SECURITY ADVISORY

CYBER STASH

October, 2024

CVE-2017-11882

SideWinder APT | StealerBot Campaign

Context

SideWinder APT — also referred to as APT-C-17, Baby Elephant, Hardcore Nationalist, Leafperforator, Rattlesnake, Razor Tiger, or T-APT-04—has been operational since at least 2012 and is believed to serve the strategic interests of the Indian state. Recently, the group has broadened its scope of operations to encompass the Middle East, Africa, and Southeast Asia.

SideWinder primarily targets military, g**overnme**ntal, telecommunications, and critical infrastructure entities across these regions. The group employs spear-phishing emails as their initial attack vector, subsequently executing sophisticated multi-stage assaults that exploit well-documented vulnerabilities, such as CVE-2017-11882. In its latest campaign, SideWinder has unveiled a new variant of "StealerBot," an advanced cyberespionage tool meticulously designed for data exfiltration, system compromise, and the facilitation of further malicious activities. This evolution in their toolkit underscores their growing capabilities and intent, marking them as a formidable threat in the cyber domain.

Mitigation

Defending against the SideWinder APT requires proactive measures:

Keep Software Updated: Regularly patch and update all software to address vulnerabilities and reduce the attack surface.

Restrict Unauthorized Software Installation: Limit user permissions to prevent the installation of unapproved applications, enhancing security against potential threats.

Block Access to High-Risk Infrastructure: Proactively restrict access to known high-risk IP addresses, ASNs, and TLDs to mitigate exposure to malicious activities.

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to provide real-time monitoring, threat detection, and automated response capabilities, enhancing overall incident response.

Technical Details

Malware Delivery

The SideWinder APT initiates its attack via spear-phishing emails containing malicious files (e.g., LNK files, ZIP files, or Office documents). These files exploit vulnerabilities such as CVE-2017-11882 to execute JavaScript or download malicious payloads from attacker-controlled remote servers and triggers a multi-stage infection chain.

Malware Analysis

SideWinder APT's latest campaign features the *StealerBot* malware, a modular espionage toolkit that is memory-resident, avoiding file-based detection on the host system. Each module of *StealerBot* performs specific tasks such as keylogging, screenshot capturing, and stealing credentials from browsers. The modular nature allows for easy updates and dynamic loading of new components.

Backdoor Command Functions

The recent SideWinder APT campaign exhibit the following backdoor command functions:

- **Keystroke Logging:** Records all keyboard input to capture login credentials and other sensitive data.
- **Screenshot Capture:** Takes regular screenshots, allowing attackers to monitor the victim's activities and sensitive documents in real-time.
- **Credential Theft:** StealerBot extracts credentials from web browsers like Chrome and Firefox and intercepts RDP credentials, facilitating further network access.
- **Command Execution:** Receives and executes commands from the command-and-control (C2) server, such as downloading files or executing additional malware.
- **Data Exfiltration:** Enables the theft of targeted files and documents for intelligence gathering.
- **Further Malware Injection:** Injects additional malicious components to expand its attack scope or persist in the system.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to SideWinder APT campaign :

Tactic	Technique	Technique Number	Description
Initial Access	Spear phishing Attachment	(T1566.001)	Malicious ZIP files containing LNK files or Office documents are delivered via spear-phishing emails to initiate the infection chain.
Execution	Command and Scripting Interpreter: PowerShell	(T1059.001)	PowerShell and JavaScript scripts execute commands that download secondary payloads.
Persistence	Boot or Logon Autostarts Execution	(T1547)	Malware ensures persistence by modifying system startup settings or creating new user accounts.
Privilege Escalation	Exploitation for Privilege Escalation	(T1068)	SideWinder exploits known vulnerabilities to escalate privileges within the infected system.
Defense Evasion	Signed Binary Proxy Execution	(T1218)	Legitimate Windows binaries like MSHTA and regsvr32 are used to load malicious payloads, bypassing security measures.

Cyber Threat Intelligence

The recent campaign by SideWinder APT, featuring the StealerBot malware, signifies a notable escalation in the group's espionage capabilities. Targeting government and military organizations in the Middle East and Asia, SideWinder employs spear-phishing emails containing ZIP files with malicious LNK shortcuts or Office documents. Once executed, these files trigger PowerShell commands that download the StealerBot payload.

StealerBot is a modular malware designed for data exfiltration and credential theft, with capabilities including keystroke logging, screenshot capture, and the harvesting of browser-stored credentials. Its fileless execution from memory, coupled with encrypted HTTPS communications, complicates detection by traditional antivirus solutions.

This campaign demonstrates SideWinder's strategic blend of low-level attack vectors and sophisticated evasion techniques. By leveraging publicly available tools alongside custom components, the group appears deceptively simple, yet their operational planning reveals a high level of sophistication. As StealerBot enhances their espionage efforts, organizations in the region must remain vigilant, utilizing advanced EDR solutions to detect fileless attacks and monitor unusual network behavior.

References

IOCs:

- https://securelist.com/sidewinder-apt/114089/

Malicious URLs:

- hxxps://dynamic.nactagovpk[.]org
- hxxps://nventic[.]info/mod/rnd/214/632/56/w3vfa3BaoAyKPfNnshLHQvQHCaPmqNpNVnZMLxXY/1/1712588158138/bf7dy/111e9a21?name=inpl64
- hxxps://nventic[.]info/mod/rnd/214/632/56/w3vfa3BaoAyKPfNnshLHQvQHCaPmqNpNVnZMLxXY/1/1712588158138/0ywcg/4dfc92c?name=stg64
- hxxps://nventic[.]info/mod/rnd/214/632/56/w3vfa3BaoAyKPfNnshLHQvQHCaPmqNpNVnZMLxXY/1/1712588158138/3ysvj/955da0ae?name=rflr
- hxxps://split.tyoin[.]biz/7n6at/g3mnr/1691394613799/f0f9e572

Public Intelligence:

- https://securelist.com/sidewinder-apt/114089/
- https://thehackernews.com/2024/10/sidewinder-apt-strikes-middle-east-and.html
- https://kaspersky.africa-newsroom.com/press/kaspersky-identifies-sidewinder-apt-expanding-attacks-with-new-espionage-tool?lang=en
- https://www.businesstechafrica.co.za/security/2024/10/21/kaspersky-identifies-sidewinder-apt-expanding-attacks-with-new-espionage-tool/