製品概要

サーバーへのエクリプシウム

概　説

攻撃者は当然ながら、最も価値の高いターゲットを探しますが、ほとんどの企業にとって、それはサーバを意味します。これらの重要な資産は、今日の「大物狙い」のランサムウェアや、組織に最大のダメージを与えようとする攻撃者にとって、究極のターゲットとなっています。これらの攻撃者やその他の脅威の主体は、従来のセキュリティ管理を回避・無力化するために、ファームウェア層の脆弱性や脅威にますます目を向けるようになっています。

Eclypsiumの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、ローカル、クラウド、ハイブリッド環境のいずれでホストされているかにかかわらず、サーバ内のファームウェア、ハードウェア、コンポーネントを容易に識別、検証、強化することができます。これにより、ローカル環境、クラウド環境、ハイブリッド環境を問わず、サーバー内のファームウェアレベルのデバイスインベントリ、脆弱性評価、パッチ適用、脅威の検知と対応、サーバーインフラ全体のサプライチェーンリスク管理を自動化するツールが、初めてセキュリティチームに提供されることになりました。

ファームウェアへの攻撃の現状

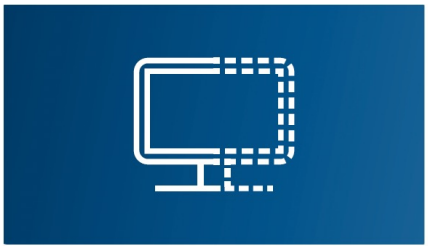
ファームウェアへの攻撃は増加傾向にあり、サーバは攻撃者のお気に入りのターゲットになりつつあります。最近の業界分析によると、過去2年間で80%の企業がファームウェア攻撃を受けたことがあります。同時に、ランサムウェアの攻撃者は、混乱を引き起こすことと、「二重恐喝」スキームの一部としてデータを盗むことの両方を目的として、サーバーに重点的に取り組んでいます。例えば、ランサムウェア「Cl0p」は、最近、Accellion File Transfer Appliancesを標的にして、企業からの支払いを要求しています。同様に、「Colonial Pipeline」の背後にあるランサムウェアグループ「DarkSide」も、攻撃の一環として企業のサーバのファームウェアを標的にしたり、データを盗んだりすることで知られています。

コアとなる機能

サーバー向け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、ローカルおよびクラウド上の多数のサーバを完全に可視化し、制御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

エンタープライズサーバ内のファームウェア、ハードウェア構成、および数十個のコンポーネントの自動化と継続的な可視化を実現します。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、コンポーネント、属性、または変更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、バックドアを含む既知および未知のファームウェアの脅威を検出します。古くて脆弱なファームウェアやデバイスの誤設定によるリスクを積極的に特定します。

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実現可能なマルウェアの存在をプロアクティブに検出します。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、自動で警告を受け取ることができます。

クラウドベースのリモート検証、アップデート、およびパッチ適用

古いファームウェアや脆弱性のあるデバイスをリモートでパッチやアップデートすることで、サーバを安全な状態に保ちます。ベアメタルのサービスプロバイダやデバイスのファームウェアの脆弱性や、デバイスを危険にさらす可能性のある誤った設定をリモートで評価します。再プロビジョニングされたサーバのファームウェアが適切にリフラッシュされ、既知の良好な状態であることを確認し、すべてのデバイスが、強化されたファームウェアの設定を使用するよう、適切に構成されていることを確認します。

サプライチェーン・リスクマネジメント

購入前に機器ベンダーやサービスプロバイダーを評価し、脆弱性や安全でないコンポーネントや構成を特定します。新たに取得したシステムを検証し、サプライチェーン上で侵害されていないことを確認するとともに、脆弱性やSBOMへの予期せぬ変更を積極的に特定します。

ハードウェアまで含めた仮想環境の保護

仮想環境は依然としてハードウェアに依存しており、物理ホストのファームウェアに脆弱性や脅威があると、仮想化資産が危険にさらされます。Eclypsiumを使えば、チームは仮想化戦略が安全なハードウェアの基礎の上に構築されていることを確実にすることができます。Eclypsiumは、VMware ESX環境をサポートする基盤となるハードウェアのインティグリティを容易に監視し、脆弱性を発見し、適切なアップデートを適用することができます。

詳細な機能と特徴

認識 : サーバー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、BMC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、ストレージドライブ、PCIeデバイス、IntelのManagement Engineなど、さまざまなローレベルコンポーネントから詳細な情報を収集し、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サーバー、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、すべてのファームウェアとデバイスの設定を分析し、デバイスのセキュリティ姿勢に影響を与える問題を検出します。これにより、リスクに基づいてデバイスを特定・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
- **デバイスをリスクでソート** - 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、デバイスにアクティブな脅威の兆候がないか分析します。これには、既知および未知の脅威の検出に加え、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監視が含まれます:

- **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

サーバーのためのEclypsium : 対応デバイス

Eclypsiumは、幅広いサーバーメーカー、デバイス、およびそれらの基盤となるコンポーネントをサポートしています。EclypsiumはWindows、 Linuxオペレーティングシステムをサポートし、Dell、HPE、Lenovo、Quanta、Supermicroなどのサーバー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。Eclypsiumは、ファームウェアのインティグリティ監視や、VMware ESX環境でのリスク管理やパッチ管理もサポートしています。

対応OS

以下のOSの64ビット版に対応しています。

- 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
- Windows 7、8、8.1、10
- macOS 10.12（"Sierra"）から11.4（"Big Sur"）まで

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されており、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。