Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

ZipLine Campaign Spins Web Around U.S. Supply Chain Manufacturers with MixShell

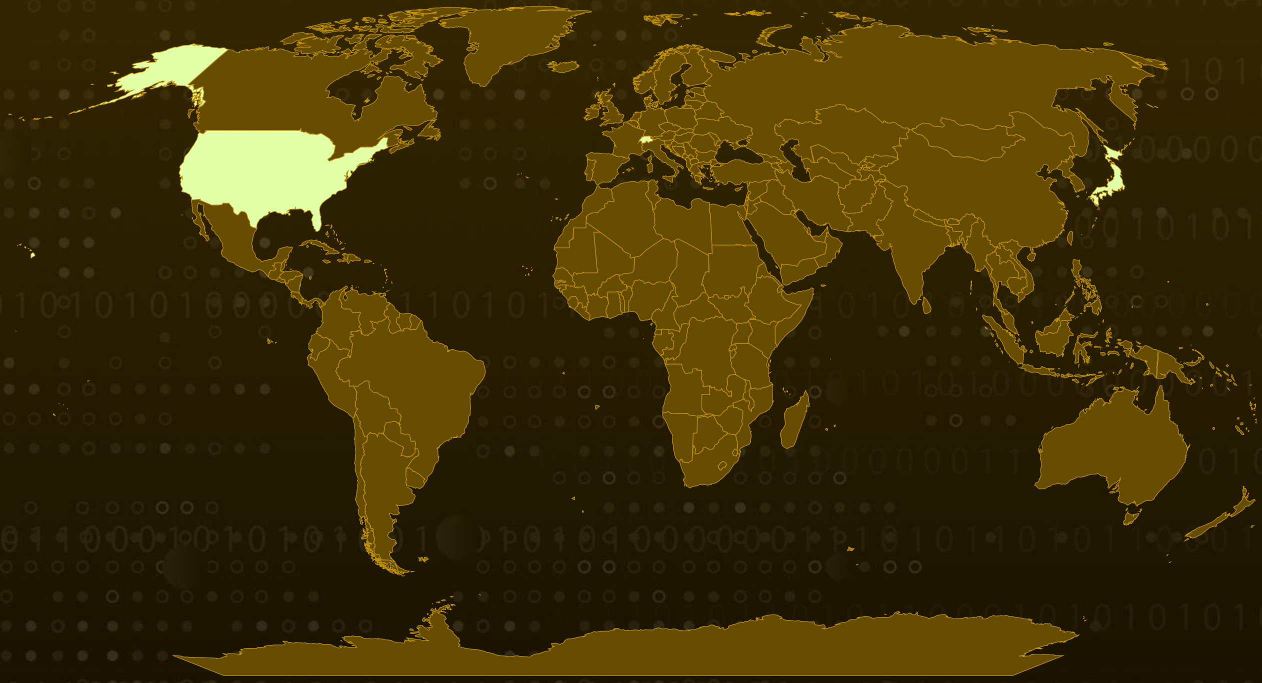
Date of Publication	Admiralty Code	TA Number
August 28, 2025	A1	TA2025261

Summary

Campaign: ZipLine
Malware: MixShell
Targeted Regions: United States, Singapore, Japan, Switzerland
Targeted Industries: Manufacturing, Semiconductors, Consumer goods, Media, Construction, Engineering, Aerospace, Defense, Biotech, Pharmaceuticals, Energy, Utilities, Electronics

Attack: The ZipLine campaign is a targeted social engineering operation against U.S. supply chain - critical manufacturers, where attackers build trust through extended, business-like conversations initiated via company "Contact Us" forms. Through credible email exchanges and pretexts such as NDAs or AI transformation initiatives, they establish legitimacy before distributing malicious ZIP archives hosted on trusted platforms, which ultimately deploy the in-memory malware known as MixShell.

Attack Regions



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

Attack Details

#1

A social engineering campaign known as ZipLine is actively targeting supply chain critical manufacturing companies, primarily in the United States. The attackers disguise their operations as legitimate business interactions, ultimately delivering a custom in-memory malware implant called MixShell.

#2

Unlike traditional phishing schemes that rely on unsolicited emails, ZipLine reverses the approach. The attackers initiate contact through a company's public "Contact Us" form, tricking the victim into starting the conversation. From there, they sustain convincing, business-oriented email exchanges for up to two weeks before introducing a malicious ZIP file.

