UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00024

ICEDID TROJAN – NEW VERSION

DATE ISSUED: 21st August 2020

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

OVERVIEW

Originally a banking Trojan, IcedID has seen a new resurgence and new version that is able to avoid common detection methods with malicious actors taking advantage of the global Covid-19 pandemic crisis.

BREAKDOWN

Circulated via a recent phishing campaign, which distributes emails as the result of Business Email Compromise (BEC), the new version of IcedID has been seen to attach to documents disguised as things like invoices. Circumvention methods include password protected attachments, key word obfuscation, steganography and macro codes that are minimalistic in efforts to avoid detection. Its second stage downloader utilises the Microsoft DDL (Dynamic Link Library) where code is stored and used by multiple applications at any time. If the attachment is opened, a 3-stage attack is launched from a zipped folder. This attack begins with macros in a Microsoft Word document, which upon execution Visual Basic (VB) downloads DDL and saves it as a PDF and installs the regsvr32 service for added persistence. The second stage downloads a malicious PDF DDL from a host in Russia and the macro will call the regsvr32 to execute this file. This DDL downloads and executes a PNG file and decrypts it. By blending with benign domains such as apple.com, twitter.com and microsoft.com the downloader is able to avoid detection by sandboxes and other filtering mechanisms. The final stage downloads the IcedID executable main module. This trojan may also be deployed alongside Emotet (See Cyber Guidance Issue 0014) and is used in a similar manner to steal sensitive information and passwords, monitor browser activity and make changes in the system without the user's knowledge or consent, such as joining it to a botnet.

REMEDIATION STEPS

- Educate and inform staff around detection of phishing emails and social engineering attacks
- Monitor network for suspicious inbound and outbound connections
- Scan devices using anti-malware software to detect any running malware

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/icedid-trojan-rebooted-evasive-tactics/158425/
PC Risk:	https://www.pcrisk.com/removal-guides/14542-icedid-trojan
Security Intelligence:	https://securityintelligence.com/posts/breaking-the-ice-a-deep-dive-into-the-icedid-banking-trojans-new-major-version-release/