Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

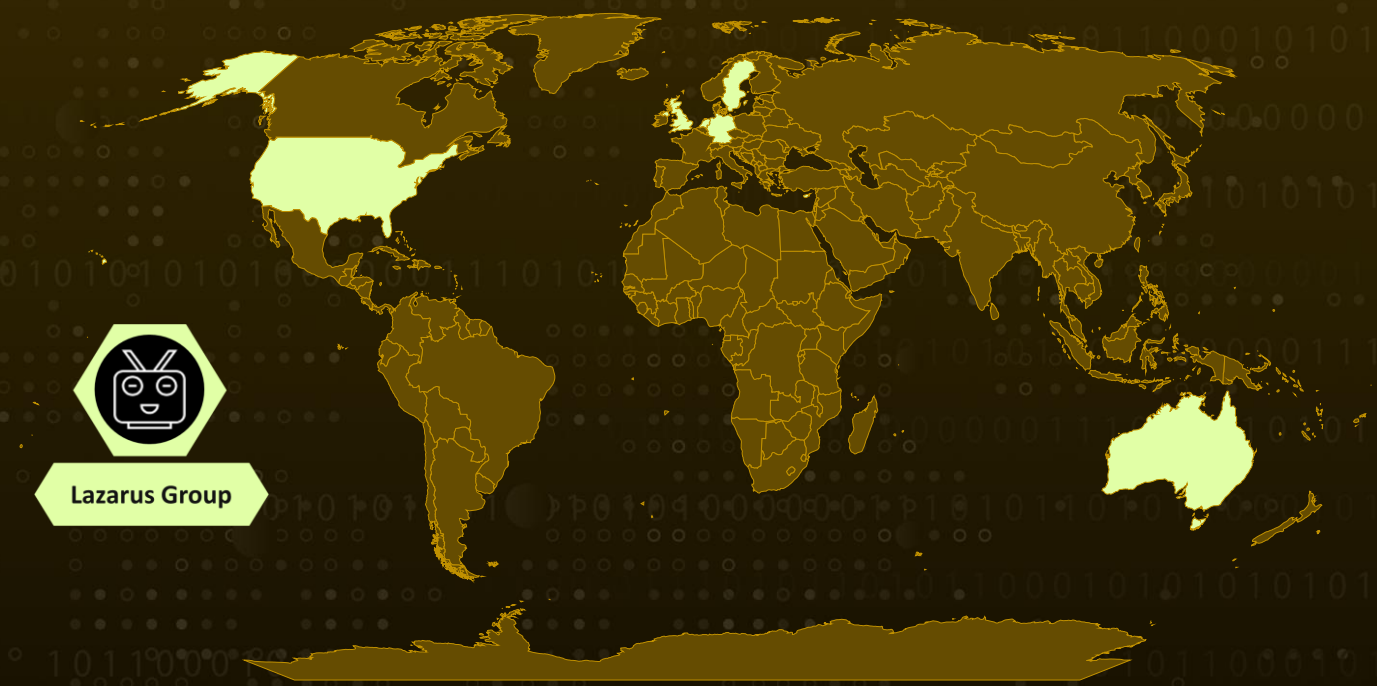
North Korean Hackers Weaponize Job Offers Featuring MISTPEN

Date of Publication	Admiralty Code	TA Number
September 24, 2024	A1	TA2024370

Summary

Threat Actor: Lazarus Group (aka UNC2970, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor, Citrine Sleet, Gleaming Pisces)
Malware: BURNBOOK, TEARPAGE, MISTPEN Backdoor
Targeted Countries: United States, United Kingdom, Netherlands, Cyprus, Sweden, Germany, Singapore, Hong Kong, Australia
Targeted Industries: Energy, Aerospace
Attack: Lazarus Group, a North Korea-linked cyber-espionage organization (also known as UNC2970 and TEMP.Hermit), has been observed conducting job-themed phishing campaigns, referred to as "Operation Dream Job," targeting the energy and aerospace sectors. The ultimate objective is the deployment of the MISTPEN backdoor, delivered through the BURNBOOK launcher.

Attack Regions



Attack Details

#1 A North Korea-affiliated cyber-espionage group, Lazarus Group (also known as UNC2970 and TEMP.Hermit), has been observed using job-related phishing schemes to target individuals in the energy and aerospace sectors.

#2 The campaign, dubbed "Operation Dream Job," involves the group engaging victims through email and WhatsApp, eventually sending a malicious archive disguised as a job description in PDF format. This encrypted file can only be opened with an outdated, trojanized version of SumatraPDF, which initiates the infection chain. The end goal is the delivery of the MISTPEN backdoor via the BURNBOOK launcher.

#3 The job descriptions are specifically aimed at senior or managerial-level employees, indicating that the threat actors seek confidential and sensitive data typically accessible to high-ranking personnel. The weaponized PDF viewer triggers the execution of a malicious DLL, with the BURNBOOK C/C++ launcher responsible for dropping an embedded DLL loader, "wtsapi32.dll," tracked as TEARPAGE, which activates the MISTPEN backdoor upon system reboot.

#4 MISTPEN, a lightweight backdoor written in C, is primarily designed to download and execute Portable Executable (PE) files from a command-and-control (C2) server. In some cases, the group has been observed using compromised WordPress sites as C2 domains.

Recommendations

Encourage vigilance with unexpected job offers: Urge employees not to download or interact with unsolicited job offers, especially if the communication comes from unexpected sources or through non-professional platforms.

