Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

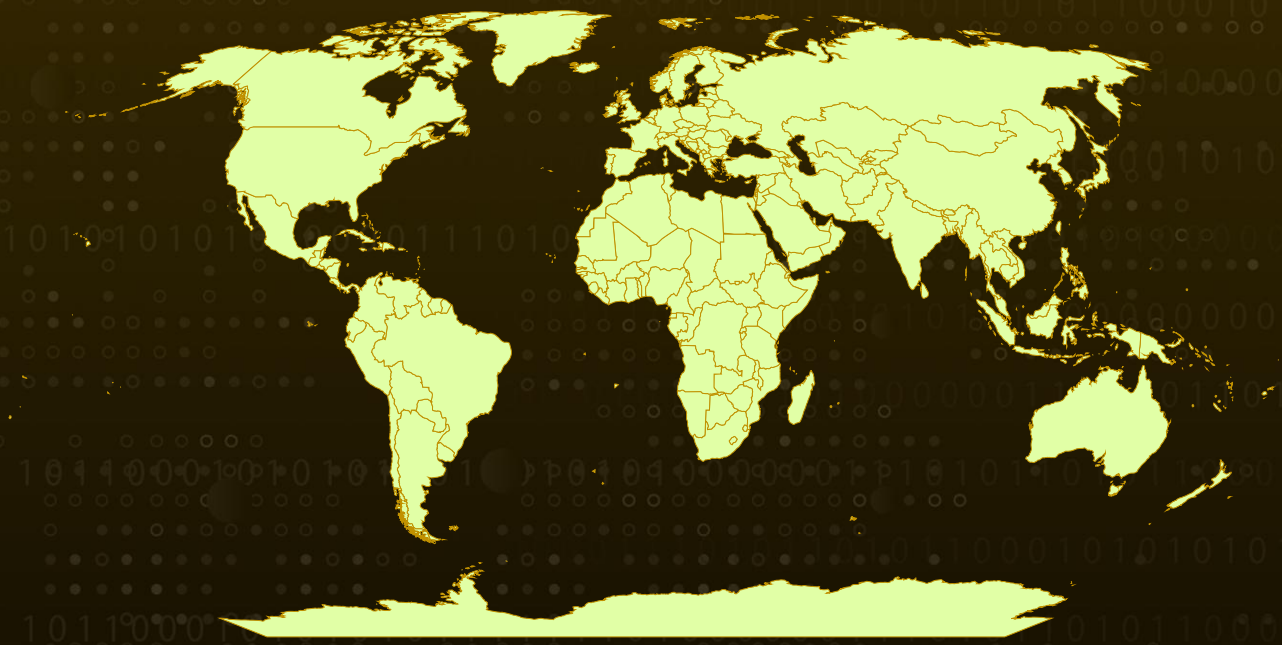
PoisonSeed: The Silent Harvest of Trust in Email Supply Chains

Date of Publication	Admiralty Code	TA Number
April 7, 2025	A1	TA2025103

Summary

Attack Discovered: March 2025
Targeted Countries: Worldwide
Targeted Industry: Enterprise organizations, VIP individuals, Cryptocurrency companies
Campaign: PoisonSeed
Attack: The PoisonSeed campaign is a clever and dangerous phishing scheme that's going after bulk email services like Mailchimp, SendGrid, and HubSpot. By crafting fake login pages that look identical to the real ones, the attackers steal credentials, grab massive email lists, and use them to blast out crypto scam emails. These emails contain "seed phrases" that seem legitimate but if a victim copies them into a wallet, they're unknowingly handing over control to the attackers. This tactic, known as seed phrase poisoning, gives the hackers access to wallets later, allowing them to drain funds over time.

Attack Regions



Attack Details

#1 The PoisonSeed campaign is a rapidly evolving phishing operation targeting both enterprise users and individuals, extending beyond the cryptocurrency industry. Threat actors compromise CRM and bulk email platforms like Mailchimp, SendGrid, Hubspot, and Zoho, crafting convincing phishing pages that closely mimic legitimate login portals. Once credentials are harvested, attackers export valuable email lists and use them to distribute phishing spam at scale. Their goal is to carry out cryptocurrency seed phrase poisoning, tricking victims into copying fake wallet recovery phrases into new wallets, phrases the attackers can later use to steal funds.

#2 In a notable incident in March 2025, Akamai's SendGrid account was compromised and used to send cryptocurrency phishing emails impersonating Coinbase. These emails falsely claimed that Coinbase was moving to self-custodial wallets, encouraging users to enter fake seed phrases. The attackers then exploited these phrases to "recover" and drain the victims' wallets.

#3 The campaign's infrastructure is linked to dozens of phishing domains by analyzing unique WHOIS "State" field entries including obscenities to identify clusters of related domains. Many of these domains, were tied to sophisticated lures mimicking trusted brands like Ledger Wallet. It was also discovered reused file paths, in phishing kits across both bulk email provider impersonation and crypto wallet scams suggesting deeper coordination and shared infrastructure between the operations.

#4 PoisonSeed exhibits notable similarities to threat groups like Scattered Spider and CryptoChameleon both associated with "The Comm" but there's no conclusive link confirming it as part of the same collective. While reused domains and malicious WHOIS values mirror Scattered Spider's tactics, PoisonSeed's phishing kits show no code overlap with those groups. Instead, suggest it may be a distinct operation, potentially a new offshoot within The Comm or an unrelated actor emulating their methods.

#5 What sets PoisonSeed apart is its apparent automation in credential harvesting and abuse: once inside a targeted email platform, attackers generate new API keys for persistence and bulk-download mailing lists. Its blend of email platform breaches, convincing phishing pages, and supply chain impersonation highlights an increasingly common enterprise-aware, multi-stage phishing approach.

