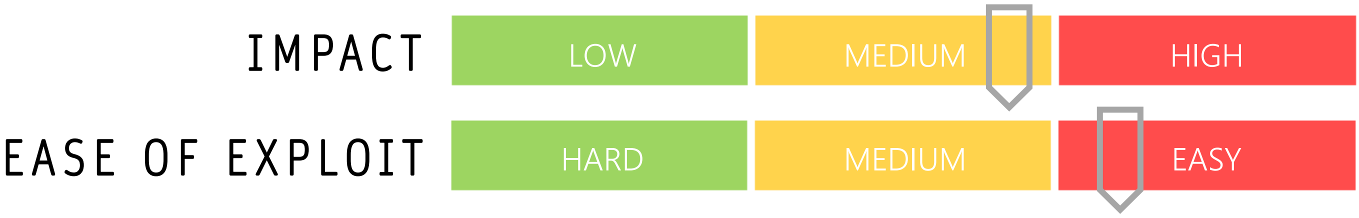
UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00047

INTERPLANETARY STORM HITS COMMON OS

DATE ISSUED: 5th October 2020



OVERVIEW

A growing botnet built by the InterPlanetary Storm malware now contains over 13,500 infected machines across 84 countries. The purpose of this botnet is presently unknown, but the potential for large scale attack is worrying, as new variants mean that Windows, Linux, Mac and Android devices are all now possible targets.

BREAKDOWN

While previous versions of the InterPlanetary Storm malware were targeting Windows and Linux machines, a new strain has emerged that is able to infect Android and Mac devices as well as those utilising ARM-base architecture. The malware allows an attacker to install bot software on the machine without the user's knowledge and creates a back door for attackers to gain access through the system. The potential uses for this growing botnet could include cryptomining operations or be used to launch DDoS attacks as speculated by Barracuda. This infection has not only been reported on personal computing devices, but also other smart of Internet of Things (IoT) devices such as TVs running Android systems or routers which use Linux as their base OS. The malware uses peer to peer networking in the InterPlanetary File System to spread through devices that are in direct communication with each other through a brute-force style attack using the SSH protocol. The newer, more persistent version can also detect and download updates for older versions of this malware and remove other processes running on the system that may hinder its execution such as debuggers or other types of malware. It is also able to detect honeypots and will install a go daemon service package to cement its persistence.

REMEDIATION STEPS

- Review configuration of any devices using SSH and monitor activity over cloud SSH access
- Implement strong access controls to all network devices, change default passwords to more secure passwords on all devices (especially IoT devices) and remove superfluous accounts.
- Monitor network and cloud environments for unusual activity, particularly outbound command requests

REFERENCES & RESOURCES

Barracuda:	https://blog.barracuda.com/2020/10/01/threat-spotlight-new-interplanetary-storm-variant-iot/
Threatpost:	https://threatpost.com/botnet-mac-android/159714/