Implement email filtering solutions: Use advanced email filtering systems to detect and block phishing emails with malicious attachments or links, particularly those containing encrypted files or unknown PDF viewers. Additionally, restrict access to executable attachments and block files from unfamiliar sources or formats that require outdated or untrusted software to open.

Application Whitelisting and Control: Block downloading and running unverified or outdated applications like the trojanized SumatraPDF that was used to launch the MISTPEN backdoor. Ensure only vetted and trusted software is allowed to run on company devices, especially for document viewing software and PDF readers.

Enforce MFA on all accounts: Require multi-factor authentication for all critical systems and email accounts to prevent unauthorized access, even if login credentials are compromised through phishing. Ensure MFA is enforced on high-value accounts and platforms, especially for senior and managerial employees who are likely to be targeted.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0010** Exfiltration	**TA0011** Command and Control
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1204** User Execution
T1204.002 Malicious File	**T1547** Boot or Logon Autostart Execution	**T1543** Create or Modify System Process	**T1574** Hijack Execution Flow
T1574.001 DLL Search Order Hijacking	**T1036** Masquerading	**T1212** Exploitation for Credential Access	**T1010** Application Window Discovery
T1083 File and Directory Discovery	**T1057** Process Discovery	**T1105** Ingress Tool Transfer	**T1574.002** DLL Side-Loading
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	BAE_Vice President of Business Development.pdf, libmupdf.dll, binhex.dll
File Path	%APPDATA%\Roaming\Microsoft\BDE UI Launcher\wtsapi32.dll, %APPDATA%\Roaming\Thumbs.ini
MD5	28a75771ebdb96d9b49c9369918ca581, 57e8a7ef21e7586d008d4116d70062a6, f3baee9c48a2f744a16af30220de5066, 006cbff5d248ab4a1d756bce989830b9, 0b77dcee18660bdccaf67550d2e00b00, b707f8e3be12694b4470255e2ee58c81, cd6dbf51da042c34c6e7ff7b1641837d, eca8eb8871c7d8f0c6b9c3ce581416ed
Domain	heropersonas[.]com
URL	hxxps[:]//graph[.]microsoft[.]com/v1[.]0/me/drive/root[:]/path/upload/world/266A25710006EF92, hxxps[:]//dstvdtt[.]co[.]za/wp-content/plugins/social-pug/assets/lib[.]php, hxxps[:]//cmasedu[.]com/wp-content/plugins/kirki/inc/script[.]php, hxxps[:]//bmtpakistan[.]com/solution/wp-content/plugins/one-click-demo-import/assets/asset[.]php, hxxps[:]//verisoftsystems[.]com/wp-content/plugins/optinmonster/views/upgrade-link-style[.]php, hxxps[:]//www[.]clinicabaru[.]co/wp-content/plugins/caldera-forms/ui/viewer-two/viewer-2[.]php

References

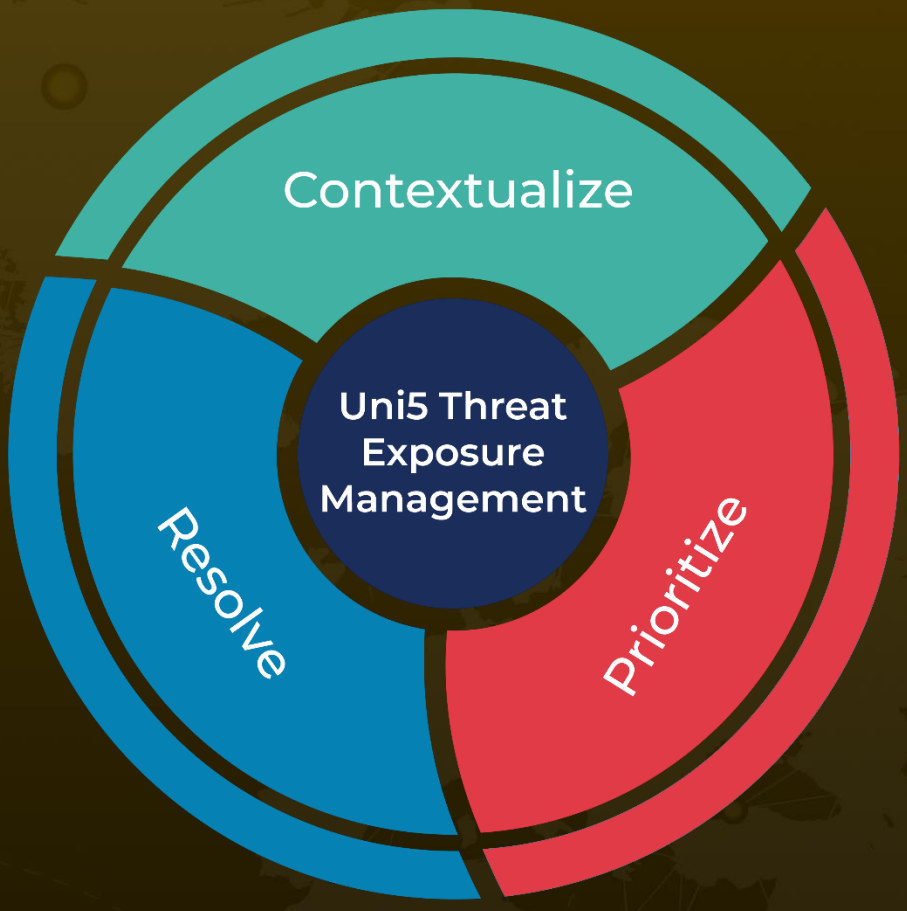
https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader

https://attack.mitre.org/campaigns/C0022/

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

September 24, 2024 • 11:30 PM

More at www.hivepro.com