Acronis
Active Protection

ランサムウェアからデータを保護

変化の激しい脅威からデータを保護

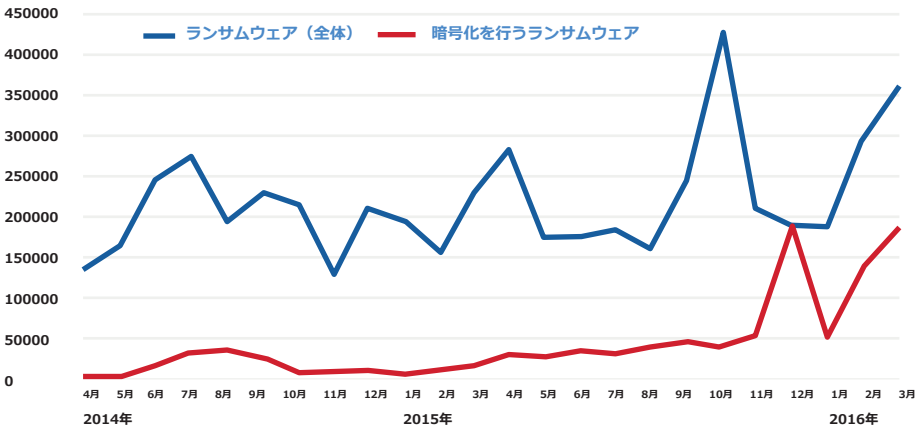
Osterman Researchの調査によると、現時点で47%の企業がランサムウェアの攻撃を受けています。2017年5月のWannaCry攻撃は世界中で発生し、この割合はさらに増加することが予測されます。残念ながら、これはランサムウェアの脅威の始まりにすぎません。

将来的にランサムウェアは、個人に恥ずかしい思いをさせたり、法的な手段を選ぶことをあきらめさせるため、攻撃者によるランダムなデータ改変をやめさせる代わりに金銭を要求する仕組みになっていくでしょう。では、ランサムウェアの実態はどのようなものなのでしょうか。

ランサムウェアとは

ランサムウェアは、感染先のデバイスに保存されている情報へのアクセスをブロックするマルウェアです。デバイスやデータのロックを解除するため、ユーザーは金銭を要求されます。通常は、広く利用されている電子マネーや仮想通貨が支払手段として使用されます。ランサムウェアには2種類のマルウェアがあります。1つはWindowsブロッカーといわれるもので、ポップアップウィンドウを表示し、オペレーティングシステムやブラウザーへのアクセスをブロックします。もう1つは暗号化を行うマルウェアです。このマルウェアにはトロイの木馬のダウンローダーが含まれ、感染に成功すると暗号化を行うランサムウェアをダウンロードします。最近では、暗号化を行うランサムウェアが主流になっています。

次のグラフでも分かるように、ランサムウェアの数は増加しています。マルウェア対策ベンダーやFBIなどの組織もこの傾向を認識しています。企業、特に中堅中小企業に対する攻撃が増加しています。



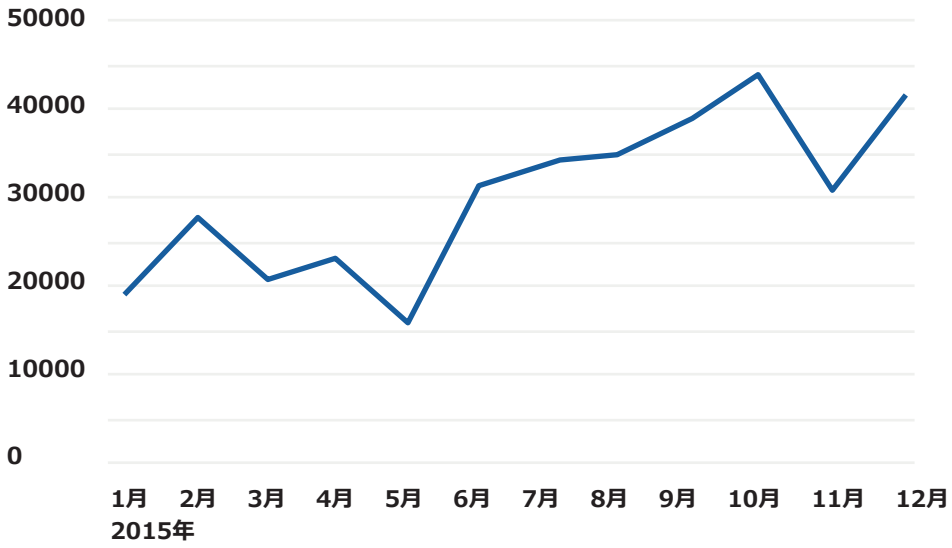
出典: Kaspersky Labのレポート
https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

