ランサムウェア対策　Host Ransomware Prevention (HRP)

はじめに

企業規模に関わらず、多くの企業が高度なマルウェアや標的型攻撃などのセキュリティの脅威により、ビジネスの生産性と継続性に深刻な被害を受けています。特に企業内の重要なデータやシステムに大きな被害を及ぼすランサムウェアは、中堅中小企業が主なターゲットになりつつあり、重大なセキュリティの脅威として認識されています。しかしながら、コストや複雑さに関わらず、多くの企業がランサムウェアによる攻撃を効果的に回避するためのリソースが不足しており、被害はますます急増する結果につながっています。WatchGuard Thread Detection & Responce (TDR) で提供される Host Sensor のコンポーネントの一つである Host Ransomware Prevention (HRP) は、被害が発生する前に、あらゆる規模の組織でランサムウェアによる攻撃を検出し、被害を未然に防止することが可能です。

ランサムウェアとは？

ランサムウェアは、高度なマルウェアの一種で感染するとＰＣ上のデータを暗号化し、ユーザは重要な情報やＰＣへのアクセスがロックアウトされます。このタイプのマルウェアは、PC やデバイスへの様々な感染経路を持っています。悪意ある Web サイトや感染された Web サイトからのバックグラウンドでのダウンロードや、フィッシングメールによる感染、攻撃キットによるシステムの脆弱性への攻撃などからも感染します。システムがランサムウェアに感染すると、コンピュータはロックされるか、データが暗号化され、業務を継続することが出来なくなります。そして、攻撃者は情報を取り戻すための身代金の要求と支払い方法、支払い期限などを指示してきます。

フィッシングメールによる感染

ランサムウェアの侵入手法で最も一般的な方法は、フィッシングメールです。攻撃者は標的となるユーザに対して、疑う余地のない送信者を偽装して巧妙にユーザーにランサムウェアを送りこみます。それらのフィッシングメールには、ハッカーの侵入につながる悪意のあるサイトへのリンクや有害なコードが含まれています。そして、標的となったユーザのデバイスだけでなく、組織全体へ感染させるためのバックドアを作成します。現在、中堅中小企業はこの攻撃手法による攻撃が急増しています。2015 年には、250 人未満の従業員の企業を標的としたスピアフィッシング攻撃の 40%以上がこの攻撃となっていました。　（Verizon）

ランサムウェアによるビジネス

サイバー犯罪者の平均的な技術レベルはあまり高くありません。しかし、ダーク Web の世界においては、マルウェアツールやサービスなどが入手できる状況となっているため、技術スキルの低い攻撃者であっても、高度なマルウェアによる攻撃が行える状況になっています。実際に、ダーク Web では、洗練されたマルウェアの変種や、特定の標的に対して設計されたマルウェアなどを入手可能なサイトも実在しています。ランサムウェアビジネスの成功により、技術スキルを持たない犯罪者が、マルウェアだけでなく、感染させるためのサービスを購入可能な「Ransomware as a service」も出現しています。従来、技術レベルの高い複数のハッカーからなる組織と高度な操作スキルが必要だったサイバー攻撃が、より頻発する状況になっています。

ランサムウェアへの対策

すべての企業、特に中堅中小企業へのランサムウェアによる攻撃は大きな脅威となっており、深刻な状況です。しかし、これらのトリッキーな攻撃手法は、逆にマルウェア検出に使用される行動分析の情報として利用が可能です。マルウェアの振る舞いや行動を分析して、マルウェアの検出に利用して攻撃を阻止出来れば、攻撃を未然に効果的に防御することが可能となります。

