ランサムウェア攻撃手法に対してどのようなカウンター防御が必要なのか？
2021 年 10 月 4 日のブログから

ランサムウェアは企業組織のネットワークをターゲットにします。ネットワーク侵入後、重要データを勝手に暗号化します。相手へデータを復号化をする代わりに膨大な金額を要求します。
ランサムウェアは実際にどのように動くのでしょうか？非常に複雑な質問です。ランサムウェアの種類によって起動の仕方も変わってきます。このことからランサムウェア攻撃を防御するには多様な対策が必要となってきます

ランサムウェア攻撃防御の具体的なケースもこれから見ていきましょう。3つのメジャーなランサムウェアと攻撃手法を説明します。

Conti(コンティ ランサムウェア)
Conti は 2020 年に初めて確認されました。2020 年に最初に登場したコンティランサムウェアは、ハッシュ値 API を使用して、カーネル内の低レベルの OS サービスを呼び出します。これらのコールにより、ランサムウェアは、メモリーとプロセスに対しカーネルレベルのアクセスを取得できるため、機密ファイルや情報を盗むことができます。Conti はサイバーセキュリティコミュニティーで出回っていて、Wizard Spier と呼ばれるそうです。典型的なランサムでお

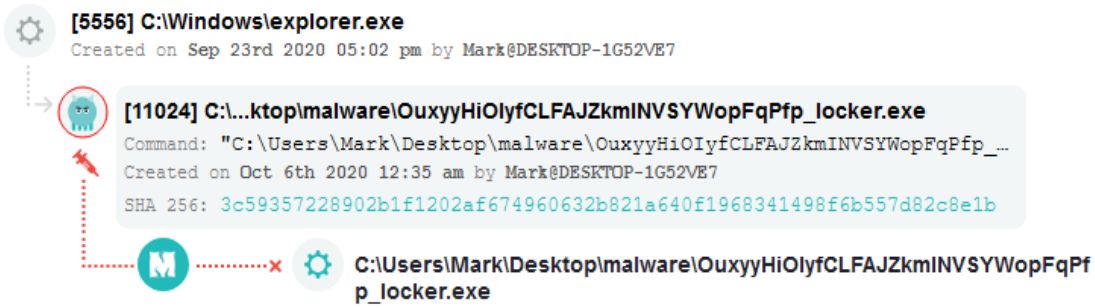
金を払わないと機密データ（情報）を公開すると脅します。

Conti が潜伏されているのが顕著に表れ始めたのが 2020 年後期頃です。ランサムウェア開発者がマルウェア検知ツールなどを回避できるようにアップデートを行いました。Conti の現バージョンは unhooking 機能を実行させることで検知回避が実現可能となりました。この unhooking 機能というのは典型的なセキュリティツールでシステム内に悪意のあるアクティビティを検知するものです。

Conti ransomware protection Conti ランサムウェアを防御

Conti の変種株の場合ですが、防御の重要な点は、オペレーションシステムファイル内の API hooks が削除されるのを防ぐことで unhooking 機能を無効にさせることができます。

Minerva Armor のユーザーは実際にこの Conti 変種株の攻撃に出会い防御することができました。他の製品では Conti 変種株からの攻撃を検知することは不可能ですが、Minerva は攻撃を防御しました。下記の図はその攻撃試行のプロセスイベントです。



