標的型攻撃グループTA428が防衛・航空関連組織に対して使用したマルウェアnccTrojanについて

insight-jp.nttsecurity.com/post/102gr6l/ta428ncctrojan

Hiroki Hada

本日の記事は、SOC アナリスト 小澤 文生、小池 倫太郎の記事です。

これまでのブログ[1][2][3] でTmangerとそれに関連するマルウェアについて紹介しました。Tmangerは私達が2020年2月に、TA428のOperation LagTime ITについて行ったリサーチ で観測したマルウェアです。詳細はVB2020 localhostでの発表資料[4]を参照していただきたいと思いますが、そのリサーチではTmanger以外

にも未知のマルウェアを観測しました。私達はそのマルウェアをnccTrojanと呼んでおり、これまでに4つのバージョンを確認しています。今回はnccTrojanについて、解析結果を共有します。

nccTrojan

nccTrojan（あるいはMsmRATとも呼ばれる）はTmangerと同様に、TA428が使用するRATです。私達はロシアやモンゴルといった東アジアの防衛・航空関連組織に対する攻撃でnccTrojanが使用されていることを複数観測しています。

nccTrojanは攻撃の初期段階（Royal Road RTF Weaponizerによって生成されたRTFを開くこと）で実行されることもありますし、より攻撃が進行した横展開後に実行されることもあります。しかし、TA428が使う他のRAT（SPIVYやCotx RAT）とは異なり、観測数は極めて少なく、これまでほとんど知られていませんでした。私達の調査では、少なくとも2019年3月頃には開発されており、2020年11月にも使用が確認されています。

nccTrojanにはv1とv2の2つのメジャーバージョンが存在すると考えられます。それぞれの中ではより細かくマイナーバージョンが区切られており、例えばv1はv1.6やv1.7が存在しますが、それらの実装にはそれほど大きな差は存在しません。しかし、v1とv2の実装はかなり異なっており、一見すると同一のマルウェアファミリであるとは考えられません。私達は「同一の攻撃グループ（TA428）、攻撃キャンペーン（Operation LagTime IT）で使用されていること」「PDBパスの共通点」からv1とv2を同一のマルウェアファミリとして扱っていますが、v2が登場してからもv1が使用されることがあり、v1とv2は独立した関係にあるのかもしれません。そのため、以下ではv1とv2のそれぞれの機能・特徴について、解析結果を示します。

Analysis Result

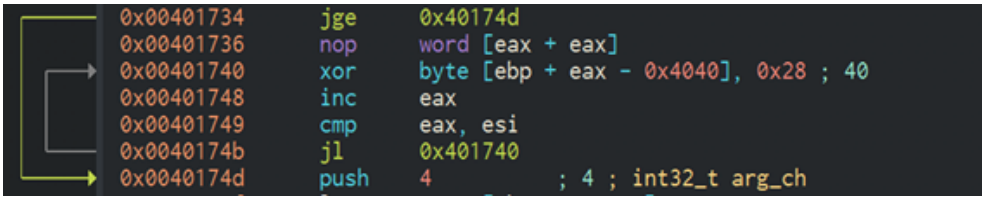
Version 1

私達が発見した最も古いnccTrojanは2019年3月頃のv1.6です。その後、2020年11月にもv1の使用を観測しました。その際の検体はバージョン情報が含まれていないものの、v1.6と極めて類似しており、ほとんどの機能は同一でした。そのため、以下ではv1.6について扱います。

ファイル名	PDBパス
OSE.EXE	C:\Users\abc\Desktop\cTrojan\1.6\HK\Release\Microsoft Synchronization Manager.pdb

OSE.EXEは起動すると、まずMutexのチェックを行います。msm_1.6_Mutex というMutexが既に作成されている場合、その時点で終了します。存在しない場合、新たに作成し、処理を継続します。このMutexの値はバージョンによって異なっており、例えばv1.7の場合は msm_1.7_Mutex というMutexが作成されます。msm というのはPDBパスに含まれている Microsoft Synchronization Manager の略であると考えています。Mutexを作成しない検体もあり、例えば2020年11月に観測された検体はMutexを作成しません。

その後、C&Cサーバーと通信を行い、コマンド操作を受け付けます。トラフィックは0x28でXORされています。



v1には以下のようにファイル操作やリモートシェル、プロセス操作など、RATとしての基本的なコマンドが実装されていることを確認しています。

Command	Function
"0000"	何もしない
"1000"	ディスク情報の送信
"1001"	ファイル情報の送信
"1002"	ファイルの削除
"1003"	プログラムの実行
"2000"	リモートシェルの起動
"2001", "2002"	リモートシェル上でのOSコマンドの実行
"3000"	ファイル転送用接続の確立
"3001"	ファイル転送用接続の切断
"3002"	ファイル転送用接続上での感染端末へのファイルのアップロード
"3003"	ファイル転送用接続上での感染端末からのファイルのダウンロード
"4000"	プロセスリストの送信
"4001"	プロセスの停止

Version 2

v2はv1とは異なり、攻撃がさらに進行した段階（横展開後でシステム権限を既に持っている状態）で使用されます。また、起動の方法もv1とは異なっており、v2はインストーラによってサービスに登録されることで動作します。

私達が観測したnccTrojanはInstsrv.exeとWindowsResKits.dllの2つのファイルから成ります。

ファイル名	PDBパス
Instsrv.exe	C:\Users\abc\Desktop\Service\Release\Instsrv.pdb
WindowsResKits.dll	C:\Users\abc\Desktop\cTrojan\2.1\HK\Release\Client.pdb

