Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

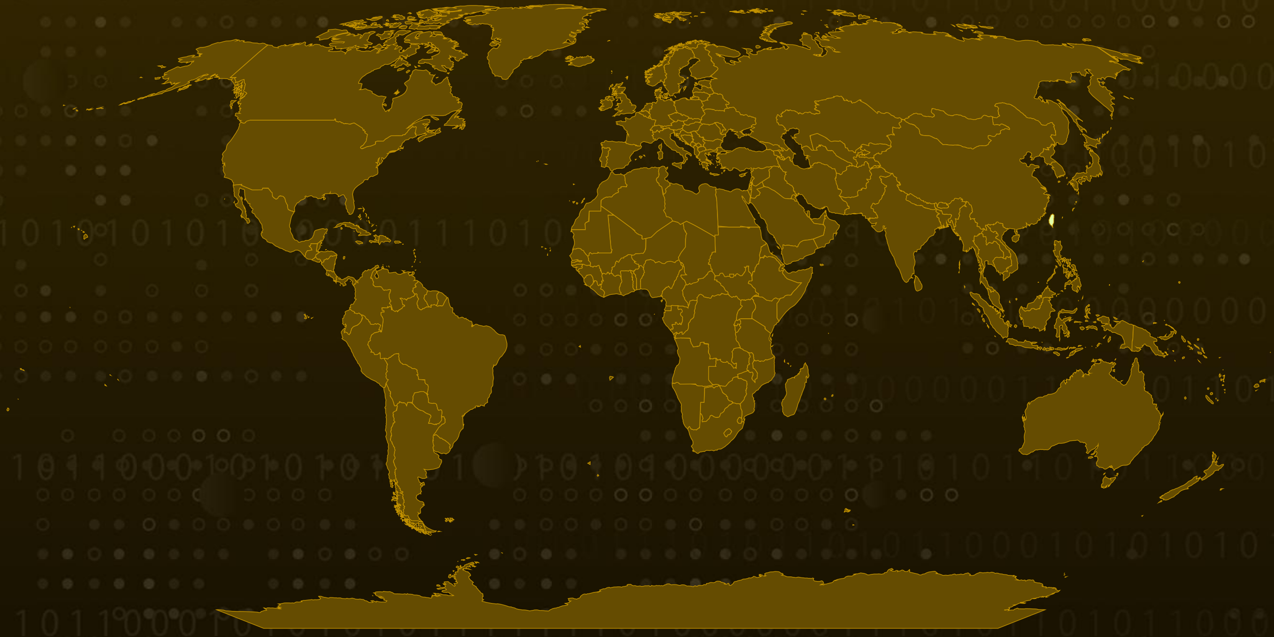
Stealth in the System: HoldingHands RAT Masquerades as Tax Bureau

Date of Publication	Admiralty Code	TA Number
June 18, 2025	A1	TA2025192

Summary

Attack Commenced: March 2025
Targeted Country: Taiwan
Affected Platforms: Microsoft Windows
Malware: HoldingHands RAT (aka Gh0stBins)
Attack: A stealthy cyberattack targeting Taiwanese users in early 2025 disguised itself as official tax emails, tricking victims into opening malware-laced attachments. Behind the scenes, a modified Remote Access Trojan called HoldingHands quietly hijacked systems, using layers of encryption, privilege escalation, and Windows system tools to evade detection and stay hidden. This highly targeted campaign evolved over time, with attackers refining their methods and using familiar-looking files to gain user trust while silently taking control of infected machines.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 In March 2025, a targeted phishing campaign emerged against organizations in Taiwan. Attackers posed as government agencies or business partners, sending deceptive emails themed around taxes, pensions, and invoices. These messages included ZIP file attachments that, once opened, initiated a multi-stage infection chain. Hidden within the archive was a malicious dynamic link library (DLL) which, when executed, enabled deeper system compromise. In the final stage, the attackers deployed HoldingHands (aka Gh0stBins), a remote access trojan (RAT) designed to maintain long-term access and control over infected systems.

#2 The phishing emails often included PDF attachments crafted to appear legitimate, encouraging recipients to click on embedded links. In some cases, the malware was hidden inside password-protected ZIP files to evade detection and analysis. Once extracted, these files triggered a sequence that quietly decrypted and launched malicious code in the background, using legitimate-looking programs to disguise its activity.

#3 The malware checked for signs of analysis, such as low system memory, and terminated itself if it detected a virtual environment. It also attempted to gain elevated privileges by mimicking trusted system processes. If successful, it created registry entries to mark the system as infected and dropped additional components into key system folders. To avoid reinfection or detection, the attack ceased if it found specific files indicating a prior compromise.

