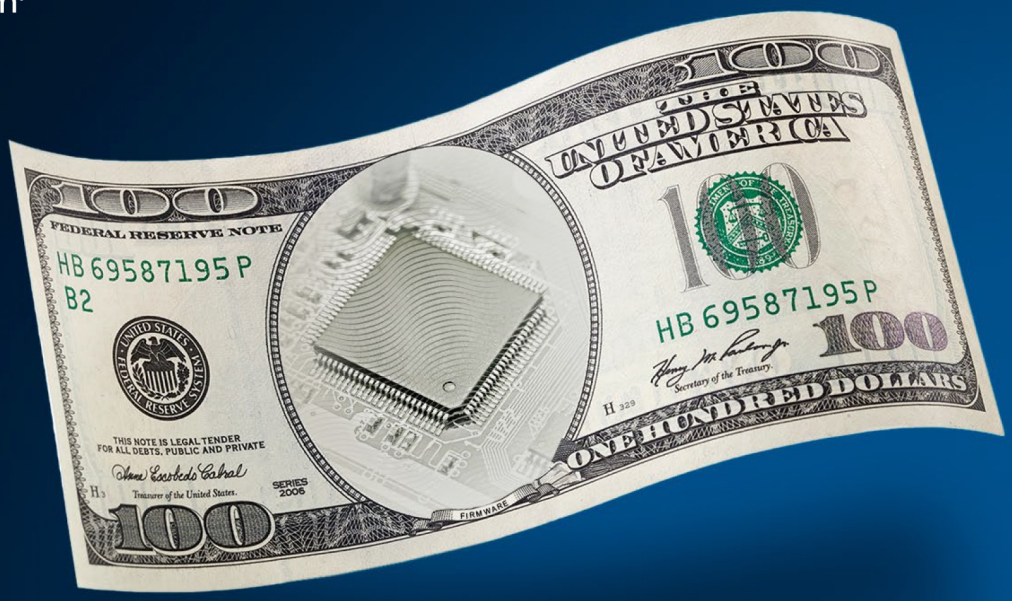


文中のハイパーリンクは英文のサイトとなっております、日本語をご希望される場合はブラウザの翻訳機能等をご使用ください。

ファームウェアがランサムウェアの引き金の第1位

ランサムウェアは、今日、組織が直面する最も広範で有害な脅威の1つであり続けています。ランサムウェアは新しい問題ではありませんが、最近、攻撃の量、巧妙さ、そして最も重要なのは、被害者に与える被害が大幅に増加していることです。企業は最も有利なターゲットであり、成熟した高度に専門化、組織化されたランサムウェア攻撃が、企業のインフラを侵害し、企業のセキュリティ制御を回避することに特化して発展してきました。

多くの企業にとって、デバイス内のファームウェアは、攻撃対象領域の中で最も目に付きにくく、最も保護されていない部分であることに変わりはありません。
ランサムウェアの攻撃者は、このギャップを、ファームウェアに特化した様々な新しい技術、ツール、手順（TTP）で捉え、最大限の被害をもたらすために、組織内にアクセスし、持続することを可能にしてきました。VPN、ネットワーク機器、セキュリティ・インフラストラクチャ内のファームウェアは、最も一般的な初期アクセス・ベクターの1つとなっています。同様に、エンドポイントデバイス内のファームウェアの脅威は、ランサムウェアの攻撃者が持続性を維持し、従来のOSレベルの制御を覆すことを可能にします。

このホワイトペーパーでは、こうしたランサムウェアの動向や最近の動向、特にファームウェアやデバイスレベルの攻撃が今日の攻撃で果たす重要な役割に焦点を当てます。

このホワイトパーパーでは以下を学ぶことができます：

- ランサムウェアの最新の成長および進化の原動力となっているもの
- ランサムウェアの経済的な仕組みと、それが企業のファームウェアにとって意味すること
- 攻撃者は、ランサムウェア攻撃の複数のフェーズでファームウェアをどのように使用するか
- ランサムウェアは、どのように国家的な脅威行為者の技術を採用しているのか
- ファームウェア・レベルでランサムウェアを防御する方法