#3

To strengthen credibility, the attackers often pose as potential business partners and request the signing of a Non-Disclosure Agreement (NDA). Once trust is established, they deliver a ZIP archive hosted on the trusted Heroku platform. Inside the archive lies a weaponized Windows shortcut (LNK) file, which executes a PowerShell-based loader. This loader deploys MixShell, an in-memory implant equipped with DNS-based command-and-control (C2) capabilities, enhanced persistence, and stealth mechanisms.

#4

Once deployed, MixShell provides the attackers with a range of capabilities, including remote command execution, file operations, reverse proxying, stealth persistence, and deeper infiltration into the network. A PowerShell variant of MixShell further enhances evasion through anti-debugging, sandbox bypassing, scheduled task persistence, and advanced reverse proxy features. The ultimate motives of the ZipLine campaign remain unclear.

#5

Recent waves of the campaign show an evolution in tactics. A new variation leverages an AI transformation pretext, in which the attacker claims to support the target organization in implementing AI-driven operational efficiencies. Posing as an internal initiative, the phishing email frames the request as an "AI Impact Assessment" survey. To add urgency and legitimacy, it suggests that company leadership specifically requested the recipient’s input to shape future decisions.

Recommendations

Strengthen Email and Communication Security: Monitor and flag unusual use of Contact Us forms that lead to prolonged unsolicited business conversations. Deploy advanced email filtering solutions capable of analyzing content for social engineering patterns, not just malicious attachments. Implement warning banners for emails originating from external sources, even when they appear business-oriented.

Control File and Attachment Handling: Restrict execution of Windows shortcut (LNK) files and PowerShell scripts from email attachments. Sandbox and automatically scan ZIP archives before they reach end-users, even if they are hosted on trusted platforms like Heroku.

Harden Endpoint and Network Defenses: Deploy EDR solutions capable of detecting in-memory implants, PowerShell-based loaders, and DNS tunneling activity. Monitor for abnormal DNS traffic patterns that may indicate command-and-control communications. Apply strict controls on persistence mechanisms, such as scheduled tasks and reverse proxy configurations.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**T1594** Search Victim-Owned Websites	**T1190** Exploit Public-Facing Application

T1566 Phishing	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1204 User Execution	T1204.002 Malicious File	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1055 Process Injection	T1140 Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	T1036 Masquerading	T1082 System Information Discovery	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1071.004 DNS	T1090 Proxy	T1090.001 Internal Proxy
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e69d8b96b106816cb732190bc6f8c2693aecb6056b8f245e2c15841fcb48ff94, d39e177261ce9a354b4712f820ada3ee8cd84a277f173ecfbd1bf6b100ddb713, f531bec8ad2d6fddef89e652818908509b7075834a083729cc84eef16c6957d2, 2c7bc0ebbbfa282fc3ed3598348d361914fecfea027712f47c4f6cfcc705690f, 71dec9789fef835975a209f6bc1a736c4f591e5eeab20bdff63809553085b192, 83b27e52c420b6132f8034e7a0fd9943b1f4af3bdb06cdbb873c80360e1e5419, f5a80b08d46b947ca42ac8dbd0094772aa3111f020a4d72cb2edc4a6c9c37926,

TYPE	VALUE
SHA256	15d024631277f72df40427b8c50e354b340fac38b468f34826cc613b4650e74c, 155bccbd11066ce5bf117537d140b920f9b98eaa0d3b86bdc8a04ac702a7a1ef, 4dcff9a3a71633d89a887539e5d7a3dd6cc239761e9a42f64f42c5c4209d2829, d6e1e4cc89c01d5c944ac83b85efa27775103b82fece5a6f83be45e862a4b61e, 81c1a8e624306c8a66a44bfe341ec70c6e3a3c9e70ac15c7876fcbbe364d01cd, 36b065f19f1ac2642c041002bc3e28326bec0aa08d288ca8a2d5c0d7a82b56e6, f44107475d3869253f393dbcb862293bf58624c6e8e3f106102cf6043d68b0af
Domains	lvprocurement[.]com, kprocurement[.]com, lamyconsulting[.]com, trilineconsulting[.]com, hancockconsulting[.]com, caultonconsulting[.]com, chipmanconsulting[.]com, kgmstrategy[.]com, crosleyconsulting[.]com, humcrm[.]com, tollcrm[.]com, atriocrm[.]com, vnrsales[.]com, zappiercrm[.]com, crmforretailers[.]com
IPv4	172[.]210[.]58[.]69, 212[.]83[.]190[.]143, 5[.]180[.]221[.]108, 185[.]180[.]221[.]108
URLs	hxxps[:]//signstream-docs-de3fa399b173[.]herokuapp[.]com, hxxps[:]//collab-sign-8e36fa762841[.]herokuapp[.]com, hxxps[:]//viewshare-4a47630892e1[.]herokuapp[.]com, hxxps[:]//legal-sign-8ec8b9f1edb2[.]herokuapp[.]com, hxxps[:]//docsign-hub-3295a03470c3[.]herokuapp[.]com, hxxps[:]//signflow-e15eda21396d[.]herokuapp[.]com, hxxps[:]//webmailapp-0e6cff4089a4[.]herokuapp[.]com, hxxps[:]//clear-sign-e69444a8e4ea[.]herokuapp[.]com, hxxps[:]//signhub-view-09a16562134b[.]herokuapp[.]com, hxxps[:]//mail-serve-9a5d4f13e3a7[.]herokuapp[.]com,

