Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

UTA0388: AI-Powered Targeted Operations Leveraging GOVERSHELL

Date of Publication

October 10, 2025

Admiralty Code

A1

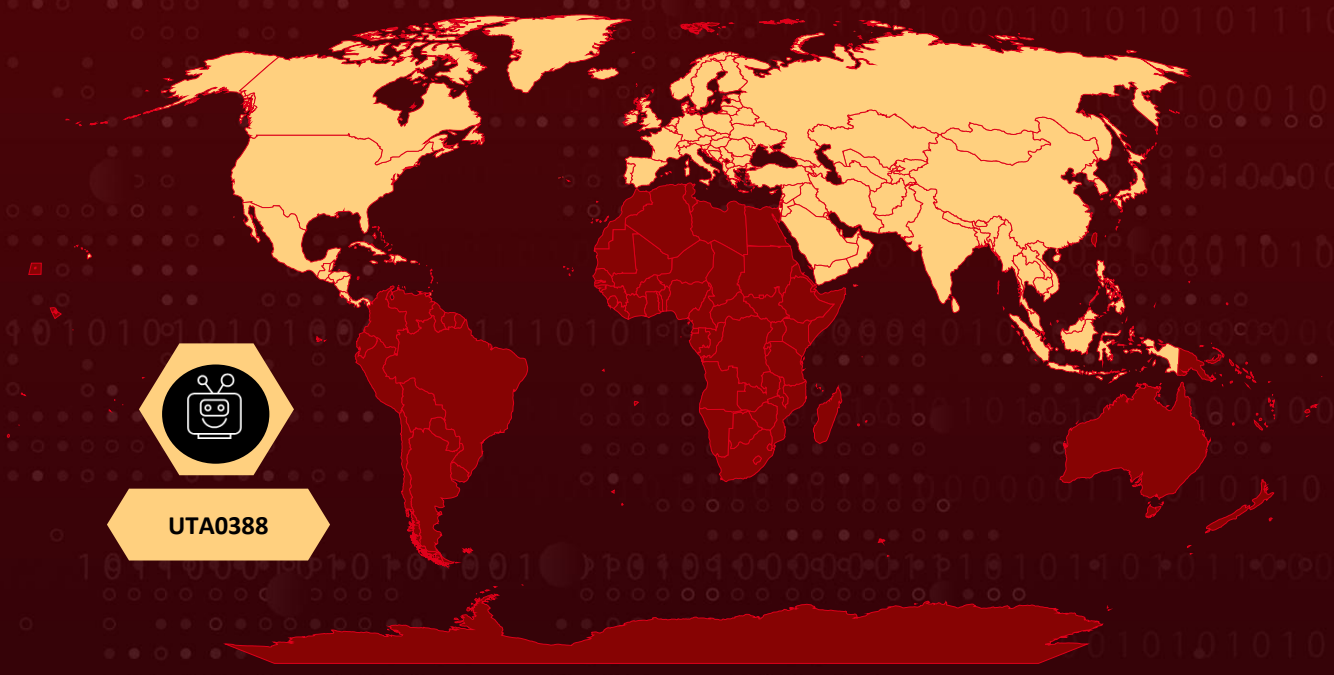
TA Number

TA2025311

Summary

First Seen: March 2025
Targeted Countries: North America, Asia, and Europe
Targeted Platforms: Windows
Targeted Industries: Manufacturing, Investment firms, Semiconductor
Threat Actor: UTA0388 (aka UNK_DropPitch)
Malware: GOVERSHELL
Attack: The China-aligned threat actor UTA0388, also known as UNK_DropPitch, has integrated Large Language Models (LLMs) like ChatGPT into its cyber operations to accelerate and scale targeted attacks. The group focuses on intelligence gathering and economic espionage, primarily against investment firms and Taiwanese semiconductor companies. Its operations rely on multilingual, rapport-building spear phishing, delivering malicious archives that exploit search-order hijacking to deploy the GOVERSHELL backdoor. By leveraging AI for phishing content and malware refinement, UTA0388 has enhanced the sophistication and efficiency of its campaigns.

Attack Regions



Attack Details

#1

The China-nexus threat actor UTA0388, also referred to as UNK_DropPitch, has recently drawn attention for incorporating Large Language Models (LLMs) such as ChatGPT into its operational workflow. While this does not introduce fundamentally new offensive capabilities, it significantly increases the speed and scale of campaign preparation. UTA0388 primarily conducts intelligence-gathering and economic espionage, focusing on major investment firms and companies within the Taiwanese semiconductor industry.

#2

The group's operations revolve around highly tailored, multilingual spear-phishing campaigns. Recent campaigns indicate a shift toward "rapport-building phishing," in which operators establish trust through fabricated personas and multilingual correspondence, often in English, Chinese, or Japanese, before delivering malicious links hosted on legitimate cloud services such as Netlify or OneDrive.

