Contents

[**G0080 Cobalt Group** 2](#_Toc179358250)

[**I. Introduction** 2](#_Toc179358251)

[**II. Tactics** 2](#_Toc179358252)

[**III. Techniques** 2](#_Toc179358253)

[**IV. Procedures** 3](#_Toc179358254)

[**V. Summary** 5](#_Toc179358255)

[**References** 6](#_Toc179358256)

## **G0080 Cobalt Group**

## **I. Introduction**

The Cobalt Group, also known as Cobalt Gang or Cobalt Spider, is a sophisticated cybercriminal organization that has been active since at least 2016. Unlike many state-sponsored APT groups, Cobalt Group is largely motivated by financial gain. They are notorious for targeting financial institutions, particularly banks and ATM networks, across Europe, North America, and Southeast Asia. The group's name comes from their use of a penetration testing framework called Cobalt Strike.

## **II. Tactics**

Cobalt Group's tactical approach is characterized by

1. ***Targeted Financial Attacks***

It focuses on compromising banking systems, ATM networks, and financial software.

1. ***Social Engineering***

They rely heavily on sophisticated phishing campaigns to gain initial access.

1. ***Living off the Land***

The group uses legitimate tools and software to blend in with normal system operations.

1. ***Multi-stage Attacks***

Cobalt group employs a deployment of a series of tools and techniques to progressively gain deeper access to target systems.

1. ***Adaptive Techniques***

Continuous evolution of tactics to bypass security measures and avoid detection.

## **III. Techniques**

Cobalt Group employs a range of sophisticated techniques

|  |  |
| --- | --- |
| **Techniques** | **Description** |
| Spear-phishing Campaigns (T1566) | Use of carefully crafted emails with malicious attachments or links, often impersonating financial institutions or vendors. |
| Exploitation of Public-Facing Applications (T1190) | Targeting of vulnerabilities in web-facing applications for initial access. |
| Custom Malware Deployment | Use of custom malware such as CobInt and More\_eggs backdoors |
| Legitimate Penetration Testing Tools | Extensive use of Cobalt Strike framework for post-exploitation activities (T1588.002) |
| Command and Control (C2) Infrastructure | Use of compromised websites and legitimate cloud services for C2 communication (T1102.002). |
| Credential Access | Deployment of keyloggers and credential dumping tools (T1003) |
| Lateral Movement | Use of stolen credentials and exploitation of network vulnerabilities (T1210) |

## **IV. Procedures**

Cobalt Group's typical attack chain follows this sequence

***1. Initial Access***

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

b. In some cases, vulnerabilities in public-facing applications are exploited.

***2. Execution and Persistence***

a. Upon successful compromise, an initial payload is deployed, often a lightweight downloader.

b. This downloader then fetches and installs more sophisticated malware, such as CobInt.

c. Persistence is established through various methods, including scheduled tasks and registry modifications.

***3. Privilege Escalation***

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

b. Tools like Mimikatz are often used for credential dumping and privilege escalation.

***4. Defense Evasion***

a. Cobalt Group uses sophisticated obfuscation techniques to avoid detection.

b. They often leverage legitimate tools and processes to blend in with normal system operations.

***5. Discovery and Lateral Movement***

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

b. Lateral movement is achieved using both stolen credentials and exploits, focusing on identifying systems involved in financial transactions.

***6. Collection and Exfiltration***

a. Once access to financial systems is obtained, the group often deploys specialized malware to interact with banking systems or ATM networks.

b. Data exfiltration is typically conducted in stages, with stolen data being carefully encrypted and disguised.

***7. Impact***

a. In many cases, the final stage involves unauthorized financial transactions or ATM cash-outs.

b. The group has also been known to deploy ransomware in some operations.

## **V. Summary**

Cobalt Group has quickly established itself as a powerful cybercriminal group known for its complex work and preference for the financially motivated attacks. Their operations have affected a number of institutions with many of the heists said to have netted the perpetrators tens of millions of dollars.

One of Cobalt Group’s noticeable strategies is the ability to effectively use of Cobalt Strike penetration testing framework. But with this fake substance, they use what looks like a legitimate security tool, to show that they are sophisticated tech-savvy criminals. Their phishing campaigns are equally as good, commonly where they imitate financial institutions, vendors, or job applicants with highly targeted bait messages that are personalized to their victims’ interests. Such a level of detail in social engineering shows that much is known about how the financial industry operates. A quality demonstrated through the functional groups is the flexibility in their behavior as they change strategies in response to countermeasures adopted by the targets through increased awareness of cyber threats.

Cobalt Group operate globally, attacked financial institutions in different continents and the recent rise underscores modern day cybercrimes and the difficult that the financial sector in particular and industry in general face in combating the activities of well established and highly capable group(s). The operations of these structures have facilitated positive changes in the security measures within the financial industry especially in regard to threat intelligence sharing and improved security control mechanisms.

## **References**

MITRE ATT&CK. (2023). "Cobalt Group, G0080." <https://attack.mitre.org/groups/G0080/>