アンラボ・セキュリティレター

Press Ahn

2016.2　Vol.26

理想 vs. 現実におけるランサムウェア対応方法

残酷な悪の化身、ランサムウェア詳細分析 その２

理想 vs. 現実におけるランサムウェア対応方法

最近、新・変種ランサムウェアが持続的に発見され、企業だけでなく個人ユーザーにも被害が急増している。ランサムウェアはマルウェア作成者にとって金稼ぎの手段として認識され、広範囲なターゲットに向けた無差別攻撃が行われている状況だ。今回のプレスアンでは、韓国で恐怖の対象になっているランサムウェアの現況について1部と 2部に分けて詳細に分析し、第一部のランサムウェアの概要に続いて今回は第二部をお届けする。

ランサムウェアの進化

最近話題になっているランサムウェア関連事件を見ると、映画で登場しそうな「データを人質にとる」手法が現実のものになったことが分かる。Teslacrypt、CryptoWall、Teeracなど、感染手法や詳細動作によって多様な名前で呼ばれるランサムウェアの特徴を見ると、PCユーザーにとって大事な文書、画像などのデータファイルを無断で暗号化して身代金を要求する明白な犯罪化傾向が顕著だった。

[図1] ランサムウェアの攻撃プロセス

ランサムウェアは直近 1~2年の間に金銭的な被害をもたらすことから一般ユーザーにも知られ始めたが、実はファイル暗号化機能を持つ「トロイの木馬」タイプのマルウェアとしてかつてから存在していた。また感染させてお金を要求することで、ハッキングの目的を露わにする面では「にせ物ワクチン」や「画面ロックマルウェア」のような scarewareタイプの進化版ともいえる。Scarewareは、見た目は正常なセキュリティプログラムだが、実際はセキュリティ機能がなくただ金銭のみ目的にするソフトウェアを言う。最近蔓延しているランサムウェアは、身代金の要求に応じなければ暗号化ファイルを復元できないことから、被害者にとって致命的なダメージを与える悪質なマルウェアだ。

	成り済ましセキュリティプログラム	画面ロックマルウェア	ファイル暗号化ランサムウェア
マルウェア感染有無	○	○	○
金銭要求有無	○	○	○
金銭要求に応じない時の被害範囲	継続的なポップアップウィンドウなど PC 利用を妨害	システム画面のロック― または起動を妨害	文書、画像など暗号化
金銭要求に応じない時の事後処置	可能 **(簡単)** ・該当するプログラム削除 ・AVエンジン最新アップデート後に駆除	機能 **(複雑だが可能)** ・安全モード起動 → システム復元 ・起動可能 USBで専用ワクチン駆除	**不可** ・暗号化キーの復元不可 ・知られた復元キーは制限的

[表1] 悪質なマルウェア比較

違うようで似たもの同士「ランサムウェア」と「知能型マルウェア」

最新のエンドポイント・セキュリティソリューションは、ビヘイビア検知またはエクスプロイト遮断といった積極的な診断技術を搭載し、一度の攻撃で致命的なダメージを与えるランサムウェア感染に対応している。しかしランサムウェア作成者もまた、防御壁を回避するための進化を続けていて多様な新・変種ランサムウェアが絶えずユーザー PCのデータを暗号化するためにいたちごっこを続けている。

