Phishing Email Attacks by the Larva-24005 Group Targeting Japan

A asec.ahnlab.com/en/86535/

February 26, 2025

AhnLab SEcurity intelligence Center (ASEC) has identified the behavior of Larva-24005 breaching servers in Korea and then establishing a web server, database, and PHP environment for sending phishing emails.

Larva-24005 is using the attack base to target not only South Korea but also Japan. The main targets are those who are involved in North Korea and university professors who are researching the North Korean regime. They have set up a C2 server for their phishing email attacks and are disguising the email body as a ZOOM meeting link or a web portal login page to prompt users to click on them.

This blog post describes the process of Larva-24005 threat actor securing their attack infrastructure and a phishing email attack case that targeted Japan.

1. Larva-24005

Larva-24005 is a sub-group of the Kimsuky threat group known to receive support from North Korea. The name was newly given according to AhnLab’s threat actor naming system. The group is believed to exploit the RDP vulnerability of poorly protected Windows systems for initial access. After gaining access, they install RDPWrap, an open-source utility that activates RDP connections in Windows operating systems, and a keylogger developed by the group.

2. Actions Taken by Threat Actor Before Sending Phishing Emails

2.1 Securitng Attack Infrastructure

The threat actor breached South Korean systems using the Remote Desktop Protocol (RDP) to establish an infrastructure for sending phishing emails. While the exact method used to obtain the credentials used in the breach is unknown, it is believed that they either used brute force attacks or exploited previously obtained credentials.

It was confirmed that Larva-24005 is exploiting the BlueKeep vulnerability when securing certain infrastructures. The BlueKeep vulnerability (CVE-2019-0708) is a remote code execution (RCE) vulnerability found in the Remote Desktop Protocol (RDP). This vulnerability allows sending malicious packets to the RDP service to execute remote commands. The Kimsuky threat group has been exploiting the BlueKeep vulnerability for a long time, and more details can be found in the AhnLab SEcurity intelligence Center (ASEC) Blog post, “[Kimsuky] Operation Covert Stalker.” The BlueKeep vulnerability can only be exploited against operating systems that are vulnerable, which are versions below Windows 2008 R2. It does not affect the systems that use the latest OS.

2.2. Installing XAMPP

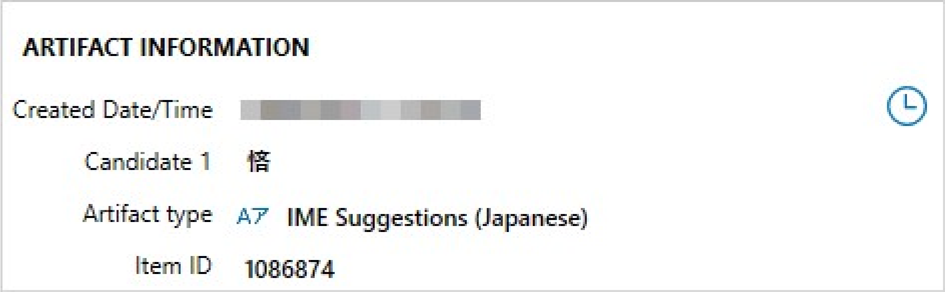
After the threat actor secured the attack infrastructure, they installed XAMPP, an integration package that includes Apache, MariaDB, PHP, and Perl, all of which are required to run a web server. The threat actor uses XAMPP to manage the entire C2 environment and stores the keylogger's result files and the victim's information from the phishing emails in text file format. Additionally, the threat actor installs PHPMailer to implement the phishing email sending feature. PHPMailer is a library that allows users to easily send emails using PHP code. The mailer.lib.php file in the configuration components specifies the sender's email address for the phishing emails. The account used in the attack was originally created for a web portal, but all of these accounts are currently suspended.

- "invoice_nerolpy@kakao.com"
- "naver-no-reply@kakao.com"
- "www.invoice@kakao.com"
- "www.navercorp@kakao.com"
- "www.naver.reply@kakao.com"
- "invoice_hometax@kakao.com"
- "navercorp-rep1y@daum.net"
- "invoice.norep1y@daum.net"
- "nonghyupcorp@daum.net"
- "f****07@knd.biglobe.ne.jp"

Table 1. List of email addresses used by the threat actor in phishing

2.3 Installing Japanese Input Method Editor

The threat actor installed a Japanese Input Method Editor (IME) in their attack infrastructure. An IME is a software that allows users to enter characters and symbols that are not on their keyboard. Generally, Korean Windows systems do not have Japanese IMEs installed. It is likely that the threat actor installed a Japanese IME in their attack infrastructure to send phishing emails targeting Japan or to perform searches in Japanese.



