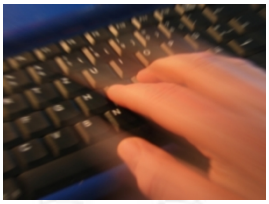


Neue InterPlanetary Storm Malware-Variante zielt auf IoT-Geräte - Infizierte Geräte öffnen Hintertür für Cryptomining, DDoS und andere großangelegte Angriffe

Die cyberkriminelle Organisation hinter der Malware InterPlanetary Storm hat eine neue Variante veröffentlicht, die neben Windows- und Linux-Rechnern nun auch Mac- und Android-Geräte ins Visier nimmt. Die Malware baut ein Botnetz auf, das derzeit etwa 13.500 infizierte Computer in 84 verschiedenen Ländern der Welt umfasst, und diese Zahl wächst weiter.
Die erste Variante von InterPlanetary Storm, die auf Windows-Rechner abzielte, wurde im Mai 2019 aufgedeckt, und im Juni dieses Jahres wurde über eine Variante berichtet, die in der Lage ist, Linux-Rechner anzugreifen. Die neue Variante, die Barracuda-Forscher erstmals Ende August entdeckten, zielt auf IoT-Geräte wie beispielsweise Fernseher, die auf Android-Betriebssystemen laufen, sowie auf Linux-basierte Maschinen wie Router mit schlecht konfiguriertem SSH-Dienst. Das Botnetz, das diese Malware aufbaut, verfügt zwar noch über keine klare Funktionalität, aber bietet den Betreibern der Kampagne eine Hintertür in die infizierten Geräte, sodass diese später für Cryptomining, DDoS oder andere groß angelegte Angriffe missbraucht werden können.

Die Mehrzahl der von der Malware infizierten Rechner befindet sich derzeit in Asien.

- 59% der infizierten Computer befinden sich in Hongkong, Südkorea und Taiwan.
- 8% in Russland und der Ukraine
- 6% in Brasilien
- 5% in den Vereinigten Staaten und Kanada
- 3% in Schweden
- 3% in China
- Alle anderen Länder verzeichnen 1% oder weniger (Deutschland aktuell 0,5%)

Funktionsweise der neuen InterPlanetary Storm-Malware

Die neue Variante der InterPlanetary Storm-Malware verschafft sich Zugang zu Rechnern, indem sie einen Wörterbuch-Angriff auf SSH-Server ausführt, ähnlich wie FritzFrog, eine weitere Peer-to-Peer-(P2P)-Malware. Sie kann sich auch durch den Zugriff auf offene ADB-Server (Android Debug Bridge) Zugang verschaffen. Die Malware erkennt die CPU-Architektur und das Betriebssystem ihrer Opfer, und sie kann auf ARM-basierten Rechnern ausgeführt werden, eine Architektur, die bei Routern und anderen IoT-Geräten recht häufig anzutreffen ist. Die Malware wird als InterPlanetary Storm bezeichnet, da sie das IPFS (InterPlanetary File System)-p2p-Netzwerk und die zugrunde liegende libp2p-Implementierung verwendet. Dadurch können infizierte Knoten direkt oder über andere Knoten (bspw. Relays) miteinander kommunizieren.

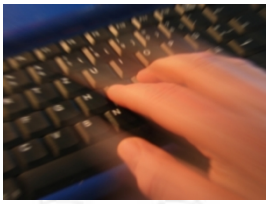
Spezielle Eigenschaften der neuen Variante

Diese Variante von InterPlanetary Storm ist in Go geschrieben, verwendet die Go-Implementierung von libp2p und ist mit UPX gepackt. Sie verbreitet sich unter Verwendung von SSH-Brute-Force und offenen ADB-Ports und stellt Malware-Dateien für andere Knoten im Netzwerk bereit. Die Malware ermöglicht auch Reverse Shell und kann Bash Shell ausführen. Die neue Variante verfügt über mehrere einzigartige Funktionen, die dazu beitragen sollen, dass die Malware persistent bleibt und geschützt wird, nachdem sie einen Rechner infiziert hat:

- Sie erkennt Honeypots. Die Malware sucht nach der Zeichenfolge "svr04" im Standard-Shell-Prompt (PS1), die zuvor vom Cowrie Honeypot verwendet wurde.
- Sie aktualisiert sich automatisch. Die Malware vergleicht die Version der laufenden Instanz mit der neuesten verfügbaren Version und aktualisiert sich entsprechend.
- Sie versucht, persistent zu bleiben, indem sie einen Dienst (system/systemv) installiert, unter Verwendung eines Go Daemon Package.
- Sie stoppt andere Prozesse auf dem Rechner, die eine Bedrohung für die Malware darstellen, wie zum Beispiel Debugger und konkurrierende Malware.

Maßnahmen zum Schutz vor neuer InterPlanetary Storm-Variante

- Ordnungsgemäße Konfigurierung des SSH-Zugriffs auf allen Geräten: Dies bedeutet, dass Schlüssel anstelle von Passwörtern verwendet werden, was den Zugriff sicherer macht. Wenn die Passwort-Anmeldung aktiviert ist und der Dienst selbst zugänglich ist, kann die Malware die schlecht konfigurierte Angriffsfläche ausnutzen. Dies ist ein Problem,



das bei Routern und IoT-Geräten häufig auftritt, sodass sie leichte Ziele für diese Malware darstellen.

• Verwendung eines Cloud Security Posture Management Tools zur Überwachung der SSH-Zugriffskontrolle, um jegliche Konfigurationsfehler zu vermeiden, die schwere Folgen haben können. Bei Bedarf sollte ein gesicherter Zugriff auf Shells bereitgestellt werden; anstatt die Ressource im Internet Bedrohungen auszusetzen, sollte eine MFA-fähige VPN-Verbindung bereitgestellt und die Netzwerke für die spezifischen Anforderungen segmentiert werden, statt den Zugriff auf breite IP-Netzwerke zu gewähren.