Kaseya社への攻撃で使用されたランサムウェア「REvil」をCrowdStrike Falconが阻止した方法

July 7, 2021 | Karan Sood - Liviu Arsene | エンドポイントとクラウドのセキュリティ

- マネージド・サービス・プロバイダー（MSP）を主な顧客とするITソフトウェアメーカー Kaseya社が、ランサムウェアREvil（レビル）の攻撃を受けた
- CrowdStrikeがランサムウェアREvilを攻撃者グループ「PINCHY SPIDER」と関連付けた
- CrowdStrike Falcon®プラットフォームが、ランサムウェアREvilから私たちのお客様を保護
- Falconプラットフォームが、機械学習と振る舞いベースの検知機能により、REvilの実行を初期段階で阻止

リモート管理ソフトウェアベンダー Kaseya 社に対する、ランサムウェア REvil による攻撃によって、CrowdStrike のお客様に危険が及ぶことはありませんでした。それは、**CrowdStrike Falcon プラットフォーム**が、お客様のシステム上で Revil ランサムウェアの攻撃をブロックしたからです。Falcon プラットフォームは、機械学習とふるまいベースの検知機能を用いて、攻撃の初期段階で REvil ランサムウェアを特定し、ブロックすることができます。Falcon をご利用のお客様は、保護機能を最大限に活用するために、CrowdStrike が推奨するポリシーである「不審なプロセス (Suspicious Processes)」の検知を有効にしてください。

CrowdStrike Intelligence は、**REvil ランサムウェアとその開発を行う攻撃者グループ PINCHY SPIDER の進化**を 2018 年から追跡しています。このグループは、かつて流行したランサムウェア「GandCrab」の開発にも関与していたと考えられています。REvil（別名 Sodinokibi）と GandCrab との類似性から、CrowdStrike Intelligence はこれらの関係性を疑いました。

何がおきたのか

7 月 2 日（金）に、REvil ランサムウェアのオペレーターは、Kaseya VSA の侵害に成功しました。Kaseya VSA は、Kaseya の顧客インフラストラクチャを監視および管理するためのソフトウェアです。**Kaseya 社の公式発表**によると、REvil ランサムウェアのオペレーターは、**ゼロデイ脆弱性**を利用して悪質なアップデートを配信し、Kaseya の約 60 社の顧客と、その顧客のサービスを利用していた 1,500 の企業に影響を与えました。

オランダのセキュリティ研究者グループ **Dutch Institute for Vulnerability Disclosure** は、以前にこれらの脆弱性を特定し、内々に Kaseya に報告していました。最近の報告によると、REvil のオペレーターは、現在 CVE-2021-30116 として追跡されている当時非公開の脆弱性を利用したと考えられています。

Kaseya は、この問題に対処するためのパッチリリースの準備中であるため、VSA サーバーをオフラインにしておくことをオンプレミスのパートナー企業に推奨しています。一方、REvil のオペレーターが**当初、7,000 万米ドルの身代金を要求**し、100 万台以上のシステムを感染させたと主張していたことも報告されています。驚くべきことに、REvil のオペレーターが**身代金の要求額を 5,000 万米ドルに引き下げ**、すべての被害者にユニバーサルデクリプターを提供することを申し出た可能性も示唆されています。

CrowdStrike Falcon が、ランサムウェア REvil からお客様を保護した方法

Falcon プラットフォームは、クラウド、機械学習、ふるまい検知の叡智を活用し、**ランサムウェア**などの高度な攻撃や脅威から組織を守るために、ゼロから設計されました。

