Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

APT37 Operation ToyBox Story Exposes Cybersecurity Blind Spots

Date of Publication	Admiralty Code	TA Number
June 12, 2025	A1	TA2025185

Summary

Attack Commenced: March 8, 2025
Campaign: Operation ToyBox Story
Threat Actor: APT37 (aka RICOCHET CHOLLIMA, Reaper, TEMP.Reaper, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt)
Malware: RoKRAT
Targeted Region: South Korea
Targeted Industries: Governments, Think Tanks, Activists (Civil Society)
Attack: In March 2025, the North Korea-linked APT37 group launched Operation ToyBox Story, a spear-phishing campaign leveraging fileless malware and advanced social engineering to infiltrate strategic targets within South Korean networks. The operation's calculated exploitation of legitimate platforms signals a concerning evolution in state-sponsored espionage.

Attack Regions

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-41128	Microsoft Windows Scripting Languages Remote Code Execution Vulnerability	Microsoft Windows	✓	✓	✓

Attack Details

#1

In March 2025, a spear-phishing campaign orchestrated by the North Korea-linked threat group APT37 surfaced. Codenamed Operation ToyBox Story, the operation was executed with notable precision, disguising malicious invitations as official correspondence from a respected South Korean national security think tank.

#2

To enhance credibility and entice its targets, primarily activists, scholars, and policy experts focused on North Korea, the attackers referenced a legitimate event titled "Trump 2.0 Era: Prospects and South Korea's Response." The campaign's delivery mechanism relied on exploiting trusted cloud storage services, with Dropbox serving as the primary platform. Victims received compressed ZIP archives containing weaponized LNK shortcut files.

#3

Once extracted and opened, these shortcuts silently executed obfuscated PowerShell commands, triggering a fileless malware infection chain. This method successfully bypassed traditional file-based detection systems and marked a calculated evolution in APT37's operational playbook. Two phishing emails were particularly notable.

#4

One impersonated a subject matter expert, claiming to share intelligence on North Korean troop movements to Russia, with a malicious Dropbox-hosted ZIP archive linked through a disguised Hangul Word Processor (HWP) document. The other posed as a conference invitation from the think tank, leading recipients to a similar Dropbox-hosted malicious archive.

#5

Inside these archives, LNK files acted as the first-stage payload, launching embedded PowerShell commands that initiated a multi-phase, fileless attack sequence. This chain incorporated obfuscated batch scripts, dynamic code execution, and XOR-transformed shellcode, ultimately deploying RokRAT, a sophisticated remote access trojan long attributed to North Korean espionage operations.

#6

Once active, RokRAT harvested sensitive system information, captured live screenshots, monitored process activity, and maintained encrypted communications with its command-and-control infrastructure via cloud APIs on platforms such as Dropbox, pCloud, and Yandex. APT37 stuck to familiar tools and tactics. RokRAT’s core code and encryption routines remained largely unchanged from earlier campaigns, reflecting the group’s reliance on proven malware with updated delivery methods.

Recommendations

Use Email Pre-Processing: Develop custom email filters that flag inbound emails containing geopolitical event keywords, fake conference invites, or sensitive regional topics, routing them for manual review before delivery. Enforce enhanced scrutiny or temporary quarantines for inbound emails originating from high-risk geopolitical regions or flagged IP ranges.

Ensure Strong File Integrity Monitoring: Regularly check for unauthorized file changes and the creation of suspicious files on endpoints, such as files masquerading as PDFs. Monitoring tools should be configured to alert when files, especially in ZIP archives, deviate from normal behavior.

Detect Fileless Malware Persistence Techniques: Harden detection around persistence mechanisms typically leveraged by fileless malware. Monitor for new scheduled tasks with unfamiliar or obfuscated names. Unexpected registry Run/RunOnce entries. WMI Event Consumer registrations created by PowerShell or script processes. These activities, particularly when seen together, should trigger incident response workflows.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1566.002** Spearphishing Link	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1059.001** PowerShell	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1140 Deobfuscate/Decode Files or Information	**T1082** System Information Discovery	**T1057** Process Discovery	**T1033** System Owner/User Discovery

