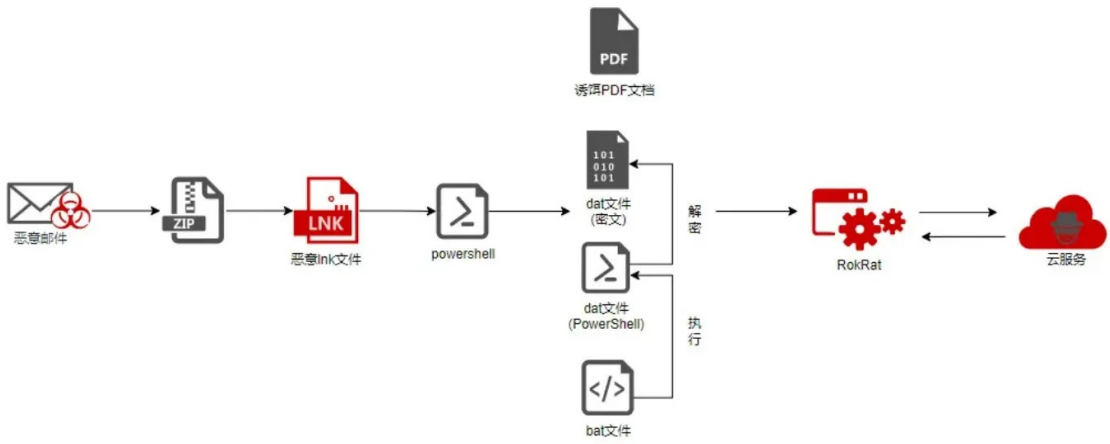
APT-C-28 Group Launched New Cyber Attack With Fileless RokRat Malware

cybersecuritynews.com/apt-c-28-group-launched-new-cyber-attack-with-fileless-rokrat-malware/

Balaji N February 20, 2025



Cyber Attack With Fileless RokRat Malware

The 360 Advanced Threat Research Institute has uncovered a sophisticated cyber espionage campaign orchestrated by the North Korean-linked threat actor APT-C-28, also known as ScarCruft or APT37.

The group, active since 2012, has shifted tactics to employ fileless malware delivery mechanisms for deploying its signature RokRat malware, targeting government personnel and corporations across South Korea and Asia.

This evolution marks a significant escalation in the group's ability to evade traditional security defenses while stealing military, economic, and political intelligence.

Historical Context of APT-C-28's Operations

APT-C-28 has long been associated with cyber operations targeting strategic industries, including aerospace, chemicals, and healthcare.

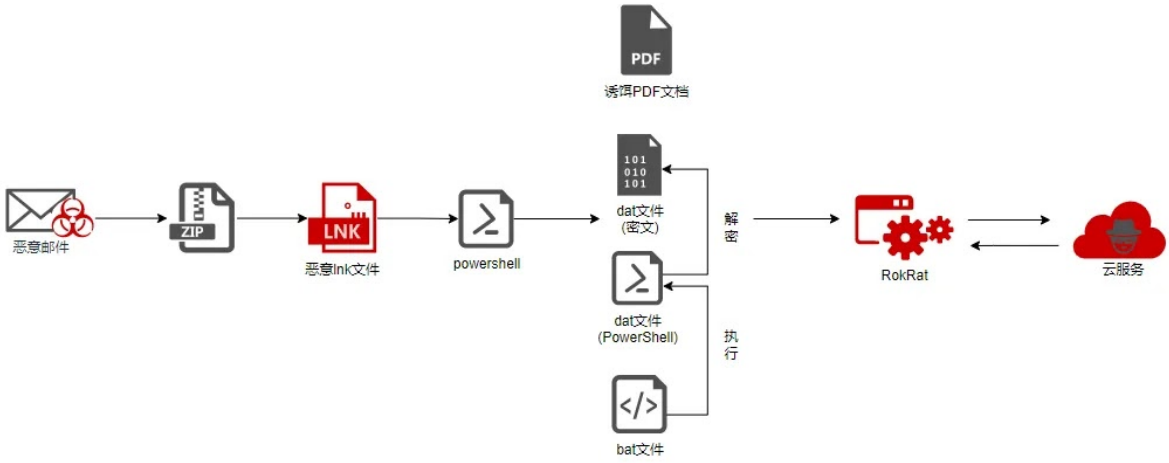
Since 2016, RokRat has served as the group's primary remote access tool (RAT), enabling persistent network infiltration and data exfiltration.

The malware's cloud-based infrastructure allowed operators to dynamically update payloads, but recent campaigns show a pivot toward embedding malicious components directly within phishing email attachments.