#4 A tampered Windows component was also used to ensure the malware only executed under specific conditions, for instance, when launched by trusted system processes and when antivirus software was inactive. After gaining persistence, the malware renamed and moved files within the system to survive reboots and continue operating undetected.

#5 This March activity aligns with an earlier campaign observed in January 2025, in which a targeted phishing operation against Taiwanese users delivered a variant of the **Winos 4.0** malware. The infrastructure and tactics used in both incidents suggest a single threat actor refining their tools and delivery methods. By leveraging stealth and layered infection strategies, the group maintains a strong foothold within targeted environments. The campaign's ultimate goal appears to be the theft of sensitive data, likely to support future attacks or broader cyberespionage objectives.

Recommendations

Be cautious with suspicious emails: Watch out for unexpected emails, especially ones that claim to be from government agencies or business partners. If you receive messages like fake tax notices or unexpected invoices, don’t click anything right away. Instead, confirm their legitimacy through trusted, official sources.

Think twice before opening ZIP attachments: Avoid opening ZIP file attachments especially if they're password-protected or contain multiple files. These are often used by attackers to sneak malware past security tools.

Limit user privileges: Restrict admin rights on user accounts. If malware does get in, limited privileges can help stop it from spreading or doing serious damage.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1036 Masquerading	T1204 User Execution
T1204.001 Malicious Link	T1574 Hijack Execution Flow	T1574.001 DLL	T1027 Obfuscated Files or Information

T1140 Deobfuscate/Decode Files or Information	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	T1497 Virtualization/Sandbox Evasion
T1082 System Information Discovery	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1656 Impersonation

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	154[.]91[.]85[.]204, 154[.]86[.]22[.]47, 156[.]251[.]17[.]17, 206[.]238[.]179[.]173, 206[.]238[.]220[.]60, 206[.]238[.]199[.]22, 154[.]91[.]85[.]201, 206[.]238[.]221[.]182, 206[.]238[.]196[.]32, 154[.]91[.]64[.]45, 206[.]238[.]115[.]207, 156[.]251[.]17[.]12, 107[.]149[.]253[.]183
Domains	00-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com, 6-1321729461[.]cos[.]ap-guangzhou[.]myqcloud[.]com, twzfte-1340224852[.]cos[.]ap-guangzhou[.]myqcloud[.]com, cq1tw[.]top, twcz[.]pro, twczb[.]com, twnc[.]ink, twnic[.]icu, twnic[.]ink, twnic[.]ltd, twnic[.]xin, twsa[.]top, twsw[.]cc, twsw[.]club, twsw[.]info, twsw[.]ink, twsw[.]ltd, twsw[.]pro, twsww[.]vip,

TYPE	VALUE
Domains	twsww[.]xin, twswz[.]top, twswzz[.]xin, twtgtw[.]net, twzfw[.]vip
SHA256	6558dfb070421c674b377a0a6090593fa0c44d5b0dec5325a648583f92175ce2, d3a270d782e62574983b28bd35076b569a0b65236e7f841a63b0558f2e3a231c, a8430ce490d5c5fab1521f3297e2d277ee7e7c49e7357c208878f7fd5f763931, 7d3f352ded285118e916336da6e6182778a54dc88d4fb7353136f028ac9b81e0, 143f434e3a2cac478fb672b77d6c04cdf25287d234a52ee157f4f1a2b06f8022, c25e80cd10e7741b5f3e0b246822e0af5237026d5227842f6cf4907daa039848, 7263550339c2a35f356bb874fb3a619b76f2d602064beada75049e7c2927a6dc, a8b6c06daeede6199e69f4cafd79299219def5bf913a31829dede98a8ad2aaa9, 6fcd6aef0678d3c6d5f8c2cb660356b25f68c73e7ee24fbb721216a547d17ffa, ed72721837c991621639b4e86ffe0c2693ef1a545741b5513d204a1e3e008d8c, 65edd9e1a38fd3da79c8a556eb2c7c595125ffec9f7483e2e6e189a08cc5d412, 0a0375648bc9368bccfd3d657d26976d5b1f975381d1858d001404d807334058, e809582faccdd27337aa46b4a11dd11f5d0c7d7428ebdc8c895ea80777e4da5f, 59d2433264d8ec9e9797918be3aa7132dbeb71e141f6e5c64c0d6f1cb4452934, ac957ba4796f06c4bf0c0afb8674bbeb30eb95cef85bc68ced3ee1aa30e3acff, 9296adb71bc98140a59b19f68476d45dbb38cc60b9e263d07d14e7178f195989, 636c2ccffce7d4591b0d5708469070b839f221400b38189c734004641929ae05, 31ffa4e3638c9e094275051629cc3ac0a8c7d6ae8415bbfcacc4c605c7f0df39, da3deea591b59b1a0f7e11db2f729a263439a05f3e8b0de97bbac99154297cea, e2269b38655a4d75078362856c16594e195cd647c56b8c55883b8e1286baa658, 52632d9e24f42c4651cf8db3abc37845e693818d64ab0b11c235eddf8e011b2f, 7200155f3e30dbbd4c4c26ce2c7bd4878ab992b619d80b43c0bd9e17390082fc,