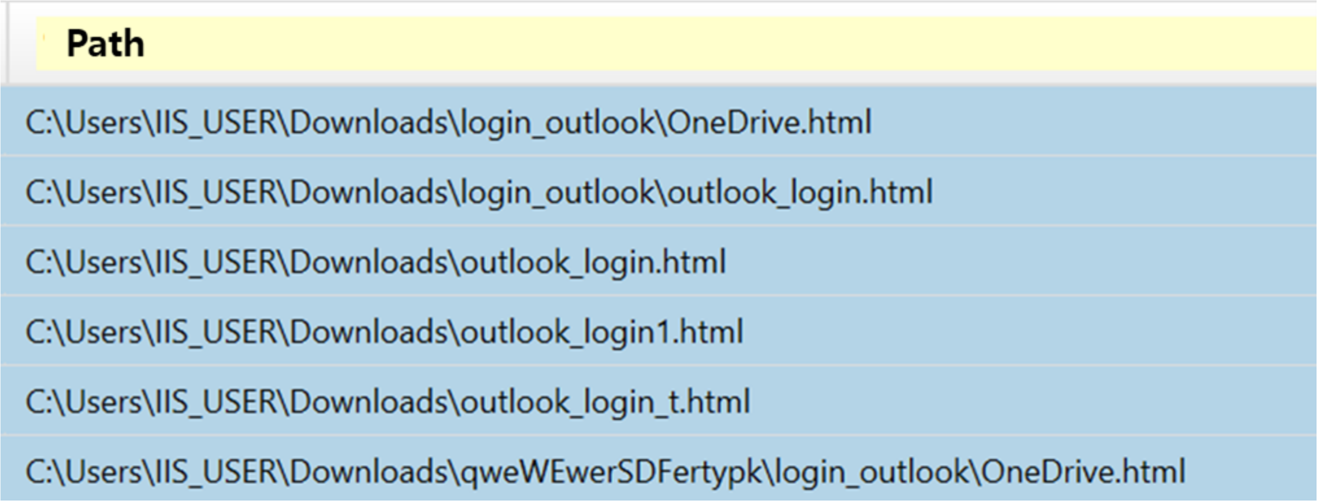
ARTIFACT INFORMATION

Created Date/Time	[redacted]
Candidate 1	悟
Artifact type	Aア IME Suggestions (Japanese)
Item ID	1086874

Figure 1. Japanese input system installed by the threat actor

2.4 Setting Up the Phishing Page

The threat actor saved the phishing pages they had prepared in the download folder of the IIS_USER account and the XAMPP home folder. The IIS_USER account is created by Larva-24005 after securing the attack infrastructure. These phishing pages are disguised as legitimate services such as iCloud, OneDrive, Outlook, Naver, and Google, and are used to steal user credentials. However, only traces of the phishing pages were found in the attack infrastructure, and the files had already been deleted and could not be recovered.



Path
C:\Users\IIS_USER\Downloads\login_outlook\OneDrive.html
C:\Users\IIS_USER\Downloads\login_outlook\outlook_login.html
C:\Users\IIS_USER\Downloads\outlook_login.html
C:\Users\IIS_USER\Downloads\outlook_login1.html
C:\Users\IIS_USER\Downloads\outlook_login_t.html
C:\Users\IIS_USER\Downloads\qweWEwerSDFertypk\login_outlook\OneDrive.html

