Operation Artemis: Analysis of HWP-Based DLL Side Loading Attacks

By Genians

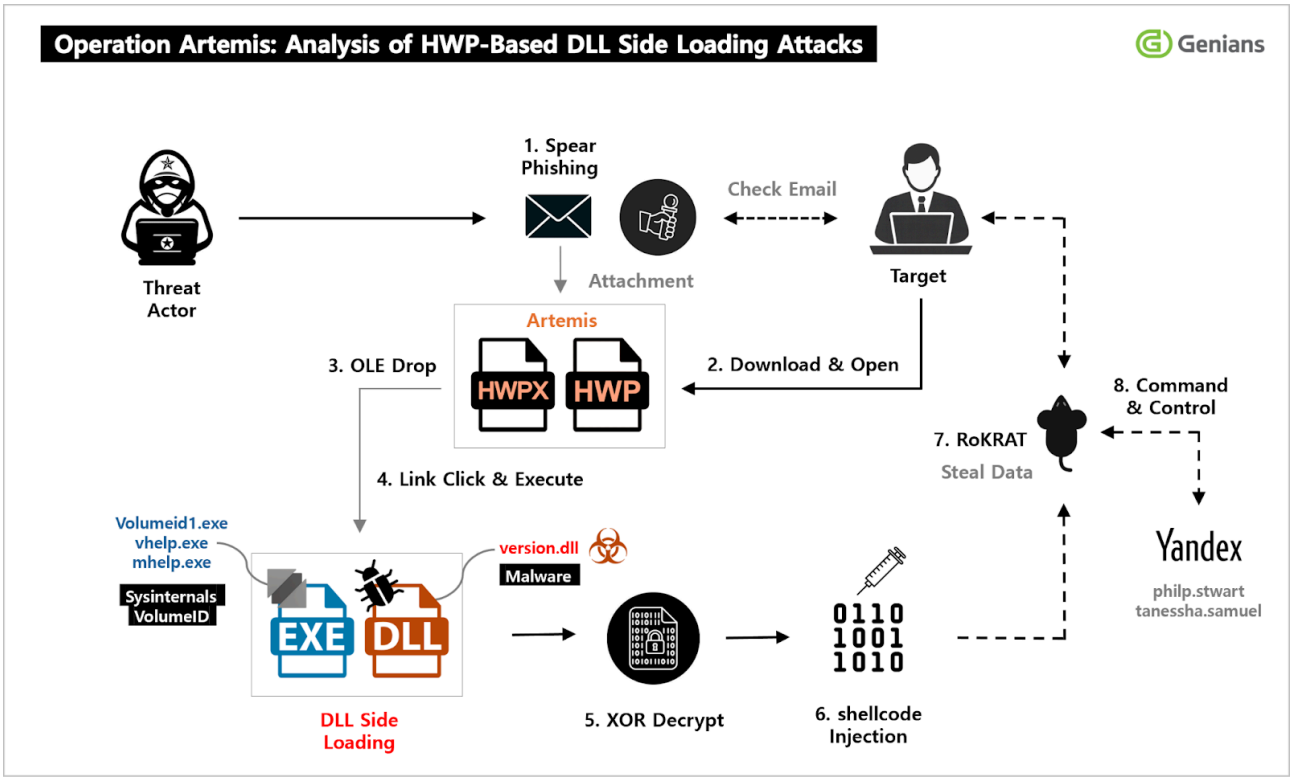
Published: 2025-12-21 · Archived: 2026-04-05 14:04:39 UTC

◈ Key Findings

- The threat actor poses as a writer for Korean TV programs and reaches out to targets for casting or interview arrangements.
- A short self-introduction and legitimate-looking instructions are used to build trust.
- The attacker distributes a malicious HWP file disguised as a pre-interview questionnaire or event guide document.
- The attack combines initial HWP execution with DLL side loading to evade signature-based detection.
- Real-time monitoring through an EDR solution is essential for identifying abnormal behavior.

1. Overview

Genians Security Center identified the “Artemis” campaign conducted by the APT37 group. The threat actor embedded a malicious OLE object inside an HWP document in a covert manner. The attack chain is triggered when the user trusts the document content and clicks the hyperlink.



[Figure 1-1] Overview of the Attack Flow

When the OLE object was loaded, the threat actor used a masquerading technique launching a legitimate process first. This multi-stage procedure leverages legitimate execution flow to evade detection by signature-based security solutions. Subsequently, the payload was executed by calling a malicious DLL within the execution context of the legitimate process.

This tactic is intended to evade detection by intricately combining initial execution with privilege escalation. **However, Endpoint Detection and Response (EDR) solutions can identify such abnormal execution flows through anomaly detection rules.**

In our previous report titled "RoKRAT Shellcode and Steganographic Threats: Analysis and EDR Response Strategies," published on August 4th, we provided a detailed overview of APT37's LNK shortcut–based and HWP OLE–based attack cases. That analysis also described the steganography technique used in the image file that was additionally downloaded after the DLL side-loading stage.

As these examples illustrate, the threat actor continues to employ malicious HWP documents alongside its LNK-based strategy, highlighting the need for heightened user awareness.

This campaign is characterized by a detection-evasion strategy that leverages legitimate processes, a multi-stage execution chain, and sophisticated techniques that blend normal execution flow with malicious behavior. In particular, running the malicious payload under the context of a legitimate process significantly increases the difficulty of analysis, making identification and response more challenging.

Overall, this attack demonstrates APT37's ongoing pattern of highly developed reconnaissance and infiltration activities. It also indicates that the group continues to refine its capabilities by leveraging advanced technical methods.

2. Background

On October 27, 38 North, a U.S.-based media outlet specializing in North Korea, published a report titled "HWP as an Attack Surface: What Hancom's Hangul Word Processor Means for South Korea's Cyber Posture as a US Ally."

According to the report, the Hangul Word Processor (HWP) document format, which is widely used as a standard in South Korea, has effectively become a fixed attack surface. The report notes that North Korean cyber operators have repeatedly exploited this format in their attempts to infiltrate government, military, and key industrial networks in South Korea.

In practice, HWP-based attacks continue to be observed in South Korea. From the threat actor's perspective, the behavior of malware can shift at any time depending on the environment and conditions, and the range of available tactics is extremely broad.

It is therefore critical to identify which techniques are being used and to strengthen response capabilities based on that understanding to prepare for similar threats.

Accordingly, this threat intelligence report aims to provide a detailed analysis of the background and tactical characteristics of an attack scenario that occurred in the field, offering the foundational insight needed to develop appropriate response measures.

3. Attack Progression

3-1. Steganography + DLL Side Loading

The initial intrusion occurred through an HWP document delivered via spear-phishing. When the malicious OLE object embedded in the document was executed, it ultimately provided the attacker with initial access to the user environment.

