KASPERSKY

ランサムウェアに対抗する カスペルスキーの多層防御

～ワークステーションとサーバーの実践的な対策とは～

www.kaspersky.co.jp

ランサムウェアは悪意のあるソフトウェア（マルウェア）の中でも特に進化が早く、その被害が拡大していますが、その一番の要因は攻撃の手軽さにあると言えるでしょう。ランサムウェアを使った攻撃では、サイバー犯罪者は苦労して企業ネットワークに侵入し、重要なデータを盗み出した上で販売したり、効果の疑わしい未知の脆弱性を購入したりする必要がありません。感染した被害者から身代金の入金をただ待ってさえすればよいのです。最近ではアフィリエイトプログラムも準備されているので、直接被害者からの身代金を受けとる必要すらありません。プログラムの進化も見逃せません。もともとは画面をロックして支払いを要求するだけの単純なものだったランサムウェアは、今日では非常に高度で危険なソフトウェアへと進化し、データを人質に取る手口も巧妙化しています。個人はもちろん企業や政府機関、警察や病院ですら例外なくターゲットを拡大しているランサムウェアによる攻撃を回避するには、万全で真に有効な対策を施す必要があります。

ランサムウェアの脅威と特性

ランサムウェアとは、暗号化技術を悪用したマルウェアの一種で、トロイの木馬に分類されます。感染にはメールの添付ファイルか改竄サイトへの誘導が用いられます。いずれかの手段でランサムウェアに感染させられるとエンドポイント上のデータが暗号化もしくはロックされてしまいます。暗号化の対象となるデータには、写真やドキュメント、データベースなどが含まれ、「人質」となったデータの復号（元に戻す）と引き替えに「身代金」が要求されます。

犯罪者は身代金の受け取りからアシが付かないよう、支払いにはビットコインを代表する仮想通貨が用いられ、ランサムウェアと C&C（指揮統制）サーバーとの通信には、Tor と呼ばれる匿名性の高いネットワークが使われます。たとえこの通信を傍受することができても、Tor や従来の暗号化アルゴリズムを用いた非正統的な暗号スキームを使用することにより、ファイルの復号は事実上不可能です（たとえば、Trojan-Ransom.Win32.Onion は、これらすべての手法を使用しています）。

また、ランサムウェアの一種である Crypto-lockers の中には、復号に対してだけでなく、「Web 閲覧の履歴を全関係者に送りつけるぞ」といった脅しによって、支払いを要求するものもあります。

ランサムウェアの広がり

	Kaspersky Security Network により検知されたランサムウェア
2014 年	121,238
2015 年	448,430
合計	554,267

2015 年の一年間で Kaspersky Security Network (KSN) が観測したランサムウェアによる攻撃は、前年のほぼ 4 倍に急増し、およそ 45 万件を数えました。この中には、CryptoWall を始め TeslaCrypt や TorrentLocker、Locky、悪名高い CTB-Locker、ACCDFISA および GpCode など多数の異なる種類のランサムウェアが含まれます。次の表は、2015 年の欧州での KSN の統計データですが、この数値からもその範囲の広さと数の豊富さがうかがい知れます。

2015

カスペルスキーでの検知名	ユニークユーザー数（KSN）	ユニークユーザー数合計（KSN）	マルウェアの別名
Trojan-Downloader.JS.Cryptoload + Trojan-Ransom.Win32.Bitman	80,017 1,163	81,180	TeslaCrypt
Trojan-Ransom.NSIS.Onion + Trojan-Ransom.Win32.Onion	16,491 8,571	25,062	CTB-Locker
Trojan-Ransom.Win32.Cryptodef	7,346	7,346	CryptoDefense（初期バージョン）、CryptoWall（後期バージョン）
Trojan-Ransom.Win32.Snocry	4,998	4,998	
Trojan-Ransom.Win32.Cryakl	4,955	4,955	
Trojan-Ransom.Win32.Crypren	1,681	1,681	
Trojan-Ransom.Win32.Shade	1,390	1,390	
Trojan-Ransom.Win32.Crypmod	1,173	1,173	
Trojan-Ransom.Win32.Rack	717	717	TorrentLocker
Trojan-Ransom.Win32.CryFile	395	395	

中でも Locky は、今年 2016 年 2 月に発覚したロサンゼルスの病院（Hollywood Presbyterian Memorial Hospital）に対するランサムウェア攻撃に使用されたと考えられており、もっとも活発なランサムウェアツールの 1 つです。

日本でも vvv ウイルスの名前で騒がれた TeslaCrypt は、2015 年 2 月に最初の検体が確認されましたが、その後も続々とその亜種が登場しています。このトロイの木馬は主にゲーム関連のファイル（セーブデータやユーザー情報など）をターゲットとしているため、海外メディアでは広くコンピュータゲームの「呪い」とも呼ばれています。

ランサムウェアへの対策

こうしたランサムウェアの脅威に対抗するため、カスペルスキーでは現存するランサムウェアのみならず、今後発生しうる新たな攻撃にも真に対抗しうる様々なテクノロジーを製品に実装しています。

