مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

VEILDrive: Threat Campaign Exploits Microsoft SaaS Services

Tracking #:432316486

Date:08-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a newly identified threat campaign dubbed "VEILDrive" targeting critical infrastructure and leveraging Microsoft's SaaS suite for malicious activities.

TECHNICAL DETAILS:

A newly identified threat campaign dubbed "VEILDrive" has been uncovered by Hunters' Team AXON, targeting critical infrastructure and leveraging Microsoft's SaaS suite for malicious activities. This ongoing campaign exploits trusted Microsoft services such as Teams, SharePoint, Quick Assist, and OneDrive to distribute spear-phishing attacks, store malware, and establish command and control (C2) infrastructure.

The malware associated with VEILDrive is a Java-based .jar file that lacks obfuscation, making it unusually readable and straightforward, yet it has evaded detection by leading security tools, including a top-tier Endpoint Detection and Response (EDR) solution and all engines on VirusTotal.

Attack Methodology
The VEILDrive campaign initiates its attack through social engineering tactics on Microsoft Teams. The threat actor impersonates IT team members and requests access to employees' devices using the Quick Assist remote utility tool1. This approach exploits the trust users place in internal IT communications and legitimate Microsoft services. Once access is gained, the attacker deploys a Java-based malware (.jar file) on the compromised device. This malware is notable for its lack of obfuscation and well-structured code, making it unusually readable. Despite its simplicity, the malware has proven highly effective at evading detection.

Command and Control Infrastructure:
VEILDrive employs a novel OneDrive-based Command and Control (C2) method. This technique leverages the trusted Microsoft cloud infrastructure to establish communication between the compromised devices and the attacker's control servers. By using legitimate cloud services for C2, the campaign significantly reduces the likelihood of detection by traditional network monitoring tools

Malware Characteristics:
The Java-based malware used in the VEILDrive campaign exhibits several unique characteristics:

- Zero obfuscation, making the code easily readable and analyzable.
- Well-structured and straightforward implementation.
- Successful evasion of top-tier EDR solutions and all VirusTotal engines.
- Utilization of OneDrive for command and control operations

These features highlight a critical security concern: even non-obfuscated, simple malware can bypass modern detection mechanisms when leveraging trusted cloud services.

Indicators of Compromise (IOC's):

- Entra ID tenants used by the attacker (Look for outgoing DNS request toward those domains):
  - SafeShift390[.]onmicrosoft[.]com
  - GreenGuard036[.]onmicrosoft[.]com
- File IOCs (SHA256):
  - ROMServer.exe
    a515634efa79685970e0930332233aee74ec95aed94271e674445712549dd254
  - HookDrv.dll
    1040aede16d944be8831518c68edb14ccbf255feae3ea200c9401186f62d2cc4
  - ROMFUSClient.exe
    7f61ff9dc6bea9dee11edfbc641550015270b2e8230b6196e3e9e354ff39da0e
  - AledensoftIpcServer.dll
    d6af24a340fe1a0c6265399bfb2823ac01782e17fc0f966554e01b6a1110473f
  - ROMwln.dll
    7f33398b98e225f56cd287060beff6773abb92404afc21436b0a20124919fe05
  - IP Addresses:
    - 40.90.196[.]221
    - 40.90.196[.]228
    - 38.180.136[.]85
    - 213.87.86[.]192

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Implement strict access controls and multi-factor authentication for all Microsoft SaaS services, especially Teams, SharePoint, and OneDrive.
- Regularly audit and monitor user activities within Microsoft services for suspicious behavior or unauthorized access attempts.
- Enhance email filtering and anti-phishing measures to detect and block spear-phishing attempts originating from compromised Microsoft accounts.
- Deploy and maintain up-to-date EDR solutions capable of detecting and responding to novel threats, including those leveraging legitimate cloud services.
- Conduct regular security awareness training for employees, focusing on recognizing social engineering tactics and phishing attempts via Microsoft Teams and other collaboration platforms.
- Implement network segmentation and zero-trust architecture to limit the potential impact of compromised accounts or devices.
- Regularly review and update incident response plans to include scenarios involving attacks leveraging cloud services and SaaS applications.
- Establish and maintain secure configuration baselines for all Microsoft services used within the organization.
- Implement robust logging and monitoring solutions that can detect anomalous activities across Microsoft SaaS services.

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.hunters.security/en/blog/veildrive-microsoft-services-malware-c2