カメラ サイバー ロックダウン

テクニカル ホワイトペーパー

概要

Eagle Eye カメラ サイバー ロックダウンは、Eagle Eye Security Camera VMS の一部としてリリースされたサイバー セキュリティ機能です。カメラ サイバー ロックダウンは、カメラがインターネットと通信するのをブロックし、攻撃がカメラに及ばないようにします。また、カメラに埋め込まれた可能性のあるトロイの木馬がインターネットと通信することを許可しません。 この機能により、ビデオ監視システムのサイバー セキュリティが大幅に向上し、必要なサイバー セキュリティ メンテナンスの量が削減されます。

Eagle Eye カメラ サイバー ロックダウンの全体的な効果は、サイバー セキュリティ違反からの保護と、カメラによって生成されるサイバー セキュリティ問題の削減です。 カメラのファームウェア アップデートは通常サイバー セキュリティにとって重要ですが、カメラがロックダウンされているため、これらのメンテナンスの必要性が軽減されます。

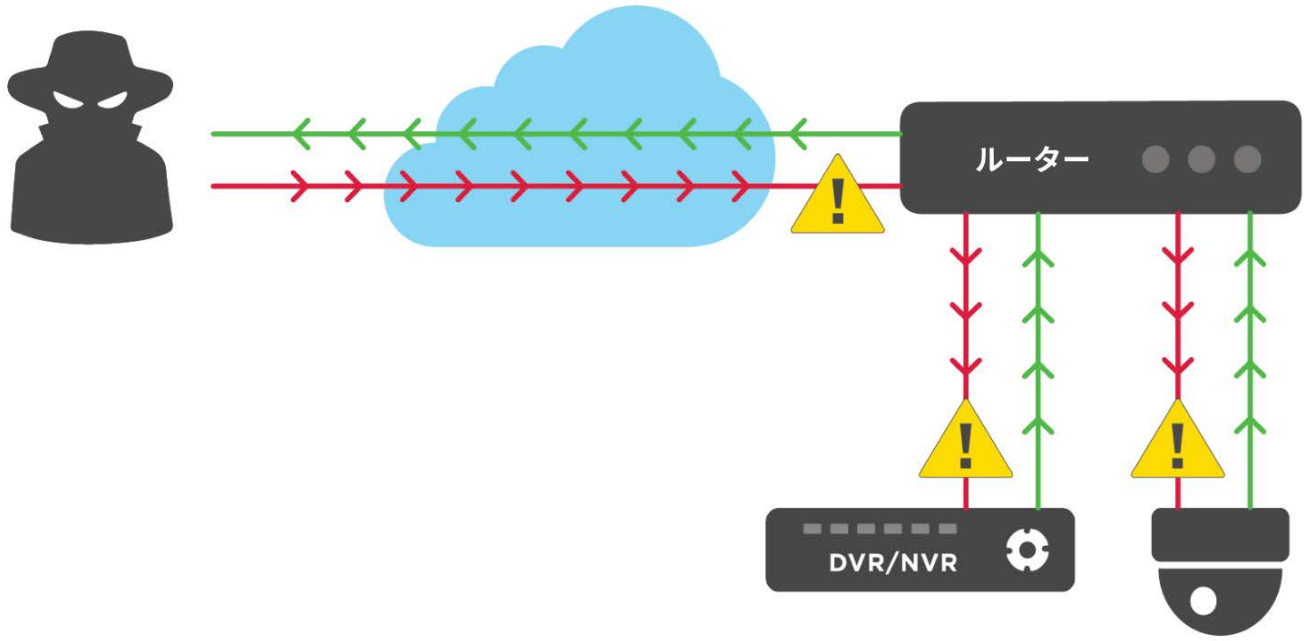
監視カメラには、以下のようなサイバー セキュリティに関するさまざまな問題があります：

1. カメラは世界各地にある多くの企業によって製造されています。 これらの企業の多くは、政治的、政府的な影響が未知です。
2. 多くのカメラは、1 つの会社によって製造され、異なる会社によって製品名が付けられ、販売されています。カメラがどこの誰が製造しているのかを知ることは多くの場合困難です。 カメラの本当の製造者を追跡することは困難なことがあります。
3. 多くのカメラサ プライヤーやメーカーは、サイバー セキュリティを怠っており、十分なテストを行ったり、カメラのサイバー セキュア性を向上する知識を持っていません。 カメラを選択するときにこれらの事を知ることは困難です。
4. 多くのカメラ サプライヤーは、サイバー セキュリティの欠陥に対応する適切なファームウェア アップグレードを随時提供しません。 ファームウェアのアップグレードをまったく提供しない企業もあります。
5. 大量の監視カメラのファームウェアをアップグレードする場合、非常に時間がかかることがあります。
6. 多くの監視カメラユーザーは、サイバー セキュリティの脆弱性が発見されたときにカメラファームウェアのアップグレードを実行するためのプロセスを用意していません。 ほとんどの場合、サイバー セキュリティの脆弱性を追跡し、それに対応するためのプロセスがありません。