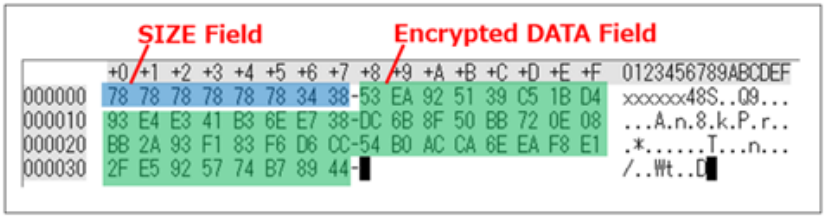
Instsrv.exeはその名のとおりインストーラで、WindowsResKits.dllをシステムディレクトリにコピーし、サービスとして登録します。

サービス名	イメージパス
Microsoft Windows Resource Kits	%SYSTEMROOT%\System32\svchost.exe -k WindowsResKits

WindowsResKits.dllはServiceMainから起動されると、DLL 内部にある暗号化されたConfigを復号します。

項目	値
C&Cサーバー	45.77.129.213:443
バージョン	v2.1[exe]
アクティベーションコード	ncc

その後、C&Cサーバーにアクセスし、 C&Cサーバーから受信したコマンドが14（コマンド制御のアクティベート）で、さらにそのコンテンツがConfigデータのアクティベーションコードと一致している場合、バックドアとしてのコマンド受信処理が有効化されます。 C&Cサーバーとのアクセスは独自のTCP通信を行い、TCPペイロードは以下のような形式になっています。

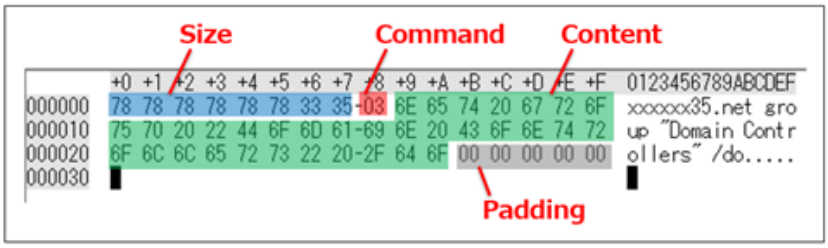


TCPペイロードは、8バイトのSIZEフィールドと暗号化されたDATAフィールドで構成されています。SIZEフィールドは、DATAフィールドの長さを10進数の文字で記載し、無効な桁数は文字「x」で表した、ユニークな値となっています。

DATAフィールドはAESによって暗号化されています。鍵とIVは以下のとおりです。

項目	値
鍵	9815113714127809 69AFC3AB2072018709A83A3332466A8B56FF3FAB8E6C3DAA
IV	2042123224315117031B1A0A3CCDA53F

暗号化されたDATAフィールドを復号すると、以下のような構造になっています。



復号されたDATAフィールドには、C&Cサーバーからのコマンドとそのコマンドに関連するコンテンツが含まれています。AESはブロック暗号方式であるため、コンテンツの長さに応じて末尾にPaddingは追記されています。また、先頭8バイトはコマンドとコンテンツの長さを表していますが、TCPペイロードのSIZEフィールドと同じ表記方式が使用されています。

実装・観測されているコマンドとその機能は以下のとおりです。使用されるコマンドの値はv1と大きく異なっていますが、コマンドの機能は概ね同じ内容で構成されています。

Command	Function
2, 29	リモートシェルの起動
3	リモートシェル上でのOSコマンドの実行（マルチバイト）
4	リモートシェル上でのOSコマンドの実行（ASCII）
5	ディスク情報の送信
6	ファイルリストの送信
8	プログラムの実行
10	ファイルやフォルダの削除
12	感染端末からのファイルのダウンロード
14	コマンド制御のアクティベート

15, 17	感染端末へのファイルのアップロード
19	プロセスリストの送信
21	プロセスの停止
22	何もしない
23	ファイルのコピー
26	ファイルの移動

ツール

nccTrojanはv1でもv2でも、C&Cサーバーと通信する際のデータはエンコードされています。v1は単純なXORであるため復号は容易ですが、v2は多少複雑な構造となっています。そこで、私達はv2のトラフィックをデコードして内容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。

ダウンロード ページの「C&C Traffic Decryption Tools for Tmanger/nccTrojan」からダウンロードいただけます。

さいごに

nccTrojanはv1もv2も両方とも、現在でも継続して開発が続いており、使用されているRATです。ロシアやモンゴルなどの航空・軍事組織に対する攻撃で多用されていますが、Tmangerのように他の攻撃グループと共有する可能性があります。今後も引き続き警戒していく必要があるでしょう。

IOC

C&Cサーバー

- custom.songuulcomiss[.]com (103[.]106.250.239)
- 95[.]179.131.29
- 45[.]77.129.213
- news.niiriip[.]com (51[.]89.133.251)

ファイル情報

Version	SHA256	PDB
N/A	21d1324c4ff4d68453d6745a1467ef3a cf8a853052e3425d12ad85c9b631f968	N/A

1.6	4c22eb33aa1d10511eaf8d13098e2687e44eaebc5af8112473e28acedac34bea	C:\Users\abc\Desktop\cTrojan\1.6\HK\Release\Microsoft Synchronization Manager.pdb
2.1	4651c51c86e4fc1a2bcad81936970ea549742a89316fa28e26433e94a8f13b66	C:\Users\abc\Desktop\cTrojan\2.1\HK\Release\Client.pdb
2.2	3be516735bafbb02ba71d56d35aee8ce2ef403d08a4dc47b46d5be96ac342bc9	C:\Users\abc\Desktop\cTrojan\2.2\HK\Release\Client.pdb

参考文献

[1] NTT Security Japan, Panda's New Arsenal: Part 1 Tmanger

[2] NTT Security Japan, Panda's New Arsenal: Part 2 Albaniiutas

[3] NTT Security Japan, Panda's New Arsenal: Part 3 Smanager

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