注意：出張者のラップトップをサイバーセキュリティの脅威から守るために

高リスク国のIT資産をファームウェアのインプラントやバックドアから保護するための新たなアプローチ

世界経済は、歴史上最も活気に満ち、相互に結びついています。一方で、最も競争の激しい世界でもあり、国家は知的財産、技術、企業秘密を盗むための戦略的手法として、サイバー攻撃に目を向けています。その一例として、米国の通商製造政策局は最近、他国が“サイバー・スパイ活動を含む様々な手段による組織的な経済スパイ活動を行っている…”と結論付けています。しかし、個人や企業は、多くの国や潜在的にリスクの高い場所でビジネスを行ったり、そこへ出張したりする必要もあります。このような場合、現地の従業員も出張中の従業員も、スパイ活動の格好の標的となり得ますので、高度なサイバーセキュリティの脅威から保護しなければなりません。

このような攻撃を受ける危険性のある組織の多くは、出張者へのノートPCの貸し出し、出張中にアクセスできるデータの量と種類の制限、ハードディスクの暗号化、出張後のデバイスのワイプなどの予防策を講じています。しかし、経験豊富な攻撃者は、ファームウェアやハードウェアレベルの攻撃を用いてこれらの対策を破り、数分でノートPCを危険にさらし、再インストールしても検知されないようにできることも熟知しています。インプラントやバックドアは、長年にわたって国家支援を受ける攻撃者が好んで使用してきたサイバー攻撃ツールですが、これまで、デバイスがファームウェアレベルで侵害されているかどうかを簡単に評価する方法はありませんでした。企業の中には、この脅威を深刻に受け止め、リスクの高い国への渡航後はラップトップを廃棄するところもあります。

しかし、もっと良い方法があります。新しいカテゴリーのファームウェア保護プラットフォームは、ファームウェアの分析、監視、および脅威の検知を自動化したアプローチを提供し、サイバーセキュリティチームが、旅行中やリスクの高い場所での作業中に使用するデバイスの完全性を確保できるようにします。この新しいセキュリティ層は、最も洗練されたインプラントやバックドアをも検出することができ、旅行者向けノートPCプログラムにおけるファームウェアのセキュリティギャップを解消します。

誰がターゲットになるのか？

ほぼすべての組織がスパイ活動の標的になる可能性がありますが、他の組織よりもリスクが高い分野や個人もあります。国家の重要な目標の一つは、新しい独自技術を獲得することであり、そのためには新技術を開発するあらゆる組織が最重要ターゲットとなります。しかし、これは研究に従事している大学やその学生・職員にも当てはまります。

同じように、国が支援する企業が市場で優位に立つために、コスト情報や製造スケジュールなどの予測情報などの企業秘密を取得しようとする悪者もいます。この問題は民間企業にとどまらず、政府関係者、人権団体、NGOなども国家ぐるみの攻撃の対象となる危険性があります。

これらのケースでは、多くの国家的攻撃者にとって、「誰が」が「何を」と同様に重要であることが多いです。組織の幹部、開発者、研究者などは、彼らがアクセスできるシステムや情報に基づいて、価値の高いターゲットとなります。そのため、組織は、重要な役割を担う従業員の移動中の保護を優先することを検討する必要があります。

高リスク国における企業のIT資産保護の現状

多くのサイバーセキュリティチームは、リスクの高い国への旅行の際には、旅行者にノートPCを自宅に置いてもらい、代わりに旅行用に特別に準備されたノートPCを貸し出しています。通常、このデバイスは暗号化されており、旅行に必要なデータとアプリケーションのみが格納されており、カメラ、Wi-Fi、Bluetooth、USBデバイスなどの機能は無効になっています。

また、携帯電話を持たずに旅行することや、国内で借りた携帯電話を使用することを勧められることもあります。さらに、ホテルの部屋や金庫は安全ではありませんので、デバイスを放置しないようにする必要があります。

企業のシステムインフラを防御する

返却されたノートPCは、従来のセキュリティツールで危険性をチェックされた後、通常はワイプされてサービスに戻されるか、場合によっては廃棄されることもあります。

しかし、これらのプログラムには限界があります。出張用に別のデバイスを用意するコストに加えて、多くの社員は普段使っているデータやツールにアクセスしたい、あるいはアクセスする必要があります。機能やデータが制限されると、生産性が低下し、そもそも出張の価値がなくなってしまいます。第二に、出張後にウイルス対策スキャンを実行してデバイスを再イメージングしても、ファームウェアやハードウェアレベルの脅威に対する可視性や保護は得られません。これらの脅威は数分でラップトップを危険にさらし、再イメージング後も目に見えない形で持続する可能性があります。

