マルウェアがサンドボックスから検知行動回避するとき
2022 年 2 月 28 日 Minerva のブログから

昨今、高度なマルウェアは、ネットワークへ不正侵入に成功しても、真っ先に攻撃を実行してネットワークを破壊しようとはしません。代わりにネットワーク内に攻撃の足掛かりを築き、マルウェアは検知されないように回避を試みます。検知回避行動は昨今のマルウェアの特長であり、既存でインストールされているアンチウィルスソフトをすり抜けてしまっていることです。
過去のブログでも昨今のマルウェアは検知回避をするテクニックをご紹介しましたが、今回はサンドボックスを検知してマルウェアが行動回避するお話をします。

サンドボックスとは何か？マルウェアはなぜサンドボックスに対し、検知回避をしようとするのか？
サンドボックスは分離された環境でマルウェアが仕掛けられている疑わしいファイルをテスト及び分析をするためにある製品です。サンドボックスは、通常のネットワークシステムで稼働しているようにマルウェアを誘き寄せます。この方法により、本番環境でマルウェアに感染せずにどのようなマルウェアであるか分析できます。サンドボックスはすでに知れ渡っていることから、マルウェア開発者は、サンドボックス内にいるという判断材料機能を実装し、これらの仮想環境でマルウェアが検知されるのを回避します。つまり本番環境のネットワーク上に侵入する機会を伺い行動を控えているのです。以下はマルウェアがサンドボックスから回避する項目です。

テスト環境で調査
サンドボックスに侵入しているか確認するためにマルウェアがまず行うことは、サンドボックス環境内に侵入しているのかどうかを判断します。その際に多数のシステムクエリーを発信します。

- **Registry** - レジストリーが、通常ではありえないインストール済アプリケーション数が非常に少ない場合、これはサンドボックス環境にいることを示します。
- **Hostname** - いくつかのサンドボックス製品はあるホスト名又はホスト名にあるキャラクターを含んでいます。
- **稼働しているプロセス数** - 通常ではありえない稼働プロセス数が非常に少ない数である場合は、サンドボックス環境内であることを示します。
- **USB ドライブとプリンター** - 周辺機器が存在している場合、本番環境にいることを示します。
- **ハードディスクサイズ** - 通常のマシンではディスク容量が 100 ギガを超えていますが、通常ではありえないディスク容量が少ないとサンドボックスである事を示します。
- **スクリーン画像度** - 現在では低質画像(例:800×600 画像)である場合は、現実的に誰もオフィスワークできない画像質です。
- **CPU 数** - 通常は低 CPU 数であると仮想環境であることを示します。
- **RAM サイズ** - 現実的でない低 RAM 数(例:1 ギガ)である場合、サンドボックス環境であることを示します。
- **サンドボックスエージェント** - いくつかのサンドボックス製品はエージェントベースです。
- **Malware.exe** - 便宜上のことですが、多くのサンドボックス製品は監視対象のファイル名を malware.exe に似た名前へ変更します。多くのマルウェアはサンドボックス上に存在する malware.exe ファイルをクエリーします。

これらチェック項目の内、サンドボックスの存在が判明すると、マルウェアは行動せず、サンドボックスの存在が消えるまで待機して、本番環境のネットワークへの侵入を待ちます。

ユーザインタラクション検知

本番環境はマウスのクリックや動き、キーボードの打ち込み、ドキュメントのスクロールなどによる、ユーザインタラクションの行動のように、いくつかのサンドボックス製品は本番環境に見せかけるようにユーザインタラクションをエミュレート(実際とは異なる別のハードウェアやソフトウェアの環境を疑似)します。しかしあるマルウェアはユーザインタラクション行動に対し見極めることが可能で非常にスマートです。マルウェアがユーザインタラクションを判別できない時やサンドボックスがエミュレートしていることを判別すると、行動をストップします。

タイムベース回避

多くのサンドボックスは疑わしいファイルがプロセスに影響が生じる場合に備え、ファイルを保管したりはしません。サンドボックスはエンドユーザーのマニュアル操作に依存する製品です。

よってマルウェアはサンドボックスがタイムアウトするまで、沈黙を守り続けます。また通常サンドボックス環境では実行されないリブートやログインなどのアクションが発生するまで待ち続ける傾向があります。これのアクションが取られたのち、マルウェアは攻撃の足掛かりを開始します。

このような賢いマルウェアに対し、Minerva はどのように防御するのか？

Minerva の敵対的環境防御システムはOSとプロセス間に完璧に制御できる防御層が形成されております。今回のケースではサンドボックス内でマルウェアの検知回避行動に関して、Minerva はマルウェアの実行を効果的にストップします。