Eagle Eye カメラ サイバー ロックダウンは、さまざまなベンダーが関連し、ファームウェアのアップグレードが不十分で、いくつかのメーカーではサイバー セキュリティへの関心が低いことを考えると、サイバー セキュリティの深刻な問題を解決するための効果的な方法となります。

問題点

従来の DVR は、サイバー攻撃からの保護をほとんど、またはまったく提供していません。 ファイアウォールに統合されているケースは非常に稀です。十分なサイバー セキュリティ テストを行っている人はほとんどいません。 適切にファームウェアのアップグレードが行われる事はほとんどありません。 パッチ OS の脆弱性はごくわずかしか発見されません。 セキュリティ上の脆弱性に対するファームウェアのアップグレードはほとんどありません。 問題の根源は、従来の DVR では、インターネットから直接（以下の図の赤線を参照）DVR にライブや録画ビデオを表示する必要があるということです。 これは、ビデオがモバイルデバイスまたはリモートビューアに転送される方法です。 DVR にこの接続がない場合、ビデオは敷地内でしか見ることができず、ローカル視聴のみを受け入れる意欲のある顧客はごく少数しかおりません。



DVR はインターネットから直接接続することができるため、簡単にサイバー犯罪者や他の攻撃者によって攻撃され、悪用される可能性があります。 ユーザーは、侵入されることを避けるために常に警戒が必要です。調査によると、インターネットに接続されている DVR は、通常 1 日に 100 回以上攻撃されることがあります。

カメラは DVR / NVR またはルータに接続されます。 カメラがルータまたはスイッチに直接接続されている場合、それらは直接攻撃される可能性があります。 DVR に接続されている場合、DVR によっては直接攻撃を受けるか、または DVR が侵入された場合に攻撃される可能性があります。

パート 2： トロイ / スパイウェア / ウイルスがプリインストールされているケース

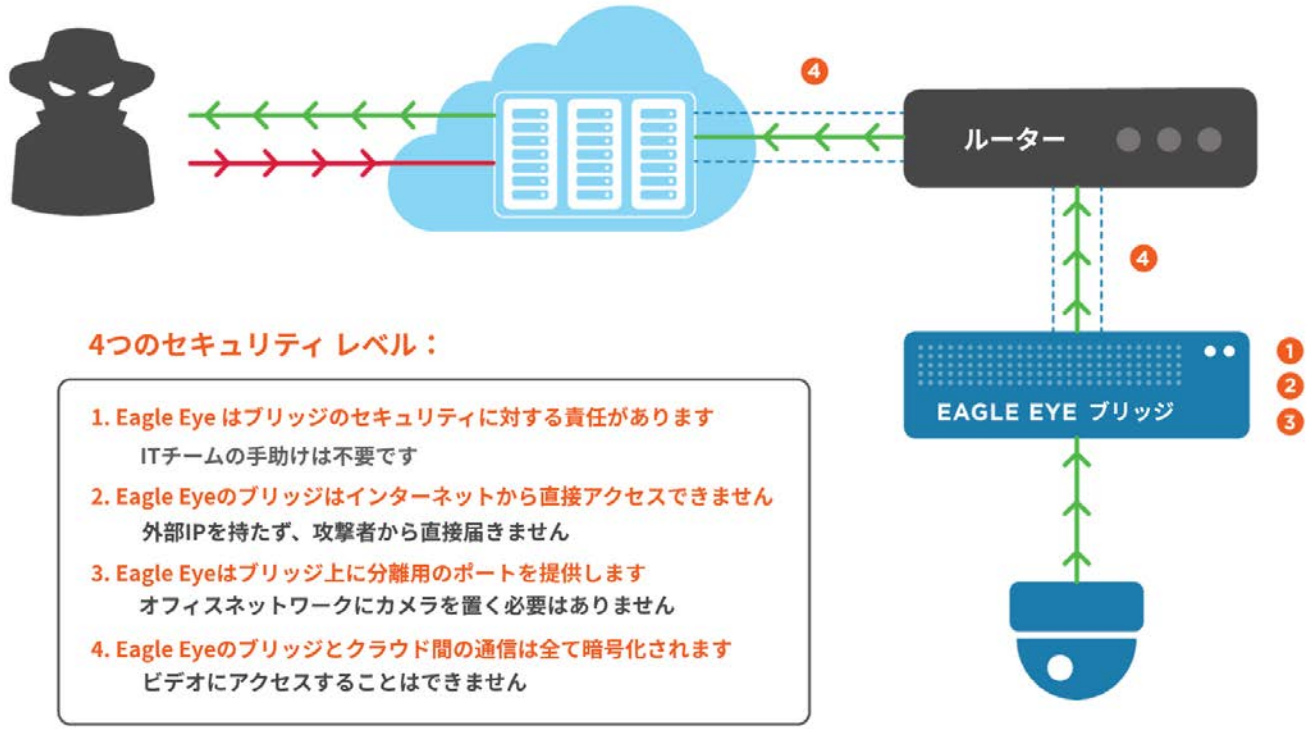
製造元によってカメラ、DVR、および NVR に対してスパイウェア、トロイの木馬、またはウイルスがプリインストールされている重要な懸念があります。これは、意図的または偶発的に既に侵入されたハードウェアをサプライヤーが販売した場合に起こります。これが発生した多く事例が文書化されています。

