Panda's New Arsenal: Part 1 Tmanger

By NTTセキュリティ・ジャパン株式会社

Published: 2020-10-15 · Archived: 2026-04-05 13:44:14 UTC

By Hiroki Hada

Published October 15, 2020 | Japanese

はじめに

2020年2月、私達はAPT攻撃グループ”TA428”による攻撃キャンペーン”Operation LagTime IT”についてリサーチを行っていました。攻撃者は私達の監視しているシステムに侵入し、様々な侵害活動を行いました。彼らはPoison IvyやCotx RATを使ってコンピュータのコントロールを得た後、更に侵害を深めるために横展開を行いました。攻撃者はEternal Blueを悪用して同一ネットワーク上のいくつかのホストに移動することに成功すると、そのうちの1つのホスト上で興味深いマルウェアを動かし始めました。PDBにTmanger と書かれたRATは今までに見たことがない未知のマルウェアでした。

このときの侵害について、極めて詳細な調査結果をVB2020 localhostにて発表しました[1]が、ここでは全3回に分けてTmangerとそれに関連すると思われるマルウェアについて紹介します。第1回目である今回はTmangerを扱います。

Tmanger

TmangerはTA428によって利用されているRATです。図 1に示すように、PDBにTmangerと書かれていたことから、私たちはそう呼んでいます。Tmangerはおそらく Tmanager の打ち間違いです。次回以降の記事で紹介しますが、Tmangerに関連すると思われるものに Smanager というマルウェアが存在することが理由の1つです。このマルウェアの作者は意図しているのかは分かりませんが、このような打ち間違いが他にもいくつか見られます。例えば Entery や Waston という文字列もその1つです。

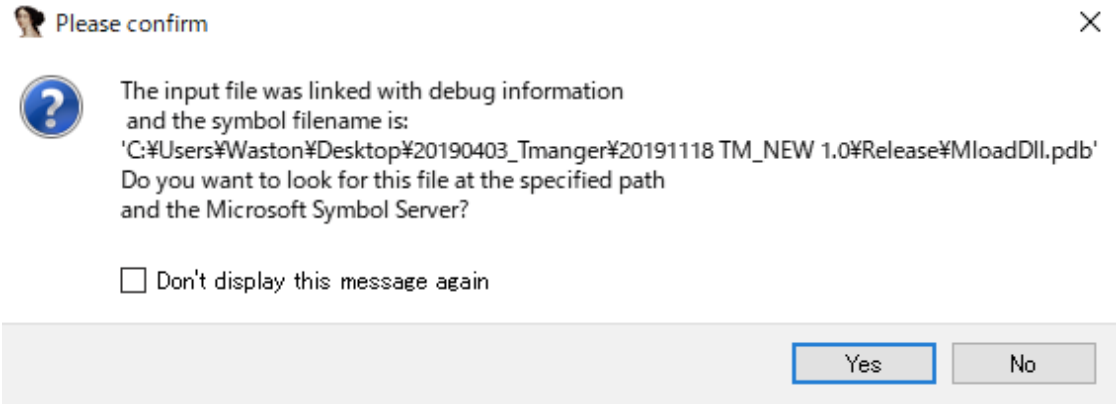

図1 TmangerのPDB情報

Tmangerは非常に活発に開発が続いており、関連すると思われる検体も存在します。Tmangerは私達が観測した攻撃以外にも、TA428の本来の標的であるモンゴルや、一帯一路政策に関わるベトナムに対しても利用されている可能性があります。

TA428はTickやTontoなどの他のAPTグループとRoyal Road RTF Weaponizerを共有していることが報告されています[2][3]が、Tmangerも他のAPTグループと共有されている可能性があります。しかし、その明確な証拠は発見していません。

Analysis Result

私達はTmangerをバージョン1.0 ~ 4.5まで観測しています。基本的にTmangerは SetUp、MloadDll、Clientの3つのパートから成ります。それぞれのパートでいくつかの挙動バリエーションがありますが、基本的な役割は以下のとおりです。

名称	概要
SetUp	MloadDllを展開し、実行する
MloadDll	Clientを展開し、実行する
Client	RAT本体

名称はそれぞれのEXEやDLLの内部名やPDBから付けており、攻撃者も私達の分類と同じように扱っていると考えられます。それでは、それぞれについて詳しく見ていきましょう。

