UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00106

MATRYOSH BOTNET USES ANDROID FOR DDOS

DATE ISSUED: 15th February 2021

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Using the Andoid Debug Bridge, a new botnet called Matryosh – after the nesting Russian dolls, is using the Mirai Malware Framework and hiding it's activity using Tor to target Android devices to launch Distributed Denial of Services (DDoS) attacks.

BREAKDOWN

The Matryosh botnet – named so for it's many nested and layered functions is being propagated through the Android Debug Bridge (ADB) interface command line utility that is included in the Software Development Kit provided by Google for Android. By using the Tor network, the botnet is able to hide its malicious activities and prevent it's servers from being located and taken down. Further measures to protect the Command-and-Control (C2) centre are undertaken at the communication level to create obstacles for those attempting to perform static analysis or perform IOC simulations. Because the ADB is completely unauthenticated and listening on port 5555, anyone is able to connect to an affected device while it is online and access the device as a root user. These administrative privileges mean arbitrary code and malicious commands may be issued by anyone connected to any device running Android OS, including IoT devices such as SmartTVs. Detections by anti-malware software have shown the botnet is using the Mirai malware framework that has a history of mass DDoS attacks, and adapted this with a number of novel alterations and functions.

REMEDIATION STEPS

- Use ant-malware detection and remediation software on any android devices where possible.
- Ensure default security settings such as passwords are changed.
- Monitor network activity for any suspicious or anomalous behaviour.
- Block traffic to port 5555 where possible.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/android-devices-prone-to-botnets-ddos-onslaught/163680/
Threatwatch:	https://www.binarydefense.com/threat_watch/matryosh-botnet-spreading-through-android-devices/
ZDNet:	https://www.zdnet.com/article/android-devices-ensnared-in-ddos-botnet/