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

CYBER GUIDANCE ISSUE 00200

ZLOADER TROJAN SPREADS BY GOOGLE ADS

DATE ISSUED: 20th September 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The most recent campaign incorporates attackers creating fake advertisements for popular applications such as Discord, TeamViewer, Zoom and Java plugins to lure in victims, sending them to fake site to download the ZLoader Trojan. Abusing the Google Adwords to make their advertisements appear first is proving a successful tactic to establish a foothold using new and improved stealth and exfiltration capabilities.

BREAKDOWN

ZLoader has the typical characteristics of most banking Trojans intended to steal cookies, passwords and sensitive information from victims as well as being used as a typical "Loader" used to establish a backdoor and for deploying other malware - including ransomware. Researchers discovered that in one instance the cybercriminals managed to obtain a legitimate certificate from Flyintellect Inc. – potentially a company registered solely for the purpose of acquiring those certificates. Obfuscation and circumvention is mostly achieved by exploiting legitimate Windows functions. The first stage of malware installation is a signed .MSI file which creates the directory " *C:\Program Files (x86)\Sun Technology Network\Oracle Java SE"* dropping the "setup.bat" file and once executed by the built-in Windows cmd.exe function drops a second script "updatescript.bat". The third stage dropper tackles Windows Defender using a PowerShell cmdlet Add-MpPreference, obscuring the malware from detection. The fourth stage "tim.exe" file (a backdoor version of the legitimate wextract.exe function) is executed through Windows explorer.exe function after downloading from the URL "hxxps://pornofilmspremium.com/tim[dot]exe," breaking the parent/child correlations used by Endpoint Detection and Response (EDR) to detect and address malware. The final payload tim.dll is executed by the Windows regsvr32 function allowing attacker to proxy through a signed binary. The connection is established with the TIM botnet and further evasion techniques commence with the download of another script "nsudo.bat" which performs a number of operations.

REMEDIATION STEPS

- Disable users ability to download and execute software from non-approved (white-listed) sites
- Check for Indicators of Compromise (IoC) from the sources provided and check network monitoring tools and logs to detect anomalous behaviours.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/zloader-google-adwords-windows-defender/169448/
Bleeping Computer https://www.bleepingcomputer.com/news/security/new-zloader-attacks-disable-windows-defender-to-evade-detection/