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

CYBER GUIDANCE ISSUE 00125

PURPLE FOX MALWARE HAS WORMING CAPABILITIES

DATE ISSUED: 29th March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Purple Fox malware is known malware that has developed some interesting new capabilities to carry out worm-like self-propagation and brute-forcing passwords by exploiting Server Message Block (SMB) protocol.

BREAKDOWN

The target of choice has historically been Windows machines since its establishment in 2018 and with these new tools in the arsenal, internet facing devices are now at risk of infection. Previously user interaction was a critical step in the establishment of Purple Fox, but Guardicore Labs have discovered that these days a machine can be compromised through SMB and spread by itself. Once access is gained, a persistence is achieved with the creation of a new service which will proceed to install Purple Fox through the iteration of a range of URLs, including the Microsoft Installer (MSI) to download the malicious package that poses as a Windows Update. Each version has a different hash making it difficult to create links between the various MSI versions. Payloads are extracted and decrypted, the Windows Firewall is modified to prevent other attackers exploiting the same machine and the rootkit is instated, hiding various registry keys, values and files. A forced reboot occurs so that the Dynamic Link Library (DLL) of the malware can be added to the system DLL file after renaming itself and from there it begins the propagation process through port scanning on port 445. The noted most vulnerable servers are those running Internet Information Services (IIS) version 7.5 and Microsoft FTP. At this stage, in excess of 2,000 servers have been hijacked.

REMEDIATION STEPS

- A list of Indicators of Compromise (IoC) can be found in the GitHub reference below.
- Secure internet facing servers in a demilitarized zone and update to the latest version of the OS.
- Close port 445 and turn off unnecessary network services such as SMB and FTP where possible.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/purple-fox-malware-windows-worm/164993/
ZDNet	https://www.zdnet.com/article/purple-fox-malware-evolves-to-propagate-across-windows-machines
GitHub	https://github.com/guardicore/labs_campaigns/tree/master/Purple_Fox