WatchGuard ThreatSync テクノロジーによる統合

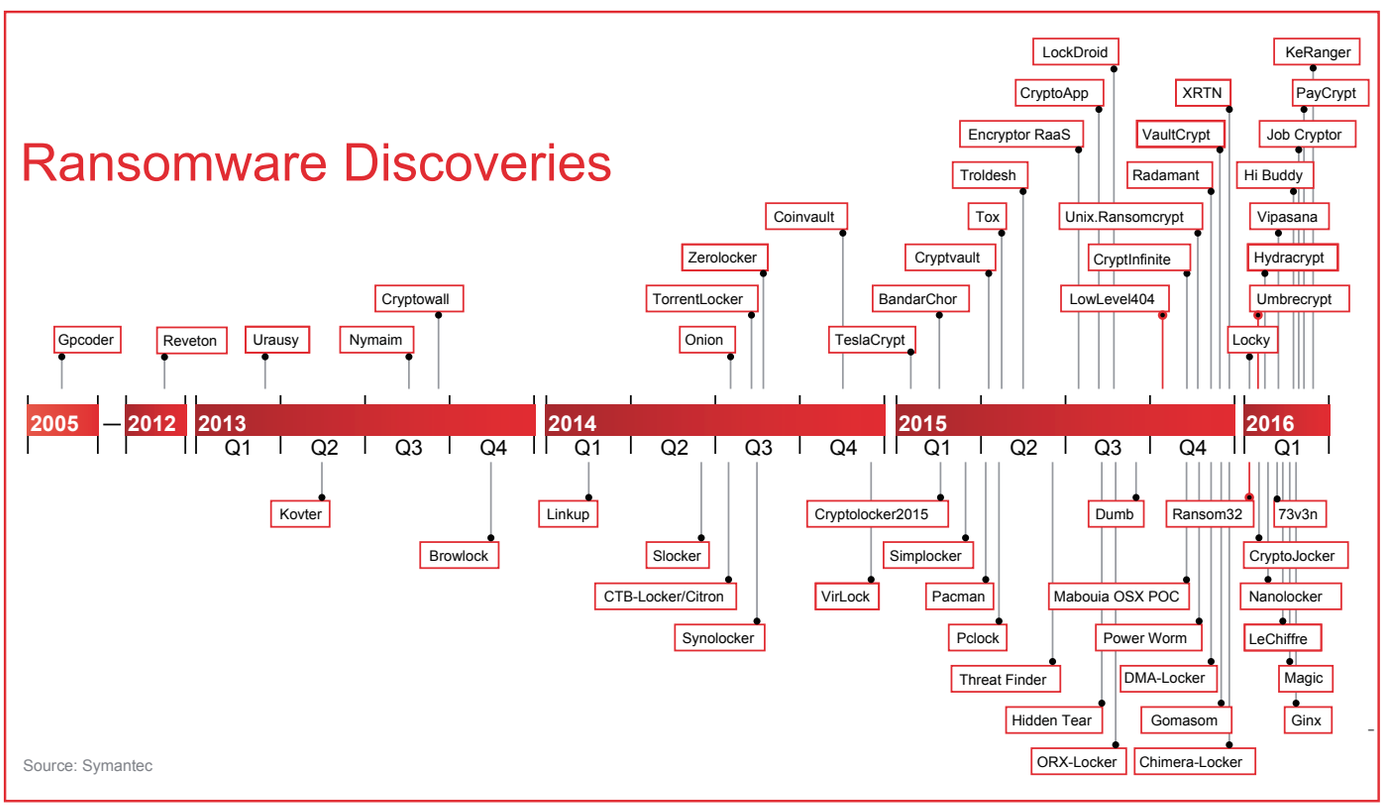
イントロダクション

ハッカーはますます高度化し、中堅中小企業に対し、高度なマルウェア攻撃を実行するようになっています。これらの脅威は、セキュリティ上の最も脆弱な侵入経路として、エンドポイントデバイスを攻撃することで組織に侵入し、その後社内ネットワークに活動範囲を広げます。

