

[Joint Cybersecurity Advisory] Operation Double Barrel (The Relationship Between a State-Sponsored Threat Actor and the Gunra Ransomware Group)

By ATCP

Published: 2026-07-29 · Archived: 2026-09-25 02:01:04 UTC

This technical analysis report was prepared as **part of the joint cybersecurity advisory titled “Advisory on Cyberattacks Targeting Korean Citizens and Businesses by State-Sponsored Hacking Groups”** issued by the Republic of Korea’s National Intelligence Service (NIS), National Police Agency (NPA), Korea Internet & Security Agency (KISA), and Financial Security Institute (FSI).

Overview

AhnLab SEcurity intelligence Center (ASEC) identified evidence that a state-sponsored threat group continuously distributed malware from 2025 through the first half of 2026 by exploiting vulnerabilities in Korean financial security software installed when using financial and institutional services. The attackers induced targets to access malicious URLs through various methods, including watering hole and spear-phishing attacks, and then exploited the vulnerabilities to ultimately install backdoor malware. In particular, legitimate Korean websites across various industries, including media organizations, educational institutions, healthcare institutions, and manufacturing companies, were confirmed to have been abused in watering hole attacks during this period.

Similarly, attack cases were identified in which the same financial security software vulnerabilities were exploited, but Gunra ransomware was ultimately installed to encrypt files and exfiltrate sensitive organizational information. Although the two attacks differed in their ultimate objectives and payloads, numerous commonalities were identified, including the vulnerabilities exploited during initial access, the malware installed, SSH key fingerprints, and network infrastructure such as download and reverse tunneling addresses.

These commonalities suggest that although **the state-sponsored threat group** and **the Gunra ransomware group** appear to be separate threat actors with different ultimate objectives, they may have shared certain techniques, tools, and infrastructure or collaborated to a limited extent during the attacks. Although ASEC cannot definitively determine the relationship between the two threat actors based solely on the information identified to date, it named this campaign “**Operation Double Barrel**” likening the common attack flows and indicators of technical links to two barrels aimed in the same direction.

Based on the activities of the state-sponsored threat group continuously identified from 2025 through the first half of 2026, this report analyzes watering hole and spear-phishing attack cases that occurred in 2026. In particular, it examines vulnerabilities in the financial security software A and the financial security software I, Korean financial security software products exploited in the attacks, as well as the staged payload delivery process. It also analyzes the backdoors ultimately installed, including Struggle (SIGNBT 3.0) and Brandoor (COPPERHEDGE), along with the tools abused during the attacks. In addition, the report examines the possibility of a supply chain attack

based on the fact that multiple websites abused in watering hole attacks were associated with the same Korean website development and management company. Finally, it compares commonalities in the vulnerabilities, malware, credentials, and network infrastructure identified in the state-sponsored threat group's attack cases and the Gunra ransomware attack cases to analyze the relationship between the two attacks.

For more detailed information, please refer to the attached report.

Korean Report : [\[AhnLab\]Operation Double Barrel\(KOR\)\(2026.07.30\).pdf](#)

English Report : [\[AhnLab\]Operation Double Barrel\(ENG\)\(2026.07.30\).pdf](#)

Table of Contents

Overview

Report

1. Watering Hole Attack Cases

1.1. Watering Hole Attacks

1.1.1. Overview of Watering Hole Attacks

1.1.2. Indicators of a Supply Chain Attack Through a Server Hosting Provider and Website Development/Management Company

1.1.3. Notable Attack Cases

1.1.4. Domain Registrant Information

1.2. Spear-Phishing Attacks

1.2.1. Overview of Spear-Phishing Attacks

1.2.2. Notable Attack Cases

2. Vulnerability and Malware Analysis

2.1. Exploited 0-day Vulnerabilities

2.1.1. Analysis of a Vulnerability in the Financial Security Software A

2.1.2. Vulnerability of the Financial Security Software I

2.2. Malware Analysis

2.2.1. Backdoor – Struggle (SIGNBT 3.0)

2.2.2. Backdoor – Brandoor (COPPERHEDGE)

2.2.3. Privilege Escalation Tool

2.2.4. Dropper

3. Gunra Ransomware Group and Suspected Collaboration Case

3.1. Attack Case Analysis

3.2. Indicators of Technical Links

3.2.1. Use of the Same Watering Hole Page and Exploitation of a Vulnerability of the Financial Security Software A

3.2.2. Installed Malware and Its Characteristics

3.2.3. SSH Key Fingerprint

3.2.4. Network Infrastructure

3.2.5. Anti-Forensic Techniques

Conclusion

AhnLab Response Status

IoC (Indicators of Compromise)

File Hashes (MD5)

Related Domains, URLs, and IP Addresses

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

