Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

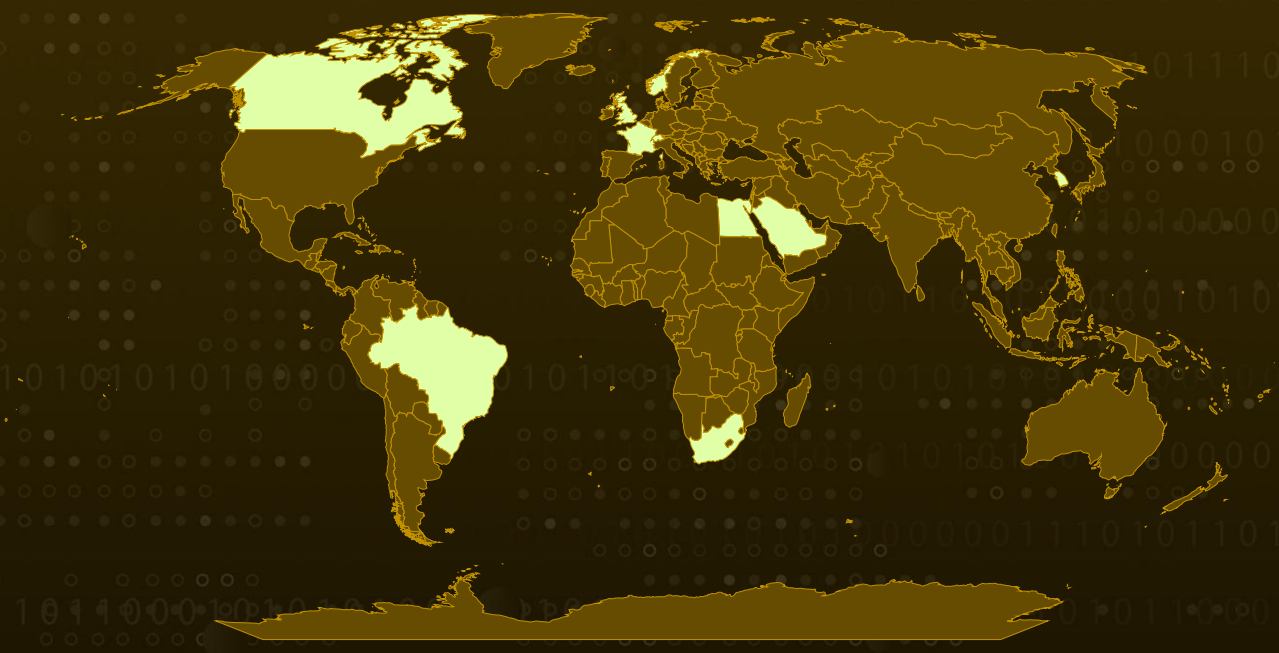
From ZIP to Zero Trust: The Finance Sector's Phishing Wake-Up Call

Date of Publication	Admiralty Code	TA Number
June 5, 2025	A1	TA2025174

Summary

Attack Discovered: May 15, 2025
Targeted Countries: UK, Canada, South Africa, Norway, South Korea, Singapore, Switzerland, France, Egypt, Saudi Arabia, Brazil
Targeted Industries: Banking, Insurance, Energy, Mining, Semiconductor, Finance, Tourism
Attack: Cybercriminals are targeting finance leaders with convincing phishing emails posing as career opportunities from Rothschild & Co. Behind the scenes, a hidden script quietly installs remote access tools, creates secret admin accounts, and enables full control of the victim's device all without raising alarms. This stealthy attack uses clever CAPTCHA tricks and phishing PDFs to bypass security, making it dangerously easy to overlook.

Attack Regions



Attack Details

#1 A stealthy spear-phishing campaign has been targeting CFOs and senior finance professionals across banking, energy, insurance, and investment sectors in regions including Europe, Africa, Canada, the Middle East, and South Asia. Disguised as a high-level leadership opportunity from Rothschild & Co, the attack was engineered to trick recipients into downloading a malicious file under the guise of a recruitment brochure.

#2 The email directs targets to a Firebase-hosted page, presenting a downloadable ZIP file that unpacks into a Visual Basic Script (VBS). Once executed, this script installs a remote access tool called NetBird, based on the WireGuard protocol, along with OpenSSH. The malware quietly creates a hidden local administrator account, enables Remote Desktop, configures firewall rules, and ensures persistence through scheduled tasks—all without alerting the user.

#3 A standout feature of this campaign is its use of a deceptive CAPTCHA gate. Victims are first shown a fake CAPTCHA screen, which, once solved, decrypts and redirects to the actual malicious URL. This technique is designed to bypass detection by security systems that typically block phishing pages protected by Cloudflare Turnstile or Google reCAPTCHA.

#4 The script not only sets up remote access but also removes visible traces of compromise by hiding shortcuts and cleaning up after itself. However, it leaves behind a VBS file to maintain a foothold. The hidden admin account uses the credentials user and Bs@202122, with the password set to never expire allowing continuous unauthorized access.

#5 Further analysis linked this activity to older phishing sites and payloads using similar techniques, including Firebase-hosted domains that are now inactive. Indicators from these operations match patterns seen in campaigns impersonating financial regulators, suggesting a well-resourced actor capable of recycling and evolving their methods.

