UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00062

GITPASTE-12 WORM TARGETS LINUX SERVERS & IOT

DATE ISSUED: 10th November 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Using the popular GitHub and Pastebin, attackers are housing component code that houses 12 different attack modules. This new worm targets Linux-based x86 servers and Internet of Things (IoT) or "Smart" devices that are based in ARM and MIPS Central Processing Units (CPUs).

BREAKDOWN

Juniper Threat Labs discovered the worm dubbed "Gitpaste-12" in mid-October. The initial phase of the attack is to compromise a system by exploiting 11 known vulnerabilities that affect Apache Struts (CVE-2017-5638), Asus routers (CVE-2013-5948) the Webadmin plugin for opendreambox (CVE-2017-14135 and Tendra routers (CVE-2020-10987). There is also the possibility of attempted brute-forcing of passwords followed by the upload of the main shell script to the targeted machine which will download and run the malware. A cron job is established to execute every minute, presumably to push updates to a botnet command and control server and the download and execution of a script ensues from "https://raw[.]githubusercontent[.]com/cnmnmsl-001/-/master/shadu1". This script is able to disable many security features such as firewalls, selinux, apparmor and monitoring softwares as well as cloud security agents which leads researchers to believe an intended target is likely to be cloud infrastructure. There is also a cryptomining module for Monero cryptocurrency. The malware intercepts readdir system calls preventing administrators from gaining information about running processes in the environment. A library is also contained and loaded by the malware allowing execution of further malicious code from a Pastebin repository. To self-propogate, the worm can select a random /8 CIDR group and performs a scan to locate any machines in the address range to infiltrate. Alternatively, it will use ports 30004 (TCP) and 30005 (SOAP/HTTP-based protocol) to communicate with network switches, routers and auto-configuration servers.

REMEDIATION STEPS

- Ensure all security and patching is up to date on all devices
- Ensure network monitoring and analysis is conducted regularly to detect any abnormal outbound and inbound network traffic
- Use appropriate endpoint and network protection and detection methods to isolate malicious activity and applications

REFERENCES & RESOURCES

Threatpost https://threatpost.com/gitpaste-12-worm-linux-servers-iot-devices/161016/