今日のランサムウェアに暗号化されてしまったデータの復号は、現在のテクノロジーでは開発者のミスといった一部の例外を除けば事実上不可能であるため、事前の対策が要となります。感染してしまった場合の最も有効な対策は、データのバックアップです。しかし、専用ソフト等による一般的なバックアップでは、バックアップ後に変更されたデータを保護できないだけでなく、せっかくのバックアップデータを暗号化されたデータで、上書きしてしまう危険もあるため万全なソリューションとは言えません。

ワークステーションのセキュリティ

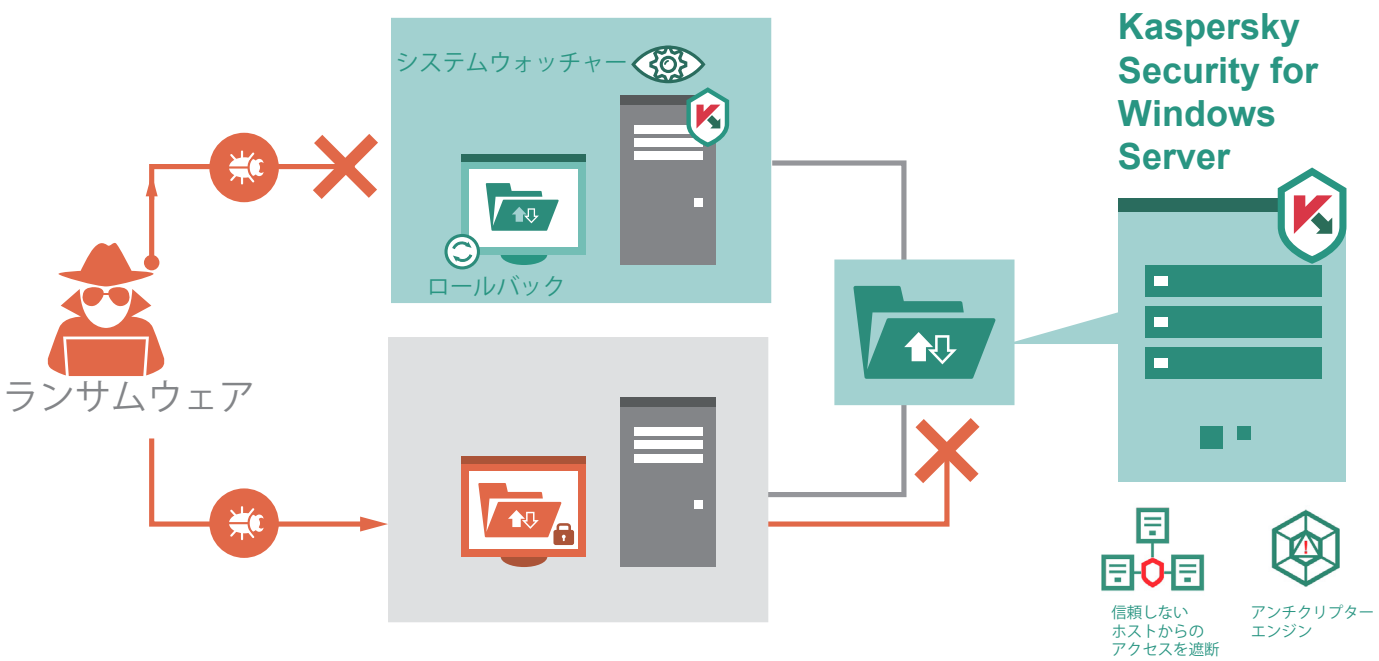
Kaspersky の製品では この弱点を補うため、エンドポイント向けの製品に「システムウォッチャー」を搭載しています。カスペルスキーのシステムウォッチャーはファイルの変更を監視し、ファイルに対する疑わしいアプリケーションの挙動を検知したタイミングで、保護されたファイルのバックアップコピーを作成します。さらにそのアプリケーションがランサムウェア（または他の悪意のあるマルウェア）だと判定された場合、システムウォッチャーはマルウェアを削除し、改ざんされたファイルを自動的にバックアップコピーからロールバック（改竄前の状態に復元）します。この一連の処理の間、ユーザーに表示されるのは通知のみで、作業が中断されることもなく、特別なアクションも不要です。

システムウォッチャーは、ユーザーのデータを安全に保つと同時に、次の攻撃に利用される身代金という名の攻撃資金や開発費を削減することにも役立ちます。システムウォッチャーに加え、アプリケーションの起動と権限を制限する「アプリケーションコントロール」のルールを設定することで、ランサムウェアのリスクをさらに軽減することができます。カスペルスキーはリアルタイムに更新される、10 億を超えるファイルが登録されたホワイトリストを提供しており、ホワイトリストに登録されていないアプリケーションをブロックする「デフォルト拒否」ポリシーの実行により未知の脅威がもたらすリスクを大幅に低下させます。