すべてのサイバーセキュリティと同様に、ランサムウェアの防御には、協調的で多層的なアプローチが必要です。

このホワイトペーパーにより、セキュリティ・リーダーおよびIT担当者は、現実の攻撃においてファームウェア層が果たす重要な役割と、ファームウェア・セキュリティが従来のセキュリティ制御をどのように補完できるかを迅速に学ぶことができます。

企業のシステムインフラを防御する

ランサムウェアは拡大する問題

ランサムウェアの攻撃は、より一般的になり、被害が拡大し、組織にとってより高い代償になり続けているため、ランサムウェアの企業リスクは過去最高になっています。最近の調査によると、北米におけるランサムウェア攻撃は、標的型攻撃の増加により、過去数年間で158%も増加しています。また、ランサムウェアの平均支払額は20万ドル以上、平均ダウンタイムは23日に増加するなど、組織に与える金銭を含むダメージは増加し続けています。

ランサムウェアの増加の背景には、さまざまな要因があります。特に、ランサムウェアは、サイバー犯罪者に非常に直接的な金儲けの手段を提供します。ランサムウェアの実行者は、データを盗んで闇市場で転売する代わりに、被害者から直接恐喝することで、攻撃が成功した場合に直ちに収益化することができるのです。これはまた、より多くの種類の企業データとシステムが、攻撃者にとって実行可能なターゲットになることを意味します。従来は、ペイメントカードのデータなど、簡単に転売できるデータのみが標的でした。ランサムウェアの場合、無効にするデータやシステムは、被害者にとって価値のあるものであればよいのです。つまり、組織の運営を支えるあらゆるデータやシステムがターゲットになるのです。

二重の恐喝の増加など、最近の動向はこの傾向をさらに加速させています。二重の恐喝を行うランサムウェアは、暗号化に加えて、あるいは場合によっては暗号化の代わりに、機密データを流出させます。そして、攻撃者は、支払いを要求したり、情報を公開すると脅したりする。これは当然ながら、事実上あらゆる組織の秘密、知的財産、あるいは個人的なコミュニケーションまでもがランサムウェアの標的となり得ることを意味します。

このため、攻撃者の狩場は大きく広がっています。事実上、あらゆる組織が標的となり、あらゆる機密データやシステムが収益化される可能性があるのです。

ランサムウェアの経済

ランサムウェア攻撃や攻撃者を指すのが一般的ですが、ランサムウェアの事象には、通常、攻撃の特定のフェーズに高度に特化した様々な脅威主体が関与していることを認識することが重要です。これには以下が含まれます。

ランサムウェア開発者 - 実際のランサムウェアそのものを構築する開発者です。これらの開発者は、企業へのダメージを最大化するために、できるだけ早くデータを調整し、暗号化するマルウェアに特化しています。開発者はその後、実際の攻撃でコードを使用する他のグループにランサムウェアを販売することになります。

Initial Access Brokers (IABs) - IABsは、ランサムウェアのサプライチェーンにおいて最も重要な役割を担っています。これらの攻撃者は、企業へのアクセスを獲得し、他の犯罪者に転売できるような永続的な存在を確立することを専門としています。これには、信頼できるアクセスを確保するために、ある程度の特権の昇格、横移動、永続的なテクニックが含まれることがよくあります。これから説明するように、ファームウェアのエクスプロイトとテクニックは、IABの武器として重要な役割を果たすようになりました。

オペレーターとアフィリエイト - ランサムウェアのオペレーターとアフィリエイトは、前のフェーズで提供されたランサムウェアとアクセスを使用して、実際のランサムウェア攻撃を実行します。一部の関連会社は、攻撃の影響を最大化するために、さらなる横方向の移動に特化する場合があります。オペレーターは、実際のランサムウェアを実行し、恐喝のフェーズを管理します。このフェーズは、ランサムウェア・アズ・ア・サービス（RaaS）として提供されることが多くなっており、オペレーターは基盤となる関連会社を追加してアクセスを販売します。