これらの脅威に対する防御には、エンドポイントとネットワークを連携させることで、よりスマートで強力なセキュリティの提供を可能にします。ThreatSync は、Threat Detection & Response（ＴＤＲ）の脅威スコアリングと脅威インテリジェンスを活用した相関分析プラットフォームであり、あらゆる規模の企業に対応するものです。

拡大する脅威

何年もの間、中堅中小企業は企業組織を悩ます標的型攻撃からは無縁のものと思われてきました。しかし、MaaS（Malware as a Service）等、サービスとしてマルウェアを生成するような非合法組織の急増により、マルウェアの取得が容易になり、またその展開がより広範囲になりました。



現在ハッカーは、大企業の場合と同様に、中堅中小企業への攻撃においても同じ投資回収率を得られるようになったのです。

さらに、ランサムウェアが容易に入手できるようになったことは、高度な攻撃に関する従来のストーリーをひっくり返しました。ハッカーは、重要情報の搾取に専念する必要がなくなり、ビジネス活動にとって重要なデータへのアクセスを遮断するだけで済むようになりました。そして身代金の金額を妥当なものにすることで、ほとんどの企業は身代金を躊躇なく支払ってしまいます。

ネットワークを把握する

ネットワーク内で起こっていることを明確に把握することは不可欠です。どのデバイスが接続されているか、通常どのくらいの帯域幅を消費しているか、そしてどのようなリスクが潜んでいるかを知ることで、セキュリティと生産性を向上させることができます。 Firebox®からのネットワークイベントの情報フィードは、単体でも貴重な情報をもたらしますが、エンドポイントと脅威インテリジェンスからフィードされるデータと組み合わせるとさらに強力になります。

ウォッチガードの革新的なThreatSync テクノロジは、Firebox で有効になっているWebBlocker、Reputation Enabled Defense（ＲＥＤ）、Gateway AntiVirus、パケットフィルタリング、APT Blocker などトータルセキュリティスイート（Total Security Suite）に含まれる複数のセキュリティサービスから収集されたデータを活用します。たとえば、Firebox でブロックされた脅威は、他のルートによってエンドポイントに感染している可能性があります。エンドポイントが感染している場合、ThreatSync は修復措置を実行して、その脅威を止めることができます。

エンドポイントでのアクティビティの表示

エンドユーザーは、最も狙われるターゲットであり、どの組織にとっても最も脆弱な攻撃ポイントとなる傾向があります。これらのデバイスがファイアウォール配下に置かれていると安心かもしれませんが、それを突破された場合、どうなるでしょうか。または、社外のリモートオフィスや支社の従業員はどうなるのでしょうか？既存のアンチウイルスのソリューション等は、既知の脅威がエンドポイントに侵入するのを防ぐのに優れていますが、アンチウイルス等で保護されていないデバイスは、組織のセキュリティに最大のリスクをもたらします。

あらゆる規模の企業が、どのデバイスがネットワークに接続しているかを知るだけでなく、そのデバイスで何が起きているのかを知ることは非常に重要です。 IT管理者は、TDRのコアコンポーネントであるWatchGuard Host Sensor を使用して、エンドユーザデバイス上の悪意のある挙動を継続的に監視および検知できるようになります。Fireboxと連携しながら、ThreatSync は、このデータを収集、分析することで、脅威の可視化を実現します。

脅威インテリジェンスを活用する

脅威フィードは、既知のマルウェアシグネチャのリストであり、世界中から収集され、定期的に更新されます。これらのリストは、新しい脅威があなたの環境に侵入し、重要データにアクセスすることを止める上で非常に重要です。これらのリストを構築して管理するビジネスを行う多くのベンダーがありますが、通常利用には高いコストがかかります。

ＴＤＲは、これらの脅威インテリジェンス機能を中堅中小の企業組織まで拡張して提供します。ThreatSync は、Firebox とHost Sensor から収集したイベントデータをさまざまな脅威フィードと比較して、脅威が他の場所にあるかどうかを迅速に判断します。脅威が検知された場合、Firebox やホストセンサと迅速に連携して感染を阻止します。