TYPE	VALUE
SHA256	e516b102a2a6001eafb055e42feb9000691e2353c7e87e34ddaa99d7d8af16fd, a9ddd4e4d54336ce110fdc769ff7c4940f8d89b45ee8dc24f56fc3ea00c18873, a12d17cca038cdbf79b72356e5d20b17722c7b20bd2ee308601bac901890f3f4, b1ac2178c90c8eafd8121d21acbae7a0eb0cbc156d4a5f692f44b28856a23481, a6c1629b4450f713b02d24f088c4f26b0416c6a7924dcf0477425f3a67a2e3ff, 3ce81c163ddedb132116cdf92aae197ced0b94f3fc3d1036f5c41b084a256a03, a19fdfc131e8fbe063289c83a3cdefb9fb9fb6f1f92c83b892d3519a381623db, db15f45f69f863510986fb2198a8a6b3d55d8ccc8a2ed4bb30bc27bdd1bf151c, bf1a7938f61a9905e1b151c7a5f925a2ce3870b7c3e80f6e0fc07715bdc258b7, f42c6949c6d8ecf648bacca08cde568f11ec2663221a97dae5fbf01218e8775a

References

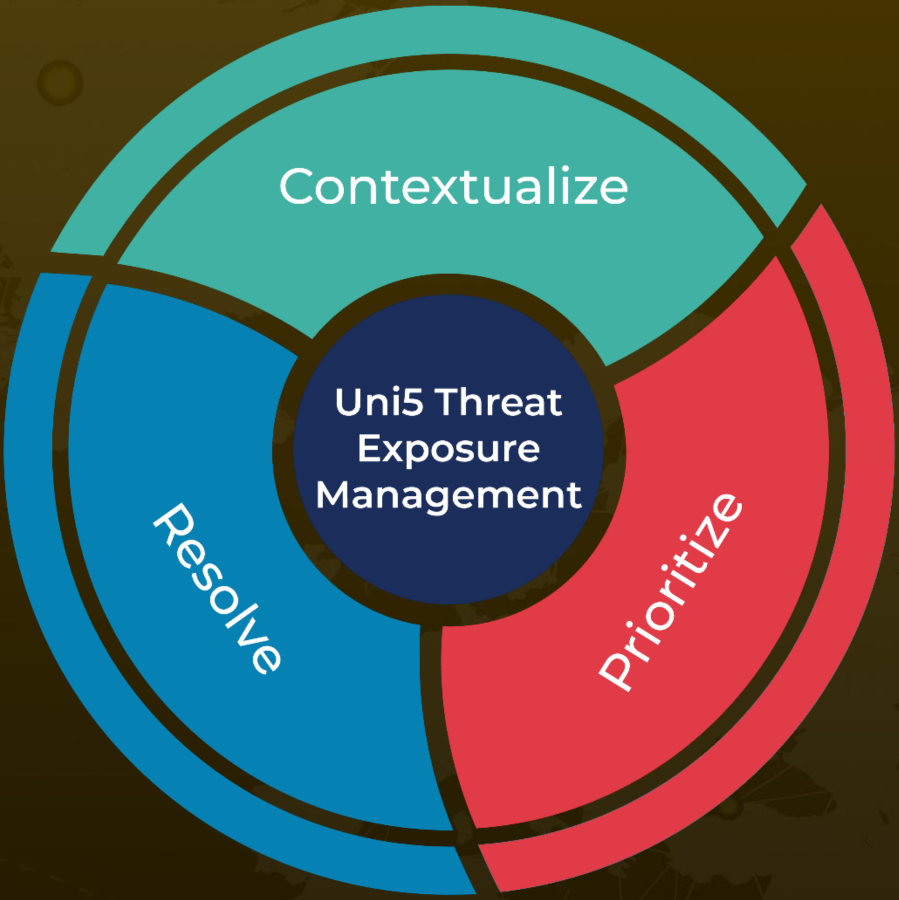
https://www.fortinet.com/blog/threat-research/threat-group-targets-companies-in-taiwan

https://hivepro.com/threat-advisory/winos4-0-stealthy-malware-campaign-targets-taiwanese-enterprises/

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

June 18, 2025 • 6:00 AM

More at www.hivepro.com