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

CYBER GUIDANCE ISSUE 0271

PLUGX MALWARE INFECTS REMOVABLE USB DEVICES

DATE ISSUED: 30th January 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new version of PlugX malware spreads itself to additional systems by infecting attached removable USB devices. It hides malicious files in the device and then infects any Windows hosts the device is connected to. It has the potential to remain undetected and spread to air-gapped systems.

BREAKDOWN

The Palo Alto Network team discovered a variant of PlugX malware that locates sensitive files on the compromised system and copies them to a hidden folder on an attached USB device. It uses a Unicode character to create a new directory in the attached USB devices which prevents the Windows operating system from rendering the directory name, concealing its existence. These directories are, however, visible on Linux machines. A shortcut (.LNK) is created in the root folder of the USB device to execute the malware from the hidden directory. The PlugX malware will then copy itself onto any removable device attached to the machine by hiding inside a recycle bin folder. When a victim clicks on the shortcut it infects the system with the PlugX malware, but it also opens a new window to show the user's file on the USB device, making the shortcut appear legitimate.

REMEDIATION STEPS

- Use anti-malware detection and remediation software on all endpoint devices.
- Monitor network activity for any suspicious or anomalous behaviour.
- Create policies for your organisation regarding the use of removable USB storage devices and enforce these with technology controls and rules in your available toolset.

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/plugx-malware-hides-on-usb-devices-to-infect-new-windows-hosts/