Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

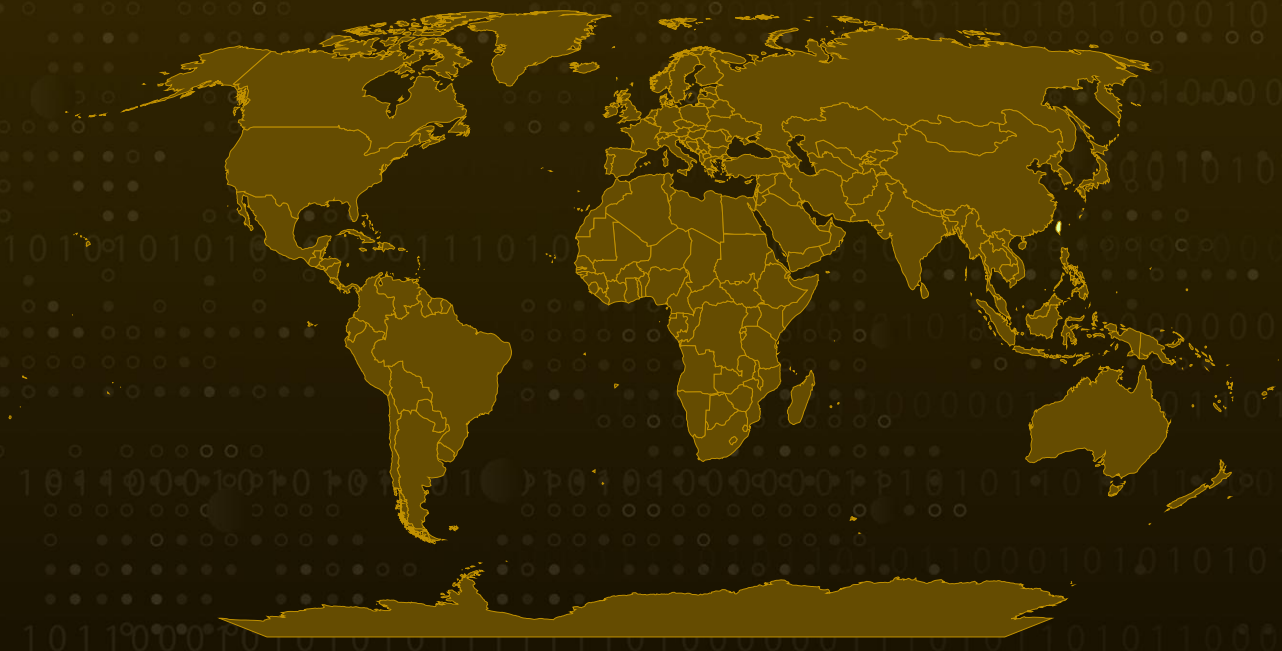
Winos4.0: Stealthy Malware Campaign Targets Taiwanese Enterprises

Date of Publication	Admiralty Code	TA Number
February 28, 2025	A1	TA2025062

Summary

Attack Discovered: January 2025
Targeted Countries: Taiwan
Affected Platforms: Microsoft Windows
Malware: Winos4.0
Attack: A new phishing campaign is actively targeting companies in Taiwan, deploying the Winos 4.0 malware under the guise of official emails from the country's National Taxation Bureau. The attackers are using this tactic to trick recipients into opening malicious attachments, ultimately compromising their systems. Once infected, the malware steals sensitive data, which can be leveraged for future attacks. Additionally, researchers have uncovered a second attack chain that delivers an online module capable of capturing screenshots from WeChat and online banking platforms, further expanding the threat's scope.

Attack Regions



Attack Details

#1 In January 2025, a targeted cyberattack against Taiwanese companies was uncovered, deploying Winos4.0, a sophisticated malware framework. The attack begins with phishing emails masquerading as official notices from Taiwan's National Taxation Bureau, tricking recipients into opening an attached ZIP file. Previously, Winos4.0 was distributed through gaming-related applications. Inside the archive, attackers have hidden malicious DLL files that initiate the infection. Once executed, a loader launches a rogue DLL, which then fetches and deploys the Winos4.0 module from its command-and-control (C2) server.

#2 To enhance its stealth, the attackers structured the ZIP file to mimic a legitimate directory, replacing the real ApowerREC.exe with a compromised version. When executed, the fake application calls a function that decrypts embedded data, extracting shellcode that contains key configuration details such as C2 IP addresses, registry keys, and feature flags. The malware checks system permissions by accessing the Windows registry and attempting to run ApowerREC.exe with administrative privileges. If successful, it escalates its attack, executing additional payloads.

#3 Winos4.0 incorporates multiple stealth techniques, including anti-sandboxing measures. It takes screenshots at short intervals and compares them to detect signs of a virtualized environment. If the system appears genuine, the malware downloads an encrypted payload from its C2 server and stores it in the Windows registry. Once decrypted, this payload launches eight malicious threads responsible for persistence, keylogging, clipboard monitoring, and USB device tracking. Additionally, the malware captures screenshots of applications containing specific keywords and stores them in a hidden system folder.

