

Process Monitor を用いたマルウェアの動的解析

山下恭平、塚本覇虎、奥若菜

2022 年 5 月 17 日

1 テーマ

この実験では、擬似マルウェアツール ShinoBot と Process Monitor を用いたマルウェアの動的解析を行う。

2 環境

本実験は以下の県境において実験を行う。

- Virtual Box . . . 仮想環境、今回は Windows10 をインストールしている。
- Prosess Monitor . . . 動作しているプロセスを監視し、そのログを採取するソフト。
- ShinoBot . . . RAT(Random Access Tool) 型のマルウェアを再現したソフト、web 上に設置されたサーバから感染 PC を操作できる。

3 行なったこと

感染 PC の特定のファイルを ShinoBot から命令を送り削除した時のプロセスのログと、通常の削除のログを取り、双方のログを比較しながら、怪しいプロセスの特定を行った。

4 RAT の解析

4.1 RAT と通常プロセスの比較

あああああ

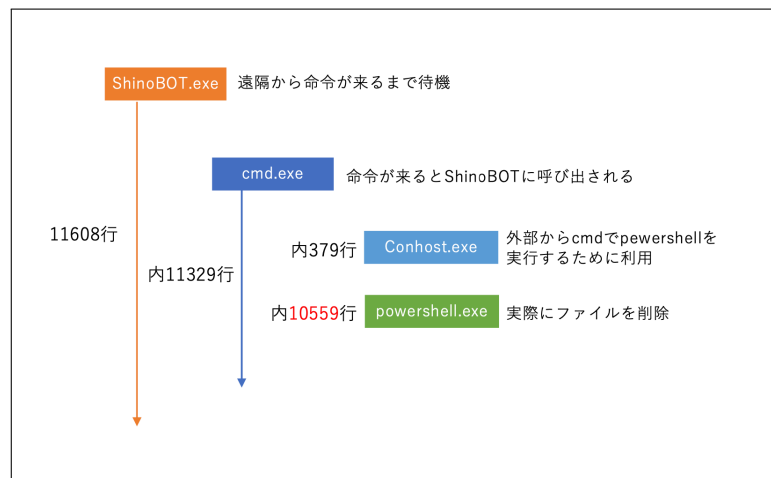


図 1

ああああ



図 2

4.2 削除に用いられた API

比較を行ったそれぞれのプロセスにおいて、実際にファイルの削除を行っていた API を確認したところ、同一の API が利用されていることが確認できた。以下はその API の詳細を示したものである。

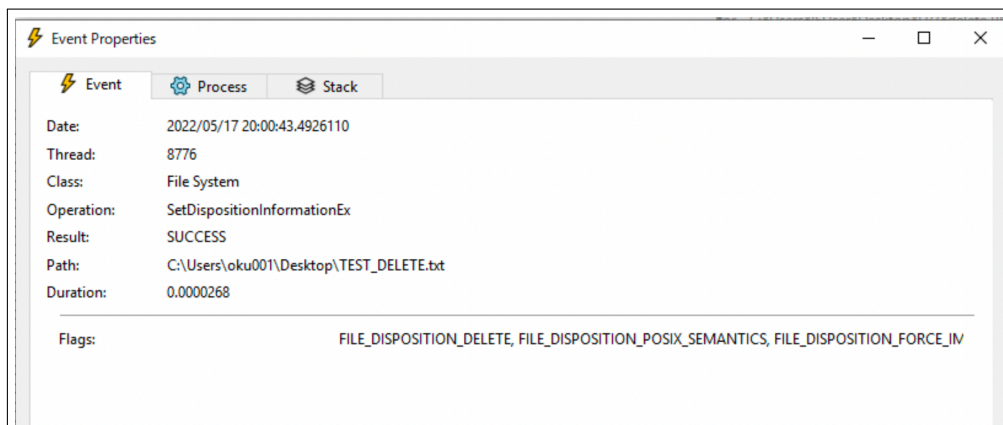


図 3

この API はマイクロソフトの公式ドキュメントにて、内容が公開されていたので、その内容を記載する。
(1)