相関分析の効力

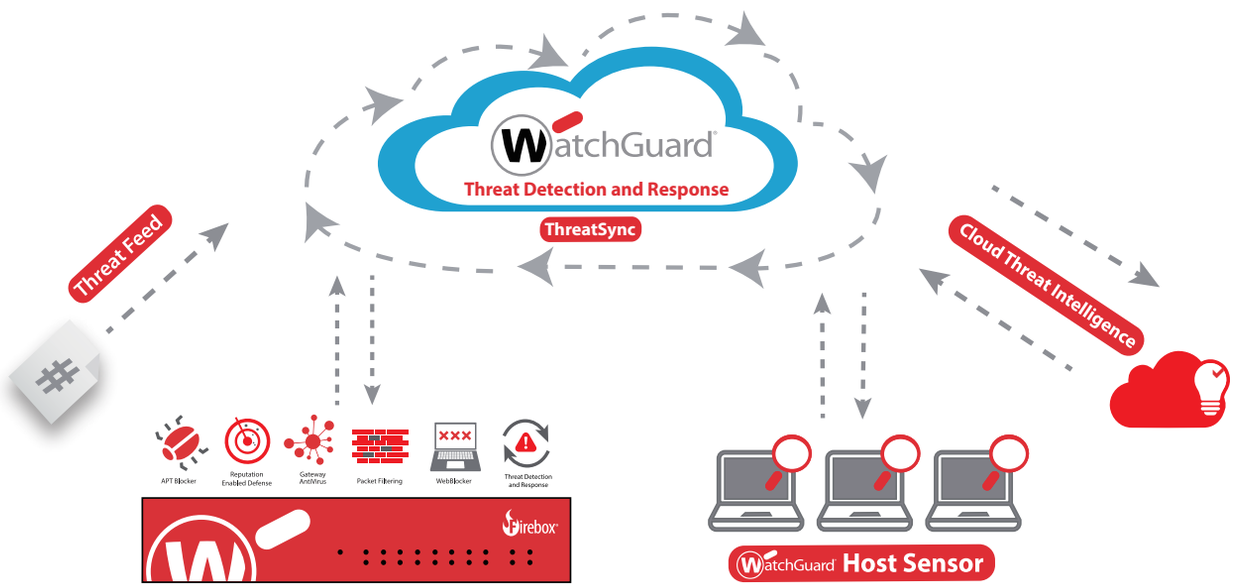
企業は長年にわたり脅威を阻止するためにセキュリティ製品を導入してきました。しかし、いくらセキュリティが優れているとしても、組織を攻撃しようとする次なる新しい脅威が常に存在します。阻止だけがセキュリティ対策上の唯一のツールにはなりえません。
ネットワークとエンドポイントそれぞれに更なる可視性をもたらす、新しいセキュリティ手法として「検知とレスポンス」の時代が到来しています。しかし、これらのシステムを別々に動作させることでは、組織に何が起きているのかを完全には伝えることができません。そこで相関分析が登場します。

相関分析は各動作の背後にある関連性を見つけるための頭脳の役割を果たします。つまり、前述した各セキュリティコンポーネントが生成した情報を利用し、点と点を結びつけ、全体を理解するものです。エンドポイントとネットワークの両方を包括的に把握することで、どれが最も深刻な脅威かをより正確に把握できます。どの脅威がエンドポイントに侵入しているかを把握することで、IT管理者は、脅威が拡散する前に、最も危険な脅威に迅速かつ確実に対処できます。

ThreatSync を使用した実践的な洞察

ThreatSync はウォッチガードのクラウドベースの相関分析および脅威スコアリングエンジンであり、ネットワークからエンドポイントまでの統合的なセキュリティとレスポンス対応を向上させます。ThreatSync は、WatchGuard Firebox, WatchGuard Host Sensor 、および脅威インテリジェンスフィードからイベントデータを収集し、このデータを関連付け、相関分析を行います。独自のアルゴリズムにより、ThreatSync は包括的な脅威スコアを割り当て、対応が必要なインシデントとして脅威をグルーピングします。