#4 To maintain long-term access, Winos4.0 disables security prompts, bypasses User Account Control (UAC), and monitors active TCP connections. The campaign employs multiple attack chains, including one that leverages Python311.dll, a module compiled from a Python script using Nuitka. This module decrypts shellcode and generates additional DLLs, which are then stored in registry values for execution. Some Winos4.0 variants include specialized modules designed to capture screenshots of WeChat conversations and online banking sessions, further expanding its espionage capabilities.

#5 Security researchers have linked Winos4.0 operations to Silver Fox (also known as Void Arachne), citing overlaps in malware usage and attack methodologies across different campaigns. The malware's reliance on registry keys and encrypted configurations makes forensic analysis challenging, allowing attackers to maintain persistence while evading detection. However, cybersecurity teams continue to track these threats, deploying countermeasures to mitigate their impact.

Recommendations

Enhance Email Security: Implement robust email filtering to block phishing emails impersonating trusted entities. Use email authentication mechanisms like DMARC, SPF, and DKIM to prevent spoofed emails. Educate employees on identifying phishing attempts, especially those mimicking government agencies.

Restrict Execution of Untrusted Files: To minimize the risk of malware infections, enforce strict application whitelisting, allowing only trusted and verified software to run. This approach prevents unauthorized executables and DLLs from being executed, particularly those originating from suspicious ZIP file attachments.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Implement Least Privilege Access: Restricting administrative privileges is crucial in preventing malware from gaining deep system access. Only essential personnel should have elevated privileges, reducing the risk of unauthorized software installations or system modifications. Non-administrative users should be blocked from executing unverified applications, ensuring that potential threats cannot take hold.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment	T1547 Boot or Logon Autostart Execution
T1113 Screen Capture	T1115 Clipboard Data	T1056 Input Capture	T1056.001 Keylogging

T1560 Archive Collected Data	**T1140** Deobfuscate/Decode Files or Information	**T1036** Masquerading	**T1204** User Execution
T1204.002 Malicious File	**T1059** Command and Scripting Interpreter	**T1059.006** Python	**T1497** Virtualization/Sandbox Evasion
T1068 Exploitation for Privilege Escalation	**T1112** Modify Registry	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control
T1025 Data from Removable Media	**T1564** Hide Artifacts	**T1082** System Information Discovery	**T1656** Impersonation

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	43[.]137[.]42[.]254, 206[.]238[.]221[.]60, 206[.]238[.]221[.]240, 124[.]156[.]100[.]172, 206[.]238[.]221[.]244
Domains	1234[.]360sdgg[.]com, 9001[.]360sdgg[.]com, 9002[.]360sdgg[.]com, 9003[.]360sdgg[.]com, 9005[.]360sdgg[.]com, 9006[.]360sdgg[.]com, 9007[.]360sdgg[.]com, 9009[.]360sdgg[.]com, 9010[.]360sdgg[.]com, ffggssa-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com, fuued5-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com, 0107-1333855056[.]cos[.]ap-guangzhou[.]myqcloud[.]com, rgghrt1140120-1336065333[.]cos[.]ap-guangzhou[.]myqcloud[.]com, hei-1333855056[.]cos[.]ap-guangzhou[.]myqcloud[.]com, chakan202501-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com, wrwyrdujtw114117-1336065333[.]cos[.]ap-guangzhou[.]myqcloud[.]com,

TYPE	VALUE
Domains	fdsjg114-1336065333[.]cos[.]ap-guangzhou[.]myqcloud[.]com, sjujfde-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com, htrfe4-1329400280[.]cos[.]ap-guangzhou[.]myqcloud[.]com, 0611-1333855056[.]cos[.]ap-guangzhou[.]myqcloud[.]com, twzfw[.]vip
SHA256	36afc6d5dfb0257b3b053373e91c9a0a726c7d269211bc937704349a6b4be9b9, 0e3c9af7066ec72406eac25cca0b312894f02d6d08245a3ccef5c029bc297bd2, 67395af91263f71cd600961a1fd33ddc222958e83094afdde916190a0dd5d79c, f4d3477a19ff468d234a5e39652157b2181c8b51c754b900bcfa13339f577e7c, c9a8db23d089aa71466b4bde51a51a8cfdcc28e8df33b4c63ce867bd381e5fe5, e2b75baeb7ed21fb8f27984f941286770d1c3c0b60fce8d7fa5b167bd24ba6dc, dffbeefc632b20d2ef867553684e9971ab76e1223e743604a5275713423b6168, 20c34b5f0983021414b168913c3da267caf298d8f0f5e3ec0ce97db5f4f48316, 6c33715a14fdc917b5b09b6e1b5dad07bb769493eafbf7ca1023830b4059e003, 75a4d75c35724140149c9c5056c1bcbd328bbe1e5d1d1ef34205ed5442d2b348, fed394a3653b7c6fcc1b277eda6e18eb0983a7e024be5b51e5188b3cfb9512e8, a067d848f099e6d1e465f9761a5b85392d550303bfa75fac920d444fd980c949, c55757075259fa4be6941dd273c4a4a2fcc29e6ba427dec124b25b299b3505fe, 64a876e6cb3cf3122febc84a00ec3e0740c054cff955164971c470e1b5e5f1bb, d4ac82de8dda9796579cd8ea0f84b43c7a980cdb0e9cdb8abe8981a2d215ed2f, 268c72f5482374660a132d1b91cac0c04b4724a214db4f052eb421e36c282921, 0a4bbb998bd3a3bcc72cf759689a5656dc74590b731d0affbfc317cf484ed28b, 79c64d2e77acdbcdbd35cbb29497941335d7e3ab6ebb474064f095e745f0d643, 7f22305679e46e1fd5043beb136108197c0921643ce0d680f990a3018ade485b,

