製品概要

エンドポイントへのエクリプシウム

概　説

大規模なランサムウェアキャンペーンから、国家支援を受ける高度な攻撃をするような攻撃者は、従来のセキュリティ制御からの検知を回避し、行動を隠すために、ファームウェア層の脆弱性やそれらに対する脅威にますます目を向けています。Eclypsiumファームウェア・セキュリティ・プラットフォームは、この重要なレイヤーにシンプルで自動化されたセキュリティをもたらし、企業はラップトップやデスクトップシステムなどのエンドユーザーデバイス内のファームウェアおよびハードウェアを容易に識別、検証、強化することができます。

これにより、セキュリティチームは、1つの効率的なツールの導入で、すべてのエンドユーザー資産のファームウェアレベルのデバイスインベントリ、脆弱性の評価、パッチ適用、脅威の検知と対応、サプライチェーンのリスク管理を自動化することが可能になります。

ファームウェアへの攻撃の現状

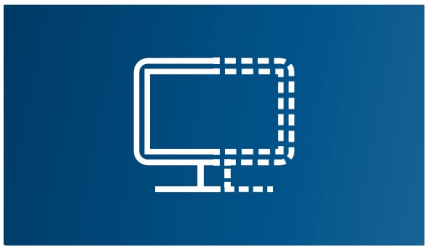
OSレベルのセキュリティが向上するにつれ、あらゆる種類の攻撃者の関心は、従来のセキュリティ製品によって比較的保護されていないファームウェア層に移ってきています。一般的なマルウェアであり、ランサムウェアの主要な構成要素でもあるTrickbotは、ファームウェアレベルでデバイスの脆弱性を自動的にスキャンする機能を追加しました。例えば、最近発見された「MosaicRegressor」というインプラントは、攻撃者が機器を無制限にコントロールし、持続させることができるものですが、このようなファームウェアレベルのインプラントは、脆弱な機器を容易に侵害することができてしまいます。

コアとなる機能

エンドポイント向けEclypsiumソリューションは、クラウドベースのファームウェア・セキュリティ・ソリューションであり、多数のエンドポイント・デバイスを完全に可視化し、コントロールすることができます。主な機能としては、以下のようなものがあります:

認識

エンドポイント・デバイス内のファームウェア、ハードウェア構成、およびコンポーネントを自動的かつ継続的に可視化します。セキュリティに影響を与える可能性のある重要なデバイス、属性、または変更点を迅速に把握することができます。



検証

すべてのファームウェアのインティグリティを検証し、ルートキット、インプラント、バックドアなどの既知および未知のファームウェアの脅威を検出することができます。古いファームウェアや脆弱なファームウェア、デバイスの誤設定によるリスクを積極的に把握することができます。

強化

パッチやアップデートをリモートで適用し、デバイスのリスクを積極的に軽減します。ファームウェアのインティグリティが変更された場合、自動的にアラートを受信し、既存のITおよびセキュリティツールとの統合により、自動応答を実現します。また、主要なSIEM、脆弱性管理、デバイス管理ツールとの統合を提供します。

具体的使用例の紹介

ランサムウェアと高度な脅威からの保護

ファームウェアに特化したランサムウェアやマルウェアの存在をプロアクティブに検知します。デバイスにファームウェアのインプラントやバックドアが存在しないことを確認します。ファームウェアのインティグリティが変更された場合には、自動的にアラートを受信します。

クラウドベースのリモートアップデートとパッチ適用

リモートで使用されている企業のデバイスやBYODデバイスに対して、デバイスを危険にさらすようなファームウェアの脆弱性や設定ミスがないかを評価します。BYODデバイスを含むすべてのデバイスが、強化されたファームウェア設定を使用するように構成されていることを確認します。

リモートワーカーと出張者のセキュリティ

遠隔地に配置されているエンドユーザのデバイスのインティグリティを監視します。デバイスのインティグリティに変化があった場合には自動でアラートを受け取り、デバイスを危険にさらす可能性のあるデバイスの姿勢の弱点を見つけます。

サプライチェーン・リスクマネジメント

新しいデバイスをリモートワーカーに直接出荷する際には、そのファームウェアが安全であり、サプライチェーン上で侵害されていないことを検証します。新たに入手したシステムを評価し、脆弱性やSBOMの予期せぬ変更を積極的に特定します。