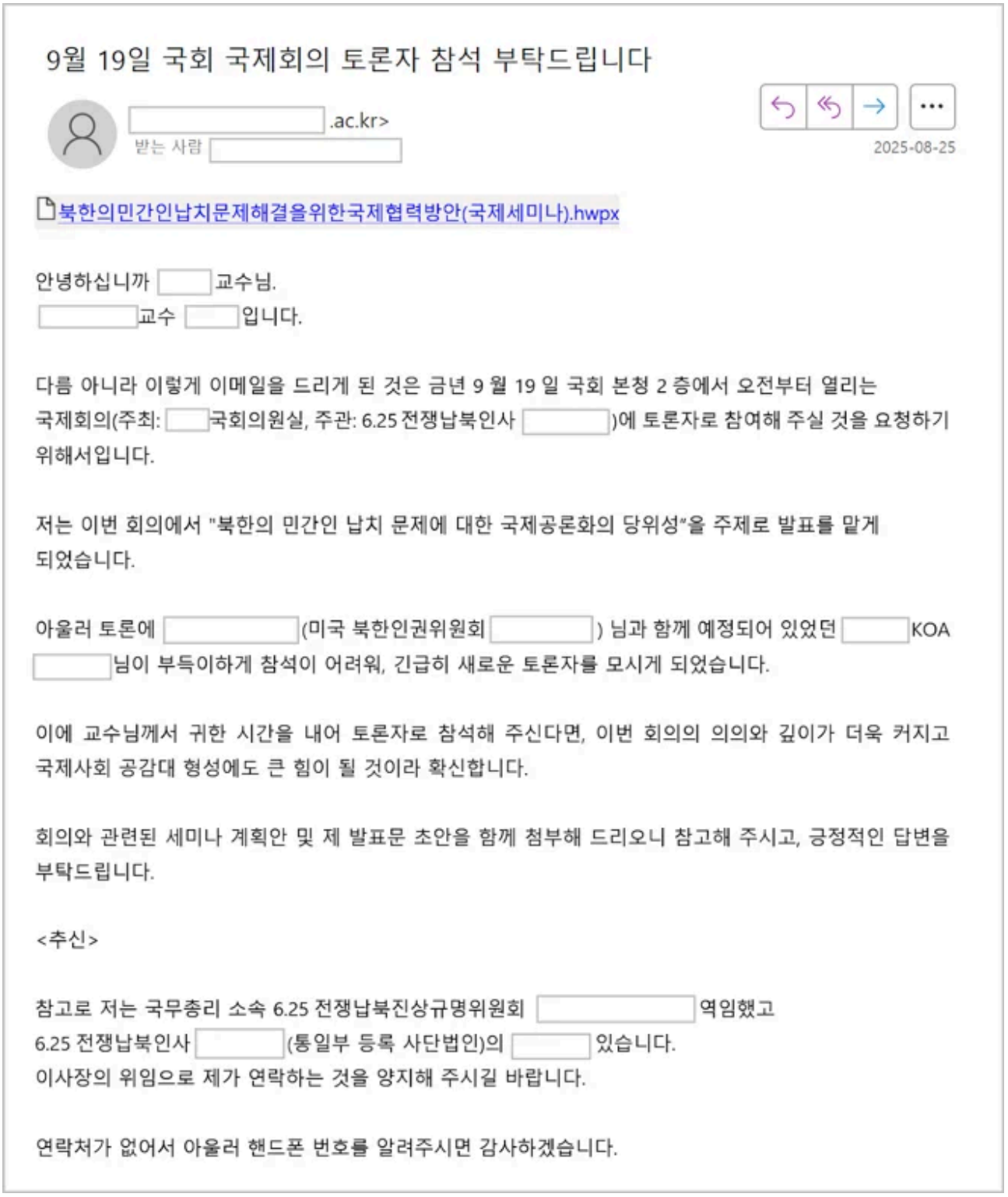
The delivered threat leveraged a combination of techniques, including steganography and DLL side loading, to conceal its execution flow. **During the side-loading stage, a system utility from Microsoft Sysinternals was abused. The attacker placed a tampered malicious DLL in the same directory as the executable, causing the program to mistake it for a legitimate DLL and load it.**

Since July, the threat actor has covertly deployed the RoKRAT module using steganography-based methods. **In particular, it was confirmed that in August the actor used a previously unreported portrait image as part of the attack.** For reference, the two grayscale images shown for comparison correspond to samples identified in July.

[Figure 3-1] Photo Used in the Steganography Attack

3-2. Attack Scenario

This report presents a comprehensive analysis of the APT campaign that was conducted continuously from August to November, beginning with the newly identified steganography-based technique discovered in August. Through an investigation of spear-phishing activity sustained over roughly 4 months, we identified how the malicious HWP documents used by the attacker evolved and became increasingly sophisticated over each iteration.



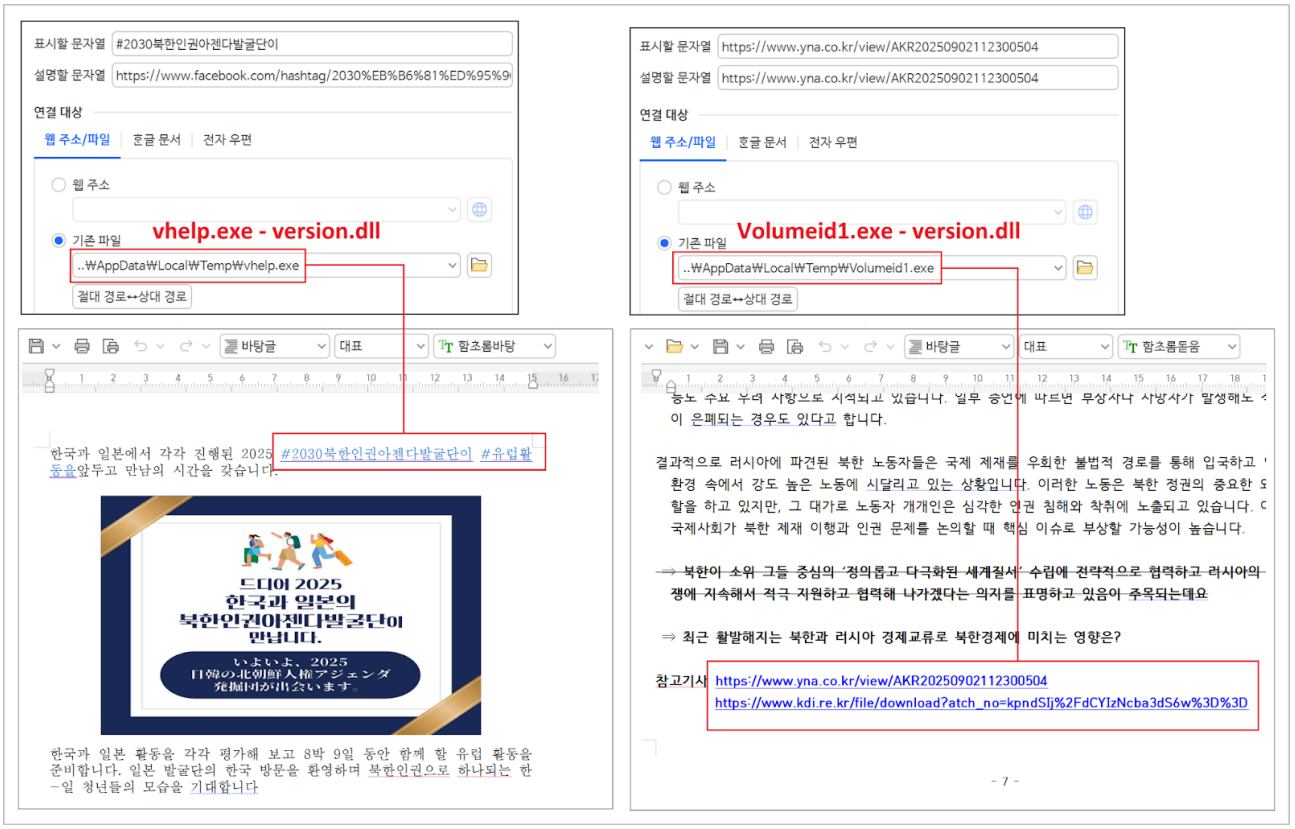
[Figure 3-2] Spear-Phishing Email Disguised as a Discussion Invitation

At the end of August, the attacker sent an email disguised as an official invitation to participate in a National Assembly international conference and impersonated a university professor with a high level of public credibility. The email included an attachment titled “북한의민간인납치문제해결을위한국제협력방안(국제세미나) *(International Cooperation Strategies for Resolving North Korea’s Civilian Abduction Issue (International Seminar)*.hwpx,” and a targeted deception tactic was used that aligned with the recipient’s area of interest.