特長

Acronis Active Protectionは、アクロニスのバックアップ技術と経験に基づいて構築された新世代のデータ保護製品です。

- ランサムウェアからバックアップデータをリアルタイムで保護。万一攻撃を受けてもデータを確実に保護
- ランサムウェアの新しい亜種や未確認の亜種が発生しても、ファイル、バックアップデータ、バックアップソフトを保護
- 簡単操作で自動処理も可能

Acronis Active Protectionにより、現在のランサムウェアだけでなく、将来発生する亜種にも対応することができます。



Symantecのレポート
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

ACRONIS ACTIVE PROTECTION™: ランサムウェアに有効な保護対策

Acronis Active Protectionは、Windowsオペレーティングシステムで機能する高度な技術です。アクロニスでは、この機能をAndroidや他のモバイル/デスクトップOSに展開する予定です。

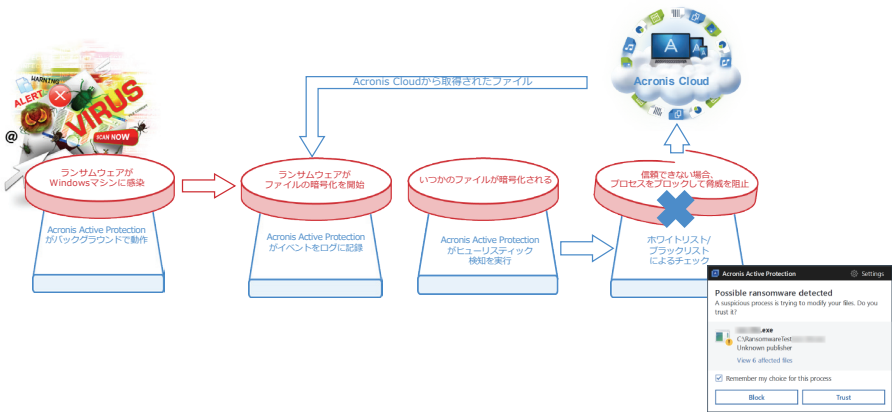
Acronis Backup 12.5とAcronis Active Protectionが搭載する特許出願中の技術は、BCP（事業継続計画）の基盤となります。

ランサムウェアによる攻撃は、できる限り早い段階で阻止する必要があります。可能であれば、ランサムウェアがファイルを暗号化する前にPC上で阻止するべきです。そのためには、ITやセキュリティの担当がランサムウェアを早期に検知し、PCやネットワークに被害が発生する前に、迅速に対応することが重要です。これは企業のユーザーだけでなく、個人のユーザーも同様です。

アクロニスは、ランサムウェアの阻止に効果的なソリューションを提供しています。この機能は、アクロニスの個人ユーザー向け製品で提供していましたが、Acronis Backup 12.5から企業向けに標準機能として提供されます。

ヒューリスティック検知

マルウェア対策でヒューリスティックという言葉が使われていますが、Acronis Active Protectionでもヒューリスティック検知のアプローチを採用しています。この方法は、シグネチャのみの場合よりも高度な検知を可能にします。1つのシグネチャは1つのサンプルしか検知できませんが、ヒューリスティック検知では、同じファミリ（類似した動作や行動パターンを持つサンプル）に属する数種類あるいは数百種類のサンプルから検知できます。ヒューリスティック検知では、プログ