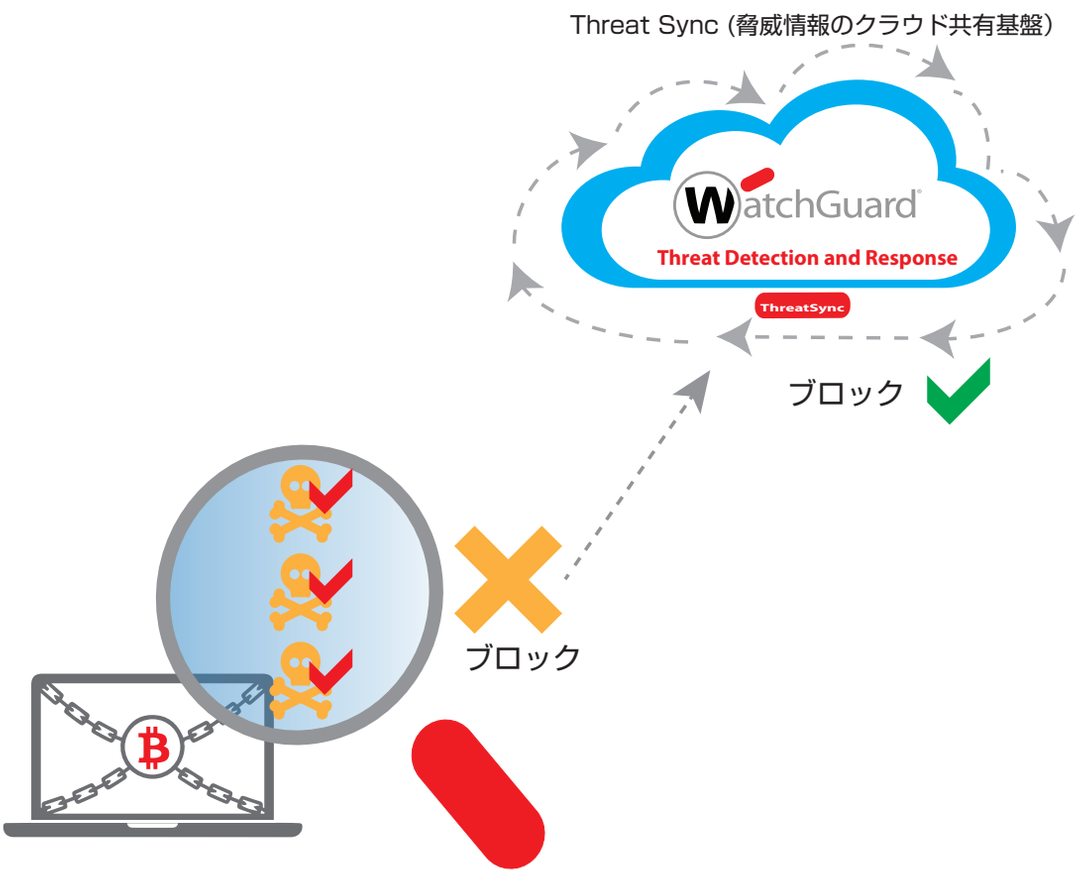
WatchGuard の最新セキュリティ・サービスである **Threat Detection and Response** には、軽量の Host Sensor 内にランサムウェア対策機能が組み込まれています。Host Ransomware Prevention(HRP) は、ランサムウェアの行動分析エンジンとデコイディレクトリハニーポットを活用して、ランサムウェアの行動との関連付けを判断する広範囲な特性を常時、監視します。行動が悪意のあるマルウェアと判断されれば、HRP はエンドポイントでのファイル暗号化が行われる前にランサムウェアを防止します。

相関分析によるトータルセキュリティ対策

WatchGuard Total Security Suite により、あらゆる規模の企業が、ランサムウェアを含む高度なマルウェアの脅威からの防御が可能になります。Total Security Suite は、ランサムウェア対策だけでなく、すべての脅威からの防御を実現し、効果的なインシデントレスポンスが可能となるセキュリティサービスです。

Firebox に実装されている多層防御によるセキュリティ機能は、ランサムウェアによる攻撃の各ステップでも有効となり、感染のリスクを削減することが可能です。WebBlocker は既知の悪意のあるサイトへのユーザーのアクセスをブロックし、危険なサイトや不適切なサイトをブロックする URL フィルタリングも可能にします。APT Blocker は、疑わしい未知の脅威をクラウド上のサンドボックスで検査し、標的型攻撃を正確に検知してブロックすることがで可能です。そして、Host Ransomware Prevention は、エンドポイントでの振る舞い検知とクラウド上の ThreatSync（脅威インテリジェンス）により、暗号化が行われる前にマルウェアを防止します。

ウォッチガードの Total Security Suite は、高度なセキュリティサービスを組み合わせ、包括的なセキュリティサービスを提供する最も有効なランサムウェア対策を実現します。



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