Figure 2. List of phishing pages used by the threat actor

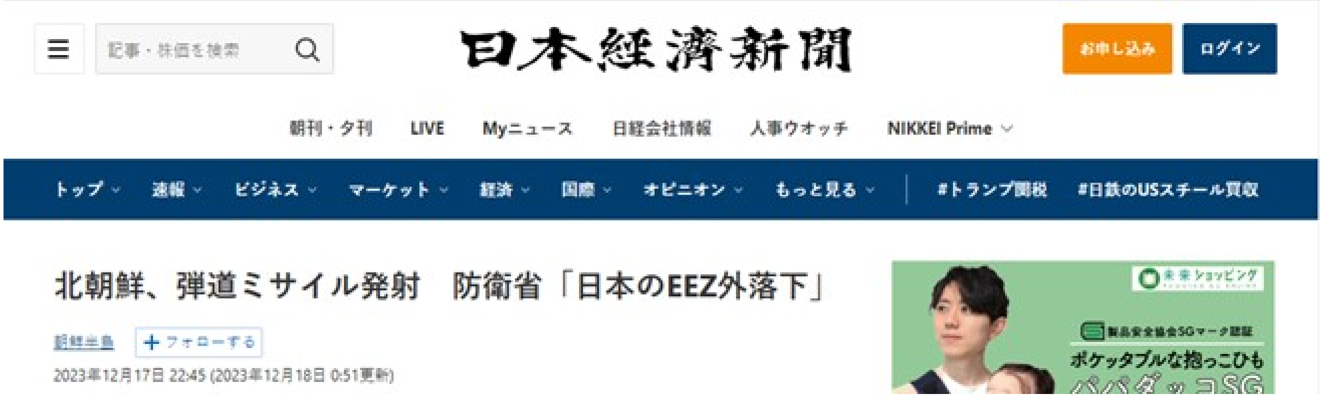
3. Methods Attackers Use to Choose Phishing Targets

The threat actor uses the web browser of their attack infrastructure (Chrome, MS Edge) to perform Google searches, add relevant keywords, and collect information on their targets through repeated searches. They also utilize the account credentials obtained through phishing emails to directly log into web portals and email platforms (Outlook, etc.) and search for additional targets and relevant information in the victim’s email inbox. Their main targets are university professors and non-profit organizations in Japan that are involved in activities related to North Korea.

- Osaka High Court (Osaka High Court ruling)
- Kisida’s Speech at the National Assembly
- Saeki Hiroaki
- Saeki Hiroaki, Group Protecting the Lives and Human Rights of Repatriated North Koreans
- Nakamura Shoichi’s Abduction to North Korea
- Japan’s Rocket in Malaysia
- Sankei Political Department Chief
- Osaka Ishin (Osaka Restoration Association)
- Tokuno, Head of the Network for North Korean Human Rights in India
- Japan-Korea Local Autonomy Research Association
- DPRK-Japan Talks

Table 2. Some of the keywords searched by the threat actor in the Chrome web browser

The threat actor also continuously collects news related to the political situation in Japan. They mainly read articles related to North Korea and Japan through the Nikkei newspaper. The following are some of the articles identified through the Chrome web browser visit history: “North Korea Launches Ballistic Missile. Japan’s Ministry of Defense says ‘Lands outside Japan’s EEZ’,” “New Japanese demands could be key to getting North Korea to talk,” and “Nikkei Reaches Highest Price in 33 Years”.



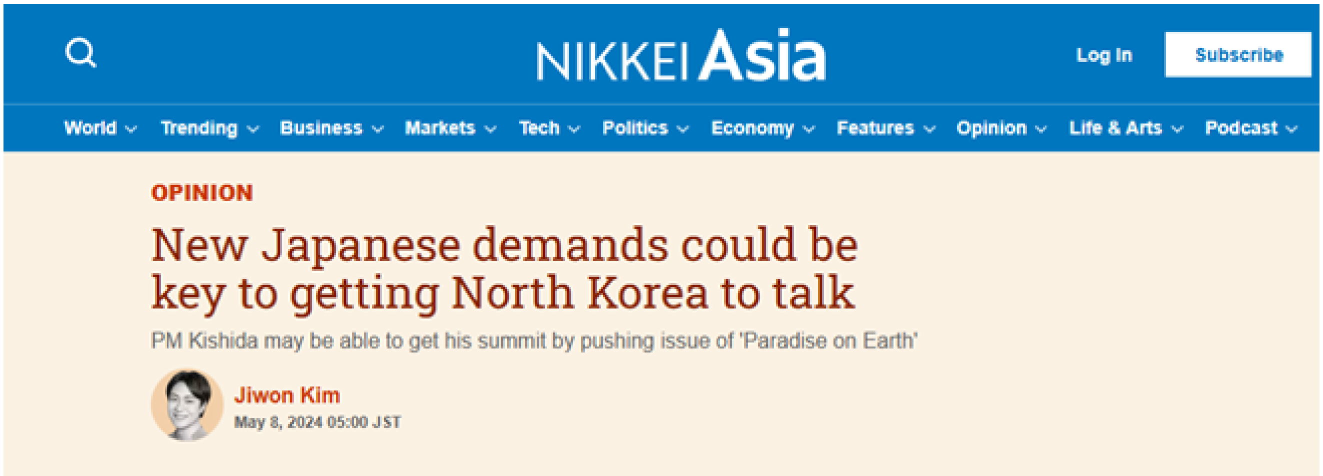
日本経済新聞

北朝鮮、弾道ミサイル発射　防衛省「日本のEEZ外落下」

朝鮮半島

2023年12月17日 22:45 (2023年12月18日 0:51更新)