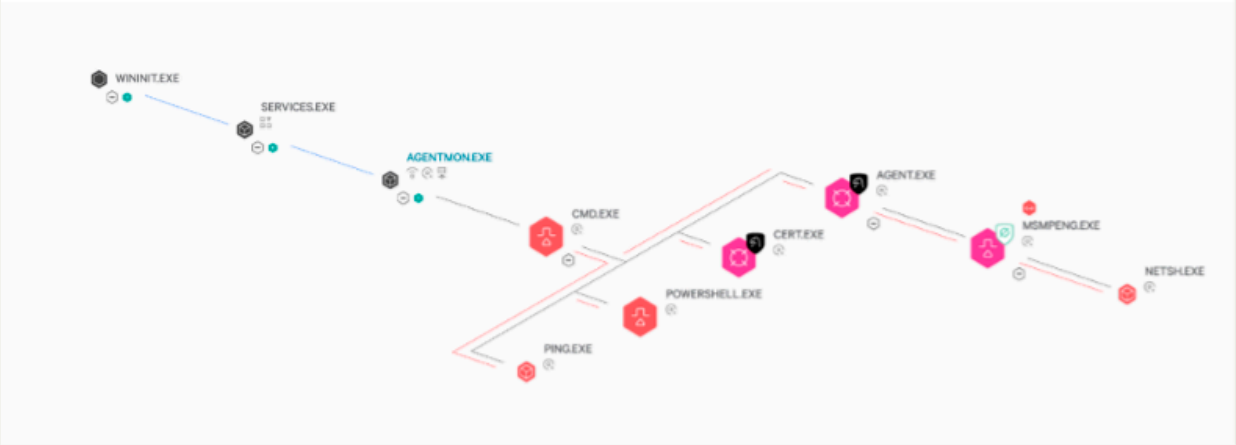
Falcon プラットフォームは、REvil などのランサムウェアを特定・防御し、顧客を保護するための階層型アプローチを採用しています。このケースでは、ランサムウェアの存在が疑われる不審なプロセスが発生した際に、Falcon センサーが攻撃を防御しました。また、センサー上とクラウド内での機械学習および**攻撃の痕跡（IOA）**データを活用したふるまい検知を用いて、REvil ランサムウェアを検知しました。また、Kaseya VSA に関連するような正当なプロセスが、悪質なコードをロードしようとしている場合でも検知できます。**Falcon OverWatch™ チーム**は常時監視を行い、国家主導の攻撃者グループや **PINCHY SPIDER** のようなサイバー犯罪者の関与が疑われるふるまいを感知した場合には、お客様が脅威に対処できるようにただちに通知します。

Falcon は、ランサムウェアに関連する不審なプロセスを特定することにより、この種の攻撃からお客様を保護する機能を備えています。Falcon プラットフォームでは、IOA を使用して不審なプロセスの実行を検知・阻止し、ペイロードが実行される前の攻撃チェーンの初期段階のうちに、ランサムウェア攻撃からお客様を守ります。

（クリックして原文ブログサイトビデオを表示）

機械学習がセキュリティ業界にもたらす効果は、事前にそのマルウェアに対する知識がなくても、ファイルの属性のみに基づいて悪意のある意図を含んでいるかを理解し、既知のマルウェアと未知のマルウェアの両方を認識できる点にあります。Falcon の機械学習は、REvil ランサムウェアにも対応し、各所で発生する攻撃を正確に特定し、ブロックします。

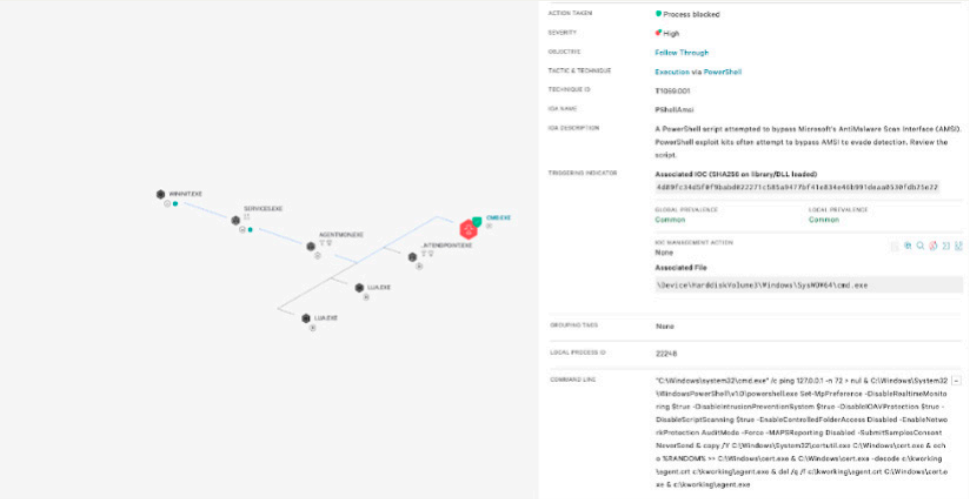
Falcon は、新出および未知の REvil サンプルを含むランサムウェアからお客様を保護するとともに、ランサムウェアを示唆する悪質なふるまいを正確に認識し、ブロックします。