Listing 1 C++

```

1
2 typedef struct _FILE_DISPOSITION_INFORMATION_EX {
3     ULONG Flags;
4 } FILE_DISPOSITION_INFORMATION_EX, *PFILE_DISPOSITION_INFORMATION_EX;

```

フラグ名	意味
FILE_DISPOSITION_DO_NOT_DELETE	システムがファイルを削除しないように指定します。
FILE_DISPOSITION_DELETE	システムがファイルを削除することを指定します。
FILE_DISPOSITION_POSIX_SEMANTICS	システムが POSIX スタイルの削除を実行する必要があることを指定します。
FILE_DISPOSITION_FORCE_IMAGE_SECTION_CHECK	システムがイメージセクションのチェックを強制的に実行するように指定します。
FILE_DISPOSITION_ON_CLOSE	システムが終了時の状態を設定またはクリアするかどうかを指定します。
FILE_DISPOSITION_IGNORE_READONLY_ATTRIBUTE	読み取り専用ファイルの削除を許可します。

表 1

4.3 怪しい点

削除におけるプロセスの大部分が一位している点、用いられる API が通常のプロセスと一致している点などを考慮すると。削除を行う一連のプロセス内にマルウェアだと特徴づけるプロセスは存在しないと考えら

れる。この時、通信ログに着目すると削除のプロセスが生成される前と、一連のプロセスが終了した後に、ShinoBot が TCP 通信を行なっていることが確認できる。RAT に感染しているコンピュータはサーバから送られてくる命令を実行するので、前後の通信によって、命令の受信、命令結果の送信を行なっていると考えられる。RAT に感染したコンピュータから、RAT を検出する方法として、通信ログの確認が有効な手段だと考えられる。

Time ...	Process Name	PID	Operation	Path	Result	Detail
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50637 -> mnd20...	SUCCESS	Length: 37, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Disconnect	thinkpad+420s:50637 -> mnd20...	SUCCESS	Length: 0, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Connect	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 0, mss: 14...
19:37:...	ShinoBOT.exe	11840	TCP Send	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 325, starti...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 5, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 112, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Send	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 325, starti...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 5, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 960, sequ...
19:37:...	ShinoBOT.exe	11840	Process Create	C:\WINDOWS\system32\cmd.e...	SUCCESS	PID: 7068, Comma...
19:37:...	cmd.exe	7068	Process Start		SUCCESS	Parent PID: 11840...
19:37:...	cmd.exe	7068	Thread Create		SUCCESS	Thread ID: 5360
19:37:...	cmd.exe	7068	Load Image	C:\Windows\System32\cmd.exe	SUCCESS	Image Base: 0x860...
～ファイル削除のプロセス～						
19:37:...	powershell.exe	11100	Process Exit		SUCCESS	Exit Status: 0, User...
19:37:...	cmd.exe	7068	Thread Exit		SUCCESS	Thread ID: 10048, ...
19:37:...	cmd.exe	7068	Thread Exit		SUCCESS	Thread ID: 3724, ...
19:37:...	cmd.exe	7068	Thread Exit		SUCCESS	Thread ID: 5360, ...
19:37:...	cmd.exe	7068	Process Exit		SUCCESS	Exit Status: 0, User...
19:37:...	Conhost.exe	7804	Thread Exit		SUCCESS	Thread ID: 8276, ...
19:37:...	Conhost.exe	7804	Thread Exit		SUCCESS	Thread ID: 6804, ...
19:37:...	Conhost.exe	7804	Thread Exit		SUCCESS	Thread ID: 10848, ...
19:37:...	Conhost.exe	7804	Thread Exit		SUCCESS	Thread ID: 8200, ...
19:37:...	Conhost.exe	7804	Process Exit		SUCCESS	Exit Status: 0, User...
19:37:...	ShinoBOT.exe	11840	TCP Send	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 362, starti...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 53, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Send	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 90, starti...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 5, sequ...
19:37:...	ShinoBOT.exe	11840	TCP Receive	thinkpad+420s:50639 -> mnd20...	SUCCESS	Length: 176, sequ...

図 4

5 参考文献

(1) マイクロソフト

https://docs.microsoft.com/ja-jp/windows-hardware/drivers/ddi/ntddk/ns-ntddk-_file_disposition_information_ex