TYPE	VALUE
URLs	hxxps[:]//docvault-share-665d141177ca[.]herokuapp[.]com, hxxps[:]//signlink-portal-37c581992418[.]herokuapp[.]com, hxxps[:]//signforge-a61a5975a04b[.]herokuapp[.]com, hxxps[:]//sharespace-link-360b265f3942[.]herokuapp[.]com, hxxps[:]//signtrack-docs-6a96b334b140[.]herokuapp[.]com, hxxps[:]//signcentral-vault-33ce0aff08dc[.]herokuapp[.]com, hxxps[:]//signcentral-7df32454744c[.]herokuapp[.]com, hxxps[:]//john-deer-apple-0c6f34d9c276[.]herokuapp[.]com

References

https://research.checkpoint.com/2025/zipline-phishing-campaign/

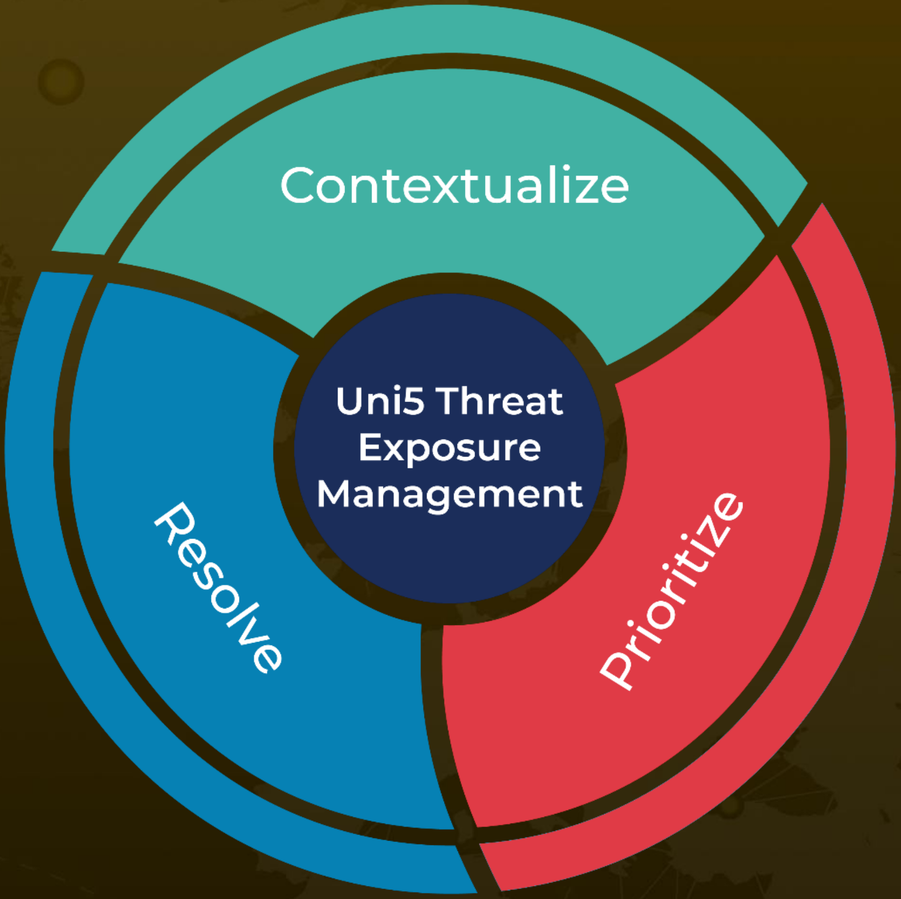
https://hivepro.com/threat-advisory/when-ai-turns-against-you-the-malvertising-trap-of-kling-ai/

https://hivepro.com/threat-advisory/operation-deceptive-prospect-romcoms-new-social-engineering-playbook/

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

August 28, 2025 • 5:30 AM

More at www.hivepro.com