（クリックで拡大）

Falcon は、攻撃チェーンにおける複数のステップを対象とする IOA で多層的なアプローチをしています。このケースでは、Kaseya のプロセスが cmd シェルを起動し、エンドポイント上の各種スキャン機能やセキュリティソリューションを無効にするといった悪質なアクションを実行しています。Falcon はこのふるまいを検知し、cmd シェルを終了させて、攻撃を阻止します。 これにより、REvil がディスクにドロップされ、MsMpeng.exe（正規の Windows Defender 実行ファイルの旧バージョン）にサイドローディングされるのを阻止します。このような機能は、マルウェアに関連する TTP（戦術、テクニック、手順）や、攻撃者のふるまいを継続的に監視することで得られる情報によって実現されています。

また、Falcon プラットフォームには、悪質なコマンドの代理実行を識別する機能があります。たとえ親プロセスが署名されたバイナリを持つ信頼できるプロセスであっても、攻撃者が VSA の脆弱性を悪用して悪質なペイロードを配信しようとする動きを効果的に検知し、防ぐことができます。この機能について、以下の図に示します。



（クリックで拡大）

Falcon プラットフォームは、REvil ランサムウェアのような脅威や、高度な攻撃者からお客様を日々守っています。我々は、階層型のアプローチを用いて、お客様にとって最も重要な資産を保護し、「侵害の阻止」という使命に常に集中して取り組んでいます。

推奨事項

1. **最新のセキュリティテクノロジを使用すること。**組織は、ランサムウェアから自社のインフラや重要な資産を守るために、適切なセキュリティテクノロジーを採用する必要があります。
2. **階層型アプローチを採用するエンドポイントセキュリティソリューションを利用**してランサムウェアを予防、特定し、お客様を保護すること。
3. **ランサムウェアの要求に応じないこと。**米国政府、法執行機関、セキュリティ企業は、被害企業はランサムウェアによる脅迫に屈すべきではないと助言しています。
4. **一人で悩まずに、エキスパートの支援やアドバイスを受けること。**セキュリティインシデントに遭った組織だけでは、調査や復旧が困難であったり、そのためのリソースが確保できない場合があります。

あなたの組織が REvil などの脅威の影響を受けているかもしれないと感じたら、CrowdStrike が**侵害調査**を行い、御社環境内の過去および現在進行中の攻撃活動を特定します。

CrowdStrike Falcon は、**Gartner 2021 Magic Quadrant for Endpoint Protection Platforms（EPP）** および **The Forrester Wave™ Endpoint Security Software As A Service** においてリーダーに選出されています。また、MITRE、SE Labs、AV-Comparatives といった主要な独立テスト機関の試験においても、その検知・保護能力が実証されています。

その他のリソース

- PINCHY SPIDERやCARBON SPIDERをはじめとする、ランサムウェアを用いる攻撃者グループについては、CrowdStrike Adversary Universeにて詳細に解説しています。
- 2021年版CrowdStrikeグローバル脅威レポートをダウンロードしてください。2020年にCrowdStrike Intelligenceが追跡した攻撃者グループに関する詳しい情報について紹介しています。
- こちらのブログでは、クラウドネイティブかつ強力なCrowdStrike Falcon®プラットフォームが、どのようにしてランサムウェアDarkSideからお客様を保護したかについて紹介しています。DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected（英語）.
- CrowdStrike Falcon Prevent™の無料トライアル版（フル機能）で、真の次世代型AVが、今日の非常に高度な脅威にどのように対抗できるかをご覧ください。

原文：How CrowdStrike Falcon Stops REvil Ransomware Used in the Kaseya Attack
https://www.crowdstrike.com/blog/how-crowdstrike-stops-revil-ransomware-from-kaseya-attack/