詳細な機能と特徴

認識 : エンドポイントの可視化とインベントリ

Eclypsiumは、システムのUEFIやBIOSファームウェア、プロセッサやチップセット、PCIデバイス、ネットワークコンポーネント、ペリフェラルデバイス、Trusted Platform Module(TPM)、Intel's Management Engine(ME)など、様々なローレベルコンポーネントから詳細な情報を収集・分析します。これにより、セキュリティチームは、以下を含むすべてのエンドポイントについて、最新の詳細な可視性を得ることができます:

- **基本的な識別情報** - IPアドレス(オプション)、MACアドレス、ホスト名、オペレーティング・システム(ベンダー、バージョンなど)などのデバイスの特徴
- **ファームウェアおよびハードウェアの詳細情報** - プロセッサ、チップセット、デバイス、ファームウェアベンダー、リリースレート、システムおよびデバイスのメーカー、モデルナンバーなど
- **ハードウェアの状態と設定** - CPU、チップセット、I/Oレジスタ、その他の関連設定
- **PCI/PCIe情報** - PCI/PCIeデバイスオプション(拡張)ROMファームウェア。
- **デバイス、コンポーネント、その他のファームウェアの詳細** - ブートローダ情報、コンポーネントのハードウェアおよびファームウェアの構成、Trusted Platform Module (TPM)の状態、ベンダー固有のファームウェア、その他のタイプのファームウェア。

検証 : 脆弱性評価とインティグリティ

Eclypsiumは、エンドポイントのファームウェアとハードウェアの設定を分析し、デバイスのセキュリティ態勢に影響を与える問題点を発見します。これにより、リスクに基づいてデバイスを特定し、調査し、利用可能なアップデートを適用してリスクを修正することが容易になります。主な機能は以下の通りです:

- 古いファームウェアの検索 - 脆弱性やその他のデバイスの問題を含んでいる可能性のある古いファームウェアを持つエンドポイントを検索します
- 脆弱性の発見 - 従来のソフトウェアによる脆弱性スキャンでは見落とされることが多い、システムやコンポーネントのファームウェアに影響を与える脆弱性やCVEを持つデバイスを特定します
- **デバイスの誤設定の発見** - BIOSの書き込み保護機能の無効化、SMIやFlashディスクリプターなどのコンポーネントのロック解除など、デバイスを危険にさらす可能性のある設定上の問題を特定します
- **エンドポイントをリスクでソート** - 累積リスクに基づいてデバイスを素早くソートします。OS、グループ、ベンダー、製品、コンポーネント、セキュリティ機能、脆弱性でフィルタリングすることで、さらに詳細な表示が可能です
- **脆弱性による検索** - 特定の脆弱性を検索して調査し、影響を受け、特定の脆弱性に対してスキャンされたすべてのエンドポイントを見つけることができます

検証 : 脅威の検知と対応

Eclypsiumはアクティブな脅威の兆候がないかエンドポイントを分析します。これには、既知および未知の脅威の検出と、デバイスのインティグリティに対する予期せぬ変化を特定するための継続的な検証が含まれます:

- **デバイスベースラインの変更** - ベースラインに変更が加えられたデバイスを迅速に特定し、価値の高いシステムに予期せぬ、あるいは計画外の変更が加えられた場合に容易に認識することができます
- **未知のバイナリの検出** - Eclypsiumは業界で最も広範な既知のベンダーのファームウェアのライブラリを維持しており、この継続的に維持されているホワイトリストに載っていないあらゆるファームウェアを識別できます
- **既知の脅威の検出** - ルートキット、ハードウェア・インプラント、バックドアなど、さまざまな既知の脅威の存在を検出します。ユーザーは独自のファームウェア固有のYARAルールをインポートし、定義することができます
- **異常な動作** - ファームウェアの動作は通常においては予測可能です。これにより、Eclypsiumはファームウェアを分析して、潜在的な脅威を示唆する異常な動作や機能を明らかにすることができます