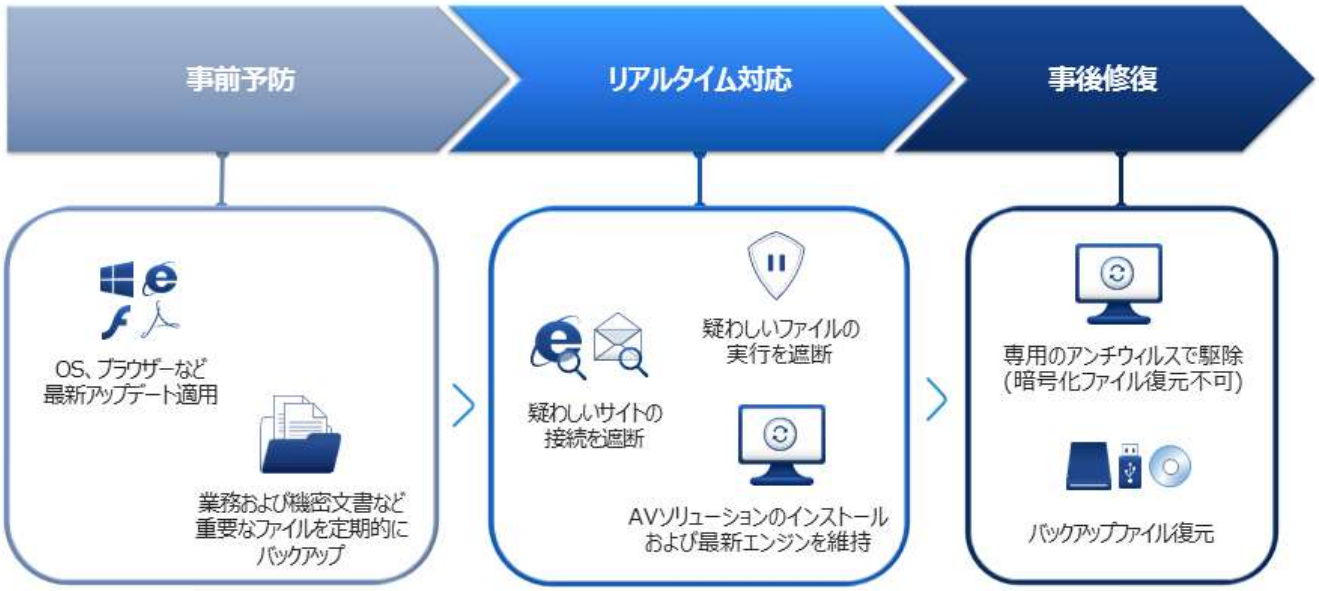
防御技術の強化にもかかわらず、エンドポイントセキュリティソリューションがランサムウェアに対して効果的に対応できない理由は、ランサムウェアも知能型攻撃で使われる多様なセキュリティソリューション回避手法を使っているからだ。

ランサムウェアは不特定多数に向けて広く配布することで被害を拡大させている。また感染後になるべくなりを潜めて長期間潜入する知能型マルウェアと異なり、ランサムウェアはファイル暗号化などの目的を達成した後、自ら前面に出て制限時間内に早く決済するように誘導する。もちろん感染や決済の過程で、攻撃者の情報が漏れないように HTTPS暗号化トラフィック及び Torなどのネットワーク技術と、電子マネー使用する徹底振りを見せている。

[図2] 知能型マルウェア vs. ランサムウェア

パッチとバックアップが最善の対処法か？

読者の中にはセキュリティ担当者も多いはずだ。最近ランサムウェアの攻撃は、セキュリティプログラムを回避するために多様な新・変種マルウェアを活用する知能型脅威になっているため、ランサムウェアを根本的に事前予防することは不可能であり、事後の被害最小化に集中した受動的な対策を取らざるを得ないと多くの方が嘆いている。一部ベンダーは、セキュリティソリューションを使ってランサムウェアを根本的に遮断できると大風呂敷をしくこともあるが、実際にすべてのベンダーが口を揃えて強調するセキュリティ鉄則は「重要な資料のバックアップ」と「セキュリティパッチ」に限る。



[図3] 一般的なランサムウェア対応プロセス

バックアップとパッチを効果的に使いこなせばリアルタイム対応が不十分だとしても、事前予防の段階でランサムウェアの感染を最小化することができる。たとえ感染したとしても、事後の復元段階でバックアップ情報を活用して正常な作業を維持できるからだ。

しかし暗号化されたファイルを復元したとして、セキュリティ担当者としてすべての状況が終わったと言えるだろうか。ランサムウェア動作過程で、ハッカーは単にファイルを暗号化してから決済を悠々と待っているわけではない。一度ランサムウェアに感染すれば、その PCはハッカーにとって潜在的な人質 (ransom)として管理されることもある。

