IMPORTANT CYBERSECURITY NEWS: WINOS 4.0 MALWARE EXPLOITS PHISHING TACTICS TO TARGET TAIWANESE ORGANIZATIONS

Vairav Cyber Security News Report

Date: February 28, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A new phishing campaign is targeting organizations in Taiwan by distributing Winos 4.0 malware under the guise of official tax-related documents. Detected by Fortinet FortiGuard Labs, the campaign tricks recipients into downloading a malicious DLL disguised as an enterprise tax inspection list. The malware, linked to the Silver Fox APT group, can log keystrokes, take screenshots, altering clipboard content, and executing commands when security prompts appear. The campaign also delivers an online module designed to capture WeChat and bank application screenshots. Researchers have noted that Winos 4.0 shares origins with ValleyRAT, both of which evolved from the Gh0st RAT family.

INCIDENT ANALYSIS

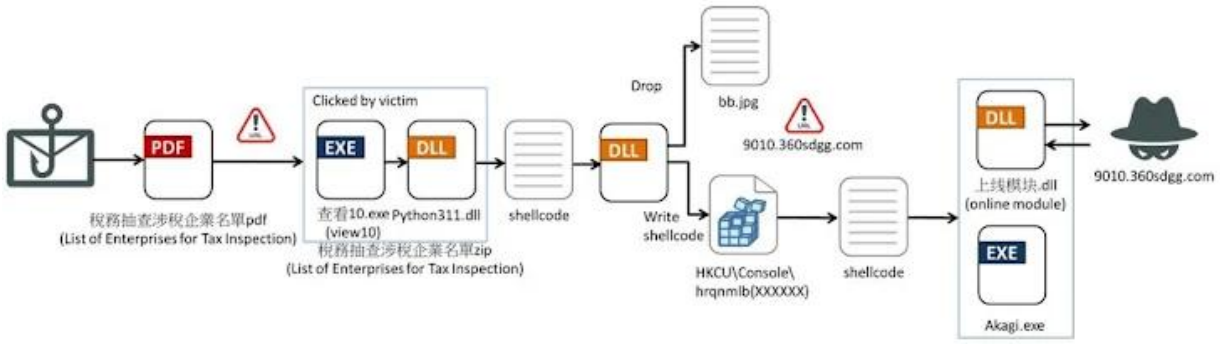

Figure 1: Infection Chain

The phishing emails impersonate Taiwan's National Taxation Bureau, urging victims to review a ZIP file attachment that contains a malicious DLL named *lastbld2Base.dll.* Once executed, the malware downloads a Winos 4.0 module from a remote server *(206.238.221[.]60)* to exfiltrate sensitive data. The malware enables attackers to monitor USB devices, execute shell commands, and manipulate security alerts from Kingsoft Security and Huorong.

Further investigations have revealed an additional attack chain distributing a module that captures screenshots of WeChat and online banking activities, posing a severe financial threat. The campaign has been attributed to Void Arachne/Silver Fox APT, which has previously used ValleyRAT and trojanized software installers. Researchers also observed the CleverSoar installer distributing Winos 4.0, which selectively infects systems based on language settings, indicating a deliberate targeting of Chinese and Vietnamese users.

Beyond this campaign, Silver Fox has also been seen using trojanized Philips DICOM viewers to deploy ValleyRAT, keyloggers, and cryptocurrency miners while leveraging a vulnerable TrueSight driver to disable security defenses.

The Winos 4.0 malware campaign highlights the evolving tactics of the Silver Fox APT group, which continues to exploit phishing lures, trojanized software, and stealthy malware to compromise victims. Organizations, especially in Taiwan, must strengthen their cybersecurity posture by enhancing email security, monitoring unauthorized software execution, and deploying robust endpoint protection to defend against such sophisticated threats.

RECOMMENDED ACTIONS

To mitigate the risks associated with this campaign, the following security measures should be implemented:

- Implement strict email filtering policies to detect phishing emails and prevent malicious attachments from being executed.
- Deploy advanced endpoint detection and response (EDR) solutions to detect and mitigate DLL-based malware infections.
- Educate employees on phishing tactics and instruct them to verify tax-related emails before downloading attachments.
- Restrict the execution of unverified DLLs and enforce strict software installation policies to prevent unauthorized applications.
- Continuously track new malware variants like Winos 4.0 and ValleyRAT to enhance proactive defense mechanisms.
- Perform frequent security assessments to identify vulnerabilities in corporate networks and implement necessary patches.

RESOURCES

https://www.fortinet.com/blog/threat-research/winos-spreads-via-impersonation-of-official-email-to-target-users-in-taiwan

https://thehackernews.com/2025/02/silver-fox-apt-uses-winos-40-malware-in.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com