このように専門性を高めることで、攻撃者はより高度な技術を身につけることができます。当然ながら、各フェーズにおける行為者は、信頼性が高く、セキュリティ制御を迂回・回避することができる技術を有していることが高く評価されます。

ランサムウェア攻撃におけるファームウェアの役割

ファームウェアは、ランサムウェア攻撃において、特に初期アクセスの獲得と継続的な持続性の確立という点で重要な要素となっています。一部のランサムウェアグループは、デバイスを無効化し、そのデータをロックする方法として、ファームウェアやブートレベルの攻撃を直接的に使用しています。ランサムウェアの「ファームウェア・アズ・ア・ベクター」志向は、Security Magazineが2021年10月31日のランサムウェアの持続性に関する記事で、実務者が犯す「6つの共通の間違い」の1つとして呼び出すほど深刻になっています。

初期アクセスのファームウェアとネットワークデバイス

VPN、アプリケーション・デリバリー・コントローラ、ファイアウォールなどの企業向けデバイスに存在するファームウェアやデバイスレベルの脆弱性は、ランサムウェアグループにとって最大の侵入口となっています。皮肉なことに、企業を保護するために信頼されているデバイスの脆弱性が、現在最も活発な侵入経路の一部となっています。

企業のシステムインフラを防御する

この流れは2020年7月、FBIがネットウォーカー・ランサムウェアがPulse Secure VPNの脆弱性（CVE-2019-11510）を狙い始めたという警告を発したことから始まりました。この脆弱性はすでに複数のAPTグループによって悪用されていましたが、今度はランサムウェアが同じ手法を採用し始めていたのです。他のランサムウェアグループもすぐに追随し、REvil、Maze、Black Kingdomが同じ脆弱性を利用していました。

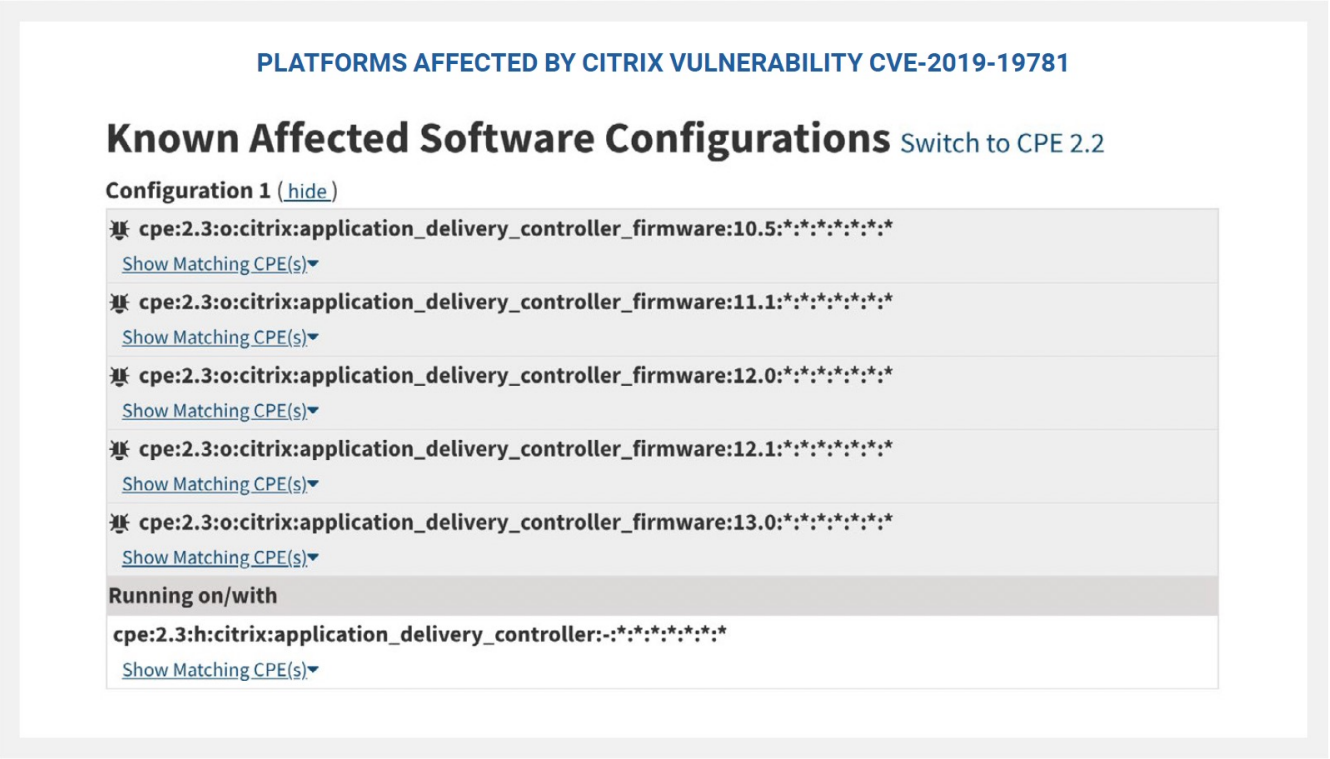
この問題は、Citrix、F5、Fortinet、Palo Alto Networks、SonicWallなどの企業インフラベンダーにすぐに広がりました。Maze、Conti、REvil のトップ 3 を含む数十のランサムウェアグループが、ネットワークデバイスを悪用して侵害の初期アクセスを行うという事態が短期間のうちに発生したのです。以下の表は、ネットワークやインフラの脆弱性を攻撃することが確認されているより有名なランサムウェアグループのいくつかを紹介しています。

