UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00049

NEW HEH BOTNET INFECTING ALL ENDPOINT TYPES

DATE ISSUED: 12th October 2020

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

OVERVIEW

Using Telnet on ports 23/2323, the newly discovered HEH Botnet is distributing Peer to Peer (P2P) malware, by using brute-force techniques and wiping infected systems of all data.

BREAKDOWN

360Netlab have discovered through capturing samples of the bot that this particularly nasty code can infect a vast range of CPU architecture including x86, ARM, MIPS and PPC which corresponds to desktop and laptop PCs, mobile and Internet of Things (IoT) devices. By brute force entry using Telnet credentials, the malware infects the target with a 'Go' language (Golang for short) based binary that is able to communicate with other infected nodes using a peer-to-peer proprietary protocol. The malicious shell script propagation module is named wpqnbt.txt and is executed after breach and retrieves programs from the compromised pomf.cat site, which contains a vast range of versions to suit the targeted victim. Once it determines the CPU architecture, it will initiate an HTTP server using the local port 80/0 to 80/9, giving a total of 10 URLs which contain various versions and languages of the Universal Declaration of Human Rights, after which the sample overlays the P2P module to the port and overwrites the declaration. Communication to its peers and command and control centre can now begin via a UDP service port and discover further peers to infect. The commands in the Bot Cmd list contain a wiper function known as "Self Destruct" which will wipe all data from its host on execution of the code. Although this Botnet may be still in its infancy, it's destructive nature makes it a grave concern

REMEDIATION STEPS

- Disable system access to port 23/2323
- Increase access control via port 23/2323 by removing all surplus accounts and increasing administration account password complexity.
- Convert P2P networks to a centralised topology where possible.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/heh-p2p-botnet-wiper-function/159974/
NetLab360	https://blog.netlab.360.com/heh-an-iot-p2p-botnet/