理想的な vs. 現実的なランサムウェアのリアルタイム対応

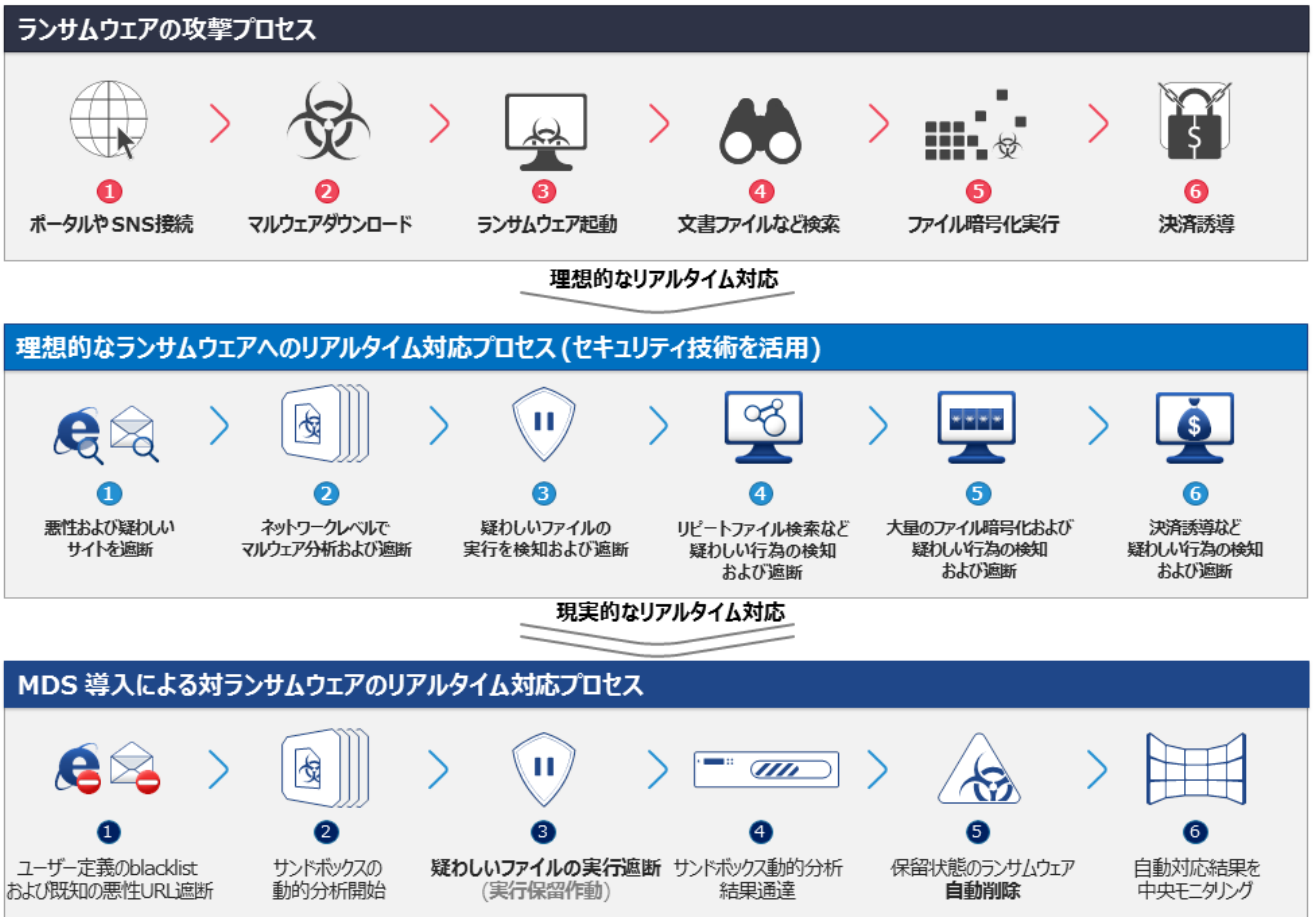
バックアップ、パッチ、アップデート及びコンピューター上の使用注意のような、ランサムウェア関連セキュリティガイドラインの順守を呼びかけるほか、セキュリティ担当者として取れる技術的な処置は何があるのか。ランサムウェア感染そのものを最小化するリアルタイムな対応は何があるか現実的な方策について考えてみよう。

