Schnelle Exploit-to-Market Strategie für IoT Geräte

By By: Feike Hacquebord, Fernando Mercês Nov 26, 2024 Read time: 6 min (1582 words)

Published: 2024-11-26 · Archived: 2026-04-05 13:50:16 UTC

Soweit uns bekannt ist, hat Water Barghest neben der Beschaffung von IoT-Exploits jeden Schritt zwischen dem Auffinden anfälliger IoT-Geräte und deren Verkauf auf einem Proxy-Marktplatz automatisiert. Alles beginnt jedoch mit der Beschaffung von Schwachstellen in IoT-Geräten: Oftmals handelt es sich dabei um n-Days, aber in mindestens einem Fall hat die Gruppe einen Zero-Day genutzt. Mit einer Liste von Schwachstellen an der Hand nutzt der Akteur Suchanfragen in einer öffentlich zugänglichen Internet-Scan-Datenbank wie Shodan, um anfällige Geräte und ihre IP-Adressen zu finden.

Danach wird eine Reihe von IP-Adressen von Rechenzentren mit einer oft langen Lebensdauer eingesetzt, um die Exploits an potenziell gefährdeten IoT-Geräten auszuprobieren. Wenn ein Exploit erfolgreich ist, laden die kompromittierten IoT-Geräte ein Skript herunter, das Ngioweb-Malware-Samples durchgeht, die für verschiedene Linux-Architekturen kompiliert wurden. Wenn eines der Samples problemlos läuft, wird die Malware Ngioweb im Speicher des IoT-Geräts des Opfers ausgeführt.

Damit ist die Infektion nicht persistent, ein Neustart würde sie entfernen. Wenn Ngioweb ausgeführt wird, registriert es sich bei einem Command-and-Control-Server (C&C) und erhält häufig innerhalb weniger Minuten die Anweisung, eine Verbindung zu einem der 150 Zugangspunkte des privaten Proxy-Anbieters herzustellen. Es folgen ein Geschwindigkeitstest und ein Test des Name Servers. Die Informationen werden an den Marktplatz gesendet und dort aufgelistet. Die gesamte Prozedur von der ersten Infektion bis zur Bereitstellung des Bots als Proxy auf dem Marktplatz kann nicht länger als 10 Minuten dauern. Dies zeigt einmal mehr die Professionalität und Reife dieses Bedrohungsakteurs, der bereits seit mehr als fünf Jahren aktiv ist.

Derzeit setzt Water Barghest etwa 17 Mitarbeiter auf virtuellen privaten Servern (VPS) ein, die kontinuierlich Router und IoT-Geräte auf bekannte Schwachstellen überprüfen. Sie laden auch Ngioweb-Malware auf frisch kompromittierte IoT-Geräte hoch. Water Barghest arbeitet wahrscheinlich schon seit Jahren auf diese Weise, wobei sich die IP-Adressen der Arbeiter im Laufe der Zeit langsam ändern. Auf diese Weise konnte Water Barghest über Jahre hinweg ein regelmäßiges Einkommen erzielen.

Entwicklung der Ngioweb-Malware

2018: Ramnit-betriebenes Windows-Botnet

Der Ngioweb-Malware-Stamm geht auf das Jahr 2018 zurück, als Check Point Research aufdeckte, dass er durch einen Ramnit-Trojaner verbreitet wurde. Damals zielte Ngioweb auf Computer mit Microsoft Windows ab. Die Malware war bereits darauf ausgelegt, einen infizierten Computer in einen bösartigen Proxy Server zu verwandeln. Einige Samples reichen sogar bis 2017 zurück, aber die C&C-Domain, die der Malware ihren Namen gibt, wurde 2018 registriert.

2019: WordPress Server-Botnet

2019 entdeckten Netlab-Forscher die Linux-Variante von Ngioweb. Die Malware funktionierte ähnlich wie ihre frühere Windows-Version, hatte aber zusätzliche Funktionen für den Domain Generation Algorithm (DGA). Laut Netlab bestand das Botnet hauptsächlich aus Webservern, auf denen WordPress installiert war, was darauf hindeutet, dass der Bedrohungsakteur eine WordPress-Schwachstelle - oder ein WordPress-Plugin - ausnutzen könnte.