The 2024 iteration of RokRat retains core functionalities but introduces refined evasion techniques. Unlike earlier versions that relied on cloud services for payload delivery, the latest attacks embed encrypted shellcode within malicious LNK files, reducing reliance on external servers likely flagged by security systems.

Phishing Campaigns and Initial Compromise

Attackers begin by crafting highly tailored phishing emails, leveraging legitimate content from official websites to impersonate credible sources.



Attack flow chart

These emails contain ZIP attachments housing malicious LNK files disguised as documents related to North Korean affairs, diplomatic policies, or trade agreements. For example, one decoy document mimicked a South Korean government memo about inter-Korean economic collaboration.

When victims execute the LNK file, a multi-stage payload deployment sequence triggers:

1. **PowerShell Script Activation**: The LNK file invokes PowerShell to extract embedded files, including decoy documents, batch scripts, and encrypted RokRat shellcode.
2. **In-Memory Payload Decryption**: A malicious batch script executes a secondary PowerShell script, applying XOR decryption to reveal the RokRat shellcode. This fileless approach avoids writing malicious files to disk, complicating detection1.

3. **Thread Execution**: The decrypted shellcode spawns a new thread to load the final RokRat payload, which connects to command-and-control (C2) servers while masquerading network traffic as Googlebot user agents.

Technical Innovations in RokRat's 2024 Variant

Recent samples reveal updates to RokRat's operational protocols:

- **Enhanced Anti-Forensics**: Post-execution cleanup scripts now delete startup entries, batch files, and registry keys more comprehensively than prior versions (Table 2)1.
- **Modular Payload Retrieval**: New C2 commands (e.g., "1," "2," "5," "6") enable dynamic fetching of secondary payloads from attacker-specified URLs, allowing real-time mission adjustments1.
- **Process Hollowing**: The malware injects decrypted PE files into legitimate processes like *explorer.exe*, further obscuring malicious activity from endpoint detection tools.

A critical forensic artifact is RokRat's use of hardcoded strings such as `--wwjaughalvncjwiajs--` in C2 communications and XOR keys derived from PowerShell script patterns. Security teams can hunt for these indicators in memory dumps or network logs.

The shift from cloud-dependent payloads to self-contained LNK files reflects APT-C-28's adaptation to improved defensive measures.

Security vendors' rapid takedowns of malicious domains likely forced the group to minimize external dependencies. Despite these changes, code overlaps with historical RokRat samples such as identical encryption routines and C2 response handling strengthen attribution to the ScarCruft ecosystem.

Geopolitical analysis suggests the campaign aligns with North Korea's intensified intelligence-gathering efforts amid ongoing diplomatic tensions. Targets include entities involved in sanctions enforcement, nuclear negotiations, and cross-border trade.

Mitigation and Defensive Recommendations

To counter APT-C-28's evolving tactics, the 360 Advanced Threat Research Institute advises a layered defense strategy:

Organizations should deploy advanced email filtering solutions capable of detecting weaponized LNK files and script-based payloads. Behavioral analysis tools that flag PowerShell spawning from LNK executions can disrupt initial compromise attempts.

- **Memory Scanning**: Deploy tools that monitor for reflective DLL loading and unauthorized thread creation, hallmarks of fileless malware.

- **User Agent Blocking**: Block outbound connections masquerading as Googlebot (e.g., `User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1)`), a known RokRat signature.
- **Application Allowlisting**: Restrict execution of PowerShell and LOLBINs (Living-Off-the-Land Binaries) to authorized directories.

Regular security training should emphasize phishing recognition, particularly document-themed lures targeting geopolitical topics. Simulated exercises can improve incident response readiness for multi-stage intrusions.

APT-C-28's latest campaign underscores the group's commitment to refining intrusion techniques against high-value targets. While RokRat's core functionalities remain consistent, its delivery mechanisms and anti-forensic measures continue to evolve, demanding proactive defense postures.

The cybersecurity community must prioritize intelligence sharing and adversary-centric hunting to mitigate risks posed by this persistent threat actor.

Indicators of Compromise (IOCs)

- Hashes: `936888d84b33f152d39ec539f5ce71aa`, `5adfa76b72236bf017f7968fd012e968`
- Network Signatures: HTTP requests containing `--wwjaughalvncjwiajs--`
- Decryption Keys: XOR keys derived from PowerShell scripts with `bxor` patterns1.

Recent Posts

VMware Patches Multiple 47 Vulnerabilities VMware Tanzu Greenplum Backup & Components

Guru Baran - April 9, 2025

VMware has released critical security updates to address 47 vulnerabilities across multiple VMware Tanzu Greenplum products, including 29 issues in VMware Tanzu Greenplum Backup...