Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Ruby Jumper: APT37's Cloud-to-Air-Gap Espionage Framework

Date of Publication	Admiralty Code	TA Number
March 03, 2026	A1	TA2026059

Summary

First Seen: December 2025
Targeted Regions: Worldwide
Targeted Platform: Windows
Threat Actor: APT37 (aka ScarCruft, Reaper, TEMP.Reaper, Ricochet Chollima, 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: RESTLEAF, SNAKEDROPPER, THUMBSBD, VIRUSTASK, FOOTWINE, and BLUELIGHT
Campaign: Ruby Jumper
Attack: The Ruby Jumper campaign showcases APT37 at its most methodical and adaptive, chaining together stealth, cloud abuse, and air-gap bridging into a single cohesive espionage framework. What begins as a seemingly harmless LNK file quickly unfolds into a multi-stage infection sequence that carves hidden payloads, deploys RESTLEAF, and leverages Zoho WorkDrive for covert command-and-control. From there, the operation escalates with in-memory shellcode injection, a disguised Ruby runtime for persistence, and THUMBSBD's clever use of USB drives as bidirectional data relays, effectively turning removable media into a covert communication channel. The final backdoors, FOOTWINE and BLUELIGHT, provide full surveillance and remote-control capabilities, enabling long-term monitoring even inside segmented or air-gapped environments.

Attack Regions

Attack Details

#1 A newly observed campaign dubbed Ruby Jumper showcases a disciplined and modular intrusion chain attributed to APT37. Campaign begins with a weaponized Windows LNK file, a delivery vector repeatedly used by APT37. When executed, the shortcut launches a PowerShell routine that identifies itself by file size and extracts embedded payloads from fixed offsets. These include a decoy document, an executable, a PowerShell script (search.dat), and a batch file (find.bat). The lure, an Arabic translation of a North Korean article on the Palestine–Israel conflict, suggests carefully profiled targeting. Together, these components load the first-stage implant, RESTLEAF, directly into memory.

#2 RESTLEAF abuses Zoho WorkDrive for command-and-control, marking a notable shift in infrastructure strategy. It authenticates using hardcoded refresh tokens embedded in the binary to generate valid API access tokens. After connecting, it downloads a shellcode payload (AAA.bin) and executes it through process injection. Successful infection is signaled by uploading timestamped beacon files ("lion [timestamp]") to the attacker-controlled repository.

#3 The injected shellcode operates in two stages. Stage one decrypts and injects a secondary payload into a legitimate Windows process using a one-byte XOR key. Stage two reflectively loads an embedded executable, also XOR-decoded. The loader incorporates APT37's distinctive API hashing scheme (ROR 11 for modules, ROR 15 for functions), reinforcing attribution. This second-stage payload, SNAKEDROPPER, deploys a portable Ruby 3.3.0 runtime, renames rubyw.exe to usbspeed.exe, and replaces a legitimate RubyGems file with malicious code to hijack execution.

#4 SNAKEDROPPER establishes persistence through a scheduled task named rubyupdatecheck, executed every five minutes. It also drops additional shellcode-bearing files disguised as Ruby scripts. A key component, THUMBSBD (ascii.rb), is designed to bridge air-gapped systems using removable media. It stores XOR-encrypted configuration data locally and collects detailed host reconnaissance when activated.

#5 When a USB drive is connected, THUMBSBD creates a hidden $RECYCLE.BIN directory and stages encrypted command-and-control files, effectively transforming removable media into a covert relay channel. VIRUSTASK complements this by hiding legitimate files on the drive and replacing them with malicious LNK shortcuts to trigger execution. The final payloads, FOOTWINE and BLUELIGHT, provide full backdoor functionality, including surveillance and remote command execution. BLUELIGHT further enhances resilience by leveraging cloud platforms such as Google Drive, Microsoft OneDrive, pCloud, and Backblaze for C2, enabling sustained espionage even across segmented or isolated networks.

Recommendations

- **Block Malicious LNK Execution via Group Policy:** Configure Windows Group Policy to restrict the execution of shortcut files originating from external sources, particularly email attachments and removable media, to prevent the initial infection vector used in this campaign.

- **Monitor and Restrict PowerShell Activity:** Implement PowerShell Constrained Language Mode and enable Script Block Logging to detect and prevent the malicious PowerShell commands used by RESTLEAF to carve and execute embedded payloads from LNK files.

- **Restrict Zoho WorkDrive API Access:** Evaluate and restrict outbound API communications to Zoho WorkDrive endpoints from non-authorized systems, as RESTLEAF abuses this cloud service for C2 communications using hardcoded OAuth tokens.

- **Enforce Removable Media Controls:** Deploy endpoint policies that restrict auto-execution from removable media, disable LNK file execution from USB drives, and implement write-protection where feasible to counter THUMBSBD and VIRUSTASK propagation mechanisms targeting air-gapped systems.

- **Hunt for Ruby Runtime Anomalies:** Search enterprise endpoints for unexpected Ruby interpreter installations, specifically the presence of usbspeed.exe in %PROGRAMDATA%\usbspeed, the scheduled task "rubyupdatecheck," and modified operating_system.rb files within Ruby library paths.