ThreatSync は、ネットワークとエンドポイントの両方で発生しているイベントを可視化するだけでなく、包括的な脅威スコアと優先順位付けを行うことで、情報システム部門がどの脅威が最も重大であり、直ちに対応が必要か認識できるようにします。脅威の優先順位付けにより、企業は検知と修復までの時間を短縮することができます。ThreatSync によって開始されるインシデントレスポンスの自動化には、感染ファイルの隔離、プロセスの終了、レジストリ値の修復が含まれます。



相関分析の活用：WatchGuard ThreatSync テクノロジによるランサムウェアからの防御

ランサムウェアは、あらゆる企業を苦しめる高度なマルウェアです。ここ数年、中堅中小企業や分散型企業にますます焦点が当てられてきています。このタイプのマルウェアは、悪意のある添付ファイルやURLを含むフィッシングメールで配信されることがよくあります。ランサムウェアは、デバイスにダウンロードされると、ファイルを暗号化してビジネスの生産性を停止させるために、C&Cサーバへの接続を試みます。身代金がビットコイン経由で支払われると、ハッカーはデバイスのロックを解除するために復号キーを提供します。

このタイプのマルウェアは実際にエンドポイントに感染し、ネットワークを活用して組織全体に攻撃を広げます。 セキュリティソリューションが個別に運用されている場合、エンドポイントで何が起きているかをそのネットワークが知る方法はなく、逆もまた同様であり、この危険な脅威に対して脆弱になる可能性があります。

ウォッチガードのThreatSync テクノロジは、疑わしいファイルがインストールを試みると、ホストセンサ上でイベントを検出します。マルウェアが悪意のあるサーバを呼び出そうとすると、Firebox でネットワークイベントを検出、別のインジケータが作成され、インシデントスコア全体が増加します。 ネットワークとエンドポイントの両方で発生しているイベントは、最も重大な脅威スコア10を自動的に表記します。

設定を有効にすると、ポリシーは自動的にFirebox に指示し、マルウェアが悪意のあるサーバを呼び出すのをブロックし、ファイルを隔離したり、プロセスを強制終了したり、エンドポイントにおけるレジストリ値を修復したりします。 また、マシンガイド方式によりワンクリックで手動による修復を実行することもできます。

WatchGuard Threat Detection and Response（ＴＤＲ）

Threat Detection & Response（ＴＤＲ） は、ネットワークとエンドポイントのセキュリティイベントを脅威インテリジェンスにて相関分析し、マルウェア攻撃を阻止するため検知、優先順位付け、迅速なアクションを可能にするものです。
このセキュリティサービスには、次の4つのコンポーネントが含まれます。

- ThreatSync - クラウドベースの相関分析および脅威スコアリングエンジン
- エンタープライズグレードの脅威インテリジェンス機能
- 軽量なHost Sensor
- Host Ransomware Prevention（ＨＲＰ）モジュール

さらに良いことにはTDRはウォッチガードのTotal Security Suite に含まれており、このライセンスとFireboxアプライアンスを購入することにより、企業はネットワークとエンドポイントに包括的なセキュリティサービスを手にすることができます。

Host Ransomware Prevension(HRP)に関する詳しい情報は,
www.watchguard.co.jp/TDR

ウォッチガードについて

WatchGuard® Technologies, Inc. は、ネットワークセキュリティ、セキュア Wi-Fi、ネットワークインテリジェンス製品、セキュリティサービスの世界的なリーダーであり、世界各国の75,000社以上のお客様にサービスを提供しています。ウォッチガードのミッションは中堅中小企業や多拠点をもつ分散型企業向けの理想的なセキュリティソリューションを提供し、すべての企業がエンタープライズグレードのセキュリティを容易に利用できるようにすることです。ウォッチガードの本社は、米国ワシントン州のシアトルにあり、北米、欧州、日本、アジア太平洋地域、および南米にオフィスを展開しています。
詳しくはWatchGuard.co.jp をご覧ください。

ウォッチガード・テクノロジージャパン株式会社　〒106-0041 東京都港区麻布台1-11-9 BPRプレイス神谷町5階　Tel:03.5797.7205　Fax:03.5797.7207
Mail: JPNSALES@watchguard.com