A similar case was identified in which **the attacker impersonated a writer for a major Korean broadcasting program and requested an interview related to the North Korean regime and human rights. After conducting multiple trust-building conversations, the attacker ultimately delivered a malicious HWP document.** The investigation confirmed that the names of two writers from separate broadcasting programs had been used without authorization, indicating that the attacker used this impersonation to establish social credibility with the victim.

[Figure 3-3] Spear-Phishing Message Disguised as an Interview Request

In addition to cases in which the attacker impersonated university professors or TV writers, multiple incidents were identified where the actor forged documents related to specific commentaries or events. **In these HWP-based attacks, the actor disguised the embedded OLE object as a hyperlink to prompt users to execute it.**



[Figure 3-4] OLE Hyperlink and Target File

These cases are assessed as social-engineering-based threat activities that increase contact credibility by misusing the identities of reputable institutions or experts.

3-3. Tactic Reuse

In the case of impersonating a TV writer, the actor did not use malicious links or attachments during the initial contact phase, instead establishing trust through natural conversations. It was confirmed that the actor then delivered a malicious file disguised as an interview request only to individuals who responded to the communication.

For reference, an attack scenario using the same broadcasting company writer’s identity had already been observed in early June 2023. At that time, a malicious archive named "북한이탈주민 초빙강의*(North Korean Defector Invited Lecture)*.zip" was distributed, and the malware installed through it revealed the following PDB (Program Database) information.

D:\Sources\MainWork\Group2017\Sample\Release**DogCall.pdb**

[Table 3-1] PDB Strings Embedded in the Malware

This PDB artifact string had previously been introduced in the report titled "APT37 Attack Case Impersonating a North Korean Human Rights Organization," published on May 23, 2023. Although PDB strings are now rarely observed, past samples from the same malware family repeatedly revealed various types of PDB paths.

D:\HighSchool\version 13\First-Dragon(VS2015)\Sample\Release**DogCall.pdb**
d:\HighSchool\version 13\2ndBD\T+M\T+M\Result**DocPrint.pdb**
D:\HighSchool\version 13\VC2008(Version15)\T+M\T+M\TMProject\Release**ErasePartition.pdb**
E:\Happy\Work\Source\version 12\First-Dragon\Sample\Release**DogCall.pdb**
e:\Happy\Work\Source\version 12\T+M\Result**DocPrint.pdb**

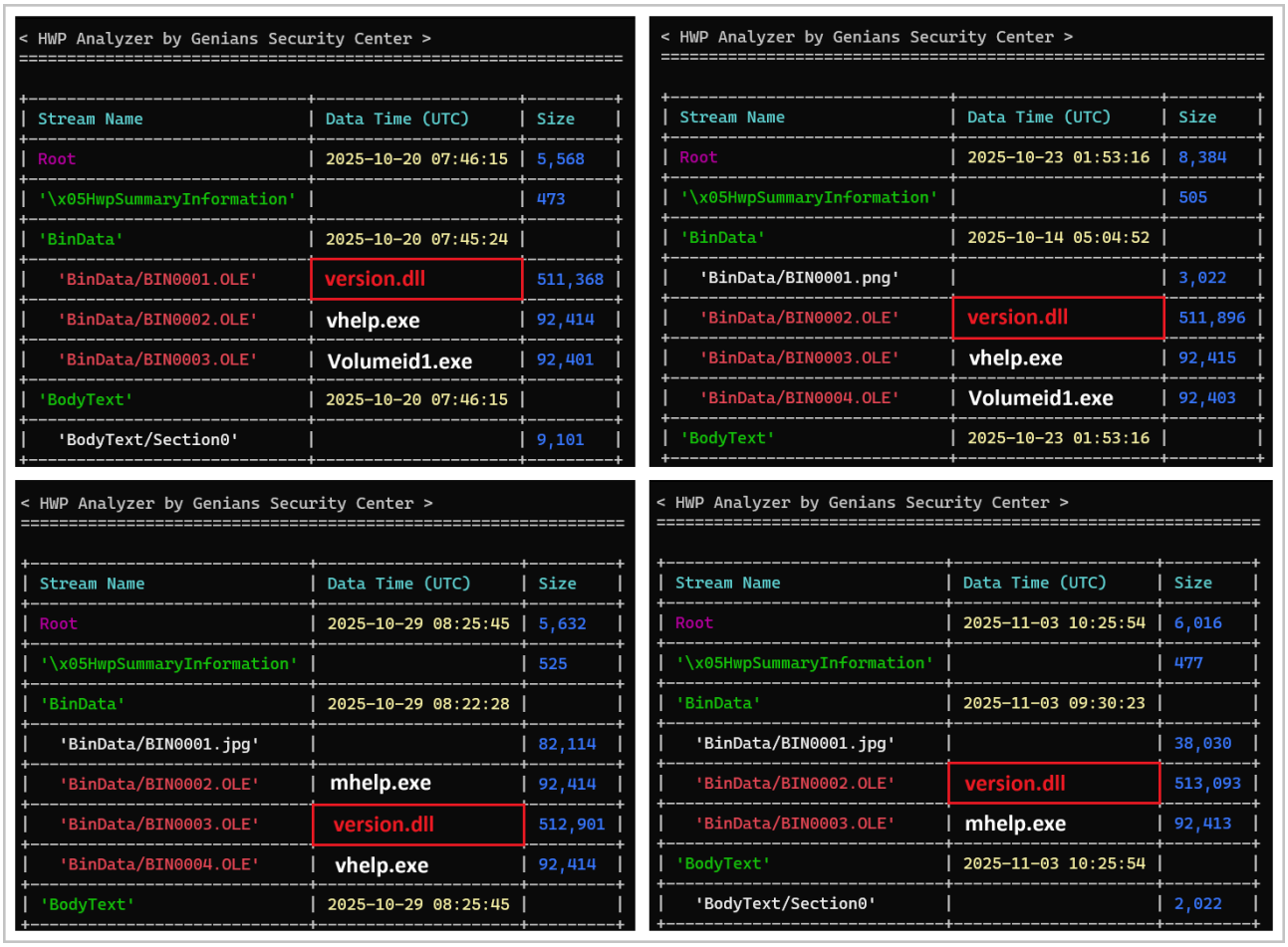
[Table 3-2] PDB Strings Identified in Malware from Related Families

There are cases in which previously used attack tactics were modified or reused in the same form. Accordingly, systematically understanding past TTPs that exhibit similar characteristics plays an important role in improving the effectiveness of responding to already known threats by providing insight into the threat landscape.

4. Detailed Analysis

4-1. HWP Structure Analysis

A comparison of the Root Entry structures across four representative HWP malicious documents used in real attacks showed that all samples contained a stream with an OLE object inside the BinData storage. This OLE embedding method is a typical pattern used for loading malicious payloads.



[Figure 4-1] Comparison of Internal Structures in HWP Malware Samples

The embedded OLE objects in all samples contained functionality that creates a malicious module named "version.dll" in the temporary directory "%TEMP%".

Additionally, depending on specific execution conditions, files masquerading under various names such as "Volumeid1.exe," "vhelp.exe," and "mhelp.exe" are also generated. All of these files are legitimate [Sysinternals VolumeId] utilities.

These executables load the malicious file named **"version.dll"** located in the same directory by performing a **DLL side-loading technique**, which allows the malicious library to run stealthily.

Because of this, pattern-based detection that relies solely on the presence of EXE processes is not effective for identifying this threat. Therefore, an EDR-based active response capability is required to monitor the point at which the "version.dll" file is introduced during the early stages of the attack chain and to detect abnormal behavior in real time.

This enables early identification of the initial intrusion and the establishment of a response strategy that blocks the execution of subsequent payloads in advance.