まずランサムウェアにリアルタイムで対応する「理想的な技術的対応」について。最初のランサムウェアは電子メールの添付ファイルまたは本文の URLリンクを通じて侵入したり、そのほか多様なルートから特定の URLを直接クリックするように誘導する場合が多い。この段階では、**疑わしい添付ファイルや URLを遮断**する技術的な処置が必要だ。

もしこの段階で適切なやり方でマルウェアを遮断できなかった場合、マルウェア専用**サンドボックスなどを利用してネットワークレベルで可能な限り速かに悪性有無を判断し、遮断**する処置が必要となる。以後の段階では、マルウェアによってエンドポイントシステムが感染し、悪意ある動作が発動される。理想的なセキュリティソリューションならば、詳細ファイル検索、大量のファイル暗号化動作を悪性と診断して**リアルタイムで遮断まで自動で実行**しなければならない。

だが、まだそこまで理想的なソリューションはまだ存在しない。疑わしい URLやファイルをリアルタイムに分析・ネットワークレベルで遮断するソリューションは存在しないうえ、エンドポイントレベルで正常ファイルの検索及び暗号化などのランサムウェアの動作を明確に判断して、その過程で暗号化できないようにリアルタイムで遮断する対応技術が搭載されたセキュリティソリューションはいまだに存在しない。勿論理論的には可能だが、セキュリティ人材が対応可能な件数の検知エラーイベントが発生する「実務 IT環境に実質的に適用可能な製品」はまだ把握されていない。

完璧ではないにしろ、疑わしい URLをリアルタイムで遮断し、ランサムウェアマルウェアが疑われるファイルを「実行しない状態」で仮想環境上で詳細分析した後、結果に基づいて実行有無を決められるとしたら、さらにこの一連のプロセスを最大限自動化できるならセキュリティ担当者としては充分考慮に値する現実的な処置ではないだろうか。