TYPE	VALUE
SHA256	594d907855d35ee7689a568e4ac43e4e0ed90de047d91b0253ef79da71ecbc08, 1f3b041eee1ece8cf6aa5c742aeb8c0ac2266cccecca7888772509227c4f8669, 514933468ac1dd9f7db4e2693f1be7f84deb35c33f8f9934fad32caaae9ef611, 7a5b26f6dd7b8e0d648e9804ec932603b7d7a5f76c7a8c537ab0c2be54f51fa9, 8b1b9a789136ca3abe25938204845c351aaf0c97c0708ade8d4d8ba4ded95ba7, 1ad1f2eec961bc7a35abeac486f843b7caece0929b13f1dab47fbdc0406ac4e3, 4c1ea827713f1eb57cc0e8e9d171d4e21d116f846b174bc05114eef5674c9653, 1a342426d59e7fdc4abfb74c2225f68382172e03b0f8d496a57ae647411f0fbd, 2ce73cbfab0beb3663c0151ba7c310e4dbf69f295d8a18114435506483d774ac, 0a4bbb998bd3a3bcc72cf759689a5656dc74590b731d0affbfc317cf484ed28b, 514933468ac1dd9f7db4e2693f1be7f84deb35c33f8f9934fad32caaae9ef611, 76ac08358f230bca3e8b8448b3c177094aeac25402b929f5f73869ec77173a44

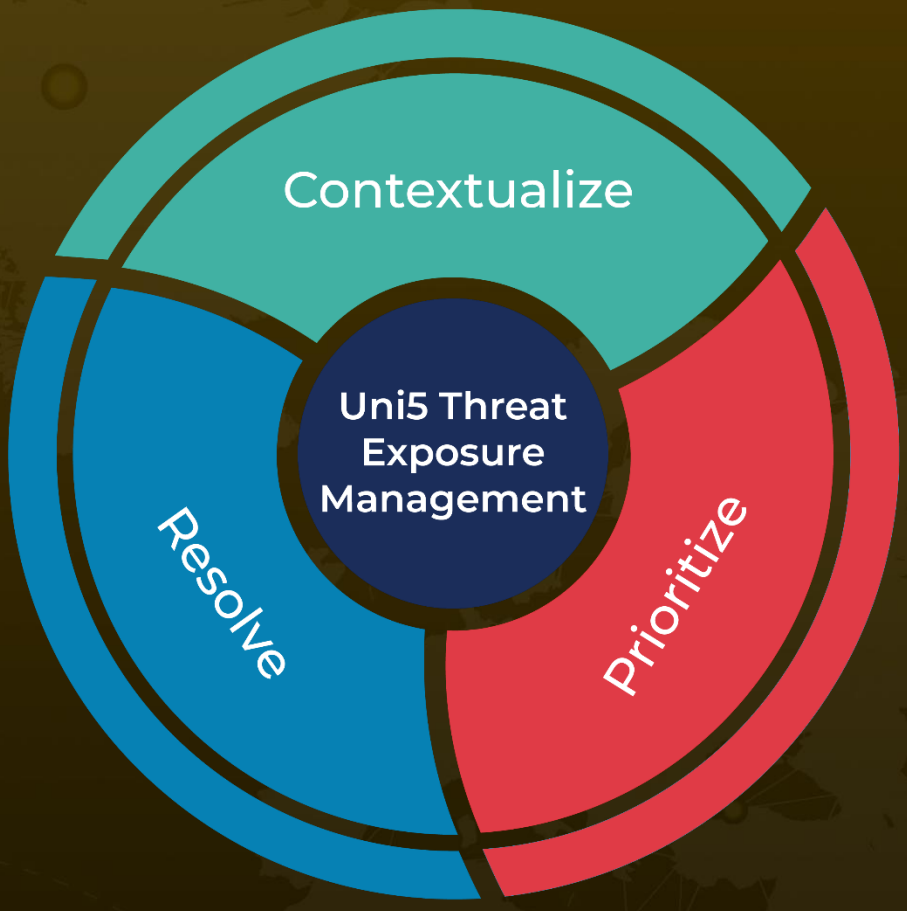
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 27, 2025 • 4:10 AM

More at www.hivepro.com