- **Monitor Scheduled Task Creation:** Deploy detection rules for the creation of scheduled tasks with names such as "rubyupdatecheck" or tasks executing binaries from %PROGRAMDATA% paths, which SNAKEDROPPER uses to maintain persistence.

- **Implement Network Segmentation and Air-Gap Verification:** Strengthen air-gap integrity by enforcing strict data transfer policies, deploying data diode solutions, and implementing physical access controls for removable media to prevent THUMBSBD from bridging isolated network segments.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1574: Hijack Execution Flow	
Defense Evasion	T1027: Obfuscated Files or Information	
	T1055: Process Injection	
	T1620: Reflective Code Loading	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1083: File and Directory Discovery	

Tactic	Technique	Sub-technique
Command and Control	T1132: Data Encoding	T1132.002: Non-Standard Encoding
	T1092: Communication Through Removable Media	
Exfiltration	T1052: Exfiltration Over Physical Medium	T1052.001: Exfiltration over USB
	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Collection	T1056: Input Capture	T1056.001: Keylogging
	T1113: Screen Capture	
	T1123: Audio Capture	
	T1125: Video Capture	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	709d70239f1e9441e8e21fcacfdc5d08, ad556f4eb48e7dba6da14444dcce3170, 098d697f29b94c11b52c51bfe8f9c47d, 4214818d7cde26ebeb4f35bc2fc29ada, 5c6ff601ccc75e76c2fc99808d8cc9a9, 476bce9b9a387c5f39461d781e7e22b9, 585322a931a49f4e1d78fb0b3f3c6212
SHA256	c07e0f01e39ae74667d3014904706b50effd1f3cb75e8130eb57729d38589ad5, cf2e3f46b26bae3d11ab6c2957009bc1295b81463dd67989075592e81149c8ec, e654df84fd6dc02ca1b312ff856ef2ca88b42a72bab31ea3168965cb946cf16e, c61c679eec1c1b43bbd01727fdfb6a69b11485931eb8569e6b20ada30bfe84af, a8b8a92d170029885d4e7763675f10eb172150f8503592677cadedc392edccf4
Domains	philion[.]store, homeatedke[.]store, hightkdhe[.]store
IPv4:Port	144[.]172[.]106[.]66[:]8080

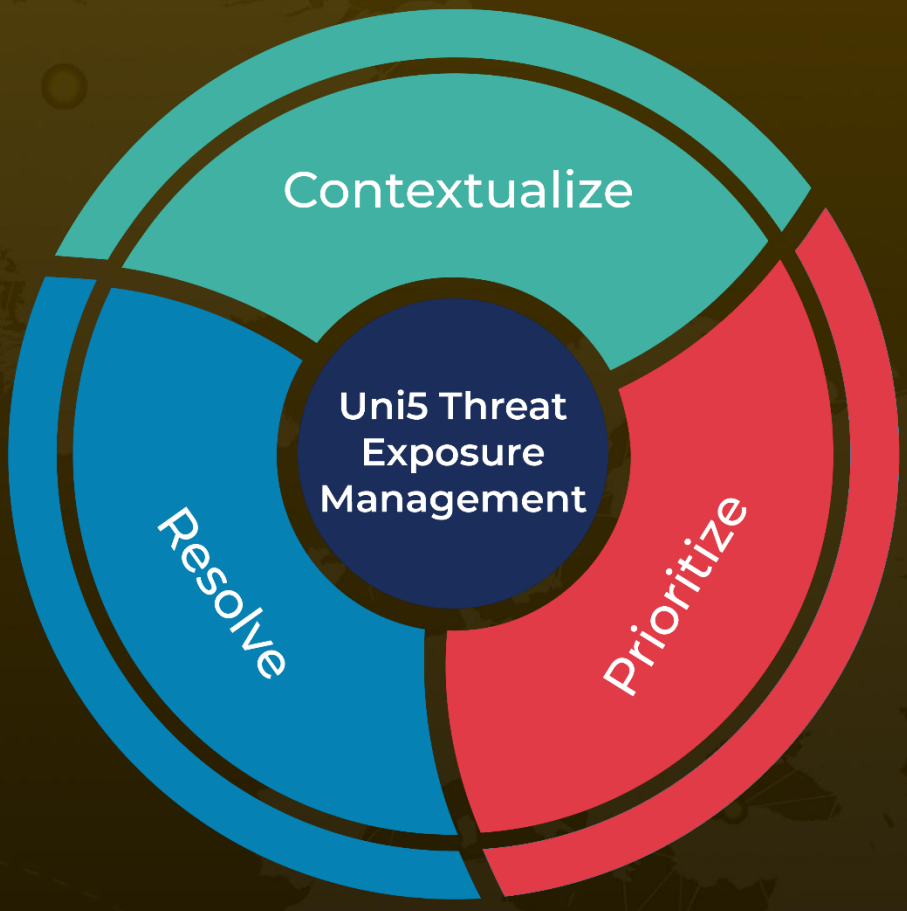
References

https://www.zscaler.com/blogs/security-research/apt37-adds-new-capabilities-air-gapped-networks

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

March 03, 2026 • 07:50 AM

More at www.hivepro.com