Some of the HWP malicious documents used at the time commonly had "Hazard" recorded in the Author field and "Artemis" in the Last Saved By field.

```
< HWP Analyzer by Genians Security Center >
[Hex Dump: red=Author, blue=Last Saved By, magenta=Last Saved Time]

Offset    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F   ASCII
00000000  FE FF 00 00 0D 00 00 00 60 B6 A2 9F 61 10 D4 11  ........`...a...
00000010  B4 C6 00 60 97 C0 9D 8C 01 00 00 00 60 B6 A2 9F  ...`........`...
00000020  61 10 D4 11 B4 C6 00 60 97 C0 9D 8C 30 00 00 00  a......`....0...
00000030  AD 01 00 00 0E 00 00 00 02 00 00 00 78 00 00 00  ............x...
00000040  03 00 00 00 90 00 00 00 04 00 00 00 9C 00 00 00  ................
00000050  14 00 00 00 B4 00 00 00 05 00 00 00 F4 00 00 00  ................
00000060  06 00 00 00 00 01 00 00 08 00 00 00 0C 01 00 00  ................
00000070  09 00 00 00 24 01 00 00 0C 00 00 00 6C 01 00 00  ....$.......l...
00000080  0D 00 00 00 78 01 00 00 0B 00 00 00 84 01 00 00  ....x...........
00000090  0E 00 00 00 90 01 00 00 15 00 00 00 98 01 00 00  ................
000000A0  00 00 00 00 A0 01 00 00 1F 00 00 00 07 00 00 00  ................
000000B0  32 00 30 00 32 00 35 00 20 00 5C D5 00 00 00 00  2.0.2.5. .\.....
000000C0  1F 00 00 00 01 00 00 00 00 00 00 00 1F 00 00 00  ................
000000D0  07 00 00 00 48 00 61 00 7A 00 61 00 72 00 64 00  ....H.a.z.a.r.d.
000000E0  00 00 00 00 1F 00 00 00 1B 00 00 00 32 00 30 00  ............2.0.
000000F0  31 00 37 00 44 B1 20 00 38 00 D4 C6 20 00 33 00  1.7.D. .8... .3.
00000100  7C C7 20 00 A9 BA 94 C6 7C C7 20 00 24 C6 C4 D6  |. .....|. .$...
00000110  20 00 34 00 3A 00 35 00 35 00 3A 00 33 00 39 00   .4.:.5.5.:.3.9.
00000120  00 00 00 00 1F 00 00 00 01 00 00 00 00 00 00 00  ................
00000130  1F 00 00 00 01 00 00 00 00 00 00 00 1F 00 00 00  ................
00000140  08 00 00 00 41 00 72 00 74 00 65 00 6D 00 69 00  ....A.r.t.e.m.i.
00000150  73 00 00 00 1F 00 00 00 20 00 00 00 31 00 32 00  s....... ...1.2.
00000160  2C 00 20 00 30 00 2C 00 20 00 30 00 2C 00 20 00  ,. .0.,. .0.,. .
00000170  35 00 33 00 35 00 20 00 57 00 49 00 4E 00 33 00  5.3.5. .W.I.N.3.
00000180  32 00 4C 00 45 00 57 00 69 00 6E 00 64 00 6F 00  2.L.E.W.i.n.d.o.
00000190  77 00 73 00 5F 00 31 00 30 00 00 00 40 00 00 00  w.s._.1.0...@...
000001A0  80 AB C3 38 A3 4C DC 01 40 00 00 00 B0 40 33 3C  ...8.L..@....@3<
000001B0  AC 4C DC 01 40 00 00 00 00 00 00 00 00 00 00 00  .L..@...........
000001C0  03 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00  ................
000001D0  01 00 00 00 00 00 00 00 01 00 00 00 00           ............

Extracted Results:
Author: Hazard
Last Saved By: Artemis
Last Saved Time @0x01AC: b040333cac4cdc01 -> 2025-11-03 10:25:54.235000
```

[Figure 4-2] Information View of the Malicious HWP Document

Based on these indicators, the threat actor who created the malicious HWP document is assessed to have used the username "Artemis," **which is why this report adopts "Artemis" as its operation name**.

As described earlier, identifying the threat element in the early phase is difficult because the first executable invoked by the HWP document is a legitimate utility.

The threat actor exploits this detection gap to perform DLL side-loading, using it to stealthily load the malicious DLL module and progress the attack.

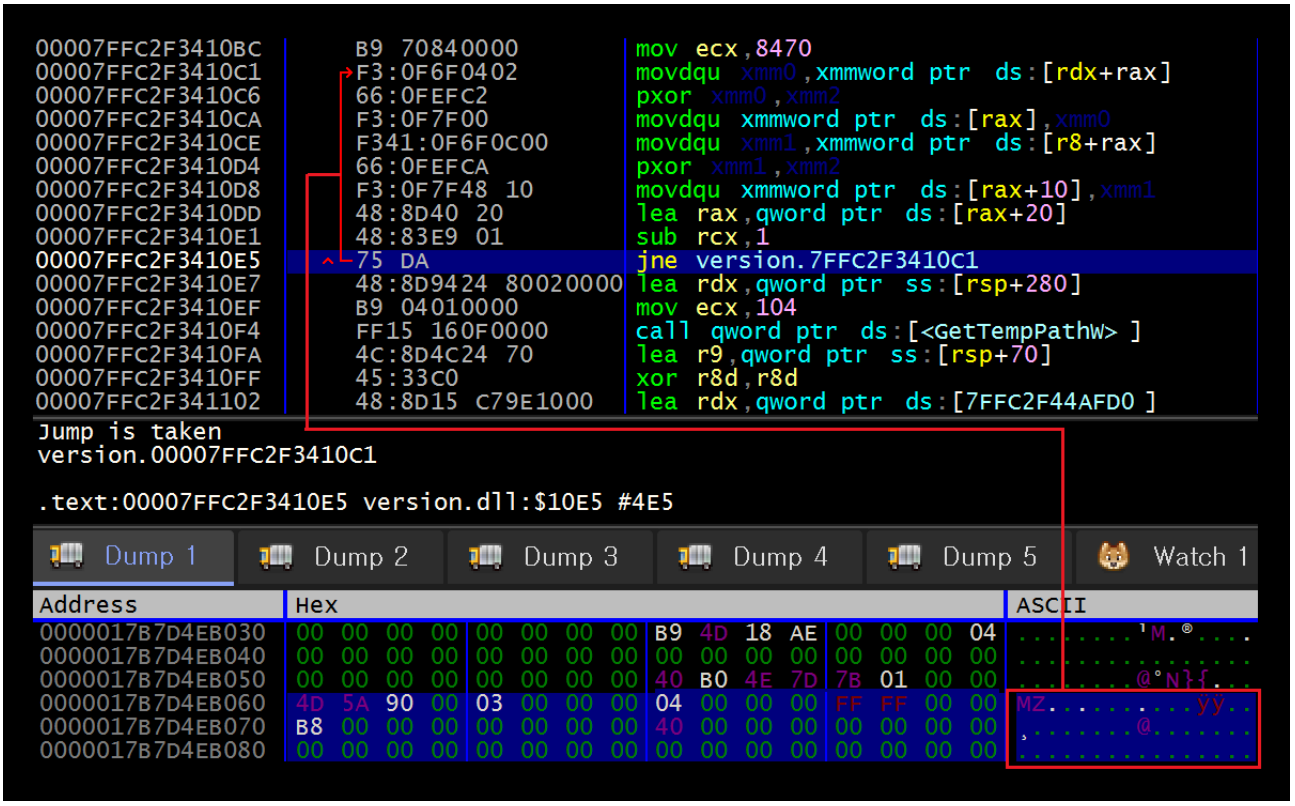
4-2. DLL File Analysis

The "version.dll" file used for DLL side-loading was continuously leveraged from October to November 2025.