SetUp

MloadDllやClientにも存在する挙動ですが、はじめにCreateEventで特定のイベント名を作成し、その成功の可否で挙動を変えます。成功した場合は実行を継続しますが、失敗した場合はその時点で終了します。これは多重起動を防ぐ目的であると考えられます。このとき、イベント名は様々ですが、私達が観測した全てのTmangerは以下の正規表現を満たします。

/[0-9a-f]{8}-[0-9a-f]{4}-4551-8f84-08e738aec[0-9a-f]{3}/

次に、IsUserAdminでユーザの権限を確認します。これ以降、Adminの場合とそうではない場合で処理が分岐します。Adminの場合とそうではない場合で、永続化の方法が異なっています。

Adminの場合

まず、XOR 0x88で以下のようなデータをデコードします。これらは後でサービス登録を行う際に使用されます。

- DFS Replication
- FTP Publishing Service
- ReadyBoost
- Software Licensing
- SL UI Notification Service
- Terminal Services Configuration
- Windows Media Center Extender Service
- Windows Media Center Service Launcher
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost
- netsvcs
- %SystemRoot%\System32\svchost.exe -k netsvcs
- MACHINE\SYSTEM\CurrentControlSet\Services\

その後、同様にXOR 0x88でデータをデコードし、得られたAPIを解決します。

- RegOpenKeyEx
- RegQueryValueEx
- OpenSCManager
- RegOpenKeyExA
- RegQueryValueExA
- RegSetValueExA
- GetSystemDirectoryA
- RegCloseKey

次に、deflateされているデータをinflateし、ランダムな4文字から成るファイル名でSystem32にDLLとして保存します。このDLLはMloadDllです。

再びXOR 0x88でAPI名をデコードし、解決します。これによって解決されたAPIはCreateServiceAです。さらに、同じ方法で以下のデータを得ます。

- SYSTEM\CurrentControlSet\Services\
- Description
- DisplayName
- ServiceDll
- \Parameters

これまでにデコードした文字列を使って、先程System32に作成したDLLをサービスとして登録します。最後に、そのサービスを起動します。

Adminではない場合

はじめにTempディレクトリにRahoto.exeというファイルがあるか確認します。存在しない場合、自分自身をRahoto.exeという名前でTempディレクトリにコピーし、レジストリのCurrentVersion\Runを使って自動起動の設定を行います。

その後、MloadDllとして動作します。

MloadDll

MloadDllはEnteryとServiceMainがエクスポート関数として実装されています。ServiceMainから実行された場合でも、最終的にEnteryが実行されるため、基本的な挙動は同一です。

はじめに図 2のようにRC4の鍵データを生成します。この処理はTmangerで共通するものです。

```
0x004010f0      movzx eax, byte [edx - 0x40]
0x004010f4      lea edx, [edx + 4]
0x004010f7      xor byte [edx - 4], al
0x004010fa      movzx eax, byte [edx - 0x43]
0x004010fe      xor byte [edx - 3], al
0x00401101      movzx eax, byte [edx - 0x42]
0x00401105      xor byte [edx - 2], al
0x00401108      movzx eax, byte [edx - 0x41]
0x0040110c      xor byte [edx - 1], al
0x0040110f      sub esi, 1
0x00401112      jne 0x4010f0
```

図2 暗号鍵を生成する処理

鍵データを生成すると、それを使ってconfigデータを復号します。図 3のように、configデータにはC&Cサーバーのアドレスとポート番号が含まれています。

アドレス	Hex	ASCII
6F7BA770	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA780	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA790	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA7A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA7B0	38 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00	80..............
6F7BA7C0	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA7D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA7E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA7F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA800	34 34 33 00 00 00 00 00 00 00 00 00 00 00 00 00	443.............
6F7BA810	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA820	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA830	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA840	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
6F7BA850	35 32 32 32 00 00 00 00 00 00 00 00 00 00 00 00	5222............

