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

CYBER GUIDANCE ISSUE 00014

EMOTET BOTNET & TROJAN RESURGENCE

DATE ISSUED: 19th July 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	**LOW**	MEDIUM	HIGH

OVERVIEW

Spam email campaigns containing malicious URLs or attachments linked to the Emotet Botnet and Trojan with worm-like capabilities have resurfaced after five months of silence, using similar techniques to previous attack campaigns.

BREAKDOWN

A number of favoured techniques as well as some new tactics are known to be used in an effort to increase the attacker's likelihood of success, such as to insert a malicious email into an existing email thread between users. These emails may include malicious URLs or attachments containing obfuscated macros laden with malicious code that will execute when the attachment is accessed. This will trigger contact with a compromised remote website through PowerShell to retrieve Emotet binary which once executed will report to the command and control center. Thereafter, a new functionality that launches a secondary threat may be pushed to the device and executed such as the Trickbot malware or Ryuk ransomware. Victims information such as contact lists, device information and credentials are also harvested and remitted.

REMEDIATION STEPS

- Educate users in how to spot malicious emails and what to do if compromise is suspected
- Employ Web Application Firewall (WAF) or firewalls with Application layer visibility and URL filtering to reduce the likelihood of accessing malicious URLs
- Use endpoint protection on all connected devices to detect and respond to attempts at malicious code execution.
- Utilize Secure Email Gateway and Spam Filtering to prevent malicious emails from reaching the intended victim.

REFERENCES & RESOURCES

Malwarebytes: https://blog.malwarebytes.com/trojans/2020/07/long-dreaded-emotet-has-returned/
Trend Micro: https://success.trendmicro.com/solution/1118391-malware-awareness-emotet-resurgence
Threatpost: https://threatpost.com/emotet-resurgence-continues-with-new-tactics-techniques-and-procedures/149914/
ZDNet: https://www.zdnet.com/article/emotet-resurgence-packs-in-new-binaries-malicious-functions/
Dark Reading: https://www.darkreading.com/attacks-breaches/emotet-malware-rears-its-ugly-head-again/d/d-id/1337119