この場合、カメラは直ちにソフトウェアが実行される、または既に実行しており、追加のコードおよび命令の取得のためにインターネット上の「司令および制御サーバ」（CCS）に連絡しようとします。たとえば、侵入されたカメラは 2019 年 1 月 15 日に CCS に接続しようとするトロイの木馬に感染している可能性があります。その日、カメラはネットワーク接続を試みて指示を出します。ほとんどのネットワークでは、任意のデバイスからのアウトバウンド接続が可能です。 VLAN またはファイアウォールを利用する、より洗練されたネットワーク構成ではアウトバウンド接続をブロックしようとしますが、これは一般的ではありません。通常のオフィス ネットワークでは、暗号化された CCS への発信接続が許可されてしまいます。このカメラでは、ローカルネットワーク、ビデオ画像、およびパスワードのファイルを簡単にハッカーに転送することができます。カメラはネットワーク上の他のコンピュータをハッキングしたり、データベースを攻撃したり、クレジットカード情報を転送したり、サービス拒否（DDoS）攻撃に参加するための指示や追加プログラムを受け取ることができます。詳細については、下記の「なぜ彼らは攻撃するのか（Why They Are Attacking）」のセクションを参照してください。

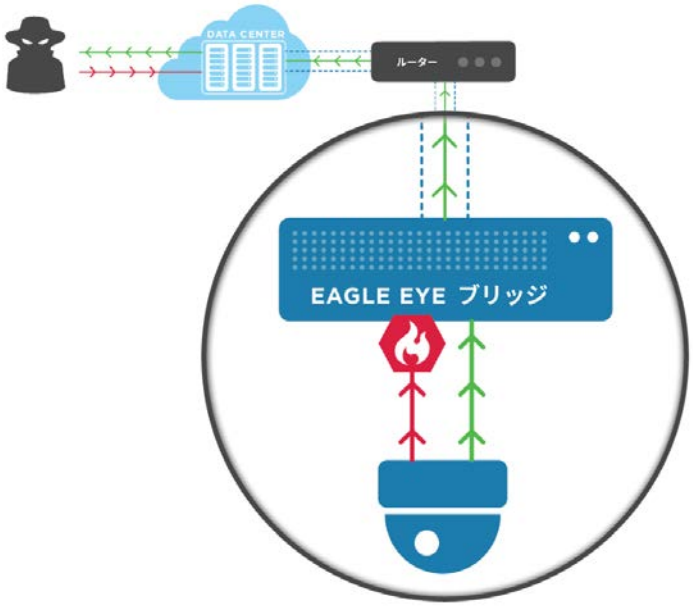
問題の大部分は、カメラ、NVR、または DVR が、サイバー セキュリティの責任を負うことのないメーカーによって提供されることです。 トロイの木馬やプリインストールされたウイルスの場合、デバイスが深刻な脅威となるためには単純にインターネットにアクセスする必要があります。