#3

The payload is typically delivered as a compressed archive (ZIP or RAR) containing a benign-looking executable paired with a malicious DLL. The actor abuses Windows search-order hijacking to force the legitimate program to load the hostile library, deploying a custom backdoor known as GOVERSHELL, an evolution of the earlier HealthKick malware. This implant provides persistent command-and-control (C2) access, supporting reconnaissance and data exfiltration activities.

#4

The strategic integration of LLMs by UTA0388 to generate realistic, multilingual phishing content and refine malware code represents a significant evolution in threat actor tradecraft. It demonstrates how advanced groups are leveraging AI to enhance existing operations and accelerate development cycles. While some associated infrastructure and accounts have been disrupted, this activity illustrates the growing role of AI-driven automation in state-linked intrusion campaigns.

Recommendations

Enhance Email Security: Deploy advanced anti-phishing solutions including sandboxing, URL rewriting, and real-time link analysis. Provide ongoing user awareness training focused on spear-phishing and social engineering tactics specific to targeted industries like semiconductor and finance.

Implement Strict Access Controls: Enforce least privilege principles, multi-factor authentication (MFA), and segmentation to limit lateral movement in case of compromise. Regularly review user access rights especially for critical systems and sensitive data repositories.

Deploy Endpoint Detection and Response (EDR): Utilize EDR solutions across Windows and relevant platforms to detect and respond to malware activities, including lateral shell sessions, DLL side-loading, and anomalous remote management tool usage.

Harden Infrastructure: Patch all systems promptly and apply security best practices for network devices, endpoint software, and cloud environments. Enable logging and monitoring for unusual activities notably backup deletions or event log tampering.

Network Monitoring: Detect anomalous outbound connections, particularly encrypted or unusual protocols to cloud-hosted or foreign domains. Use behavioral analytics to flag unusual internal communications, potential data exfiltration, or lateral movement activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0011 Command and Control
TA0005 Defense Evasion	TA0040 Impact	T1574.001 DLL Search Order Hijacking	T1574 Hijack Execution Flow

T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1036 Masquerading	T1027 Obfuscated Files or Information
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1071.004 DNS	T1203 Exploitation for Client Execution
T1588.007 Artificial Intelligence	T1588 Obtain Capabilities	T1598.003 Spearphishing Link	T1566.001 Spearphishing Attachment
T1566 Phishing	T1204 User Execution	T1204.002 Malicious File	T1486 Data Encrypted for Impact
T1059 Command and Scripting Interpreter			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:Port	80[.]85[.]154[.]48[:]443, 80[.]85[.]157[.]117[:]443, 82[.]118[.]16[.]173[:]443
IPv4	104[.]194[.]152[.]137, 104[.]194[.]152[.]152, 185[.]144[.]28[.]68, 31[.]192[.]234[.]22, 45[.]141[.]139[.]222, 74[.]119[.]193[.]175, 80[.]85[.]156[.]234, 80[.]85[.]154[.]48, 80[.]85[.]157[.]117, 82[.]118[.]16[.]173

TYPE	VALUE
Hostname	azure-app[.]store, twmoc[.]info, windows-app[.]store, cdn-apple[.]info, sliddeshare[.]online, doccloude[.]info
SHA256	2ffe1e4f4df34e1aca3b8a8e93eee34bfc4b7876cedd1a0b6ca5d63d89a26301, 4c041c7c0d5216422d5d22164f83762be1e70f39fb8a791d758a816cdf3779a9, 53af82811514992241e232e5c04e5258e506f9bc2361b5a5b718b4e4b5690040, 88782d26f05d82acd084861d6a4b9397d5738e951c722ec5afed8d0f6b07f95e, 998e314a8babf6db11145687be18dc3b8652a3dd4b36c115778b7ca5f240aae4, a5ee55a78d420dbba6dec0b87ffd7ad6252628fd4130ed4b1531ede960706d2d, ad5718f6810714bc6527cc86d71d34d8c556fe48706d18b5d14f0261eb27d942, fbade9d8a040ed643b68e25e19cba9562d2bd3c51d38693fe4be72e01da39861, 7d7d75e4d524e32fc471ef2d36fd6f7972c05674a9f2bac909a07dfd3e19dd18, 0414217624404930137ec8f6a26aebd8a3605fe089dbfb9f5aaaa37a9e2bad2e, 126c3d21a1dae94df2b7a7d0b2f0213eeeec3557c21717e02ffaed690c4b1dbd
URLs	hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ER_XG5FDkURHtsmna8vOQrIBRODKiQBKYJVKnI-kGKwX0A, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ESz4UV9JeOhOp8kiWd0Ie10ByH7eUdSRlBy2NCiNeo2LYw, hxxp[:]//1drv[.]ms/u/c/f9e3b332ce488781/Eap6_fxYFP5Eh1ZKDZaf8lMBjJNcfdba4MVcr4YfKj674w?e=fgNIj4, hxxp[:]//1drv[.]ms/u/c/F703BC98FAB44D61/ERpeLpJlb7FAkbfyuffpFJYBZ-8u2MmQH6LW5xH86B4M8w, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/rar, hxxp[:]//aesthetic-donut-1af43s2[.]netlify[.]app/file/zip, hxxp[:]//animated-dango-0fa8c8[.]netlify[.]app/file/Taiwan%20Intro[.]zip, hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/rar, hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/file/zip,

