## **APT38**

I. **Introduction**

APT38 is an very complex North Korean state-sponsored cyber threat group, also known as the Lazarus Group, HIDDEN COBRA, or Bluenoroff. Since at least 2014, APT38 has become most known for financial cyber operations, targeting banks and financial institutions globally. APT38 differs from many other APT groups in that its mission is very clear: to generate revenue for the North Korean regime in many cases through large-scale cyber heists.

## **II. Tactics**

APT38's tactical approach is characterized by

1. ***Long-term Bank Compromise***

The group is known for spending extended periods (sometimes over a year) inside a victim's network before executing their final operation.

1. ***Custom Malware Development***

APT38 invests heavily in developing and maintaining custom malware tools specifically designed for financial systems.

1. ***Living Off the Land***

The group frequently uses legitimate tools and operating system features to blend in with normal system operations.

1. ***Destructive Measures***

Unlike many financially motivated threat actors, APT38 often deploys destructive malware to cover their tracks post-heist.

1. ***Multi-stage Operations***

Their attacks typically involve multiple stages, from initial reconnaissance to final fund exfiltration.

## **III. Techniques**

APT38 employs a wide array of sophisticated techniques

|  |  |
| --- | --- |
| **Technique** | **Description** |
| **Spear-phishing (T1566.001, T1566.002)** | Use of meticulously crafted emails targeting specific employees within financial institutions.  Often leveraging job recruitment themes or industry-specific lures. |
| **Watering Hole Attacks (T1189)** | Compromise of legitimate websites frequented by employees of target institutions. |
| **Custom Malware Deployment** | The group uses custom-developed malware families such as DYEPACK, DarkComet, NESTEGG, KillDisk, and BANKSHOT.  Deployment of specialized malware designed to interact with SWIFT banking systems. |
| **Lateral Movement** | The group uses legitimate Windows admin tools like PsExec (T1021.002).  Exploitation of Active Directory and Windows SMB for network traversal (T1021.002). |
| **Command and Control (C2) Infrastructure** | Use of compromised servers worldwide as proxy C2 nodes.    Implementation of custom C2 protocols over HTTPS (T1071.001). |
| **Defense Evasion** | Timestomping of malware files to avoid temporal detection (T1070.006).    Use of code signing certificates to make malware appear legitimate (T1553.002). |
| **Credential Access** | Deployment of keyloggers and credential dumping tools like Mimikatz (T1003.001).  Brute-force attacks against network services and accounts (T1110). |

## **IV. Procedures**

APT38's typical attack chain follows this sequence

***1. Initial Access***

a. Spear-phishing emails are sent to targeted employees, often containing malicious attachments or links.

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

***2. Execution and Persistence***

a. Upon successful compromise, APT38 deploys initial stager malware, often disguised as legitimate software.

b. The group establishes multiple persistence mechanisms, including the use of scheduled tasks and Windows services.

***3. Privilege Escalation and Credential Access***

a. APT38 leverages both public and private exploits to elevate privileges within the compromised network.

b. They deploy credential harvesting tools to gather additional access credentials.

***4. Discovery and Lateral Movement***

a. Extensive network reconnaissance is conducted to map out the target's infrastructure.

b. The group moves laterally using both stolen credentials and exploits, focusing on identifying systems involved in financial transactions.

***5. Collection and Exfiltration***

a. Once access to financial systems is obtained, APT38 often deploys specialized malware to interact with SWIFT systems.

b. They manipulate transaction data and initiate fraudulent transfers to accounts under their control.

***6. Impact and Cover-up***

a. After successfully exfiltrating funds, the group often deploys destructive malware like BOOTWRECK or KILLDISK.

b. This destructive phase serves to both cover their tracks and complicate forensic analysis.

## **V. Summary**

With bold tactics and extensive reach, APT38 has gained significant attention in cybersecurity circles. One apparent example was the notorious 2016 Bangladesh Bank heist, where they managed to steal $81 million after nearly getting away with a cool $1 billion. It epitomized how well the group knew inside out international banking and how effectively they knew how to manipulate SWIFT networks.

But what really sets APT38 apart is that it holds a very unique position of being a very advanced APT group, yet at the same time, a financially motivated cybercrime operation. Its techniques and tools are as good as those of Tier-1 nation-state actors, but its main goal remains financial in nature, instead of espionage. This rare combination is thought to be driven by North Korea's need to acquire foreign currency in light of stringent international sanctions. Its operations are marked with great patience; the group is said to have spent months or even years inside target networks before pulling a heist. This careful attitude gives them an all-round view of the targets' systems and procedures. Destructive malware often follows in the wake of APT38 as a way of frustrating forensic analysis and creating noise aimed at delaying complete discovery of the attack's nature and extent after pulling off a heist. The malware arsenal deployed by the group is constantly evolving, getting more sophisticated with each passing day, and further improved in evasive technologies. Considering that international pressures on North Korea are not ceasing, APT38 is very likely to continue being one of the most outstanding threats financial institutions face worldwide, proof of how intertwined geopolitics and cybercrime can be in today's digital environment.

## References

MITRE ATT&CK. (2024). "APT38, G0088."https://attack.mitre.org/groups/G0082/