Vorteil

Mit der Sophos XG Firewall erhalten Sie alle modernen Technologien, die Sie benötigen, um Ihr Netzwerk vor Botnets, Angriffen und Bedrohungen zu schützen. Sie erhalten Advanced Threat Protection,

IPS, Sandboxing, Web und Email Protection sowie eine Web Application Firewall in einer einzigen leistungsstarken Network Protection Appliance, die sich einfach einrichten und verwalten lässt.

Die Sophos XG Firewall unterstützt auch eine ganze Reihe von VPN-Technologien für sicheren Remote-Zugriff, z. B. unsere einmalige Remote Ethernet Device (RED) Technologie, mit der Sie Ihr Netzwerk virtuell auf ein Remote-Gerät oder eine Außenstelle ausweiten können.

Die Sophos XG Firewall ist außerdem die erste Firewall mit Synchronized Security und Sophos Security Heartbeat™. Diese innovativen Technologien definieren die Abwehr und Beseitigung hochentwickelter Bedrohungen komplett neu. Auf diese Weise können Sie potenzielle Bots in Ihrem Netzwerk sofort identifizieren und bis zur Bereinigung automatisch isolieren.

Bei Sophos erhalten Sie alle Funktionen, die Sie benötigen, sowie Funktionen, die Sie bei anderen Anbietern vergeblich suchen – in einer blitzschnellen Appliance mit einfacher Verwaltung.

Sophos kann Sie auch zu Hause schützen

Die Sophos XG Firewall Home Edition und Sophos Home für Macs und PCs bieten Schutz nach Unternehmens-Standards für Ihr Netzwerk zu Hause – komplett kostenlos. Sie erhalten denselben bewährten Schutz, der weltweit Millionen von Unternehmenscomputern und -netzwerken schützt – kostenlos für den nicht-kommerziellen Privatgebrauch.

Testen Sie die Sophos XG Firewall kostenlos www.sophos.de/xgfirewall

Sales DACH (Deutschland, Österreich, Schweiz):
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

11.10.2016 WP-DE (NP)

SOPHOS