Botnets

Machen Sie sich mitschuldig?

Jemand versucht, das Internet zu zerstören.

Seit einigen Monaten flammen DDoS- (Distributed Denial of service) Angriffe wieder auf. Es ist äußerst wahrscheinlich, dass gerade irgendjemand (vielleicht eine staatliche Organisation) dabei ist, die Grenzen des Internets testen.

Diese Angriffe benutzen Tausende von Computern oder vernetzte Geräte, die vom Angreifer kontrolliert werden, um zum gleichen Zeitpunkt Anfragen an ein einziges Ziel zu senden. Diese außergewöhnliche Belastung des Internetverkehrs kann die Verfügbarkeit des betreffenden Ziels erheblich reduzieren, so dass dieses nicht mehr richtig auf legitime Anfragen (z.B. den Aufruf einer Webseite) reagieren kann. In einem solchen Fall können die Kunden des Online-Services oder der Website, denen der Angriff galt, den Dienst nicht mehr normal nutzen. Im schlimmsten Fall sind die Server des Ziels völlig überlastet und reagieren nicht mehr. Der Dienst wird dann vollständig unterbrochen.

Eins der letzten Opfer in der jüngsten Vergangenheit war OVH, einer der größten Hosting-Anbieter in Europa. OVH war einem Denial-of-Service-Angriff mit einer Datenrate von mehr als ein Terrabyte pro Sekunde ausgesetzt. Nach Aussagen des Unternehmens ist der Angriff auf ein Botnet zurückzuführen, das aus 145.607 offenbar ungeschützten IP-Überwachungskameras bestand. Das Botnetz war damit in der Lage, einen DDoS-Angriff mit einer Datenrate von über 1,5 Terrabyte pro Sekunde zu starten. Der Angriff hat zwar nicht zum Zusammenbruch der Server der Firma OVH geführt, jedoch zu einigen Verzögerungen. Wäre eine kleinere Struktur das Ziel gewesen, die Folgen wären zweifellos viel ernster gewesen. Laut Sicherheitsforscher Mustafa Al-Bassam war dies der heftigste registrierte DDoS-Angriff in der Geschichte des Internets.

Dies war nicht der erste Denial-of-Service-Angriff, der auf vernetzten Kameras beruht. Im Juni 2016 hatte die Gesellschaft Sucuri ein Botnet von 25.000 vernetzten Kameras entdeckt.

Wie entwickeln sich Botnets?

Um ein Botnet zu betreiben, brauchen Hacker die Kontrolle über viele Geräte mit Internet-Anschluss. Diese Geräte können zwei "Herren" zugleich dienen: Für ihre Besitzer arbeiten sie wie gewohnt, während sie im Hintergrund Websites auf Befehl eines Cyber-Kriminellen attackieren, ohne dass der Besitzer dies merken würde.

Vor kurzem wurde eine „Mirai“ genannte Schadsoftware (Malware) verbreitet. Dies ist ein Tool, mit dem Hacker ihre Botnets leichter erstellen können. Mirai sucht nach mit dem Internet verbundenen Geräten und probiert bekannte Standardpasswörter aus, um Zugriff zu erlangen. In der Regel ändern Menschen die Standardeinstellungen ihrer Geräte nicht, vor allem die voreingestellten Passwörter werden oft nicht geändert, was es sehr leicht macht, diese Geräte zu übernehmen und sie in dieZombie-Armeen (Botnet) der Hacker zu rekrutieren.

Angriffe wie jene der letzten Monate werden sich in Zukunft wahrscheinlich häufiger werden, da die Anzahl der vernetzten Geräte zunimmt, und im Internet verfügbare Tools die Ausnutzung ihrer Schwachstellen erleichtern.

Wer ist dafür verantwortlich?

Überwachungskameras, kabellose Drucker, smarte Uhren oder Armbänder, Fernsehgeräte, Spielzeug, Spielkonsolen, Haushaltsgeräte, die mit dem Internet verbunden sind ... die Liste ist beliebig fortführbar. All diese Geräte haben eins gemeinsam: Sie sind meist permanent mit dem Internet verbunden und haben zahlreiche Schwachstellen.