図3 configデータ

その後、deflateされているデータをinflateします。それによって得られるデータがClientです。最後に、Clientのエクスポート関数であるcallfuncを呼び出します。

Client

CreateEventなどの処理を行った後、以下のような端末情報を収集します。

- OSやアーキテクチャ情報
- ドライブ情報
- ホスト情報
- ユーザ情報

その後、スレッドが作成され、一連のループを繰り返します。はじめに、ソケットを作成し、成功するとCreateMutexで以下のMutexを作成します。

- sock_hmutex
- cmd_hmutex

次に、C&Cサーバーとの接続が確立するかチェックを行います。接続できた場合、C&Cサーバーからのコマンド操作を待ちます。コマンドのリストは以下のとおりです。

コマンド	説明
1, 17	特定のプロセスの起動
2	ディレクトリ情報の取得
3, 19, 35	クライアントからC&Cサーバーへファイルの送信
4	ファイル情報の取得
18	ファイルの削除
20, 52	メモリなどのクリーンアップ
34	CreateProcessによるプロセスの起動
36	ファイルの書き込み
50	ファイルのコピー
80, 81	キーログの取得
96	画面キャプチャの取得
それ以外	Sleep

トラフィックはRC4によって暗号化されていますが、それをデコードすると図 4のような構造になっています。

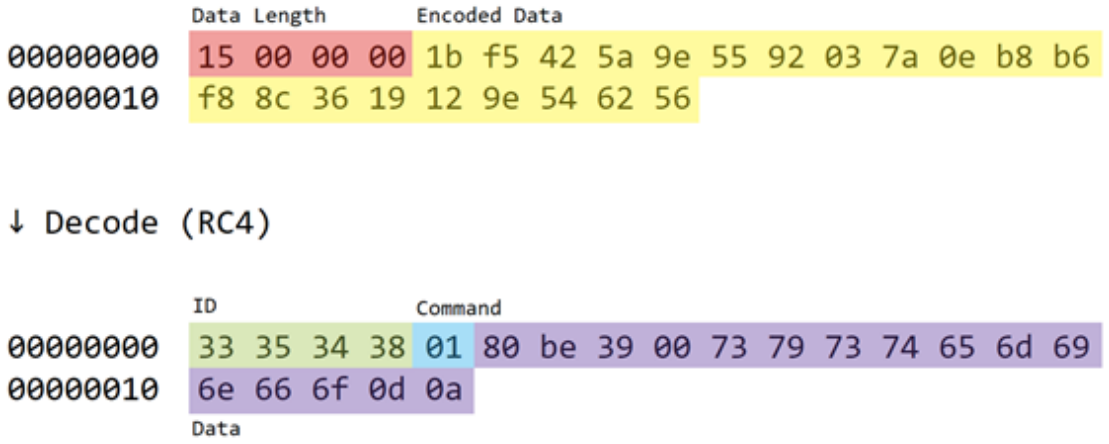

図4 トラフィックの構造

デコード後のデータの先頭に存在するIDはプロセスIDから生成されます。生成処理は以下のとおりです。

このIDによってプロセスとトラフィックを管理しています。

ツール

TmangerがC&Cサーバーと通信する際、データは暗号化されています。私達はそれをデコードし、トラフィックをパースするツールを作成しました。関連するマルウェアの解析やインシデント調査にご活用ください。

https://www.nttsecurity.com/ja-jp/Resources

さいごに

今回はTA428がOperation LagTime ITの中で使用したTmangerというRATについて紹介しました。Tmangerは活発に開発が行われており、いくつかの関連マルウェアも存在します。今後もTmangerの動向を注視していくべきでしょう。次回はTmangerに関連すると思われるマルウェアAlbaniiutasについて紹介します。