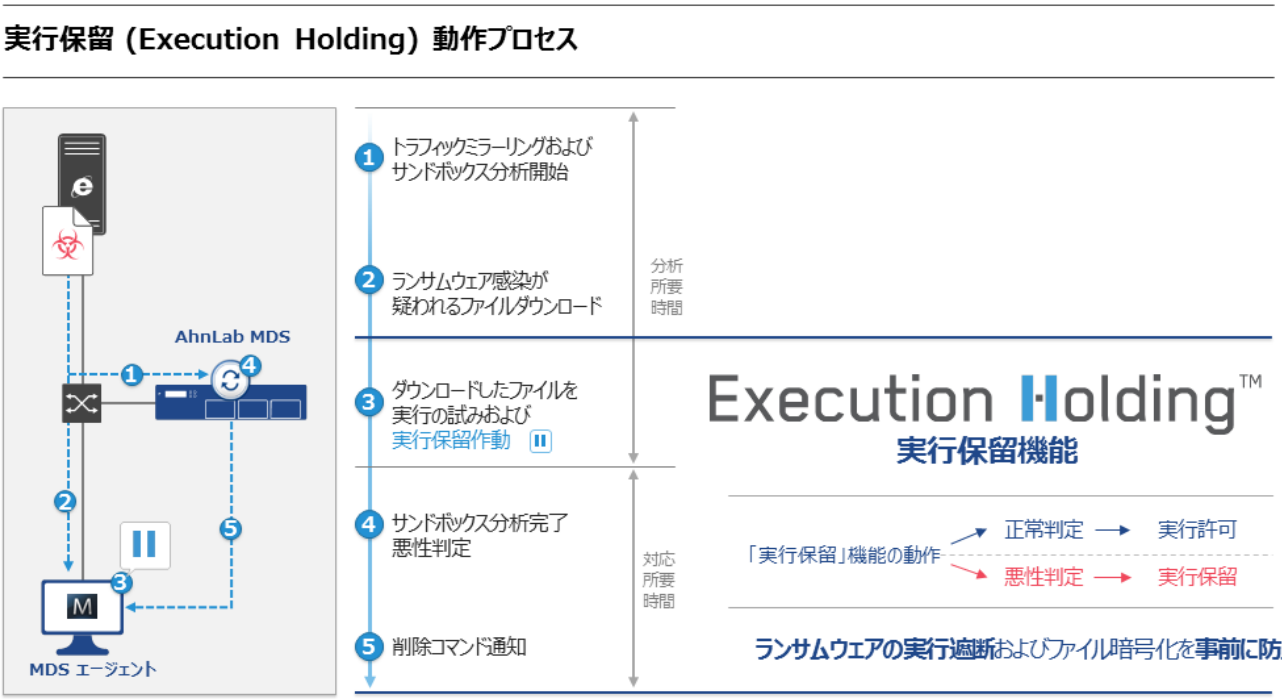


[図4] 理想的な対応 vs. 現実的な対応

すべての知能型脅威対応ソリューションにて可能か

もちろん、前述した「現実的な処置」すらも仮想環境技術を採用するすべての「知能型脅威対応ソリューション」で実現できるわけではない。

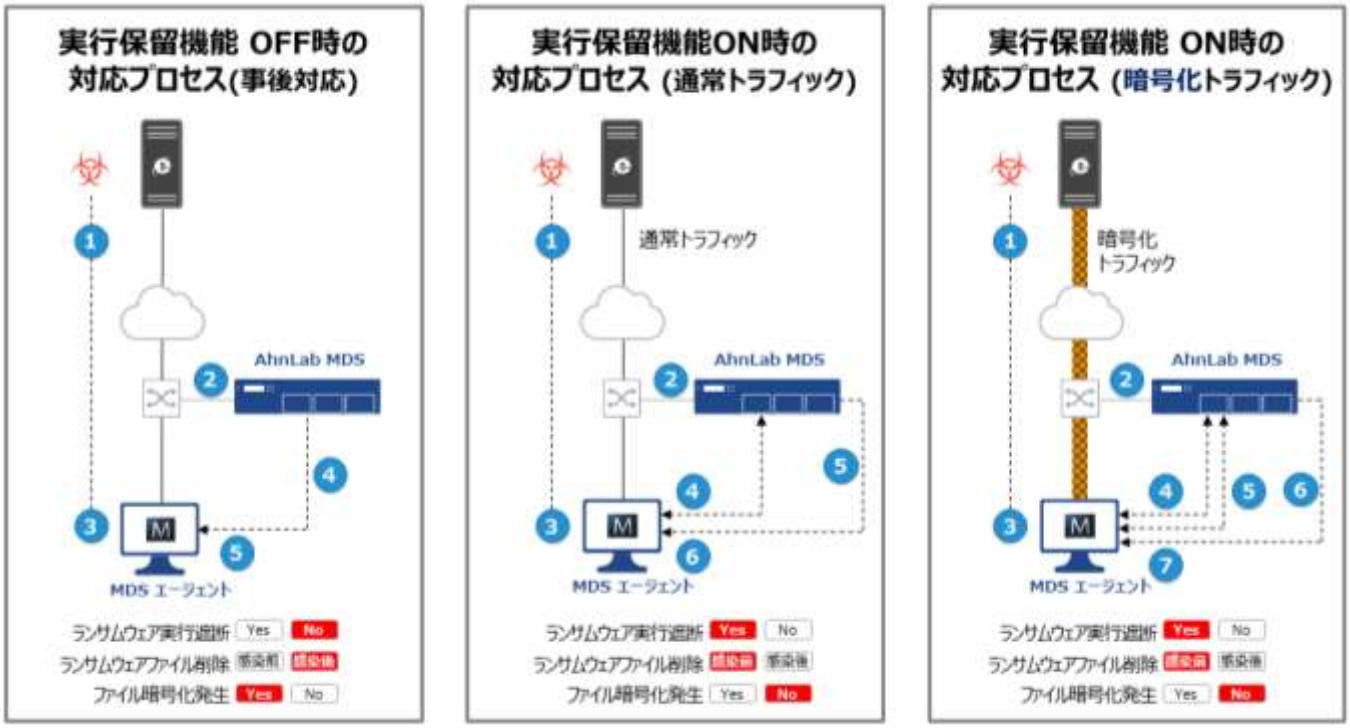
アンラボ MDSは、製品企画段階から「エンドポイントレベルのリアルタイム対応」を掲げ、2011年基準で仮想環境のサンドボックスベース知能型脅威対応ソリューションとして世界初「**MDS エージェント**」という軽量化された専用エージェントを搭載した。また進化する脅威と APTの対応例を反映した「**実行保留(Execution Holding)**」機能を追加適用し(2013年)、未知の脅威を検知することに留まっている競争社とは異なり、検知した未知の脅威に対する**自動遮断**という差別化された機能を搭載している。