Figure 3. Article #1 (North Korea Launches Ballistic Missile. Japan’s Ministry of Defense says ‘Lands outside Japan’s EEZ’) opened by the threat actor



OPINION

New Japanese demands could be key to getting North Korea to talk

PM Kishida may be able to get his summit by pushing issue of 'Paradise on Earth'

Jiwon Kim

May 8, 2024 05:00 JST

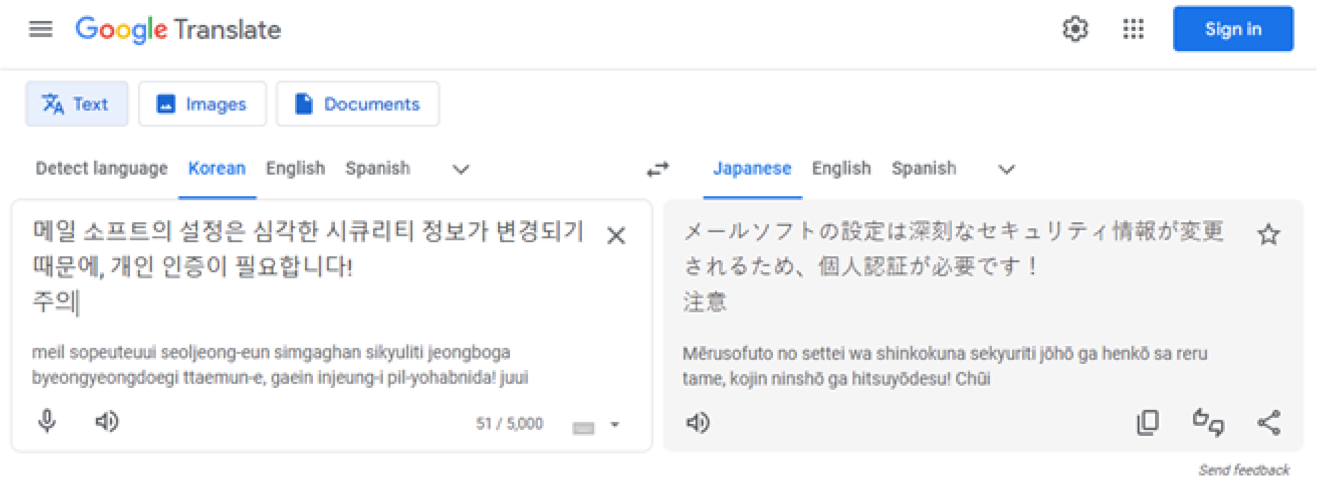
Figure 4. The article that the threat actor read (New Japanese demands could be key to getting North Korea to talk)

4. Sending Phishing Emails

After gathering enough information on their targets, the threat actor used PHPMailer installed in the attack infrastructure or logged in to the victims’ accounts to send phishing emails.

The phishing emails sent by Larva-24005 can be categorized into two main types: attaching a compressed malicious file or inserting a malicious URL in the email body. In this case, the latter method was used. The phishing email contains topics that would be of interest to the recipient or is disguised as a message from someone they know.

There is also a case where the threat actor translated Korean into Japanese using Google Translate. As shown in the figure below, the translated phrase is intended to be used in the phishing email body.



메일 소프트의 설정은 심각한 시큐리티 정보가 변경되기 때문에, 개인 인증이 필요합니다!
주의

meil sopeuteuui seoljeong-eun simgaghan sikyuliti jeongboga byeongyeongdoegi ttaemun-e, gaein injeung-i pil-yohabnida! juui

51 / 5,000

メールソフトの設定は深刻なセキュリティ情報が変更されるため、個人認証が必要です！
注意

Mērusofuto no settei wa shinkokuna sekyuriti jōhō ga henkō sa reru tame, kojin ninshō ga hitsuyōdesu! Chūi

Figure 5. The threat actor translating Korean to Japanese using Google Translate (English translation: *"Since changes to the mail software settings affect critical security information, user authentication is required"*)

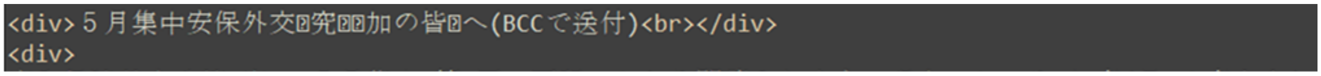
The cases introduced below are based on the logs of keyloggers installed by the threat actors in the victims' systems.

