Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

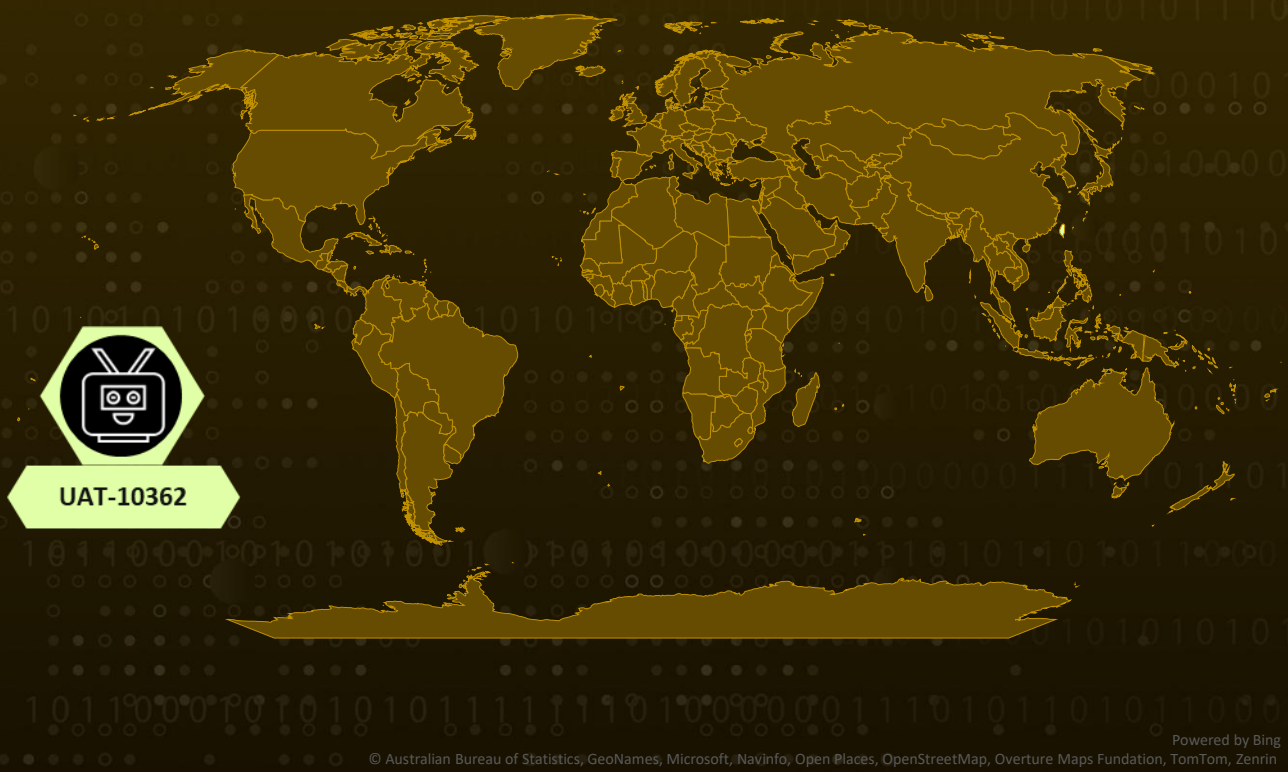
UAT-10362 Deploys LucidRook Malware Against Taiwanese NGOs

Date of Publication	Admiralty Code	TA Number
April 10, 2026	A1	TA2026096

Summary

First Seen: October 2025
Targeted Region: Taiwan
Targeted Platforms: Windows (64-bit)
Targeted Products: Microsoft Windows, Deployment Image Servicing and Management (DISM), Trend Micro Worry-Free Business Security Services (impersonated)
Targeted Industries: Non-Governmental Organizations (NGOs), Education (Universities)
Threat Actor: UAT-10362
Malware: LucidRook, LucidPawn, LucidKnight
Attack: UAT-10362 is a targeted threat group conducting spear-phishing campaigns against Taiwanese organizations by sending convincing emails that deliver password-protected malicious archives. The operation uses low-cost infrastructure and staged tools, including a reconnaissance component, indicating a structured approach to profiling and exploiting targets while minimizing detection.