	Ransomware														
Vendor/Product	Agrius	BlackKingdom	Conti	Cl0p	Cring	Darkside	eChoraix	FIVEHANDS	Groove	Hello	Maze	Netwalker	Other	Pay2Key	REvil
Accellion				⚠											
Cisco				⚠											
Citrix									⚠		⚠		⚠		⚠
F5													⚠		
Fortinet	⚠		⚠		⚠									⚠	⚠
Microsoft Servers				⚠					⚠	⚠			⚠		
Oracle															⚠
Palo Alto Networks													⚠		
Pulse Secure		⚠							⚠		⚠	⚠	⚠		⚠
QNAP							⚠								
SonicWall						⚠		⚠		⚠					
Sophos													⚠		
VMware						⚠			⚠				⚠		

企業のシステムインフラを防御する

これらの脆弱性の多くは、ネットワーク機器のファームウェアや統合コードに直接的に関連していることに留意することが重要です。例えば、APTやランサムウェアによって最もよく攻撃される 33 のネットワークデバイスの CVE のうち 12 は、影響を受けるコンポーネントとしてファームウェアを具体的に挙げています。これには、企業向けVPN、Ciscoルーター、Citrixアプリケーションデリバリーコントローラー、SonicWall VPNやセキュリティデバイスが含まれています。

ファームウェアが具体的に名指しされていない場合でも、これらのインフラストラクチャ・デバイス内のコードの多くは、統合されたデバイスコードに存在するため、単純な非認証スキャンでは通常見逃されることになってしまいます。たとえ脆弱性が検出されたとしても、より伝統的なオペレーティング・システムやアプリケーションに焦点を当てがちなスタッフによって、適切に優先順位が付けられない可能性があります。さらに、企業インフラ内の脅威や侵害の兆候を検出する場合、問題はさらに深刻化します。これらのデバイスの整合性を検証するには、通常、手動、専用ツール、または1回限りのベンダー固有のツールが必要になります。このため、検出作業に時間がかかり、一貫性に欠けることがあります。