IOC

C&Cサーバー

- 172[.]105.39.67
- 136[.]244.82.179

ファイル情報

SHA256	Timestamp	PDB
977bd4b7e054b84b4b62e84875ff3277dd8c039cf3ee0ded435b41025d0d2b21	(UTC) 2020-03-16 13:30:57	
88ffb081f6924261df32322f343ccb9078ee45eaa369660892585037baf59078	(UTC) 2020-03-16 13:38:19	C:\Users\sxpolaris\Desktop\2020\TM VS2015\TM_NEW 4.5\Release\MloadDll.pdb
8987b9587c1d4f6fbf2fa49eb11bb20b8b30b82d5bc988f5c882501b1f76b82a	(UTC) 2020-03-20 05:04:56	C:\Users\sxpolaris\Desktop\2020\TM VS2015\TM_NEW 4.5\Release\SetUp.pdb
85a53a2525643a84509b10d439734509203a2a74e1a167d5c3494e37a47c8c8c	(UTC) 2025-06-23 04:54:29	
86297be195acaa36ec042523a5484d9e14fd9fb4cbd977f709e75207358a3f86	(UTC) 2025-08-19 12:08:44	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 1.0\Release\MloadDll.pdb
5d3db73458eeeb6439ab921159ba447b01c7a12f7291eb4b5cf510e29a8137c6	(UTC) 2025-09-06 23:19:33	

ebe05801d32985dc954e754aed63b5cee6e889f26533b1635c1f47e42bcb483a	(UTC) 2025-09-07 14:15:16	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.0\Release\MloadDll.pdb
c60490f6fbda0a2cf1a8cd401b2f3ce9262e600268264229122a4d80e327ed4b	(UTC) 2025-09-25 17:28:16	
6fdd004d0835577749e8742c91e9f1720953faa8ecd55d3b203eddd4d6db5568	(UTC) 2025-09-25 17:29:26	
6fdd004d0835577749e8742c91e9f1720953faa8ecd55d3b203eddd4d6db5568	(UTC) 2025-09-25 17:29:26	
71fe3edbee0c27121386f9c01b723e1cfb416b7af093296bd967bbabdc706393	(UTC) 2025-09-25 17:36:46	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.4\Release\MloadDll.pdb
8109a33c573e00e7849ba2d63714703e2e7bd65dee1c2c6454951f7fc4b2f275	(UTC) 2025-09-25 17:36:46	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.4\Release\MloadDll.pdb
7807c0177cf37bce6e38ef534f804935f505a24d735baa53a18e2da766ec136b	(UTC) 2025-09-29 13:02:13	

4fcb79a73f5286ed8f2bc671b64c76dac4971a0cce10936f63d210e8e17c5fd5	(UTC) 2025-10-01 15:47:24	
e494c8916e93295338a7368f86c42fce0916b559e63d462bd1b3265b6009bf9b	(UTC) 2025-10-01 15:47:26	
d4b339f502119d4cf10d48c8c7297bbaebb22387eb7cc4447540b666d27ba166	(UTC) 2025-10-01 15:47:26	
078498d02775b64c5660ccbfdf12f31f3b810ed612e10c3dd50660cfa03ad470	(UTC) 2025-10-01 20:09:43	C:\Users\Waston\Desktop\20190403_Tmanger\20191118TM_NEW 4.4\Release\SetUp.pdb
afd457592715bdef21d02c4e4d0e80dd70cf801a9d4d9afed795494012994372	(UTC) 2025-10-05 00:17:56	C:\Users\Waston\Desktop\20190403_Tmanger\20191118TM_NEW 4.4\x64\Release\MloadDll.pdb
772e69b3d66ef5b4fdda49d3ca39a5459b8c3afce77c24ebda698aef5bdbc5c3	(UTC) 2025-10-05 15:34:41	C:\Users\Waston\Desktop\20190403_Tmanger\20191118TM_NEW 4.4\Release\MloadDll_REG.pdb
8e9fc7bd0673a88a04583dda7d42f278013aa7abc4e26de86e953cc4a6825708	(UTC) 2025-10-06 08:33:38	C:\Users\Waston\Desktop\20190403_Tmanger\20191118TM_NEW 4.5\Release\MloadDll_REG_DLL.pdb

2999e5209cf1d7fb484832278e11e4c4 950ef40e8f52a44329ed4230135f9b64	(UTC) 2025-10- 06 19:16:45	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.5\Release\ttt.pdb

参考文献

[1] VB2020 localhost, Operation LagTime IT: colorful Panda footprint

[2] Proofpoint, Chinese APT “Operation LagTime IT” Targets Government Information Technology Agencies in Eastern Asia

[3] nao_sec, An Overhead View of the Royal Road
