Contents

[**APT37** 2](#_Toc179353273)

[**I. Introduction** 2](#_Toc179353274)

[**II. Tactics** 2](#_Toc179353275)

[**III. Techniques** 3](#_Toc179353276)

[**IV. Procedures** 3](#_Toc179353277)

[**V. Summary** 5](#_Toc179353278)

[**References** 6](#_Toc179353279)

## **APT37**

## **I. Introduction**

APT37 is a state-sponsored North Korean cyber-espionage group, also referred to as Reaper, Group 123, ScarCruft, and TEMP.Reaper, Inksquid, Ricochet Chollima unveiled in the wild since at least 2012. What makes it very unique with this group is that they have consistently targeted entities in South Korea, but in recent times, this has expanded to other countries as well. APT37 is a highly sophisticated threat actor whose tactics align with the state interests of North Korea, including intelligence gathering and foreign policy related to nuclear issues and potential defectors.

## **II. Tactics**

APT37's tactical approach is characterized by

1. ***Strategic Intelligence Gathering***

The group focuses on collecting sensitive information related to North Korean interests, including government, defense, and unification efforts.

1. ***Zero-Day Exploitation***

The group has proved their ability of leveraging zero-day vulnerabilities, which indicates a high level of technical sophistication.

1. ***Social Engineering***

The group often uses thoroughly crafted social engineering tactics to manipulate targets into executing malicious code or revealing sensitive information.

1. ***Long-term Persistence***

Once access is gained, APT37 emphasizes maintaining a long-term presence in victim networks for continuous intelligence gathering.

1. ***Multi-platform Targeting***

The group has shown capabilities in targeting not just Windows systems, but also mobile devices and macOS platforms.

## **III. Techniques**

|  |  |
| --- | --- |
| **Technique** | **Description** |
| **Spear-phishing (T1566.001, T1566.002)** | The group uses tailored emails with malicious attachments or links.  They often leverage topical lures related to Korean peninsula issues. |
| **Drive by Compromise (T1189)** | The group gains access to a system through a user visiting a website over the normal course of browsing. |
| **Malware Deployment** | It uses custom malware families such as ROKRAT, POORAIM, NAVRAT, SLOWDRIFT, and many more. |
| **Exploitation of Zero-Day Vulnerabilities** | The group is known to have used multiple zero-days, including CVE-2018-0802 and CVE-2017-8759. |
| **Command and Control (C2) Infrastructure** | The group leverages social media platforms and cloud services for C2 communication (T1102).  Implementation of custom protocols over HTTP/HTTPS (T1071.001). |
| **Defense Evasion** | Process Hollowing (T1055.012) to inject malicious code into legitimate Windows processes.  Use of Obfuscated Files or Information (T1027), particularly XOR encoding of payloads. |
| **Persistence** | Creation of scheduled tasks (T1053.005).  Use of Windows Management Instrumentation (WMI) for persistence (T1546.003). |

## **IV. Procedures**

APT37's typical attack chain follows this sequence

***1. Initial Access***

a. The group use spear-phishing whereby they send emails to targeted individuals, often containing malicious attachments or links.

b. In some cases, watering hole attacks are used to compromise targets visiting specific websites.

***2. Execution***

a. Upon opening malicious documents, exploits are triggered (often leveraging zero-day vulnerabilities).

b. Initial payloads are typically lightweight and designed to evade detection.

***3. Persistence and Privilege Escalation***

a. Once executed, malware establishes persistence through various methods, including scheduled tasks and WMI event subscription.

b. The group attempts to elevate privileges, often exploiting local vulnerabilities or misconfigurations.

***4. Command and Control***

a. Malware initiates communication with C2 infrastructure, often using legitimate cloud services as a proxy.

b. Custom protocols over HTTP/HTTPS are employed for covert communication.

***5. Lateral Movement***

a. APT37 uses stolen credentials and exploits to move laterally within compromised networks.

b. They leverage tools like Mimikatz for credential dumping to facilitate further access.

***6. Data Exfiltration***

a. Sensitive documents are identified and compressed.

b. Data is exfiltrated using steganography techniques or through legitimate cloud services to avoid detection.

***7. Operational Security***

a. The group regularly updates their tools and infrastructure to evade detection.

b. They use anti-forensic techniques to complicate analysis and attribution efforts.

## **V. Summary**

The evolution of APT37 presents an interesting case study in the development of nation-state cyber capability development. From an initial, core focus on South Korean targets, it has expanded operations to include Japan, Vietnam, and Middle Eastern countries-the wider geopolitical interests of North Korea. This expansion demonstrates the close alignment between cyber operations and national strategic objectives.

However, what particularly deserves attention is the technical skill of that group. APT37 continuously shows fast exploit of zero**-**dayvulnerabilities in very popular software such as Adobe Flash Player and Microsoft Office. Their malware arsenal, including the sophisticated ROKRAT trojan, employs innovative tactics such as using legitimate South Korean social networking services for command and control. This approach effectively camouflages malicious traffic within normal network activities. Additionally, APT37's increasing focus on mobile devices, particularly Android platforms, indicates a strategic adaptation to evolving technology landscapes. The group's social engineering tactics are equally advanced, showcasing meticulous research into target profiles and interests. These characteristics collectively paint a picture of a well-resourced, highly adaptable threat actor. APT37's operations often foreshadow broader trends in the APT landscape, making them a critical focus for global cybersecurity efforts.

## **References**

MITRE ATT&CK. (2023). "APT37, G0067." https://attack.mitre.org/groups/G0067/