貸し出しノートPCのファームウェアのセキュリティギャップ

ファームウェアのインプラントやバックドアは、国家支援を受けた攻撃者が好んで使用するサイバー攻撃ツールの一つです。ファームウェアに悪意のあるコードを埋め込むことで、脅威はオペレーティングシステムよりも下位に位置し、ハードディスクの暗号化などの従来のセキュリティ管理を容易に覆すことができます。攻撃者は、感染したシステムをほぼ全能にコントロールし、可視化することができます。例えば、有名なUEFIルートキットであるLojaxは、マルウェアを使用してファームウェアモジュールを侵害し、OSを再インストールしてもシステムに再感染する可能性があります。DarkHotelのようなグループは、ホテルのWi-Fiネットワークを侵害し、偽造されたデジタル証明書を使用して、スピアフィッシングやマルウェアキャンペーンで企業幹部を攻撃しているため、旅行者用ラップトップのファームウェアがリモート攻撃に対して脆弱でないことを確認することが不可欠です。

また、このようなインプラントは、デバイスに物理的にアクセスできる攻撃者が被害者のマシンに簡単にインストールすることができます。実際には、わずか4分でインストールすることができます。これは重要な攻撃ベクトルです。というのも、フィッシング攻撃とは異なり、ユーザーが間違えてリンクをクリックしたり、添付ファイルを開いたりすることに依存していないからです。唯一の条件は、デバイスがユーザーの手元から離れることです。飛行機に乗っているとき、税関での質問を受けているとき、あるいはホテルの部屋にノートパソコンを置いたままにしているときなど、さまざまな場合が考えられます。このスタイルの攻撃は、ホテルのメイドが被害者の部屋に残されたデバイスを感染させることができることにちなんで、「邪悪なメイド」攻撃と呼ばれています。この脅威は、一度インストールされると、エンドユーザーやウイルス対策ソリューションからは見えなくなります。さらに悪いことに、旅行後にデバイスを完全に再構成し、OSを再インストールしても、脅威はマシンに残ります。

ファームウェアセキュリティへの新しいアプローチ

ファームウェアのセキュリティは、多くの組織にとって困難な課題です。ノートパソコンやその他のデバイスにおけるファームウェアレベルの侵害を検出するには、時間がかかり、専門的で希少なセキュリティスキルが必要です。

また、この作業を自動化するためのツールもありません。幸いなことに、新しいツールやイノベーションが状況を良い方向に変えつつあります。

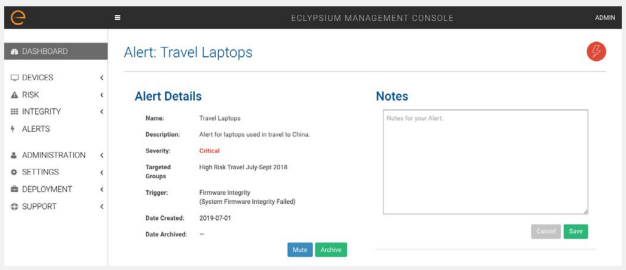
Eclypsiumでは、ラップトップ、サーバ、ネットワークデバイスの脆弱性や脅威を監視するプロセスを自動化する企業向けファームウェア保護プラットフォームを設計しました。旅行者のラップトップのセキュリティを担当するサイバーセキュリティチームにとって、Eclypsiumのプラットフォームは、デバイスの完全性を確保し、旅行中に改ざんされていないことを確認する効率的で信頼性の高い方法を提供します。

ファームウェアプロテクションの仕組み

Eclypsiumのファームウェア保護プラットフォームは、何が存在し、どのように構成されているかの詳細を収集するために、多くのサブコンポーネントを含む各システムをスキャンします。このデータを分析して、インプラントやバックドアなどのファームウェアレベルの脅威を、それらがどのように環境に侵入するかに関わらず発見します。Eclypsiumは、当社の業界研究と情報に基づいて、既知のインプラントが存在するかどうかシステムをチェックし、デバイスとそのファームウェアの動作を監視して、これまでになかった悪意のあるコードを特定します。この最後の要素は非常に重要です。国家支援を受けた攻撃者は常に新しい脅威を使用することができるからです。

ノートPCのファームウェアセキュリティベストプラクティス

ファームウェアのセキュリティに関するギャップを埋めるために、旅行者用ノートPCのセキュリティプログラムに以下のベストプラクティスを追加することをお勧めします。



- 出張前：ラップトップをスキャンし、古くて脆弱なファームウェアや、攻撃者が悪意ある攻撃を行いやすいようなデバイス保護機能が欠けていないか確認する。
- 出張中：整合性チェックの失敗や脅威の検出などの重要なイベントをサイバーセキュリティチームにリアルタイムで通知するアラートを設定し、対策を講じる。
- 出張後：ディスクを消去する前に返却されたノートPCをスキャンし、システムとそのコンポーネントの両方のファームウェアが変更されていないことを確認する。

さらに、リスクの高い国で働く従業員がいる企業には、ラップトップ、サーバ、ネットワーク機器を継続的に監視し、改ざんやインプラントがないかどうかをチェックするプログラムを推奨しています。
Eclypsiumがどのようにしてファームウェア保護のギャップを埋めることができるのか、詳しくはお問い合わせ(Email: jp-info@eclypsium.com)ください。