2020: IoT-Geräte-Botnet

2020 wendete sich Water Barghest IoT-Geräten zu. Wir fanden Ngioweb-Samples, die für viele verschiedene Architekturen kompiliert wurden. Außerdem veröffentlichte Netlab einen Blogeintrag und Intezer einen Beitrag auf X über ein aktives Ngioweb-Botnet. Laut Netlab nutzte der Angreifer neun verschiedene n-Day-Schwachstellen in IoT-Geräten aus, darunter NAS-Geräte von QNAP und Netgear, aber auch Geräte von D-Link und anderen.

2024: Erweitertes Zielspektrum

2024 erreichte das von Water Barghest geschaffene IoT-Botnet die volle Potenz. Die Prozesse, die wir in einer Reihe von EdgeRouter-Geräten fanden, entpuppten sich als eine neue Version von Ngioweb. Sie funktioniert sehr ähnlich wie ihre Vorgängerversionen.

Einzelheiten zum Ablauf liefert der Originalbeitrag.

Marktplatz für Proxy-Server

Unserer Einschätzung nach gehört ein erheblicher Teil der Exit Nodes, die ein bestimmter Marktplatz für Proxy-Server zur Miete anbietet, zu Geräten, die mit Ngioweb-Malware infiziert sind. In einigen Fällen konnten wir nachweisen, dass eine frische Ngioweb-Infektion dazu führte, dass die entsprechende IP-Adresse innerhalb weniger Minuten nach der Erstinfektion auf der Website des Marktplatzes angeboten wurde. Der Anbieter von Proxy-Servern für Privatanwender akzeptiert nur Zahlungen in Kryptowährung.

Ausblick und Schlussfolgerungen

Seit Jahren gab es mittelgroße Proxy-Botnets, ohne dass sie gestoppt oder öffentlich gemacht wurden. Beispiele hierfür sind die Botnets, die wir mit den Water Barghest- und Water Zmeu Intrusion-Sets in Verbindung bringen. Die Gruppen hinter diesen Intrusion-Sets haben ihren Betrieb im Laufe der Jahre verfeinert und ihre Abläufe in hohem Maße automatisiert.

APT-Akteure nutzten ihre dedizierten IoT-Botnets manchmal jahrelang, bevor sie vom FBI und seinen Partnern außer Gefecht gesetzt wurden. APT-Akteure und finanziell motivierte Akteure werden weiterhin ein Interesse daran haben, ihre eigenen IoT-Botnets für Anonymisierungszwecke und Spionage aufzubauen werden auch weiterhin Botnets von Drittanbietern oder kommerziell erhältliche Proxy-Dienste heranziehen.

Wir gehen davon aus, dass sowohl der kommerzielle Markt für Proxy-Dienste als auch der Untergrundmarkt für Proxys in den kommenden Jahren wachsen werden, da die Nachfrage hoch ist. Der Schutz vor diesen Anonymisierungsschichten stellt für viele Unternehmen und Regierungsorganisationen auf der ganzen Welt eine

Herausforderung dar. Gerichtlich genehmigte Schließungen von Proxy-Botnets werden zwar dazu beitragen, böswillige Aktivitäten einzudämmen, aber die Sicherung von IoT-Geräten ist dennoch von größter Bedeutung.

Wenn ein IoT-Gerät ankommende Verbindungen über das offene Internet akzeptiert, werden diese Devices von kommerziellen Scandiensten schnell online gefunden, und auch böswillige Akteure können sie über gekaufte oder gestohlene Zugänge zu diesen Internet-Scandiensten finden. Mithilfe von Scandaten können die automatisierten Skripte von böswilligen Akteuren bekannte Schwachstellen und möglicherweise sogar Zero-Day-Angriffe auf die exponierten IoT-Geräte leicht ausprobieren. Daher ist es wichtig, für IoT-Geräte eingehende Internetverbindungen zu unterbinden, wenn dies nicht geschäftskritisch ist, und Maßnahmen zu ergreifen, um zu verhindern, dass ihre Infrastruktur selbst Teil des Problems wird.