[図5] AhnLab MDSの実行保留 (Execution Holding)機能

もちろんランサムウェアの高度化も顕著で、ネットワークレベルのサンドボックスベース分析製品をバイパスするため、機能をモジュール化した複数のマルウェアで構成したものを利用し、セキュリティソリューションの検知を回避するための暗号化通信を使用する。このため SSLプロキシまたは復号化 (decryption)専用アプライアンスのような高価なソリューションを追加で構築することもある。しかし標準 SSL証明書方式に従わない非標準化暗号プロトコルを利用する場合は、該当する暗号化トラフィックを復号化できないという難点がある。

アンラボ MDSの実行保留機能は、エンドポイントレベルでトラフィック復号化およびファイル再組み合わせが完了した状態で作動するため、このような暗号化トラフィック環境でも制約なく作動できることが強みだ。



[図6] AhnLab MDSの暗号化トラフィックに対する実行保留機能の動作プロセス

サンドボックスベースの知能型脅威対応ソリューションは、特定のランサムウェアマルウェアのみ検知・分析・対応するためのものではない。

進化するランサムウェアへの完璧な対応が不可能であることは、周知の事実だ。

ランサムウェアの被害を個人の問題ではなく組織レベルでみると、被害者が属した企業や機関はパッチ・脆弱性管理、またはインターネット・電子メール使用のガイドラインが不十分であることがわかる。今後その組織への知能型攻撃が発生する可能性は、必然的に高まるだろう。これは窓の割れた車を放置するなどの環境が劣悪な場所では、そうではない場所よりも犯罪の発生率が高くなるという「Broken Window Theory」が適用される。

つまり「ランサムウェア被害発生 → 標的型攻撃の対象」への連鎖の条件が十分満たされていることを示す。我々に必要なものは、現在できる技術の枠の中で、最大の効果を得られる最善の方法を選択することにある。

<参考資料>

- アンラボ、「アンチマルウェア、インストール手法と有害性」
  http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=3&seq=16067
- 韓国IDG、「ランサムウェアから PCを保護する」(2014/01/21)
- US-CERT、Crypto Ransomware
  https://www.us-cert.gov/ncas/alerts/TA14-295A
- KISA、ハングルバーションランサムウェア「CryptoLocker」拡散注意の呼びかけ
  http://www.kisa.or.kr/notice/press_View.jsp?mode=view&p_No=8&b_No=8&d_No=1364
- Trend Micro, Ransomware Definition
  http://www.trendmicro.com/vinfo/us/security/definition/Ransomware
- McAfee,Defeat Ransomware:Ensure Your Data Is Not Taken Hostage
  http://www.mcafee.com/kr/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf
- Symantec, Ransomware:A Growing Menace
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)