U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00216

GLUPTEBA TROJAN PROVES PROLIFIC & VERY SNEAKY

DATE ISSUED: 26th October 2021

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

OVERVIEW

By infecting Windows systems and installing a backdoor, attackers are using the Glupteba malware to add to a growing botnet, as a means to distribute other malware, and to provide full access to the compromised system with some novel means to remain undetected.

BREAKDOWN

Over the last few months, various evolutions of the malware have been spotted as continuous improvements are being made and new components added by its creators. The malware is distributed in pirated software – including cracked versions of commonly used enterprise applications and video games. To avoid detection, the malware is dropped into the system but by bit and uses the EternalBlue SMB vulnerability to traverse across the network. To remain undetected, the malware uses a variety of privilege escalation tactics to install a kernel driver that can be used in a similar fashion to a rootkit by the bot and take down many other security mechanisms in the infected host. Exfiltration to the Command and Control (C2) server is hidden in encrypted bitcoin blockchains. Currently being marketed as a Malware-as-a-Service solution and an entry point for threat actors wishing to execute larger scale attacks, previous campaigns that include its use were the MosaicLoader campaign seen earlier this year (Cyber Guidance 00174)

REMEDIATION STEPS

- Install patches issued by Microsoft for Eternal Blue (2017) as this threat remains active due to the number of currently unpatched devices.
- Blacklist sites that are associated with pirated software and apply policies to inhibit users ability to search and access these sites.
- Educate users on the dangers and legal implications of downloading or executing files from known pirate or untrusted sources – remove the ability for users to run executable files on their machines without administrator approval.
- Educate users on the dangers of visiting untrusted websites or accessing links in email, chat or SMS messages.
- Run Next Generation Anti-Virus (NGAV) on endpoints to detect and isolate malicious behaviours and unauthorised downloads

REFERENCES & RESOURCES

ZD Net	https://www.zdnet.com/article/this-sneaky-malware-goes-to-unusual-lengths-to-cover-its-tracks/
Microsoft	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010