In addition, the repeated identification of the same PDB string across multiple samples indicates that these activities can be classified as a consistent threat campaign conducted by the same actor.

D:\Develop**HwpOLE**\HwpOLE\x64\Release**version.pdb**

[Table 4-1] PDB Strings Embedded in the DLL



[Figure 4-3] DLL Logic Analysis

The "version.dll" file hides its internal payload in an encrypted form using a repeated XOR pattern with a single key value (0xFA).

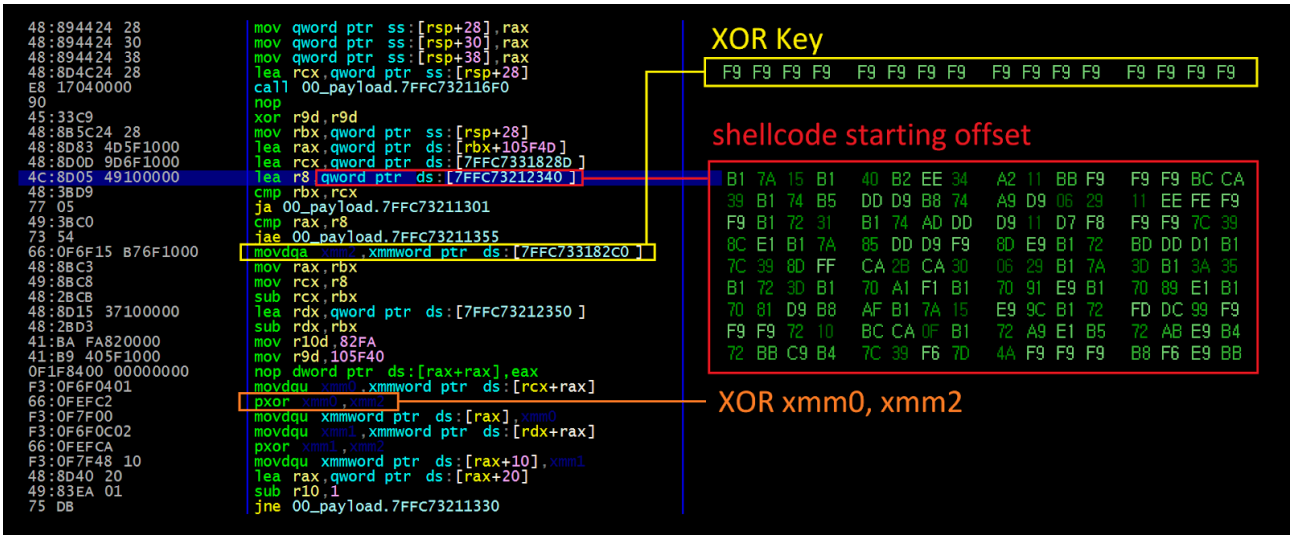
Depending on the environment, it then decrypts the payload by selecting either a standard byte-wise XOR method or a high-speed XOR method that processes 16 bytes (128 bits) at a time using SSE (Streaming SIMD Extensions).

This approach serves as an obfuscation and evasion packing technique designed to bypass signature-based detection while improving decryption speed. The decrypted payload is loaded into memory as a 64-bit DLL and contains its own PDB string.

D:\Develop**HwpOLE**\HwpOLE\x64\Release**common.pdb**

[Table 4-2] PDB Strings Contained in the Decrypted Payload

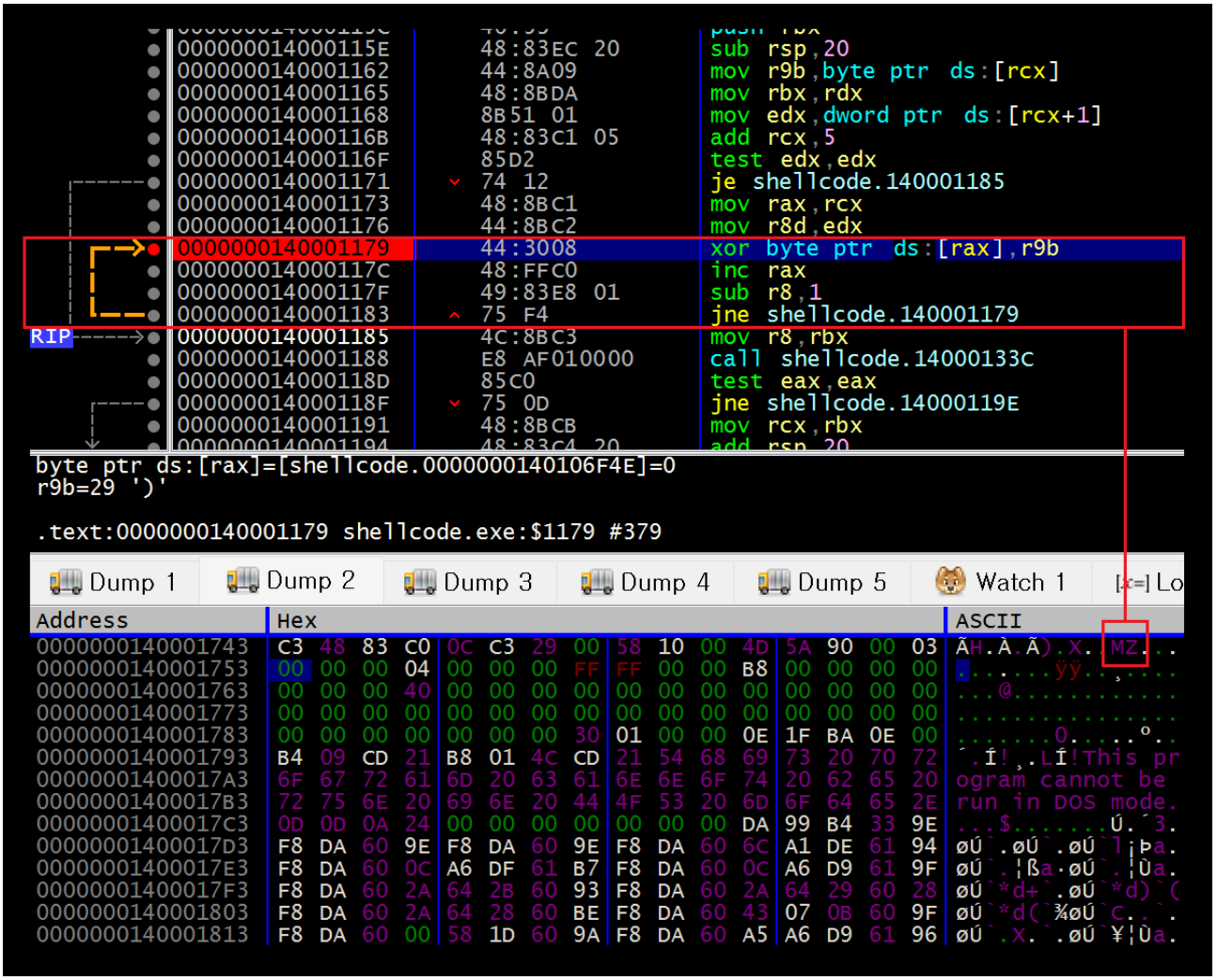
The module decrypts the encrypted block in memory using a continuous 16-byte key (0xF9) through XOR and then transfers control, clearly exhibiting the characteristics of a typical shellcode loader pattern.



[Figure 4-4] Shellcode Decryption Logic

Once all encrypted data blocks are successfully decrypted, fully functional shellcode designed for x64 environments becomes active.

This shellcode undergoes an additional XOR decryption process using a single key (0x29). Once activated, the shellcode serves as the core module that performs the functionality of the final payload, implementing the actual malicious behavior at the last stage of the attack chain.



[Figure 4-5] Final Payload Decryption Logic

The payload, ultimately activated through this multi-stage decryption process, is a typical malicious tool belonging to the RoKRAT family.