4.1 Case 1

The threat actor sent a phishing email disguised as a Zoom meeting invitation to a professor of international communications at a Japanese university. The professor had a history of writing papers about the North Korean regime, and their university email address was easily found online.

- From: FROM.teamzoom_reply@daum.net
- Subject: 0000 Invites You to a Scheduled Zoom Meeting

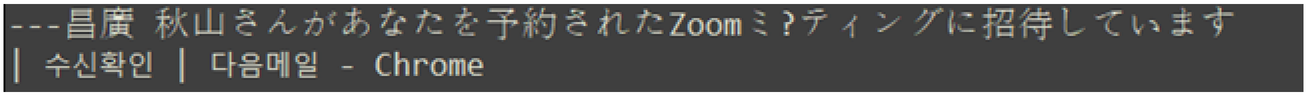
The email body contains a program guide for the security and foreign policy research group, including the presenters, topics, and schedule. It also includes a Zoom URL for the group's meetings, but this URL is not legitimate and connects to the threat actor's C2 server.



```
<div>５月集中安保外交⍰究⍰⍰加の皆⍰へ(BCCで送付)<br></div>
<div>
```

Figure 6. Phishing email content sent by the threat actor #1

After sending the phishing email, the threat actor used the read receipt feature as well to check if the victim opened the email.



```
---昌廣 秋山さんがあなたを予約されたZoomミ?ティングに招待しています
| 수신확인 | 다음메일 - Chrome
```

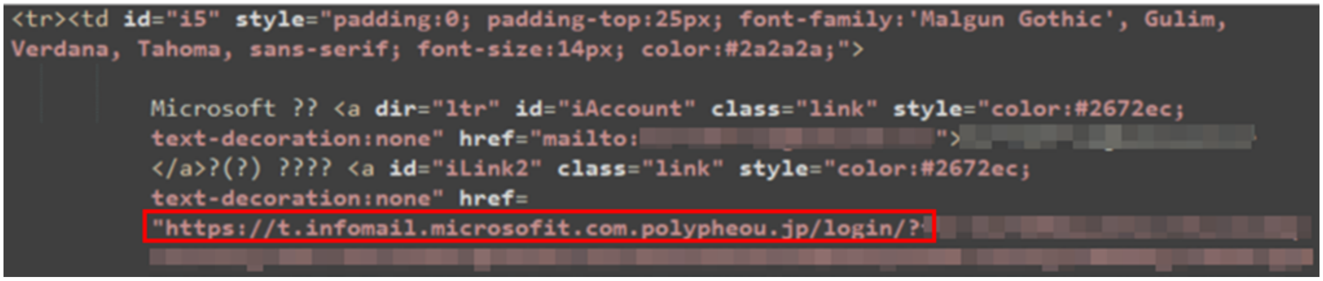
Figure 7. Phishing email read receipt history

4.2 Second Case

The threat actor sends emails with links disguised as Microsoft login pages to steal the account credentials of their targets. If a victim unknowingly enters their account credentials on the fake page, the information is transmitted to the threat actor’s C2 server. The following are the email addresses used by the threat actor.

- noreply_microprotect@naver.com
- office365_service@naver.com

The threat actor inserts a hyperlink in the email body to lure victims into a phishing page. The following image shows the content recorded by a keylogger installed by the threat actor in a victim’s system. The email body includes Japanese. Additionally, the domain “polypheou.jp” used in the attack is related to a Japanese health assistance company, but the threat actor changed the subdomain and used it as the C2 address.

