مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

New NodeStealer Malware Campaign

Tracking #:432316654

Date:20-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new variant of NodeStealer malware, transitioning from a JavaScript-based to a Python-based threat, has been identified in targeted spear-phishing campaigns.

TECHNICAL DETAILS:

A new variant of NodeStealer malware, transitioning from a JavaScript-based to a Python-based threat, has been identified in targeted spear-phishing campaigns. This advanced variant is designed to harvest a wide range of sensitive data, including financial information, browser-stored data, and most notably, Facebook Ads Manager credentials, which are critical for businesses managing advertising campaigns across Facebook's platforms. Delivered through spear-phishing emails, the malware executes sophisticated techniques to bypass security measures, culminating in the exfiltration of stolen data via Telegram.

Technical Details

Infection Chain

1. Spear-Phishing Email: The attack begins with a spear-phishing email, disguised as a copyright infringement notice. The email contains a link that leads victims to a zip file upon clicking, which appears to be a harmless document.
2. Malicious Payload: Once extracted, the zip file contains several suspicious files, including:
   - GHelper.dll
   - Nombor Rekod 052881.exe (disguised as a PDF reader)
   - license-key.exe and other files used to deploy malware.
3. DLL Sideloading: The executable Nombor Rekod 052881.exe sideloads a malicious DLL (oledlg.dll), which is then executed via a batch file. This allows the malware to bypass security software, performing its activities covertly.
4. PowerShell Execution: The malware executes encoded PowerShell commands to extract and deploy a Python interpreter and other supporting files to create a hidden directory under %LocalAppData%\ChromeApplication.
5. Persistence and Final Payload: The malware ensures persistence by adding itself to the startup folder, enabling it to execute on system boot. It then downloads and runs the final payload, which is a Python-based infostealer.
6. Final Payload and Exfiltration: The infostealer targets Facebook Ads Manager accounts and sensitive information such as credit card details and browser-stored data. The stolen information is exfiltrated to a Telegram channel via an API, ensuring that data is sent covertly to attackers.

Exfiltration and Data Theft

The malware collects various forms of sensitive information:

- Credit Card Information: Captured from browsers and other stored locations.
- Facebook Ads Manager Credentials: Targeted due to the potential for financial gain from exploiting advertising accounts.
- Browser Data: Including cookies, login credentials, and browsing history.

Indicators of Compromise:

Indicator	SHA256	Description	Detection
oledlg.dll	f813da93eed9c536154a6da5f38462bfb4ed80c85dd117c3fd681cf4790fbf71	Sideloaded DLL	Trojan.Win32.RASPBERRYROBIN.HA
active-license.bat	1c9c7bb07acb9d612af2007cb633a6b1f569b197b1f93abc9bd3af8593e1ec66	Executes the PowerShell command	HackTool.BAT.HideConsole.A
WindowsSecurity.lnk	786db3ddf2a471516c832e44b0d9a230674630c6f99d3e61ada6830726172458	Created persistence	Trojan.LNK.DOWNLOADER.D
hxxps://t[.]ly/MRAbJ		Malicious download link	Dangerous – Disease Vector
hxxp://88[.]216[.]99[.]5:15707/entry[.]txt			Dangerous – Malware Accomplice

RECOMMENDATIONS:

- Be Cautious with Suspicious Emails: Exercise extreme caution when receiving emails from unknown sources or those containing embedded links.
- Antivirus and Anti-malware Tools: Ensure that all systems are regularly scanned with up-to-date antivirus software capable of detecting the latest malware variants.
- DLL Sideloading Defense: Implement security controls that can detect and block DLL sideloading techniques, which are often used to bypass security solutions.
- Endpoint Protection: Deploy advanced endpoint protection solutions to monitor and block suspicious activities such as unauthorized DLL loading and PowerShell execution.
- Software Updates: Regularly update all software, including applications, browsers, and operating systems, to patch known vulnerabilities. Malware often exploits unpatched software to gain entry into a system.
- Monitor Outbound Traffic: Continuously monitor network traffic for unusual connections to external services, such as Telegram, which could indicate data exfiltration.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.trendmicro.com/en_us/research/24/l/python-based-nodestealer.html