PLATFORMS AFFECTED BY CITRIX VULNERABILITY CVE-2019-19781

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- cpe:2.3:o:citrix:application_delivery_controller_firmware:10.5:*:*:*:*:*:*:* — Show Matching CPE(s)
- cpe:2.3:o:citrix:application_delivery_controller_firmware:11.1:*:*:*:*:*:*:* — Show Matching CPE(s)
- cpe:2.3:o:citrix:application_delivery_controller_firmware:12.0:*:*:*:*:*:*:* — Show Matching CPE(s)
- cpe:2.3:o:citrix:application_delivery_controller_firmware:12.1:*:*:*:*:*:*:* — Show Matching CPE(s)
- cpe:2.3:o:citrix:application_delivery_controller_firmware:13.0:*:*:*:*:*:*:* — Show Matching CPE(s)

Running on/with

- cpe:2.3:h:citrix:application_delivery_controller:-:*:*:*:*:*:*:* — Show Matching CPE(s)

出典：https://nvd.nist.gov/vuln/detail/CVE-2019-19781

エンドポイントのパーシスタンスを高めるファームウェア

IABやランサムウェアの関連企業は、最初のアクセスを獲得した後、セキュリティツールから身を隠し、環境内に留まる方法として、ファームウェアをターゲットにすることが増えています。ファームウェアに悪意のあるコードを埋め込むことで、攻撃者はオペレーティングシステムを欺き、その下に潜伏することができます。ファームウェアの埋め込みとバックドアにより、攻撃者はより高度なセキュリティ制御を回避することができ、また、悪意のあるコードはオペレーティングシステムの完全な再インストールにも耐えることができるようになります。このようなファームウェアのインプラントは、MosaicRegressorやLojaxなど、さまざまなマルウェアのキャンペーンで確認されています。

この戦略は、今日、企業に影響を与えるマルウェアの中で最も一般的な形態であるTrickBotで観察されています。Trickbotは、横方向の動きと持続性に特化した高度にモジュール化されたトロイの木馬で、RyukやContiランサムウェアのキャンペーンで多用されています。TrickBotの新しいファームウェア機能であるTrickBootは、攻撃者がデバイスのUEFI/BIOSファームウェアの読み取り、書き込み、消去を可能にする、よく知られた脆弱性がないかデバイスをチェックするものです。

企業のシステムインフラを防御する

この機能は、ランサムウェア攻撃の文脈では、壊滅的な影響を与える可能性があります。侵害されたデバイスのファームウェアに悪意のあるコードを書き込むことで、攻撃者は、デバイスの完全な再イメージングに耐えられるようなデバイス内の持続性を確立することができます。デバイスのファームウェアを制御することで、攻撃者は、オペレーティングシステムを実行しているセキュリティ制御を無効化したり、回避したりすることも可能になります。また、最後の手段として、攻撃者は単にファームウェアを破壊して、デバイスを無効化することも可能です。

ファームウェアレベルでランサムウェアを防御する方法

ファームウェアは、今日の企業向けデバイスにおいて、最も特権的であると同時に最も保護されていないコードです。企業がオペレーティング・システム・レベルのセキュリティを強化する一方で、ランサムウェアやその他の脅威は、比較的無防備なファームウェア・レイヤにますますパーシスタンスを求めてきています。

ランサムウェアから身を守るには、ファームウェアが、OSやアプリケーションなどの他の重要なコードと同じレベルの可視性と保護を得られるようにする必要があります。ほとんどの組織では、ファームウェア・セキュリティの以下の重要なフェーズをサポートするために、 ファームウェア固有のプロセスとツールを追加することが必要となります。

1. **ファームウェアの特定** - ファームウェアの攻撃対象領域に対する完全な可視性を確立する。ファームウェアの特定 - ファームウェアの攻撃対象領域を完全に可視化する。すべての重要なデバイスで使用されているファームウェアとデバイス・レベルのコンフィギュレーションを可視化する。