強化 : パッチ適用、修復、脅威への対応

Eclypsiumは、プロアクティブに問題を解決し、ファームウェアのリスクを軽減するためのツールをチームに提供します。セキュリティチームは、脆弱性を修正するためにファームウェアやデバイスコードを簡単に更新し、セキュリティイベントに対応するために自動化されたアラートやワークフローをトリガーすることができます:

- **パッチマネジメントとアップデート** - Eclypsiumコンソールを介して直接問題を修復したり、APIを介してファームウェアアップデートをダウンロードしてインストールします
- **自動応答** - 強力なREST APIは、SIEMやSOARソリューションなどの他の企業のセキュリティツールと統合し、自動応答やプレイブックを起動します
- **ダイナミックアラート** - 設定可能なアラートにより、特定の脆弱性や侵害の兆候をデバイスグループで監視し、それらが検出された場合にはエンドポイントオペレーションやインシデントレスポンスチームに通知します
- **緊急パッチ** - 脆弱性や設定ミスが悪用された場合、複数の方法でファームウェアのホットフィックスアップデートを行うことができます

エンドポイントのためのEclypsium : 対応デバイス

Eclypsiumは、ラップトップ、ワークステーション、タブレットを含む幅広いエンドポイントデバイスをサポートしています。EclypsiumはWindows、MacOS、Linuxの各OSをサポートし、Apple、Asus、Dell、Fujitsu、HP、Lenovo、Quanta、Toshibaのシステムを含むほぼすべてのx86ベースのプラットフォームで動作します。

対応OS

以下のOSの64ビット版に対応しています。

- Windows 7、8、8.1、10
- macOS 10.12（"Sierra"）から11.4（"Big Sur"）まで
- Windows Server 2012、2016、2019
- Ubuntu 16.04 - 21.04
- Debian 8.x - 11.x
- RHEL/CentOS 6～8、現行のFedoraディストリビューション
- SLES 11 - 12、OpenSuse Leap 15、OpenSuse Leap 42.3

対応ハードウェアおよびチップセット

- Intelシステム - Eclypsiumは、Intel Core、Core M、Xeon、Atomベースのシステムを含む、Intel第2世代（コードネーム「Sandy Bridge」）以降のすべてのIntelシステムをサポートしています。

- AMDシステム - Eclypsiumは、以下を含むAMD ZenおよびZen2世代のCPUをサポートしています。
  - Ryzen 1xxx - 3xxxシリーズモデル
  - EPYC 7xxxシリーズモデル

インテグレーション

Eclypsiumプラットフォームは一般的なデプロイメントツールやセキュリティツールと統合することができるので、企業のデバイスをファームウェアやハードウェアレベルまで簡単に管理・保護することができます。強力なREST APIにより、企業はEclypsiumを既存のツールやプロセスと統合することができます。検証済みの統合機能は以下の通りです：

Eclypsiumのデプロイメント		可視性の向上と分析
• Airwatch by VMWare • JAMF • Microsoft Intune	• Microsoft SCCM • Tanium	• Intel intelligence feeds

システムへのアクセスと認証		セキュリティ・アナリティクス
• Cloudflare Access • Okta	• Ping Identity • Google OSS	• Kenna Security • Splunk

Eclypsiumについて

Eclypsiumは、企業向けのファームウェアセキュリティ企業です。当社の包括的なクラウドベースのプラットフォームは、ラップトップ、タブレット、サーバ、ネットワーク機器、コネクテッドデバイスなど、お客様の広範なグローバルネットワークに存在するあらゆる場所で、ファームウェアとハードウェアを識別、検証、強化します。Eclypsiumのプラットフォームは、持続的かつ密かなファームウェア攻撃からの保護、継続的なデバイスのインティグリティの提供、大規模なファームウェアパッチの提供、ランサムウェアや悪意のあるインプラントの防止を行います。セキュリティ意識の高いフォーチュン1000企業や連邦政府機関に支持されているEclypsiumは、Gartner社の「Cool Vendor in Security Operations and Threat Intelligence」、TAG Cyber社の「Distinguished Vendor」、Fast Company社の「World's 10 Most Innovative Security Companies」の1社として選ばれています。
Eclypsiumに関するお問い合わせは jp-info@Eclypsium.com へ日本語でお気軽にお問い合わせください。