サーバーのランサムウェア対策

企業ネットワーク内のワークステーションの中には、システムウォッチャーなどワークステーションを保護するランサムウェア対策が導入されていない場合もあります。そうした脆弱なホストがネットワーク上の共有 SMB/CIFS フォルダを使用する場合、電子メールや Web アクセスを経由して侵入してくるランサムウェアが、サーバー上の共有フォルダにも影響を及ぼします。そのため、企業ネットワーク全体を保護するには、ワークステーションだけでなくサーバー側のセキュリティソフトウェアによってデータを守ることが必要です。

カスペルスキーが提供する Kaspersky Security for Windows Server には、ランサムウェアを含む不正な暗号化の脅威に有効な「アンチクリプター」と呼ばれる最新のテクノロジーが実装されています。この新しい技術では、ファイル共有を含む特定のデータフォルダを監視対象に置き、アクセス前後のファイルの差異による脅威の検出を可能にします。ランサムウェアは暗号化の際にファイル内容を劇的に変化させるため、アンチクリプターによってほぼ全てのランサムウェアならびにその悪意ある挙動を押さえ込むことができます。



さらに、SMB/CIFS プロトコルから IP アドレスを特定する「Host Blocker」テクノロジーが感染ホストの感染拡大を防ぎます。

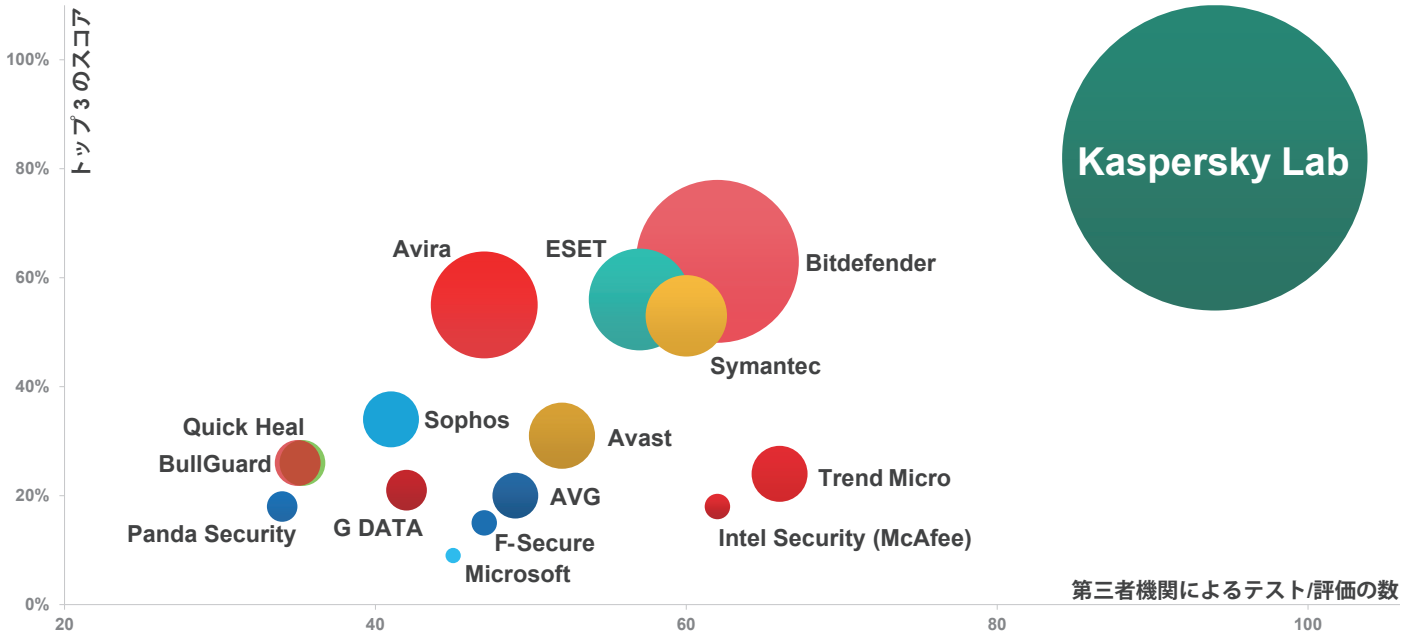
業務上、サーバー上の共有フォルダを意図的に暗号化する必要がある場合には、指定のディレクトリを例外設定することも可能です。

攻撃者の意図を先読む多層防御でランサムウェアと戦う カスペルスキーのセキュリティ

世界屈指の脅威リサーチャーとそこで蓄積される脅威インテリジェンスに基づいたカスペルスキーの先進的テクノロジーは明日の脅威を先読みし、システムウォッチャーやアンチクリプターを始めとする幾重もの多層テクノロジーによってランサムウェアのみならず、あらゆるサイバー攻撃の脅威から情報資産を守ります。

カスペルスキーは、今日まで業界のセキュリティテクノロジーを牽引し、様々な第三者機関ならびに専門誌によるテストにおいて評価され続けています。

2015年、カスペルスキー製品は 94 の第三者機関によるテストと評価に参加しました。その結果、1 位を 60 回獲得し、トップ 3 には 77 回入りました。



株式会社カスペルスキー
PMM-1010-201606