ラムが実行する一連のアクション（より正確にいうとファイルシステムのイベント）をデータベースに登録された不正な動作パターンと比較します。

この検知では、プログラムのホワイトリストとブラックリストを使用します。ホワイトリストによるチェックが必要になるのはなぜでしょう。ヒューリスティック検知では新しい脅威も検知できますが、過去の経験値や動作に基づいて識別を行うため、誤検知も発生します。このため、Acronis Active Protectionでは、ホワイトリストとブラックリストを使用して不審なプロセスを特定します。ユーザーがランサムウェアの疑いがあるプロセスをブロックすると、このプロセスはブラックリストに追加されます。このプログラムは次の再起動時に実行されません。同じランサムウェアのブロック操作を繰り返し行う必要はありません。

バックアップに侵入するためにアクロニスのソフトウェアが狙われる可能性もあります。このため、アクロニスのソフトウェアプログラムには自己防御機能を実装しています。バックアップデータに対する変更は、アクロニスのソフトウェアにのみ許可しています。また、強力な自己防御機能により、アクロニスのソフトウェアに対する攻撃やバックアップデータに対する改変を阻止します。

Acronis Active Protectionは、Windowsマシンのマスターブートレコードを監視し、ホワイトリストに登録された正規のユーティリティ以外による変更をブロックします。

Acronis Active Protectionはどの種類のファイルにも有効なのか？

Acronis Active Protectionはどの種類のファイルにも対応できますが、データを常時保護するには、次の3つの攻撃に対して対策が必要になります。

1. あらゆるファイルに対する攻撃
多くの場合、バックアップデータから被害を受けたデータを復元できます。Acronis Active Protection搭載の製品を使用すると、このような操作を簡単に実行できます。この技術はリアルタイムで動作します。暗号化されたファイルの復元は自動的に実行できます（ユーザーの確認後）。たとえば、バックアップを午前0時に行うようにスケジュールを設定し、午前11時にランサムウェアの攻撃を受けたとします。オンラインのバックアップからファイルを復元するだけでは、11時間分の作業を失うことになります。プロセスを常に監視していれば、ランサムウェアの攻撃が発生してもデータを失うことはありません。

2. ローカルのバックアップデータに対する攻撃
Acronis Active Protectionがローカルドライブを常に監視し、不正な手段によるバックアップデータの改変を阻止します。

3. 不正な手段によるクラウドバックアップの改ざん
Acronis Cloud Storageに保存されているファイルが不正なコードによって直接変更されることはありません。エンドツーエンドの強力な暗号化を行い、厳しいアクセス制御を行っています。ファイルを変更できるのは、署名付きで承認されたアクロニスのエージェントソフトウェアだけです。

ランサムウェアの攻撃を阻止する技術

次の表に、ランサムウェアが攻撃で使用する技術と手口をまとめました。

動作	説明	Acronis Active Protectionの対応
インプレースでの上書き	ランサムウェアがその場でデータファイルを開き、改ざんします。	ドライバーがヒューリスティックデータと一緒にファイルに対するアクセスをサービスに通知し、不審な動作に対してコピーオンライトを実行します。サービスがランサムウェアの処理を阻止し、ドライバーが自身のキャッシュからファイルをロールバックします。
名前の変更	ランサムウェアがデータファイルを開き、名前を変更してから改ざんします。	上記と同じ動作。
新しいファイルの作成	ランサムウェアが新しいファイルを作成し、元のコンテンツをコピーして変更し、オリジナルのファイルを削除します。	上記と同じ動作。
マスターブートレコードの上書き	ランサムウェアが物理ドライブを開き、MBRを上書きします。システムが再起動するとHDD/MFTを暗号化します（chkdsk偽装）。	ドライバーがRAW FS経由でMBRに実行されるWRITE/SCSI操作を監視し、サービスに通知します。サービスはプロセスを検証して判断します。
インプレースでの上書き、名前の変更、新しいファイルの作成と既知の正常なプロセスへのコードの挿入	ランサムウェアが、既知の正常なプロセスに不正なコードを挿入し、前述の不正なアクションを実行します。	ドライバーがサービスに挿入を通知します。コピーオンライトではなくプロセスの監視を開始するようにサービスがドライバーに指示します。不審なパターンが検知されると、クラウドからファイルを復元するようにユーザーに指示します。