5. Threat Attribution

5-1. Similar Cases Involving the APT37 Group

The Genians Security Center has previously released multiple cyber threat intelligence (CTI) analysis reports detailing major cyber operations carried out by the APT37 group.

Cross-referencing these past activities is effective for identifying the characteristics of the tactics, techniques, and procedures (TTPs) consistently employed by the group, and it enables a more precise understanding of the correlation between the group's operational patterns and strategic intent.

- RoKRAT Shellcode and Steganographic Threats: Analysis and EDR Response Strategies
- Analysis of APT37 Attack Case Disguised as a Think Tank for National Security Strategy in South Korea (Operation. ToyBox Story)

- Analysis of malicious HWP cases of 'APT37' group distributed through K messenger
- Analysis of Cyber Recon Activities Behind APT37 Threat Actor
- Beware of RoKRAT fileless attacks by APT37 group
- Attacks Masquerading as Documents Such as North Korean Market Price Reports
- Emergence of APT37 Attacks Targeting macOS Users in South Korea
- APT37 Attack Case Impersonating a North Korean Human Rights Organization

In addition, although APT37's activities are repeatedly identified through various threat intelligence reports, the cases disclosed externally through media articles or selected publications represent only a portion of the group's actual operational scale.

This information asymmetry can lead security teams within organizations or enterprises to underestimate the threat level posed by APT37, which may result in serious security complacency. Relying solely on publicly disclosed information makes it difficult to accurately assess the group's real operational scope, persistence, and infiltration capabilities.

Threat actors such as APT37, which operate strategically over long periods and in an organized manner, are likely to have conducted a considerable number of undiscovered intrusion attempts, persistent APT operations, and early-stage reconnaissance activities carried out in a covert manner.

Therefore, interpreting the threat level as low based solely on currently identified information can distort how security operations teams establish response priorities and define their defensive strategies.

This can result in poor attack surface management, weakened monitoring capabilities, and insufficient threat hunting efforts, ultimately providing highly sophisticated threat groups with opportunities for long-term infiltration and data exfiltration.

For these reasons, continuous monitoring of major state-backed threat organizations that conduct APT attacks, along with raised threat awareness, is essential. Above all, an organizational posture that guards against security complacency is critical.

5-2. Assessment of Attack Tactics

In this attack case, a sophisticated pattern was identified in which the infection vector abusing the HWP OLE structure was combined with DLL side-loading and multi-stage payload encryption and concealment techniques.

This combination of tactics is assessed as an intentional design aimed not only at evading detection but also at strategically increasing the difficulty of analysis.

In particular, the fact that the attack framework is structured to carefully obscure the execution path of RoKRAT suggests that the threat actor has continuously engaged in research and development activities to enhance the tool's stealth and persistence over a long period.

The analysis showed that the actor evades behavior-based detection by inducing legitimate processes to load the malicious DLL, while encrypting the payload across multiple layers to minimize entry points for static analysis.

This represents not a simple list of techniques but a systematically designed approach that considers the entire attack lifecycle, demonstrating clear intent and technical maturity in bypassing existing detection mechanisms.

The increasing sophistication of these techniques indicates that, separate from functional enhancements to RoKRAT itself, an ecosystem-level evolution to improve distribution, concealment, and persistence is also taking place.

This supports the assessment that the threat actor affiliated with APT37 is accumulating capabilities on the basis of long-term strategic objectives rather than operating solely within isolated campaign units.

Consequently, this attack case serves as a strong indicator that state-backed threat actors continue to evolve their tactics to evade detection, and similar multi-layered concealment strategies are highly likely to be applied more extensively in future variants and follow-on attacks.

5-3. RoKRAT Infrastructure Investigation

Analysis showed that the C2 infrastructure identified in Operation Artemis relied on Russia-based Yandex Cloud as a core node.

This aligns with the long-standing tactical patterns demonstrated by APT37, as the group has continually advanced its strategy of abusing legitimate commercial cloud services such as Dropbox, OneDrive, pCloud, and Yandex Cloud to disguise C2 traffic as normal communication.

These services provide stable availability through global CDN infrastructure and offer encrypted communication channels, making them highly suitable for threat actors to use as infrastructure for detection evasion, anonymity, and hindering geographic tracking.

In particular, APT37 was observed to employ a sophisticated operational approach in which cloud storage services are repurposed not merely for uploading or downloading data, but as multi-purpose C2 channels used for command delivery, result collection, encrypted payload hosting, and time-delayed covert operations.

Such abuse of legitimate services is a representative threat behavior that weakens traditional IP-based blocking or simple traffic filtering and complicates efforts to distinguish malicious activity from normal user traffic.

Analysis of the RoKRAT sample used in the attack identified two Yandex Cloud infrastructure account tokens. One was created in October 2023 and the other in February 2025, indicating that the actor maintained C2 accessibility by renewing and managing these account tokens over a long period.

- **Yandex Account Information #1**
    - ***y0__xCvwqD6BxiitDUgtK7BqRJKUd5n0zFOnE5JA1vpobhCHkgkZg***
    - ***philp.stwart***
    - *2025-02-20T05:29:09+00:00*
- **Yandex Account Information #2**

- ***y0__xCgjYyMBxjIhDUgqp2umhIg72AOcJ1RXdfk-fIWhJrHtL7_Iw***
- ***tanessha.samuel***
- ***2023-10-19T07:09:54+00:00***

```
  "attach": "disk:/Mail attachments",
  "messenger": "disk:/Yandex Messenger files",
  "calendar": "disk:/Meeting attachments"
},
"is_paid": false,
"revision": 1764397765559450,
"user": {
  "uid": "2135433519",
  "login": "philp.stwart",
  "display_name": "philp.stwart",
  "country": "us",
  "is_child": false,
  "reg_time": "2025-02-20T05:29:09+00:00"
},
"unlimited_autoupload_enabled": false,
"reg_time": "2025-02-20T05:29:09+00:00",
"is_idm_managed_public_access": false,
"is_idm_managed_folder_address_access": false,
"payment_flow": true,
"hide_screenshots_in_photoslice": false,
```

```
  "attach": "disk:/Mail attachments",
  "messenger": "disk:/Yandex Messenger files",
  "calendar": "disk:/Meeting attachments"
},
"is_paid": false,
"revision": 1763534900044225,
"user": {
  "uid": "1904412320",
  "login": "tanessha.samuel",
  "display_name": "tanessha.samuel",
  "country": "us",
  "is_child": false,
  "reg_time": "2023-10-19T07:09:54+00:00"
},
"unlimited_autoupload_enabled": false,
"reg_time": "2023-10-19T07:09:54+00:00",
"is_idm_managed_public_access": false,
"is_idm_managed_folder_address_access": false,
"payment_flow": true,
"hide_screenshots_in_photoslice": false,
```

[Figure 5-1] Yandex Registration Information of the RoKRAT Threat Actor

Such legitimate cloud-based threat infrastructure is difficult to completely block through the efforts of individual nations or enterprises alone.

Therefore, it is essential to establish a framework that enables the neutralization of malicious tokens and the rapid identification and termination of abused accounts through close cooperation among cloud service providers, international cyber threat response organizations, and diplomatic channels.

In addition, this cooperative framework must extend beyond simple blocking to include accelerated investigative procedures through international coordination, tracking adversary activity, and implementing measures to prevent recurrence. Through such efforts, cloud-based threat infrastructure can be effectively suppressed at a global level.

5-4. Linkage to Threat Actor

The Yandex Cloud login account used, “tanessha.samuel,” shares the same user ID as the pCloud registration account (tanessha.samuel@gmail.com) identified in Operation Toybox Story.

This is not a simple coincidence; analysis confirmed that the registration dates for both cloud services (Yandex and pCloud) match exactly, with both created on October 19, 2023.