2. **ファームウェアの検証** - ファームウェアの脆弱性をプロアクティブに特定し、実際のランサムウェア攻撃で使用されているものを優先的に特定する。すべてのファームウェアの整合性を積極的にチェックし、ファームウェアの動作を監視して、脅威や侵害の兆候を特定する。

3. **ファームウェアの強化** - 脆弱なファームウェアをアップデートし、利用可能なすべてのセキュリティ機能が有効になり、適切に設定されていることを確認する。

APTのランサムウェアの脅威アクターとの関連性

サイバーセキュリティの分野では、金銭的な動機のある攻撃者が、APT行為者が最初に使用したツールやテクニックを模倣することはよくあることです。ランサムウェアによるファームウェアの悪用は、その一例を示しています。

2020年初頭、CISAは、CitrixとPulse Secure VPNの脆弱性が国家ベースの脅威行為者の最重要ターゲットになったという警告を発しました。その後、ロシア、中国、イランの国家レベルの脅威者が、さまざまな企業ネットワーク機器やベンダーを標的としていることが、一連の追加アラートで詳細に示されたため、これはより大きな傾向の始まりに過ぎないことが判明しました。特に、ロシアの SVR 技術に関する最新のアラートでは、標的となった上位 11 件の脆弱性 (PDF) のうち 5 件がネットワーク機器に影響を及ぼしています。実際、ランサムウェアが悪用するネットワークデバイスの脆弱性の大半は、以前、国家的な攻撃で使用されたものです。つまり、企業は、ランサムウェアの今後の動向を予測する先行指標として、APTが標的とするデバイスの脆弱性を追跡しておくとよいでしょう。

同様に、ファームウェアのインプラントは、TrickBotに見られるずっと以前から、APTやその他の国家を後ろ盾にした作戦で観察されていました。2015年に公開されたHacking TeamのUEFIインプラントは、APTアクターがすでにファームウェアインプラントを作戦に使用していたことを示す例となりました。この同じコードは、後にMosaicRegressorで再利用され、ファームウェアの機能が他の脅威によって容易に取り入れられることをさらに浮き彫りにしています。

また、国家的な脅威の担い手も、ランサムウェアを作戦に直接採用しています。これは、悪名高いNotPetya攻撃へのロシアの関与など、最もよく知られた攻撃で見られました。同様に、北朝鮮の攻撃者はTrickBotに、イランの脅威者はランサムウェアのAgriusファミリーに関連しています。

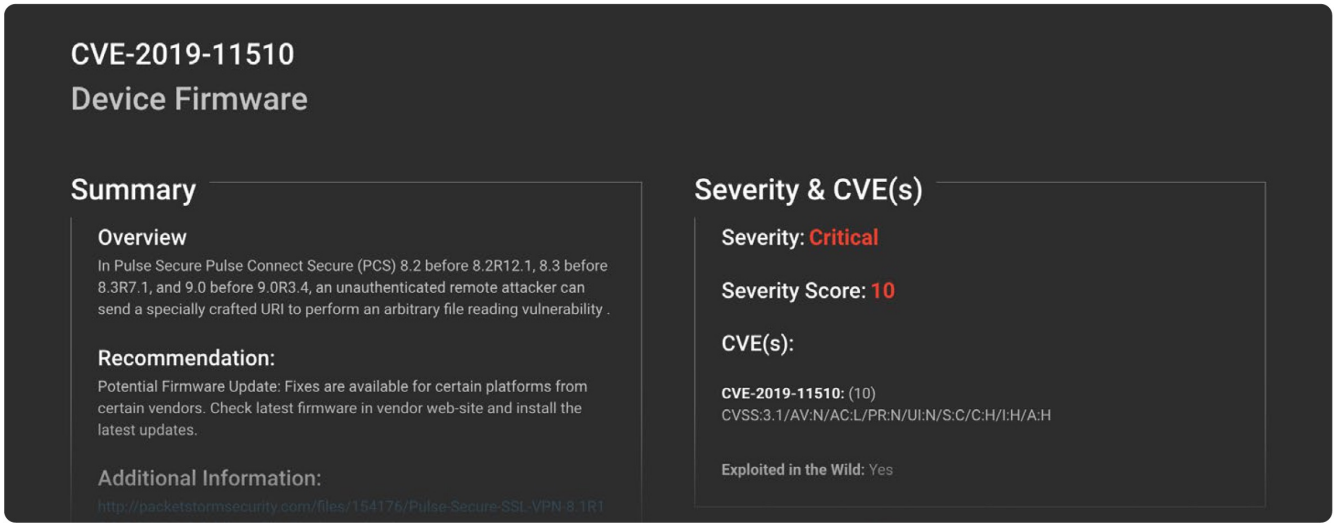
そのため、企業は、ランサムウェアに関して、単一のタイプの行為者や動機が存在するわけではないことを認識する必要があります。すべての脅威がそうであるように、セキュリティチームは、よりターゲットを絞った作戦だけでなく、広範で日和見的なランサムウェア攻撃から身を守るための備えをしなければなりません。