TYPE	VALUE
URLs	hxxp[:]//aquamarine-choux-46cb43[.]netlify[.]app/index/file/[PDF]202507_Please_check_the_document[.]zip, hxxp[:]//dainty-licorice-db2b1e[.]netlify[.]app/file/zip, hxxp[:]//dulcet-mooncake-36558c[.]netlify[.]app/file/zip, hxxp[:]//harmonious-malabi-a8ebfa[.]netlify[.]app/file/Taiwan%20Intro[.]rar, hxxp[:]//hllowrodcanlhelipme[.]netlify[.]app/file/zip, hxxp[:]//jazzy-biscotti-68241f[.]netlify[.]app/files/Intro-Doc[.]rar, hxxp[:]//ln5[.]sync[.]com/4[.]0/dl/100016f90#3d5wrb4z-hfb4iz3m-qmjzsqnq-39rn3vjv, hxxp[:]//loveusa[.]netlify[.]app/file/rar, hxxp[:]//pulicwordfiledownlos[.]netlify[.]app/file/rar, hxxp[:]//spontaneous-selkie-d3346f[.]netlify[.]app/file/zip, hxxp[:]//statuesque-unicorn-09420f[.]netlify[.]app/r, hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/rar, hxxp[:]//subtle-klepon-d73b9b[.]netlify[.]app/file/zip, hxxp[:]//vocal-crostata-86ebbf[.]netlify[.]app/files/zip, wss[:]//api[.]twmoc[.]info/ws, wss[:]//onedrive[.]azure-app[.]store/ws, wss[:]//outlook[.]windows-app[.]store/ws, www[.]twmoc[.]info, hxxp[:]//app-site-association[.]cdn-apple[.]info[:]443/updates[.]rss

References

https://www.volexity.com/blog/2025/10/08/apt-meets-gpt-targeted-operations-with-untamed-llms/

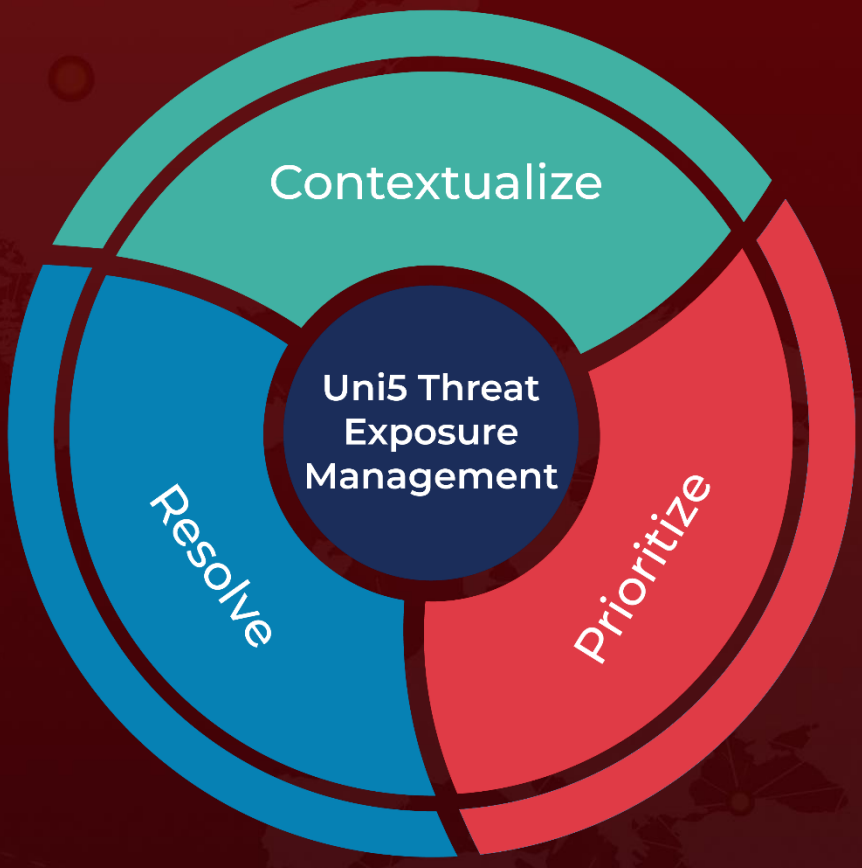
https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

https://hivepro.com/threat-advisory/taiwan-semiconductor-firms-under-siege-by-chinese-cyber-operations/

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

October 10, 2025 . 8:30 AM

More at www.hivepro.com