以下のような場合、カメラには脆弱性が含まれていることがあります：
- 悪意のある国の工場で生産された場合、トロイの木馬が含まれていることがあります
- メーカーのサイバー セキュリティに対する注意とテストが欠如している場合
- 意図的または偶発的に製造元でバックドアアカウントが含まれている可能性がある場合
- 使用中のカメラにおける製造元によるファームウェア アップグレードの提供終了
- すべてのカメラにファームウェアアップグレードを適用することが難しい場合
- 設定者による高い確率での構成ミス（通常はパスワード）

解決策： Eagle Eye カメラ サイバー ロックダウン



Eagle Eye Network は、あなたの Eagle Eye Security Camera VMS のサイバー セキュリティを確保するために、幾つかのステップを実施します：



1. Eagle Eye はネットワーク上に位置し、インターネットに接続する Eagle Eye ブリッジにパッチを当ててセキュア化する責任があります。 Eagle Eye は、あらゆるセキュリティ上の問題を迅速かつ効率的に修正します。
2. Eagle Eye ブリッジと CMVR はインターネットに直接公開されません。これらは直接アクセス可能な IP アドレスが無いため、攻撃者は直接攻撃を行なうことができません。そのため一般的な攻撃を行なうことができません。
3. Eagle Eye は、Eagle Eye ブリッジにカメラを接続するための物理的に別のポートを提供します。 これによりカメラは一般的なネットワーク上には存在せず、従業員やネットワークにアクセスできる他の人々によって到達できないことを意味します。 また、ハッカーによる外部からのカメラへの直接のアクセスも行えません。

4. Eagle Eye は AES 暗号化を使用して、ブリッジとクラウドの間で通信されるビデオデータを保護し、ハッキングの結果ビデオを取得できたとしても、決して利用可能にならないようにします。

カメラ サイバー ロックダウンと Eagle Eye 専用の CamLAN を使用することで、監視システムで使用される IP カメラよりセキュアで安全に使用することができます。

なぜ彼らは攻撃するのか（Why They Are Attacking）

ハッキングで楽しい時を過す子供たちは、もう過去のようです。盗んだ情報を販売し、侵入したシステムを使ってウェブサイトを人質に拘束するという形を取るのは、今や大きなビジネスとなっています。これらは、一般に公開しているウェブサイト、ゲームシステム、e コマースサイト、場合によっては政府システムのものであっても同じです。

ハッカーは以下のような理由で IP カメラのハッキングに興味があります：

1. クレジットカード番号、社会保障番号、その他の個人識別情報（PII）などの機密情報を取得するため
2. 顧客情報、財務諸表などの機密情報を取得するため
3. ボットネットと呼ばれる多数の侵害されたデバイス（グローバルに配信されることが多い）を利用して、分散型サービス拒否攻撃（DDoS）を介してウェブサイトやネットワークをダウンさせる

DDoS 攻撃は最も急速に流行している攻撃タイプとなり、過去数年間で件数も規模急速に拡大しています。DVR や NVR などのインターネットデバイスに接続された IP カメラは理想的なターゲットです。 これらの脆弱性は、悪用されやすい非常に危険なシステムになります。Mirai マルウェアは 2016 年 8 月から 10 月にかけて、セキュリティカメラを含むさまざまな IoT デバイスを利用した多数の DDoS 攻撃で使用されました。一旦システムが DDoS のコマとなり、ボットネットのメンバーになってしまうと、機密情報は攻撃者の手に届くことになります。

結論

監視カメラの市場は非常に競争力が激しく、様々な国の多くのサプライヤーが参加しています。 IP カメラの出所を知ることや、サイバー セキュリティに対して継続的に注力しているか、などを知ることは難しくなっています。低コストのカメラが好まれることが多いですが、それらを提供するベンダーはセキュリティ性能を切り落として、より低価格の製品を提供している可能性があります。

カメラをインターネット経由でアクセスできる場合は、カメラを武器にしたり、内部ネットワークへの入り口にしたり、ハッカーの天国にする方法はたくさんあります。

そう、自社のネットワークをしっかりと構成し、維持することは可能ですが、我々の経験では従来の方法で 20 台のカメラのネットワークを安全に保つためには、年間平均 25 時間かかります。 さらに、初期セットアップと構成には少なくとも 8 時間かかります。

Eagle Eye カメラ サイバー ロックダウンは、インターネットを介してカメラに接続する方法、またはカメラがインターネットに接続するためのほとんどすべての方法を排除し、サイバーセキュリティをはるかに上回る監視システムにすることが可能です
。