مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Fickle Stealer - Information Stealer Targeting Windows Users

Tracking #:432315969

Date:20-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new information stealer, "Fickle Stealer," targeting Windows systems to steal sensitive information from victims' computers.

TECHNICAL DETAILS:

Fickle Stealer is a sophisticated malware written in Rust, a programming language known for its performance and reliability. Stealer is distributed using a variety of strategies and has a flexible way of choosing its target.

Attack Chain Stages:

- **Delivery**:

  Four delivery methods observed:

  - VBA dropper: Word document with VBA macro executes an encoded script that drops Fickle Stealer to the Temp folder.
  - VBA downloader: Word documents directly download a PowerShell script (usually named u.ps1 or bypass.ps1).
  - Link downloader: Directly downloads bypass.ps1.
  - Executable downloader: Downloads a PowerShell script for preparatory work.

- **Preparatory Work**:

  - PowerShell script (u.ps1 or bypass.ps1) is downloaded.
  - Additional files may be added between the downloader and the script.

- **Packer and Stealer Payload**:

  - Fickle Stealer payload is executed.

Features:

- **Extensive Reach:** This stealer doesn't just target the usual suspects (common program directories). It delves deeper, searching parent directories as well, potentially uncovering hidden data. This broadens its scope for data gathering.
- **Adaptable Targeting:** Fickle Stealer doesn't rely solely on pre-programmed targets. It can receive a dynamic list of targets from its command server, making it more flexible in the data it can steal. This allows attackers to adjust their strategy and target specific systems or data types.
- **Evolving Threat:** The observation of variants receiving updated target lists indicates that Fickle Stealer is actively being developed and refined. This highlights the importance of staying vigilant against evolving threats.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Layered Security: Combine endpoint security with robust antivirus/anti-malware for advanced threat detection, prevention, and removal.
- Patch Management: Prioritize regular updates for operating systems, applications, and security software to address vulnerabilities.
- Network Segmentation & Monitoring: Limit lateral movement with segmentation and use firewalls to block malicious network traffic.
- Security Awareness Training: Educate employees on phishing, social engineering, and how to identify suspicious activity.
- Enhanced Network Defenses: Implement application whitelisting, behaviour-based monitoring, and monitor for anomalous data transfers.
- Incident Response & Threat Intelligence: Develop a plan for incidents and stay informed about current malware threats and indicators of compromise (IOCs).
- Data Backups & Least Privilege: Regularly back up data and implement the principle of least privilege to minimize potential damage.

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.fortinet.com/blog/threat-research/fickle-stealer-distributed-via-multiple-attack-chain?lctg=232952123