T1113 Screen Capture	**T1115** Clipboard Data	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1070.004 File Deletion	**T1132** Data Encoding	**T1567** Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	81c08366ea7fc0f933f368b120104384, 723f80d1843315717bc56e9e58e89be5, 7822e53536c1cf86c3e44e31e77bd088, 324688238c42d7190a2b50303cbc6a3c, a635bd019674b25038cd8f02e15eebd2, beeaca6a34fb05e73a6d8b7d2b8c2ee3, d5d48f044ff16ef6a4d5bde060ed5cee, d77c8449f1efc4bfb9ebff496442bbbc, 2f431c4e65af9908d2182c6a093bf262, 7cc8ce5374ff9eacd38491b75cbedf89, 8f339a09f0d0202cfaffbd38469490ec, 46ca088d5c052738d42bbd6231cc0ed5
SHA256	92ab3a9040f5e620bc4b76295239c5240130d968c6cbeaa7dc555d2cf19bfae1, f538ca6ef15a18d02358d93d0d4493e594550c681f771b86d75dba19d1ef5e92, 49749efacb2542c33ce824b3f75444dac17a30f3e5746e0b7e8541ae93e3e1bb, d182834a984c9f5b44ea0aca5786223a78138ff23d33362ab699c76bf6987261, 9b8218774c3abc0a449cfc490f12e81155af00ec90c2e1d630a61c29f70a98cb
IPv4	89[.]147[.]101[.]65, 89[.]147[.]101[.]71, 37[.]120[.]210[.]2
Email	rolf[.]gehrung[@]yandex[.]com, ekta[.]sahasi[@]yandex[.]com, gursimran[.]bindra[@]yandex[.]com, sneha[.]geethakrishnan[@]yandex[.]com, tanessha[.]samuel[@]gmail[.]com,

TYPE	VALUE
Email	tianling0315[@]gmail[.]com, w[.]sarah0808[@]gmail[.]com, softpower21cs[@]gmail[.]com, sandozmessi[@]gmail[.]com, tiger[.]man[.]1999[@]mail[.]ru, navermail_noreply[@]mail[.]ru
Filename	toy01.dat, toy02.dat, toy03.bat

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128

References

https://www.genians.co.kr/en/blog/threat_intelligence/toybox-story

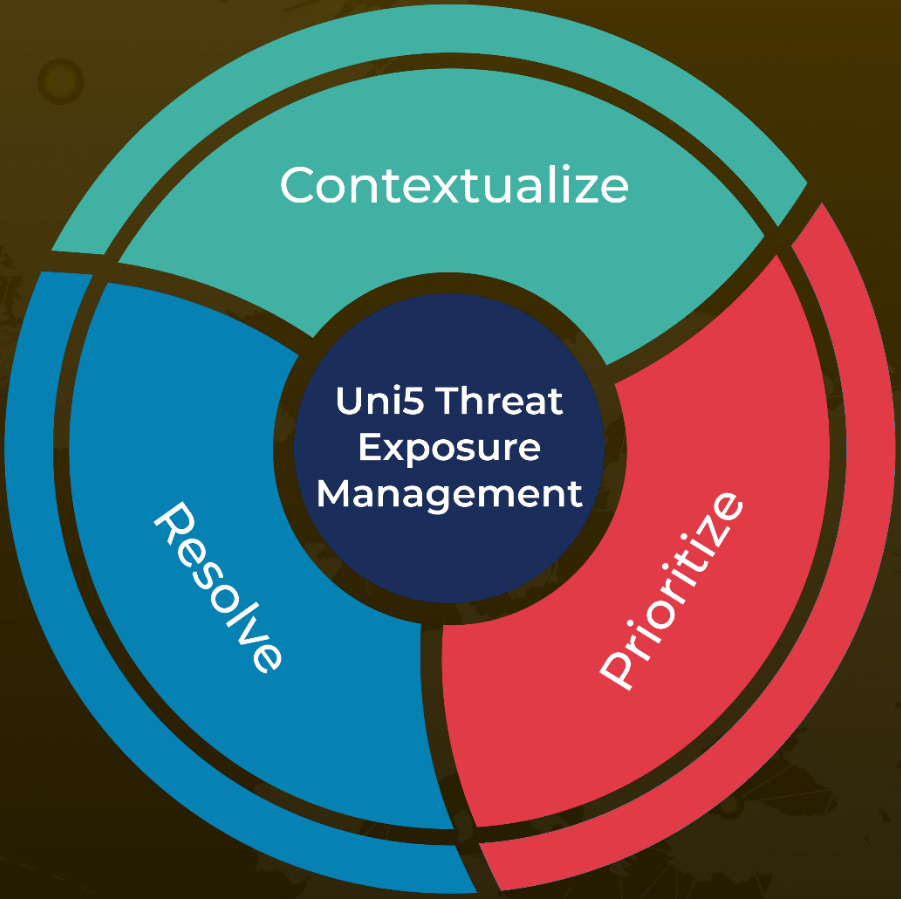
https://hivepro.com/threat-advisory/internet-explorer-zero-day-vulnerability-exploited-by-apt-37/

https://hivepro.com/threat-advisory/scarcruft-unleashes-tailored-attacks-on-cybersecurity-frontlines/

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 12, 2025 • 10:00 PM

More at www.hivepro.com