例えば多くのマルウェアは malware.exe ファイルの存在を確認します。通常の本番環境システム上では、マルウェアのクエリーに対し、当然のことながら（malware.exe）ファイルは存在しませんと返答しますが、Minerva は、マルウェアがクエリーを発信すると、クエリー通りの返答を返します。Minerva 先制防御の特長は、実際にシステム上に存在しないファイルであっても、マルウェアが確認してくるとそれに対し欺くことにより、敵の攻撃から先制防御します。

図 1: 通常のシステムでは malware.exe ファイルは”存在なし”とコマンドを返答

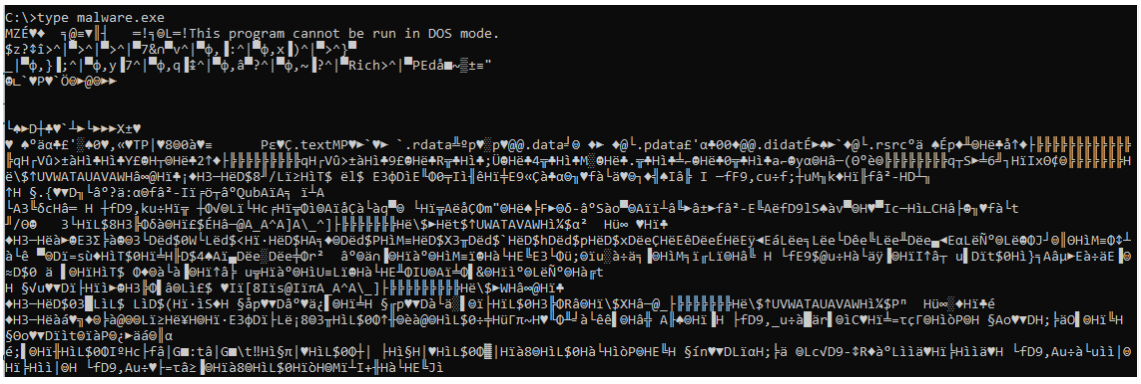

図 2: Minerva は malware.exe ファイルの存在を疑似

検知回避行動が Minerva によって防御されると、管理画面上にアラート及びイベントが履歴されるので、後で攻撃プロセスの洞察的に分析をすることもできます。

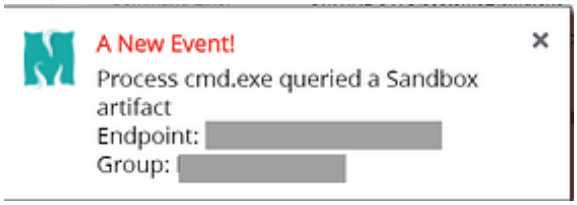

図 3: 管理画面上に cmd.exe がサンドボックスのクエリーを出した新規イベントが表示

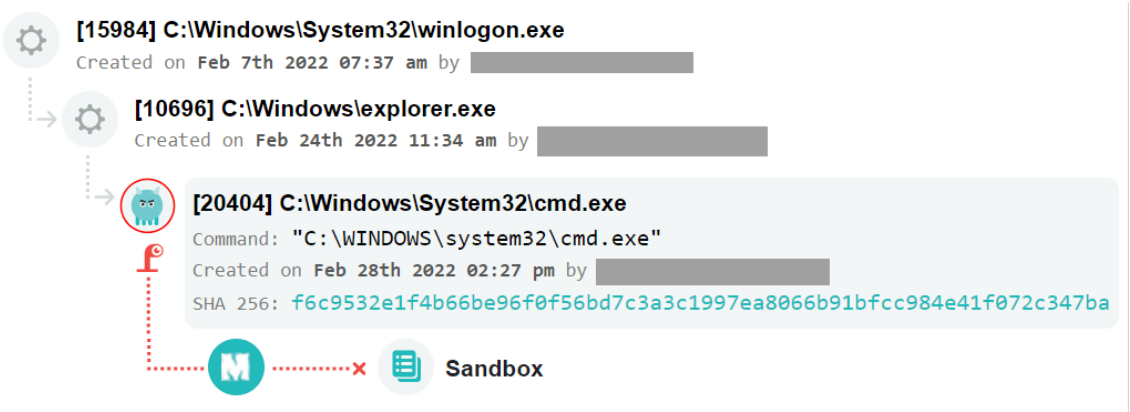

図 4: Minerva がサンドボックスをクエリーしたマルウェアを先制防御したイベント

今回はサンドボックスを検知し行動を回避する高度なマルウェアでも Minerva は徹底的に先制防御します。この他にも Minerva は少なくとも数千の検知回避手法をエミュレートする性能を持ち合わせています。先ほどにも言いましたが、これはマルウェアの高度な回避行動の一つにすぎません。今後更にマルウェアは進化を遂げあなたのネットワークへ侵入する機会を伺っていますが、Minerva は常に未知のマルウェアを先制防御するように高度なセキュリティを提供します。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。