UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00027

QBOT TROJAN REVAMPED

DATE ISSUED: 27th August 2020

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

OVERVIEW

A number of new campaigns have been detected and over 100,000 infections relating to malware colloquially known as the "Swiss-Army Knife." The QBot Trojan known for stealing information has had a revamp 12 years after it first appeared and has adopted a plethora of new technologies, including avoiding detection through evasion techniques.

BREAKDOWN

The QBot Trojan has evolved to become an Advanced Persistent Threat (APT) through modification of the base code, first discovered 12 years ago. Recently it has been seen to hitch a ride in the fresh slew of Emotet campaigns as we as the new feature enabling the malware to hijack Outlook-based email threads to spread to other machines using URLs with a zipped Visual Basic Scripts (VBS). Once executed, a specialised module extracts and uploads the most recent or relevant email threads to a hardcoded server to be used for future campaigns. As information theft is its primary purpose, this stage is also carried out to collect passwords, banking credentials, and browsing data. Connection to a Bot controller to potentially facilitate Distributed Denial of Service (DDoS) attacks as a slave node and further malware may be used and installed through web injection such as ransomware. QBot is also able to fetch an install remote updates as required.

REMEDIATION STEPS

- Practice caution when accessing emails from both unknown and known users. If in doubt, contact the sender directly to ensure the legitimacy of the email sent and the download or URL they are requesting.
- Educate users and spread awareness regarding detecting phishing and dodgy emails
- Use anti-malware software to scan devices for signs of infection
- Use URL filtering to prevent access to known malicious sites.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/revamped-qbot-trojan-packs-new-punch-hijacks-email-threads/158715/
ZDNet:	https://www.zdnet.com/article/your-email-threads-are-now-being-hijacked-by-qbot-trojan/
CheckPoint Research:	https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/
KnowBe4:	https://blog.knowbe4.com/qbot-is-back-with-new-phishing-tricks