Contents

[**G0078 Gordon Group** 2](#_Toc179357346)

[**I**. **Introduction** 2](#_Toc179357347)

[**II**. **Tactics** 2](#_Toc179357348)

[**III. Techniques** 2](#_Toc179357349)

[**IV. Procedures** 3](#_Toc179357350)

[**V. Summary** 5](#_Toc179357351)

[**References** 6](#_Toc179357352)

## **G0078 Gordon Group**

## **I**. **Introduction**

The Gordon Group, also known as APT51, Luckymouse, and Iron Tiger, is a Chinese state-sponsored advanced persistent threat (APT) group that has been active since at least 2013. This group is known for its focus on strategic intelligence gathering. It primarily targets government entities, defense industries, and other high-value organizations across many countries, with a particular emphasis on Central Asia and Russia.

## **II**. **Tactics**

Gordon Group's tactical approach is depicted by

1. ***Strategic Intelligence Gathering***

The group focuses on collecting sensitive information related to national security, defense, and geopolitical issues.

1. ***Supply Chain Attacks***

Gordon Group is known for compromising third-party software and services to gain access to their ultimate targets.

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

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

1. ***Adaptive Toolset***

The group regularly updates and modifies its malware and tools to evade detection and improve efficacy.

1. ***Dual-use Exploitation***

Gordon Group often leverages both custom and publicly available tools in their operations.

## **III. Techniques**

Gordon Group employs a range of sophisticated techniques

|  |  |
| --- | --- |
| Technique | Description |
| Spear-phishing (T1566) | Use of carefully crafted emails with malicious attachments (T1566.001).  Employment of links leading to compromised websites (T1566.002). |
| Supply Chain Compromise (T1195) | Infiltration of software supply chains to distribute malware through trusted channels. |
| Custom Malware Deployment | Use of custom malware families such as HyperBro, PlugX, and SysUpdate. |
| Exploit of Public-Facing Applications (T1190) | Targeting of vulnerabilities in web-facing applications for initial access. |
| Command and Control (C2) Infrastructure | Use of compromised legitimate websites for C2 communication (T1102.002).  Implementation of custom C2 protocols over HTTPS (T1071.001). |
| Credential Access | Deployment of keyloggers and credential dumping tools (T1003).  Brute-force attacks against exposed services (T1110). |
| Defense Evasion | Use of code signing certificates to make malware appear legitimate (T1553.002).  Timestomping of malware files to avoid temporal detection (T1070.006). |

## **IV. Procedures**

Gordon Group's typical attack chain follows this sequence

***1. Initial Access***

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

b. In some cases, compromised software updates or legitimate applications are used as initial infection vectors.

***2. Execution and Persistence***

a. Upon successful compromise, Gordon Group typically deploys a first-stage loader.

b. The loader then installs more sophisticated malware, such as HyperBro or PlugX, establishing persistence through various methods including DLL side-loading.

***3. Privilege Escalation***

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

b. They often exploit known vulnerabilities in Windows systems or third-party applications.

***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 high-value systems and data.

***5. Collection and Exfiltration***

a. Once access to valuable systems is obtained, Gordon Group deploys additional tools for data collection.

b. Exfiltration is often conducted in stages, with data being compressed and encrypted before transmission.

***6. Operational Security***

a. The group regularly updates their C2 infrastructure to avoid detection.

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

## **V. Summary**

The operation of the Gordon Group offers certain understanding of the Priorities and Tactics of Chinese Cyber Espionage. They primarily targeted Central Asian states’ authorities and military personnel, which interests coincide with China’s geopolitical concerns regarding the Belt and Road Initiative program.

However, the most interesting elements of Gordon Group’s operations include its supply chain attacks. In 2018, they were observed compromising a national data center in a Central Asian country, which allowed them to conduct watering hole attacks against a wide range of government resources. This operation showcased their ability to think strategically and compromise high-value targets that provide access to multiple end-goals simultaneously.

The group's malware arsenal is also of particular interest to the cybersecurity community. Their HyperBro backdoor, for instance, demonstrates advanced capabilities including the ability to bypass User Account Control (UAC) and leverage DLL side-loading for stealth. The continuous evolution of their tools highlights the group's dedication to maintaining their operational effectiveness in the face of improving defensive measures. Gordon Group's use of both custom and publicly available tools is another notable characteristic. This dual approach allows them to balance the need for specialized capabilities with the benefits of using more common tools that may blend in with normal system operations. It also potentially provides some level of plausible deniability, as the use of public tools makes attribution more challenging.

The group's targeting of Central Asian countries, which are often caught between the spheres of influence of China and Russia, provides an interesting geopolitical context to their operations. Their activities offer insights into China's cyber priorities in regions where it's expanding its economic and political influence. So far, as China keeps expanding its international power and moving to protect its interests, it appears that elements such as Gordon Group are expected to continue with their work in conducting cyber operations. Their activities highlight the significance of supply chain security, the lack of proper threat intelligence sharing between likely targets, and the requirement for far more advanced behavioral analytics-based detection platforms to recognize such pernicious threats.

## **References**

1. Kaspersky Lab. (2018). "LuckyMouse hits national data center to organize country-level waterholing campaign." <https://securelist.com/luckymouse-hits-national-data-center/86083/>

2. MITRE ATT&CK. (2021). "Gordon Group, G0078." <https://attack.mitre.org/groups/G0078/>