Attack Regions



Attack Details

#1

A newly identified threat group, UAT-10362, has been linked to targeted spear-phishing attacks against Taiwanese NGOs and likely universities. The attackers send carefully crafted emails that appear legitimate, using trusted mail systems. These messages include shortened links that lead to password-protected archive files, with the password provided in the email itself. Inside, two attack paths are used: one disguises a malicious shortcut file as a PDF, while the other uses a fake security application. Both methods trick users into launching the malware while showing decoy content to avoid suspicion.

#2

Once triggered, the attack quietly deploys its payload through layered techniques designed to evade detection. In one method, a shortcut file runs hidden scripts that abuse legitimate Windows tools to load malicious components. These components unpack encrypted files, rename them to resemble trusted programs, and establish persistence by placing shortcuts in startup folders. In the alternate method, a fake executable drops multiple files into the system and displays a harmless message to mislead the user. The malware also checks the system language and only proceeds if it detects Traditional Chinese, narrowing its focus and avoiding analysis environments.

#3

At the core of the attack is LucidRook, a complex and heavily concealed malware built as a Windows DLL. It integrates a Lua interpreter and additional compiled libraries, allowing it to run flexible and customizable code. The malware hides its internal logic through layered obfuscation and disables certain features to make analysis harder. Once active, it gathers detailed system data, including user information, installed programs, and running processes. This data is encrypted and packaged before being sent out of the system.

#4

For communication, the malware relies on compromised FTP servers based in Taiwan. These servers, often belonging to small businesses with exposed credentials, are used to both send stolen data and retrieve further instructions. Additional signals, such as DNS requests, confirm successful infection. Investigators also identified a related tool, LucidKnight, which collects basic system details and sends them via email. This suggests a staged approach, where targets are first evaluated before more advanced malware like LucidRook is deployed.

Recommendations

Deploy Detection Rules for DLL Side-Loading via DISM: Create endpoint detection rules to monitor for suspicious sideloading of DismCore.dll by non-standard DISM executables, particularly when launched from unusual directories such as WindowsApps or ProgramData rather than the legitimate System32 path.

Monitor for Anomalous FTP Traffic: Implement network monitoring rules to detect outbound FTP connections from endpoints to external servers, especially those transferring ZIP archives named archive4.zip or archive1.zip, as LucidRook uses plaintext FTP for C2 communications.

Detect LOLBAS Abuse of PowerShell Pester Framework: Create detection logic for suspicious execution of the Pester Build.bat script (located in C:\Program Files\WindowsPowerShell\Modules\Pester) being invoked by LNK files or with unusual command-line arguments pointing to hidden directories.

Restrict Execution from Non-Standard Paths: Implement application whitelisting policies to prevent execution of binaries from %APPDATA%\Local\Microsoft\WindowsApps and C:\ProgramData directories that are not part of approved software inventories, targeting LucidRook's persistence and staging locations.

Implement Language-Based Execution Anomaly Detection: Deploy monitoring to detect malware that queries GetUserDefaultUILanguage() as a pre-execution check, as this geofencing technique is used by LucidPawn to restrict execution to Traditional Chinese environments.