Recommendations

Strengthen Your Email Defenses: Use advanced email security tools that rely on AI to catch phishing emails, fake domains, and harmful attachments before they reach your team. These systems can spot red flags in real time and help stop threats at the door. Enable DMARC, DKIM, and SPF settings these act like ID checks for your emails, making it much harder for attackers to pretend they're you.

Never Share Your Seed Phrase Online: Treat your seed phrase like the keys to your safe never type it into a website or share it through email. A real crypto provider will never ask for it online. Only enter your seed phrase in secure, trusted wallets, ideally while offline. If someone's asking for it, it's a scam.

Use Only Official Wallet Apps & Always Verify Domains: Always download wallet apps or updates from trusted sources like the official website or verified app stores. Don't fall for fake upgrade prompts or firmware alerts that try to trick you into installing malware. And before logging into any crypto or email service, take a moment to double-check the URL.

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

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact	T1566 Phishing
T1584 Compromise Infrastructure	T1584.001 Domains	T1059 Command and Scripting Interpreter	T1059.007 JavaScript
T1587 Develop Capabilities	T1588 Obtain Capabilities	T1596 Search Open Technical Databases	T1596.002 WHOIS

T1036 Masquerading	T1195 Supply Chain Compromise	T1496 Resource Hijacking	T1586 Compromise Accounts
T1586.002 Email Accounts			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	active-mailgun[.]com, barefoots-api[.]com, cloudflare-sendgrid[.]com, complete-sendgrid[.]com, connect1-coinbase[.]com, connect5-coinbase[.]com, firmware-llive[.]com, firmware-server12[.]com, hubservices-crm[.]com, inquiry-loginp[.]com, iosjdfsmdkf[.]com, live-sso[.]com, mail-chimpservices[.]com, mailchimp-sso[.]com, mailchimp-ssologin[.]com, myaccount-hbspot[.]com, mysite-clflre[.]com, mysrver-chbackend[.]com, myw-cbw[.]com, mywallet-cbsmartw[.]com, mywallet-cbsmw[.]com, mywallet-cbupgrade[.]com, nikafk244[.]com, password-proxy-redirect[.]com, redirect-sso[.]com, response-crmsg[.]com, response-loginportal[.]com, response16-sendgrid[.]com, response20-sendgrid[.]com, responseinquiry-tos[.]com, responsesendgrid[.]com,

TYPE	VALUE
Domains	review-termsconditions[.]com, revokecblink[.]com, rseponse-manageprod[.]com, rseponse25-sendgrid[.]com, rseponsequery[.]com, server12-mchimp[.]com, server9-hubspot[.]com, server9-mailgun[.]com, server9-sendgrid[.]net, sso-account[.]com, sso-signon[.]com, support-zoho[.]com, swallet-coinbase[.]com
IPv4	212[.]224[.]88[.]188, 86[.]54[.]42[.]92

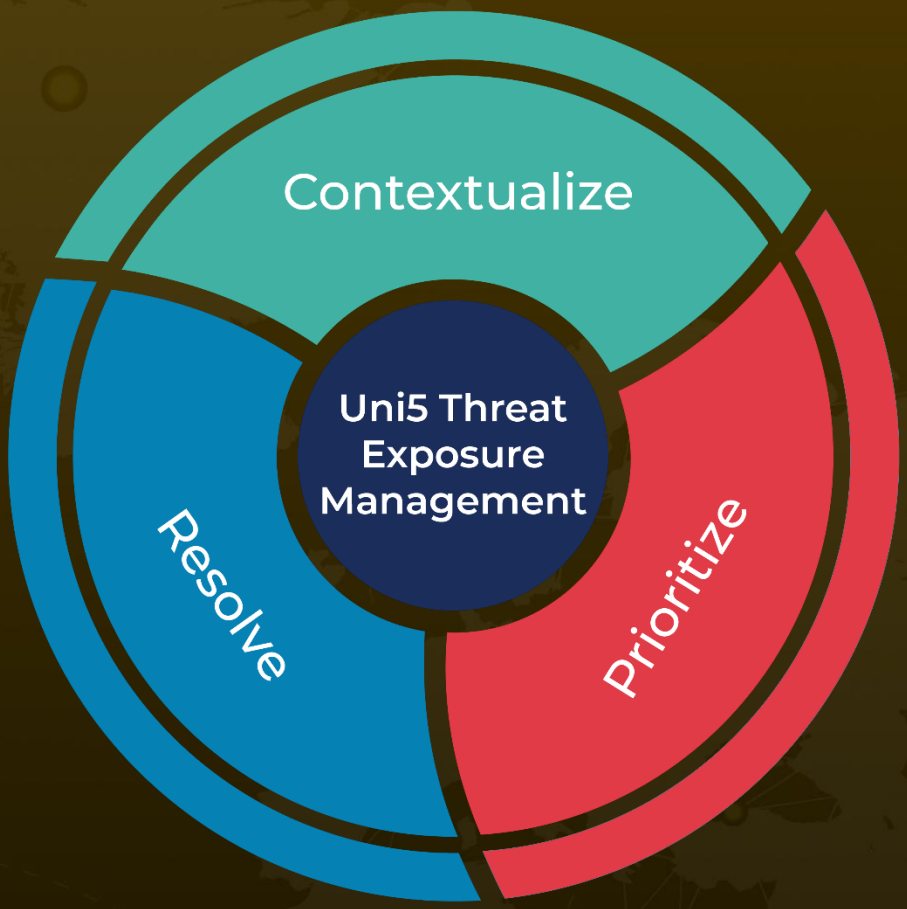
References

https://www.silentpush.com/blog/poisonseed/

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 7, 2025 • 6:00 AM

More at www.hivepro.com