企業のシステムインフラを防御する

Eclypsiumのファームウェア・セキュリティ・プラットフォームは、重要なデバイスの種類とベンダーを問わず、これらのニーズに一貫して対応するためのシンプルで自動化された方法を提供します。ランサムウェアに対する防御の観点から、Eclypsiumは以下のようなアクションを可能にします。

重要なデバイスの検出 - Eclypsiumは、ランサムウェアの攻撃者に大きく狙われているネットワーク・デバイスを含む、企業環境内のデバイスを自動的に検出することができます。Eclypsium独自の分散型ディスカバリーにより、ネットワーク・デバイスにセキュリティ・エージェントをインストールすることなく、これらの重要なデバイスを検出することができます。これにより、追加のコードを追加したり、変更ウィンドウを待つことなく、デバイスに対するセキュリティの可視性を容易に得ることができます。

ファームウェアの脆弱性とリスクの発見 - Eclypsiumは、企業向けデバイスの脆弱性を分析し、CVEやその他の弱点に特に重点を置いています。これにより、組織の既存のパッチ管理プロセスに余計なノイズを加えることなく、見落とされている重要な脆弱性を表面化させます。チームは、ランサムウェアの標的となる脆弱なネットワークデバイスを迅速に特定し、TrickBot/TrickBootの影響を受けやすいエンドポイントを容易に見つけることができます。また、このソリューションは、利用可能なすべてのセキュリティ機能が有効であり、適切に設定されていることを確認します。



脆弱性のあるデバイスのパッチとアップデート - Eclypsiumは、ファームウェアとデバイス・コードを簡単にアップデートして脆弱性を修正し、セキュリティ・イベントに対応するための自動アラートとワークフローを起動することができます。スタッフはEclypsiumコンソールから直接、またはAPI経由でファームウェアのアップデートをダウンロードしてインストールし、問題を修正することができます。

デバイスの完全性を検証し、脅威を検出 - Eclypsiumは、さまざまなコードとファームウェアを解析し、デバイスが有効でベンダーが承認したコードのみを実行していることを確認します。このソリューションは、ベンダーからの「既知の良い」コードが変更されていないことを検証し、既知の脅威の存在をチェックします。また、潜在的な未知の脅威を特定するために、必要に応じて動作分析を行います。これにより、IABやランサムウェアのオペレーターによって侵害されている可能性のあるネットワークデバイスやエンドポイントを特定することができます。

これらの重要な機能により、セキュリティチームは、ファームウェアレベルでランサムウェアから資産を保護するためのツールを手に入れることができます。サイバーセキュリティの活発な分野と同様に、攻撃者は常に進化を続け、新しい脆弱性や技術を追求しています。Eclypsiumは、ファームウェア・セキュリティとネットワーク・デバイスの重要な分野を専門としており、業界をリードするリサーチにより、新しいリスクと脅威が出現しても、組織は常に最新の情報を入手することができます。Eclypsiumプラットフォームの詳細については、jp-info@eclypsium.com までお問い合わせください。