- **pCloud Account Information**
- ***Poz17Z5rmhrc0S5SSZJIfPykZBBY1K3GcDmXzwM2kSaK1wfoS40zX***
- ***tanessha.samuel@gmail.com***

- ***Thu, 19 Oct 2023 02:34:32 +0000***

[Figure 5-2] pCloud Registration Information of the RoKRAT Threat Actor

This concurrent account registration strongly indicates that the actor operates multiple cloud infrastructures under a unified identifier, integrating and managing command-and-control (C2) and payload distribution channels.

In addition, the actor's choice to register with Russia-based Yandex and Switzerland-based pCloud at the same time suggests a strategy of evasion and concealment through geographic and legal jurisdictional separation, providing critical clues for attribution and threat tracking.

6. Conclusion

To effectively counter APT37's DLL side-loading and cloud-based concealment strategies, a multilayered defense framework that integrates EDR-driven endpoint and behavior-based detection is essential. The following are the key recommended measures.

- **Detection of Suspicious Activity Related to DLL Side-Loading**

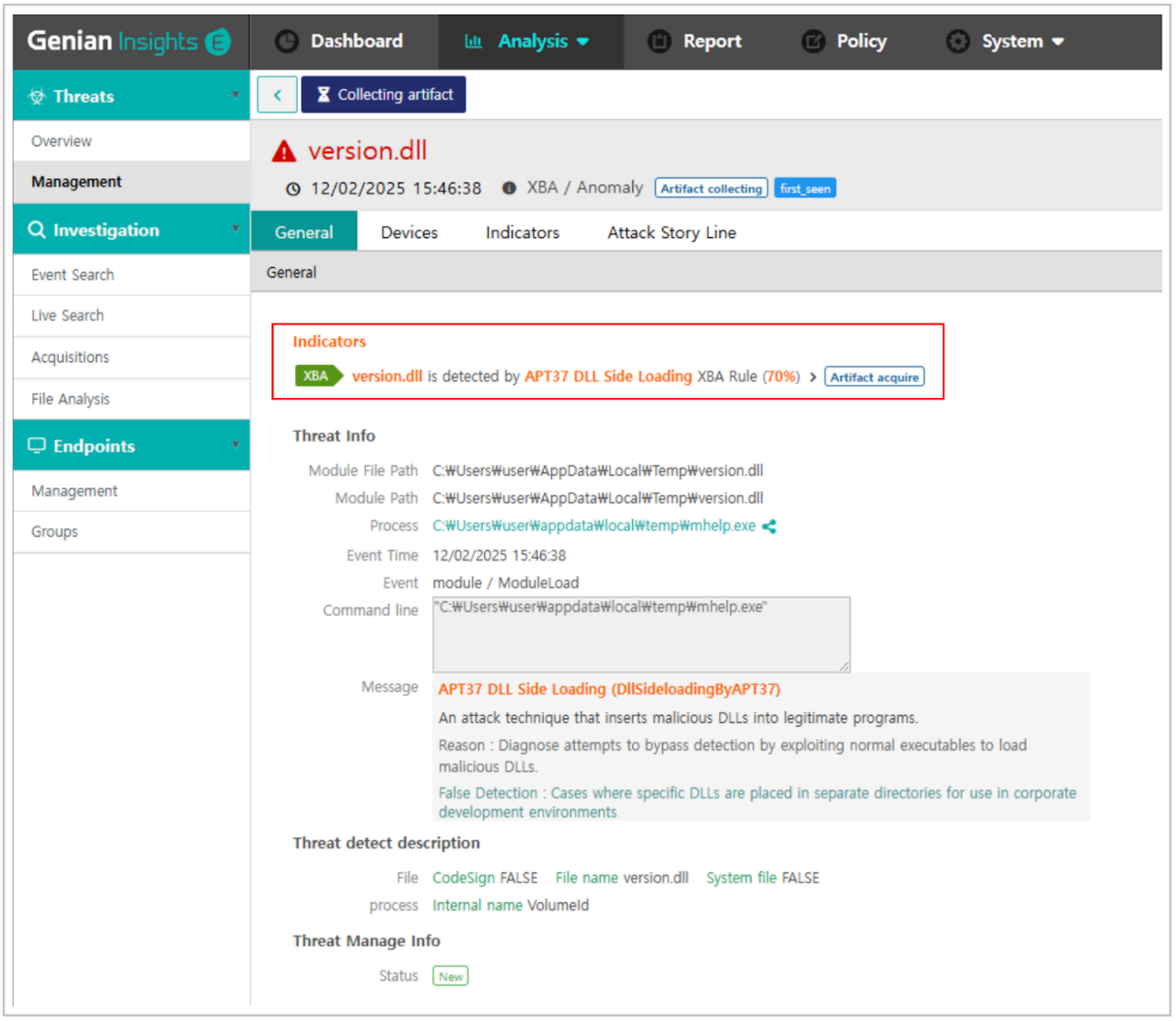
- *Monitor events where legitimate processes load DLLs from abnormal paths*

- *Elevate alert levels for digital signature mismatches*
- *Analyze whether network communication occurs shortly after the execution of a legitimate process*

- **Monitoring Abnormal Behavior of HWP and OLE-Based Executables**
  - *Track child process creation from the HWP process (hwp.exe)*
  - *Elevate alert levels when processes such as rundll32.exe, cmd.exe, or powershell.exe are spawned.*
  - *Track file drop events and temporary-folder DLL loading when OLE objects are executed.*
- **Detecting Endpoint Behavior Linked to Cloud C2**
  - *Apply higher anomaly scores when endpoints communicate with services such as Yandex, Dropbox, or OneDrive outside business hours, outside business pathways, or through non-business processes.*
  - *Classify the host for priority response when a sequential attack chain is observed, including reconnaissance, payload drop, and subsequent cloud communication.*

Genian EDR can effectively detect the DLL sideloading technique leveraged by APT37 through XBA-based detection rules, ensuring that no detection gaps.

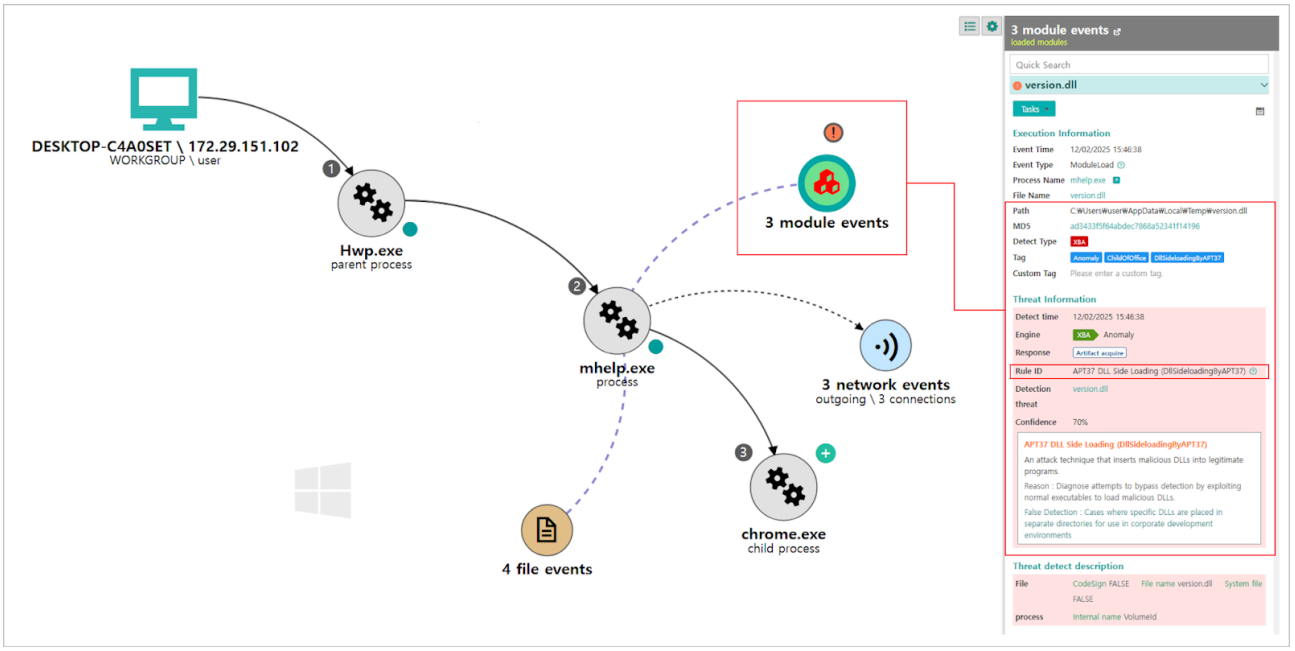
This analysis-based detection framework goes beyond simple hash matching and provides behavior-focused payload identification capabilities, enabling reliable coverage against DLL sideloading and various related attack variants.



