UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00227

EMOTET RESURFACES AFTER EXTERMINATION

DATE ISSUED: 23rd November 2021

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

OVERVIEW

After almost a year, the “world’s most dangerous malware” - thought to be gone for good after being taken down by an international police operation has resurfaced and is targeting Windows machines infected with TrickBot.

BREAKDOWN

Known for its capabilities to distribute other malware, a new version of Emotet has been spotted by researchers from Cryptolaemus, G DATA and AdvIntel launching via the TrickBot Trojan. After being disbanded by an international law enforcement operation, researchers were dubious about their initial suspicions, but after detailed analysis confirmed the DLLs have been identified as Emotet. This new version operates with similar behaviours to the original with URLs containing a random resources path and transferral of the request payload using a cookie but using a new form of encryption and a self-signed server certification to use HTTPS. Additionally, the user of “control-flow flattening to obfuscate the code” is another notable Emotet characteristic. It is too early to predict whether this new version will be as widely spread, and as devastating as its predecessor.

REMEDIATION STEPS

- Educate users on social engineering and phishing emails – how to detect them and what to do with any emails they deem suspicious received within your organisation. Emotet was widely distributed by phishing emails in the past.
- Use simulated phishing campaigns and conduct security awareness training activities to raise awareness and promote a cyber secure culture in your organisation.
- Run Endpoint Protection (NGAV) on all devices to detect and respond to unusual behaviours.
- Use network monitoring tools to detect, alert and respond to suspicious behaviours and traffic.
- Use web filtering controls set to auto-update to include newly discovered malicious URLs.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/emotet-resurfaces-trickbot/176362/
Cyber WTF	https://cyber.wtf/2021/11/15/guess-whos-back/
ZDNet	https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back