Recommendations

- **Be suspicious of unexpected job offers:** If you receive an email claiming to offer a job opportunity especially from a well-known company like Rothschild & Co take a moment to verify it independently. Don't click links or download files from unknown sources.
- **Avoid clicking on PDF links that open websites**: A real PDF should contain information, not redirect you to a strange website. If a PDF asks you to "click here to view," it's a red flag.
- **Watch out for CAPTCHA tricks:** If a website shows a CAPTCHA but then quickly redirects you elsewhere, close it. This trick is often used to hide phishing links.
- **Check for hidden users:** Regularly review user accounts on your system. If you see one you don't recognize like a "user" with admin access it could be a sign of compromise.
- **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	TA0008 Lateral Movement	TA0011 Command and Control	T1566 Phishing
T1566.002 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1059.001 PowerShell	T1105 Ingress Tool Transfer	T1218 System Binary Proxy Execution

T1218.007 Msiexec	T1543 Create or Modify System Process	T1543.003 Windows Service	T1219 Remote Access Tools
T1219.002 Remote Desktop Software	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1136 Create Account
T1136.001 Local Account	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control	T1112 Modify Registry
T1562 Impair Defenses	T1562.004 Disable or Modify System Firewall	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1021.004 SSH			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	192[.]3[.]95[.]152
URL	hxxps[:]//googl-6c11f[.]firebaseapp[.]com/job/file-846873865383[.]html, hxxps[:]//googl-6c11f[.]web[.]app/job/9867648797586_Scan_15052025-736574[.]html, hxxp[:]//192[.]3[.]95[.]152/cloudshare/atr/pull[.]pdf, hxxp[:]//192[.]3[.]95[.]152/cloudshare/atr/trm
File	Rothschild_&_Co-6745763.zip, Rothschild_&_Co-6745763.vbs, pull.vbs
MD5	4cd73946b68b2153dbff7dee004012c3, 53192b6ba65a6abd44f167b3a8d0e52d, b91162a019934b9cb3c084770ac03efe
Email Address	db2680688@gmail[.]com

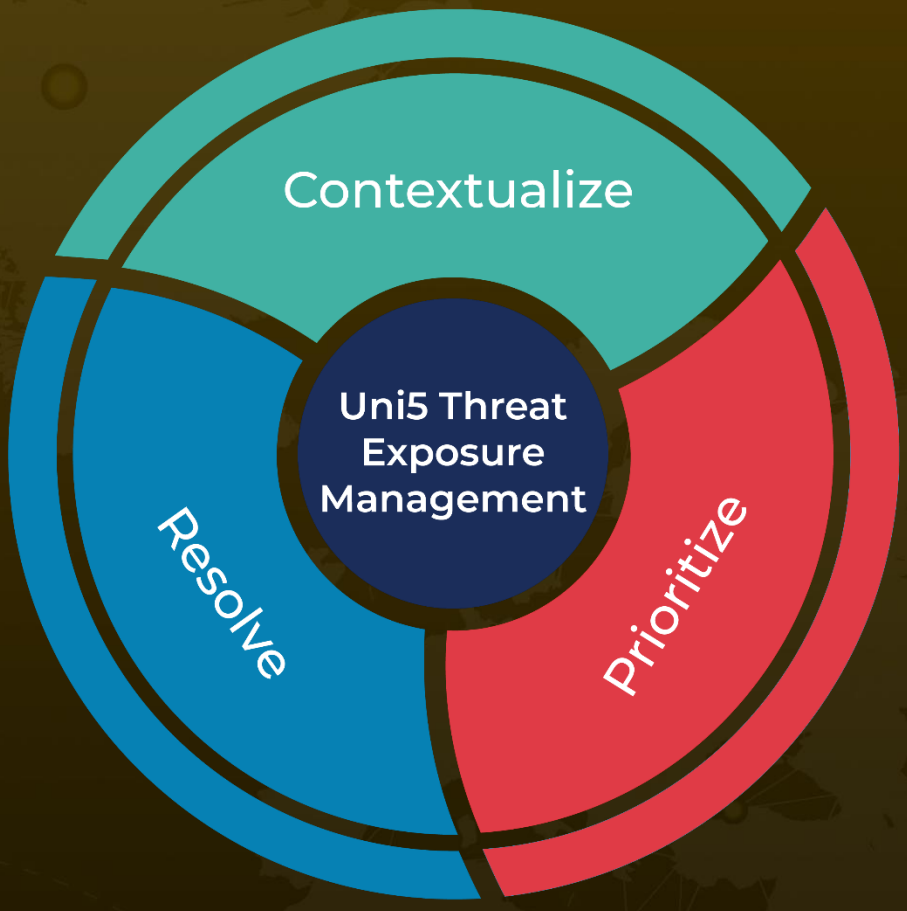
References

https://www.trellix.com/en-in/blogs/research/a-flyby-on-the-cfos-inbox-spear-phishing-campaign-targeting-financial-executives-with-netbird-deployment/

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 5, 2025 • 5:15 AM

More at www.hivepro.com