Establish DNS Monitoring for OAST Services: Monitor and alert on DNS queries to known OAST service domains such as dnslog[.]ink and digimg[.]store, as threat actors abuse these services to verify successful exploitation without deploying dedicated infrastructure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1027: Obfuscated Files or Information	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1497: Virtualization/Sandbox Evasion	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1071: Application Layer Protocol	T1071.002: File Transfer Protocols
	T1105: Ingress Tool Transfer	
	T1102: Web Service	
Exfiltration	T1048: Exfiltration Over Alternative Protocol	T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol
	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d49761cdbea170dd17255a958214db392dc7621198f95d5eb5749859c603100a, adf676107a6c2354d1a484c2a08c36c33d276e355a65f77770ae1ae7b7c36143, b480092d8e5f7ca6aebdeaae676ea09281d07fc8ccf2318da2fa1c01471b818d, c2d983d3812b5b6d592b149d627b118db2debd33069efe4de4e57306ba42b5dc, 6aba7b5a9b4f7ad4203f26f3fb539911369aeef502d43af23aa3646d91280ad9, bdc5417ffba758b6d0a359b252ba047b59aacf1d217a8b664554256b5adb071d, f279e462253f130878ffac820f5a0f9ac92dd14ad2f1e4bd21062bab7b99b839, 166791aac8b056af8029ab6bdeec5a2626ca3f3961fdf0337d24451cfccfc05d, 11ae897d79548b6b44da75f7ab335a0585f47886ce22b371f6d340968dbed9ae, edb25fed9df8e9a517188f609b9d1a030682c701c01c0d1b5ce79cba9f7ac809, 0305e89110744077d8db8618827351a03bce5b11ef5815a72c64eea009304a34, d8bc6047fb3fd4f47b15b4058fa482690b5b72a5e3b3d324c21d7da4435c9964, aa7a3e8b59b5495f6eebc19f0654b93bb01fd2fa2932458179a8ae85fb4b8ec1, fd11f419e4ac992e89cca48369e7d774b7b2e0d28d0b6a34f7ee0bc1d943c056
IPv4	1[.]34[.]253[.]131, 59[.]124[.]71[.]242
Domain	d[.]2fcc7078[.]digimg[.]store
Email	fexopuboriw972[@]gmail[.]com, crimsonanabel[@]powerscrews[.]com

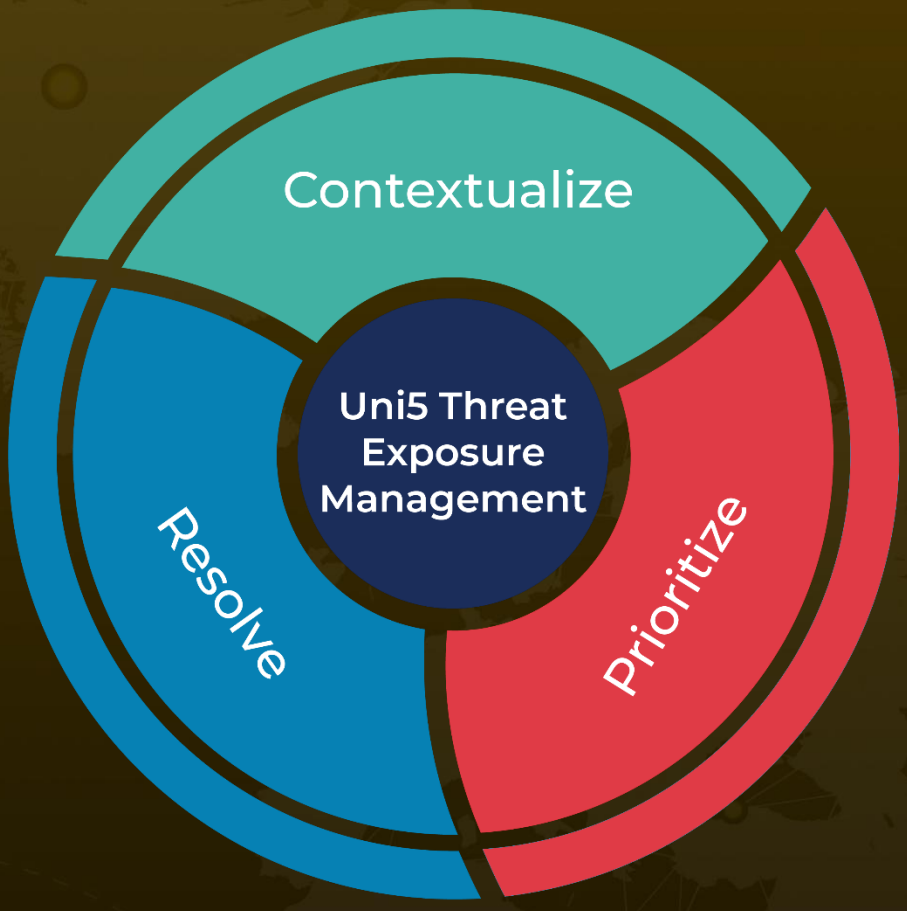
References

https://blog.talosintelligence.com/new-lua-based-malware-lucidrook/

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

April 10, 2026 • 06:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com