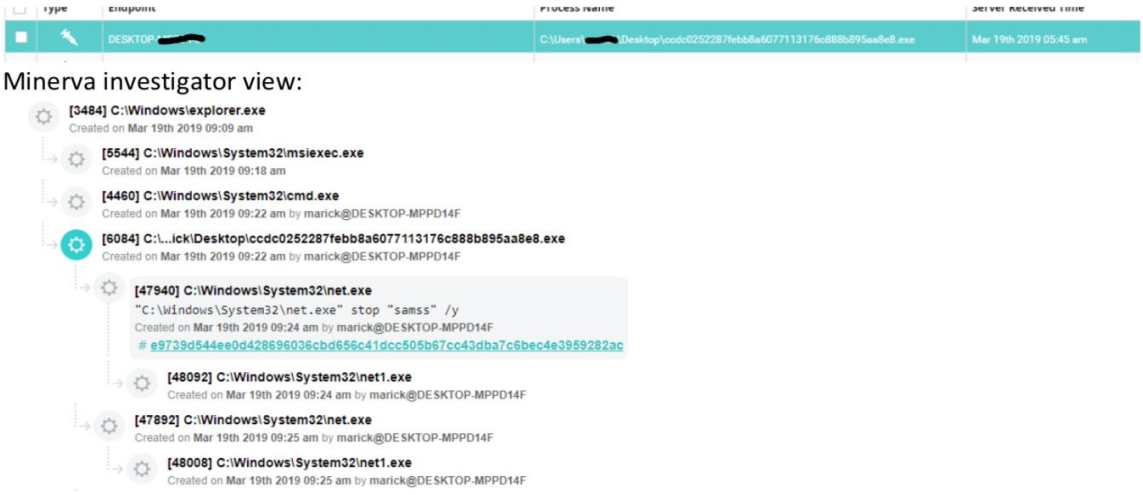
Ryuk（リューク ランサムウェア）

初めて世に出始めたのが（検知された）2018 年です。Ryuk は“質”（他のランサムウェアと比較）に特化したランサムウェアの変種株になります。特定の企業又は人に対してターゲットを絞り込み攻撃を仕掛けます。

多くの場合 Ryuk 攻撃は e-mail 又は企業内にいる特定ユーザーに対しメッセージ機能を利用してフィッシング攻撃から始まりました。ユーザーがそのフィッシングメールをクリックすると、Ryuk はユーザーの PC へ侵入して足がかりを築きます。その後ドロッパーと呼ばれるマルウェアコードが次々にダウンロードされてしまい、企業組織の重要なファイルが暗号化されてしまいます。攻撃者はファイルを回復する代わりに多額の身代金を要求しました。

Ryuk は Minerva 社が熟知しているランサムウェアの中でも特殊ですが、Minerva ユーザ

ーは実際の Ryuk 攻撃を防御しました。特に顕著的なのは、VirusTotal で初めてこの Ryuk 攻撃が明るみになる 28 日前に攻撃防御に成功しています。



Sodinokibi（REvil）

Revil は少なくとも 2019 年 4 月以来存在が確認されており、Kaseya 社に対するスペシャルクラスのランサムウェア攻撃関与で最も悪名高い集団です。ランサムウェアサービス（RaaS）は特に高度な技術が無くてもランサム攻撃を容易に実行できる商品（サービス）です。

REvil は Sodinokibi と呼ばれるプロセスインジェクション攻撃を使用しました。この攻撃はシステムが化膿しているプロセスへコードを注入し、プロエスがアクセスするメモリー、ディスク、ネットワーク又は他の可能なリソースへアクセスができるようになります。

この攻撃手法を利用して、REvil は最終的にファイルを暗号化します。頭痛の種は Sodinokibi がコードインジェクション攻撃しても検知されにくいのです。プロセスはこれらの悪意のあるコードでも正当なものであると認識しているので、セキュリティクリアランスを通過してしまいます。

2021 年 7 月に REvil はロシアを拠点にして活動している可能性が濃厚でしたが、現在は活動を急遽ストップしているようです。この背景には US サイバーコマンド部隊或いはロシア政府サイバー対策部隊によって彼らのサイトを停止したことが要因なのかもしれません。またはアメリカとロシア政府から更なる取り締まり攻撃を避けるため、彼らが自発的に活動をストップした可能性もあるようです。

REvil ランサムウェア攻撃防御
REvil による悪意のあるコードがプロセス内で検知回避されていても、Minerva は先制防御を行うことができました。

上にある図は Minerva が REvi 攻撃を防御したイベントが表示されております。VirusTotal 上でこの Sodinokibi 攻撃が明るみになる約 5 時間前に Minerva は攻撃を防いでいます。

各種のランサムウェアはそれぞれ異なる攻撃手法で実行します。オペレーティングシステム上に存在する脆弱性を突いて攻撃されるケースもあれば、フィッシング攻撃によって侵入されるケースもあるということがわかります。

今回のリポートでお伝えしたいことは、全てのランサムウェア攻撃を容易に検知して防御することは非常に困難であるという厳しい事実です。

最後に Minerva は各種ランサムウェア攻撃に対し、深い知見を備えております。これまでに数多くのマルウェア攻撃を防御しております。これは Minerva のチームが最高のサイバーセキュリティエクスパート集団であり、独自のテクノロジーを駆使した結果でございます。Minerva 製品が他のエンドポイント製品との決定的な違いは、Minerva 製品はランサムウェアはもちろんのこと、未知のマルウェア攻撃を先制防御することです。いかなる最小限の被害や損害が発生する前に攻撃をシャットアウトします。

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。