Hier sind die Wichtigsten:

- die Betriebssysteme der vernetzten Objekte haben oft Sicherheitslücken;
- das Internet ist die kostengünstigste und einfachste Lösung für die Verbindung von Objekten mit ihren „Steuerungsstellen". Die verwendeten Protokolle sind nicht immer sicher (z.B. veraltete SSL / TLS Versionen mit bekannten Sicherheitslücken);
- Hersteller vernetzter Geräte wollen ihre Produktentwicklungszeit möglichst minimieren, um vor ihren Konkurrenten auf den Markt zu kommen. Der Fokus liegt auf Ergonomie und Design, und die Sicherheit wird dabei oft ausgeblendet
- der 24/7 Online-Modus macht es sehr kompliziert, Updates zu machen und Schwachstellen zu beheben.

Aus all diesen Gründen sind vernetzte Geräte leichter zu finden als z.B. Geräte, die in einem besser gesicherten Firmennetzwerk installierte sind. Ddiese sindtrotz ihres deutlich höheren Schutzniveaus auch nicht immun gegen Angriffe. Die Moral dieser Geschichte ist, dass wir alle betroffen bzw. potenziell ohne unser Wissen „Komplizen" sind. Die Armee von Botnets besteht bereits aus Millionen von kleinen unsichtbaren „Soldaten", die bereit stehen, in Aktion zu treten. Was muss passieren, um nicht noch Neue entstehen zu lassen?

Was können wir tun?

Ein Einzelner kann nicht verhindern, dass Botnets das Internet zum Absturz bringen. Wenn wir uns jedoch alledes Problems bewusst sind und versuchen, Vorsichtsmaßnahmen zu ergreifen, kann die Anzahl der korrumpierten vernetzten Geräte aufhören, weiter anzusteigen bzw. sich sogar verringern. Jede kann seine Geräte besser schützen, so dass Mirai und ähnliche Malware nicht die Kontrolle über sie gewinnen können. Wenn jeder dies täte, würden die Botnet-Armeen erheblich reduziert werden.

1. Um zu verhindern, dass Ihr Drucker, Router oder vernetztes Gerät von Botnets verwendet werden, können Sie ein paar einfache Vorsichtsmaßnahmen treffen:
2. Ändern Sie Ihre Standard-Passwörter für alle Ihre Geräte. Verwenden Sie zuverlässige Kombinationen, die nicht ohne weiteres geknackt werden können.
3. Aktualisieren Sie Ihre Firmware für alle Geräte (vor allem ältere), wenn möglich.
4. Seien Sie bei der Auswahl eines vernetzten Objektes selektiv. Fragen Sie sich, ob es wirklich eine Internetverbindung benötigt! Wenn dies der Fall ist, beschäftigen Sie sich sorgfältig mit seinen Eigenschaften und seiner Funktionsweise. Dazu können Sie z.B. Rezensionen von Kunden im Netz lesen. Wenn Sie feststellen, dass es schwierig zu änderende Passwörter gibt, dann wählen Sie ein anderes Modell.
5. Vor allem fragen Sie sich, ob Ihre Geräte ständig an das Internet angeschlossen sein müssen. Die dauerhafte Verbindung scheint einen zusätzlichen Komfort zu bieten, kann sich aber auch gegen seine „Nutznießer" wenden. Zum Beispiel könnten ihre Überwachungskameras beginnen, Sie auszuspionieren, wenn ein Angreifer deren Kontrolle übernimmt …
6. Vernetzte Haushaltsgegenstände laufen in der Regel über einen WLAN-Router, um sich mit dem Internet zu verbinden. Je nach Router-Modell ist es möglich sein, zu kontrollieren, auf welche Art und Weise sich die Objekte mit dem Internet verbinden bzw. zu verhindern, dass sich Objekte automatisch ohne vorherige Genehmigung verbinden.

Der Kampf gegen Botnets und Denial-of-Service-Angriffe muss gemeinsam von allen Marktteilnehmern, einschließlich der Nutzer im Bereich der vernetzten Geräte durchgeführt werden. Aber auch die Hersteller müssen die Verantwortung übernehmen, indem sie das Sicherheitsniveau der vernetzten Objekte erhöhen, die sie auf den Markt bringen. Ansonsten wird eines Tages jemand wirklich das Internet „kaputt machen".

Bei Fragen bezüglich des Internetbetrugs
oder der Nutzung des Internet im Allgemeinen,
wenden Sie sich bitte an die BEE SECURE Helpline:

BEE SECURE HELPLINE
BERATUNG & HILFE
8002-1234

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxemburg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.luwww.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union
Connecting Europe Facility