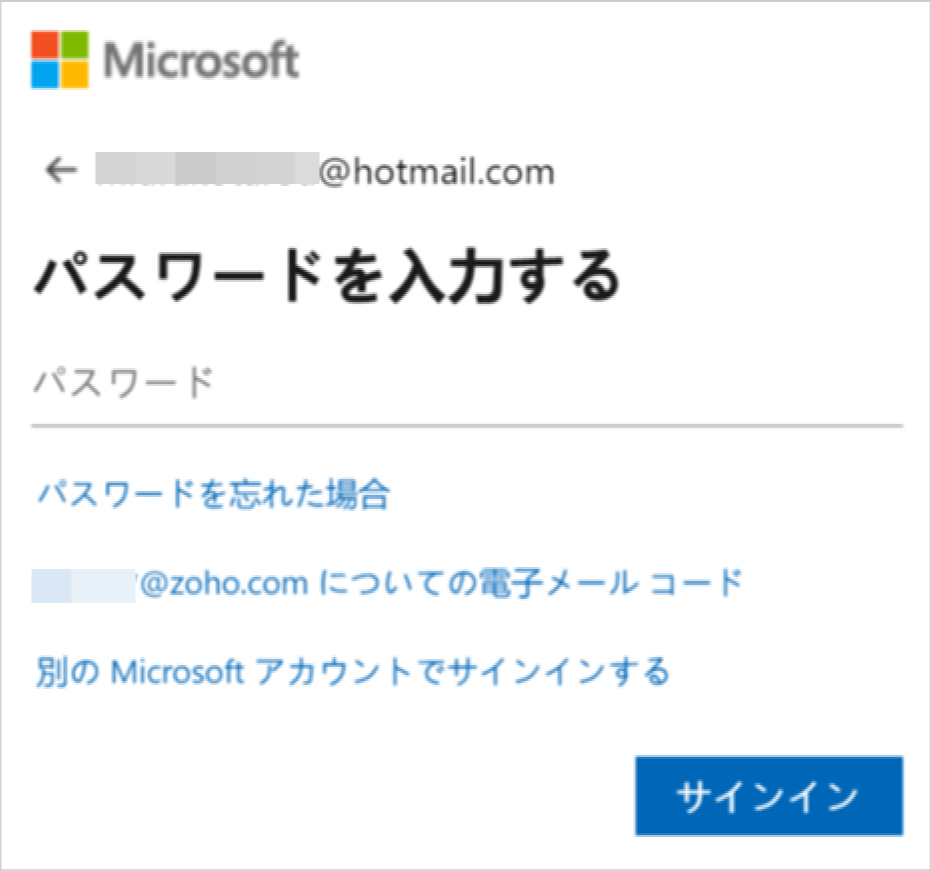


```
<tr><td id="i5" style="padding:0; padding-top:25px; font-family:'Malgun Gothic', Gulim,
Verdana, Tahoma, sans-serif; font-size:14px; color:#2a2a2a;">

            Microsoft ?? <a dir="ltr" id="iAccount" class="link" style="color:#2672ec;
            text-decoration:none" href="mailto:[redacted]">[redacted]
            </a>?(?) ???? <a id="iLink2" class="link" style="color:#2672ec;
            text-decoration:none" href=
            "https://t.infomail.microsofit.com.polypheou.jp/login/?[redacted]
```

Figure 8. The content of phishing email body #2

Upon accessing the phishing page via the URL, users are presented with a login page that contains their email address. Threat actors craft personalized phishing pages for each of their targets and send spear-phishing emails.



← [redacted]@hotmail.com

パスワードを入力する

パスワード

パスワードを忘れた場合

[redacted]@zoho.com についての電子メール コード

別の Microsoft アカウントでサインインする

Figure 9. Microsoft login phishing page

5. Conclusion

As seen in the cases above, the Larva-24005 threat group has been continuously launching attacks using various types of phishing emails against targets in Korea and Japan.

The threat actor is attempting to continuously engage in malicious behavior, such as prompting recipients to click on phishing emails and redirecting them to phishing sites disguised as legitimate websites.

Not only do they disguise themselves as legitimate websites, but they also impersonate the interests or relevant people of the targets when writing the email, so recipients must carefully check the senders' information upon receiving an email and pay special attention to opening attachments or clicking on links.

In particular, when clicking on links in emails, it is crucial to check if the URL matches the legitimate website. If there is any suspicion, refrain from entering account credentials.

MD5
b500a8ffd4907a1dfda985683f1de1df

URL

http[:]//auth[.]portal[.]pikara[.]ne[.]polypheou[.]jp/

http[:]//download[.]mail[.]naver[.]corn-file[.]kro[.]kr/

http[:]//t[.]infomail[.]microsofit[.]com[.]polypheou[.]jp/

http[:]//us06web[.]zoom[.]us[.]meet[.]polypheou[.]jp/

http[:]//www3[.]icloud[.]vbox[.]l[.]up[.]tcmp[.]polypheou[.]jp/

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