[Figure 6-1] Genian EDR-based detection view for APT37 DLL sideloading

Genian EDR’s attack storyline feature provides high visibility into the entire DLL sideloading chain, where a malicious version.dll is loaded through a Sysinternals utility spawned by the HWP process.

This allows security administrators to clearly trace each stage of the attack flow and promptly carry out anomaly analysis and response actions without delay.



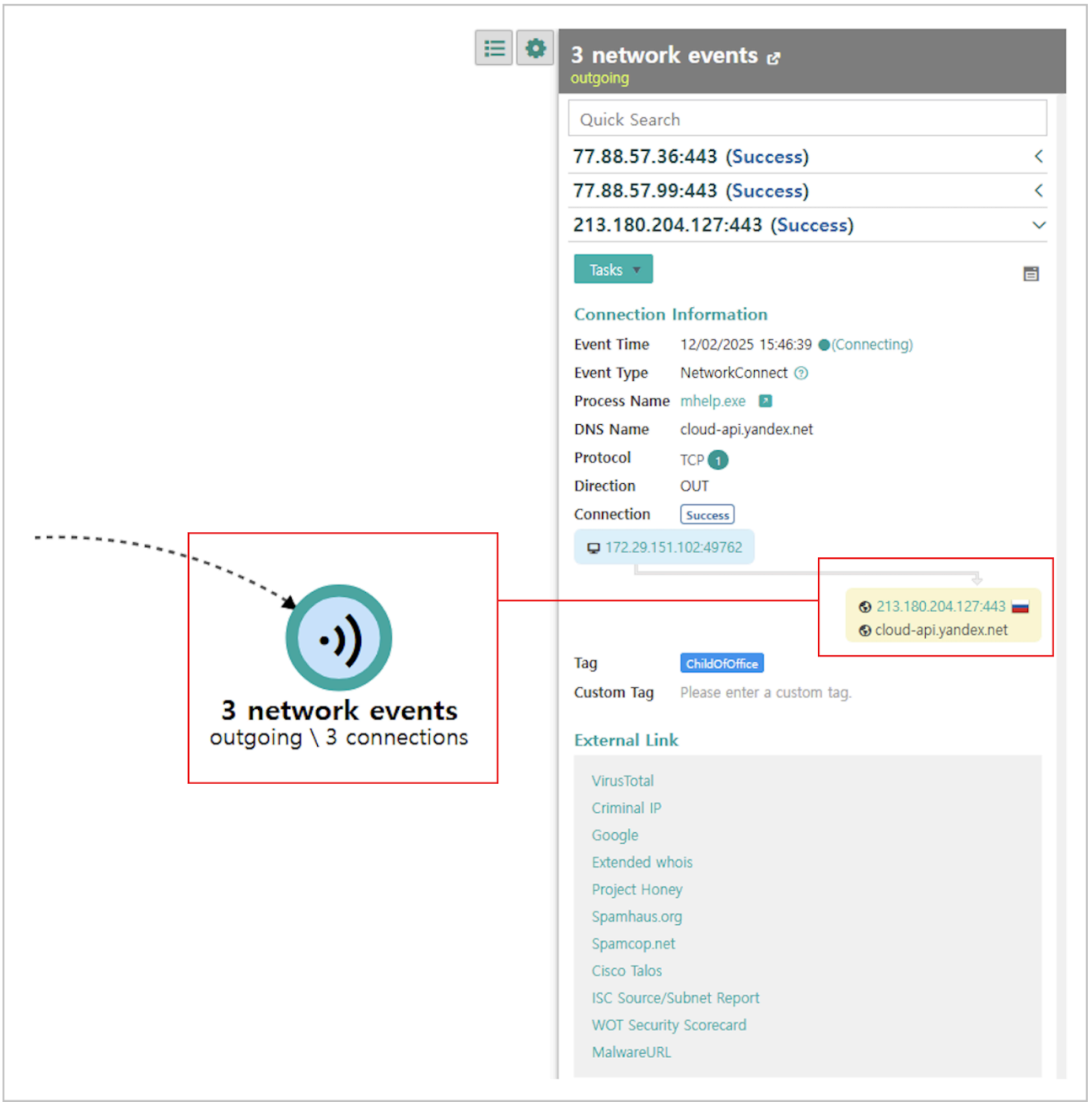
[Figure 6-2] Attack storyline view

Genian EDR also closely monitors network activity performed during the infection stage and immediately collects and identifies abnormal outbound communication attempts, particularly those directed to Yandex Cloud APIs in Russia.

Such external connections are considered key detection points because threat actors often use them as command and control (C2) servers or data exfiltration channels.

This high-visibility network analysis capability enables security administrators to promptly determine whether malicious communication has occurred and provides the supporting information needed to perform rapid response actions, including threat blocking, isolation, and forensic investigation, without delay.

As a result, it functions as a core defensive capability for detecting and responding to covert intrusion and information theft attempts at the network stage.



[Figure 6-3] Yandex Cloud communication detection view

Genian EDR’s attack storyline feature visualizes the malware’s entire execution flow in chronological order and with contextual relationships. This allows SOC operators to view the process tree, command lines, file and registry changes, and network events at a glance, and to promptly carry out required response procedures such as prioritization, isolation, blocking, and forensic collection.

The EDR collects and analyzes endpoint activity in real time, clearly presenting the flow of malicious behavior and supporting rapid containment of attack propagation through automated response capabilities. This enables organizations to detect and respond to security threats more effectively.

The EDR also integrates with forensic analysis and threat intelligence to establish a comprehensive security management framework, including identifying the cause of compromise, preventing recurrence, and blocking

internal data leakage.

In an increasingly advanced threat landscape, EDR has become an essential security component to complement traditional controls, such as anti-virus software and firewalls, which cannot detect many modern attacks.

7. IoC (Indicator of Compromise)

- **MD5**

8e4a99315a3ef443928ef25d90f84a09

17171c644307b17d231ad404e25f08b1

31662a24560b3fe1f34f0733e65509ff

a196fb11a423076f66f5e4b2d02813a9

ad3433f5f64abdec7868a52341f14196

c0cac70c93d213d113001e3410c24fd2

d2b2c6646535a62e4c005613d6a036f0

e726b59f96ab8360f323469d72b8b617

ea95109b608841d2f99a25bd2646ff43

f13a4834e3e1613857b84a1203e2e182

f3603f68aadc8bc1ea8939132f0d5252

2f3dff7779795fc01291b0a31d723aca

7e8c24bb3b50d68227ff2b7193d548dd

d287dcaeaf17c9dae8a253994502ee58

Source: https://www.genians.co.kr/en/blog/threat_intelligence/dll