ウイルス対策と従来のバックアップソフトウェアの併用よりも強固な対策

ウイルス対策と従来のバックアップソフトウェアは連携して動作しないため、これらを併用しただけではランサムウェア対策としては不十分です。従来型のマルウェア対策ソリューションで脅威を検知できないとデータを失うことになります。多くのマルウェア対策はクラウドにファイルをバックアップしません。また、従来のバックアップソリューションはマルウェアの存在を検知できません。アクロニスのエンドポイントエージェントでAcronis Active ProtectionとAcronis Cloudを併用すると、オリジナルのデータをローカルキャッシュ、ローカルバックアップまたはクラウドバックアップから復元できます。これにより、さまざまなランサムウェアの脅威を排除できます。

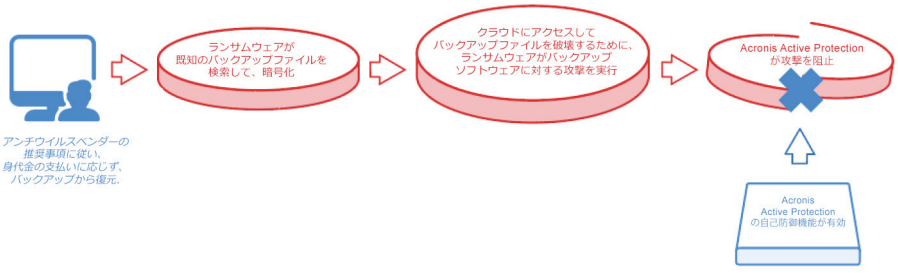
マルウェア対策ソフトウェアはサイバー犯罪者の標的となっています。検知を回避しようとするマルウェアも存在します。攻撃者は、検知を逃れるために主要なマルウェア対策の検知技術やアーキテクチャの弱点を探しています。検知回避のために暗号化されたマルウェアも存在し、このような脅威を従来のシグネチャによる検知機能で阻止することはできません。無料で提供されている多くのウイルス対策も従来型のアプローチを使用しています。このため、どのマルウェア対策ベンダーもバックアップの使用を推奨しています。クラウドバックアップソリューションを利用すると、被害はローカルマシンのデータに限定されるので、単純な攻撃による被害は回避できます。しかし、バックアップソリューションを狙った攻撃が発生する可能性もあります。

今後の脅威にも対応するAcronis Active Protection

サイバー犯罪者がバックアップを狙うのは、攻撃を短時間で成功させ、金銭を得るためです。www.nomoreransom.org/prevention-advice.htmlなどのプロジェクトでは「バックアップを作成すること」と「支払いに応じないこと」をユーザーに促しています。この2つは簡単なことですが、非常に重要です。

攻撃者はすでにバックアップデータに対する攻撃を開始しています。しかし、現在では多くのバックアップソリューションがクラウドストレージを使用しているため、攻撃には成功していません。クラウド上のバックアップを攻撃するには、クラウドにアクセスするための認証情報を取得しなければなりませんが、一般的なランサムウェアにそのような機能はありません。

攻撃者が次に狙うのはデータをクラウドに送る手段、つまりデバイス上のエージェントソフトウェアです。技術的には、ローカルエージェントに不正なコードを挿入する方法はいくつも存在します。このような攻撃を阻止できるバックアップソリューションは、Active Protectionを搭載したアクロニスの製品だけです。



Acronis

第三者機関の評価

独立系評価機関のAV-Testが、4種類の新しいプログラムにベンチマークテストを実施し、次の結果を報告しました。「このテストでは、バックアップソリューションを含むマルウェア対策の有効性を評価しました。ランサムウェアの攻撃を阻止したバックアップソリューションは[Acronis Active Protection技術]だけでした。

独立系調査機関のMRG Effitasの評価も同じ結論になりました。テスト範囲では、アクロニスの製品に「弱点は見つかりませんでした」。

第三者機関のテスト結果については、アクロニスのブログとプレスリリースをご覧ください。

詳しくは、www.acronis.comをご確認ください。