Microsoft | Malware Protection Center

脅威レポート: ルートキット

2012 年 6 月

Microsoft

Microsoft Malware Protection Center 脅威レポート: ルートキット

作成者

Heather Goudey – *Microsoft Malware Protection Center*

投稿者

Jason Conradt – *Microsoft Protection Technologies*
Peter Ferrie – *Microsoft Malware Protection Center*
Joe Johnson – *Microsoft Protection Technologies*
Scott Molenkamp – *Microsoft Malware Protection Center*
Hamish O'Dea – *Microsoft Malware Protection Center*
Oleg Petrovsky – *Microsoft Malware Protection Center*
Tim Rains – *Microsoft Trustworthy Computing Communications*
Jasmine Sesso – *Microsoft Malware Protection Center*
Jeff Williams – *Microsoft Malware Protection Center*

製品マーケティング

Ken Malcolmson – *Microsoft Trustworthy Computing Communications*

目次

はじめに

この Microsoft Malware Protection Center (MMPC) 脅威レポートでは、今日の組織と個人に脅威をもたらしている、より狡猾なタイプのマルウェアの 1 つであるルートキットについて検討します。このレポートでは、攻撃者がルートキットをどのように利用するかと、感染したコンピューター上でルートキットがどのように機能するかについて考察します。また、今日のコンピューター環境でルートキット機能を悪用する、より広く蔓延しているいくつかのマルウェア ファミリについて説明します。その後、組織がルートキットからもたらされるリスクを低減するのに役立つ推奨事項をいくつか示します。

ルートキットの目的

ルートキット (ルートキット機能) は、マルウェアにステルス機能を提供します。攻撃者は、自分が仕掛けたマルウェア ファミリがセキュリティの低下したコンピューター上に長期間とどまらない限り、成功したとは考えません。大半のマルウェアの目的は、機密データを盗み出すことやリソースを悪用することです。たとえば、コンピューターを使用して「クリック詐欺」[1] を行うことなどです。マルウェアは、攻撃者の管理下でリソースの破壊、または重要なデータの監視、フィルタリング、キャプチャ、および盗み出しを行うために、セキュリティの低下したコンピューターに潜んだままとどまる必要があります。ルートキット機能は、マルウェアが潜んだまま、その「ペイロード」つまりファイルのダウンロード、コンピューター設定の変更、キーストロークの記録などの動作を実行するために必要となるステルス機能を提供します。

ルートキットの語源

ここで少し立ち止まって、「ルートキット」という用語の語源について考えてみましょう。ルートキットは当初、攻撃者が UNIX システム上で「root (ルート)」つまり通常はシステ

[1] "Click Fraud: Cybercriminals want you to 'like' it:" Security Tips & Talk blog, http://blogs.msdn.com/b/securitytipstalk/archive/2010/07/08/click-fraud-cybercriminals-want-you-to-like-it.aspx

ム管理用に確保されている最上位レベルの特権を横取りし、その特権を利用して行われた変更を隠すために使用できる一連のツールと考えられていました。近年では、「ルートキット」または「ルートキット機能」という用語は、ステルス機能で自己を隠し、検出と削除を回避するマルウェアを指して使われるのが一般的です。

攻撃者がルートキットを使用する方法

マルウェア作成者は、コンピューター、ネットワーク、および組織のセキュリティを低下させるために膨大なリソースを費やすことができます。攻撃者はルートキットを使用することで、セキュリティが低下した状態をできるだけ長く保とうとします。攻撃者が追求するデータおよびリソースの実際の価値によって、攻撃者の労力は採算の合う行為になるだけでなく、利益を生み出す行為にもなります。データが貴重であればあるほど、攻撃者はうまく狙ったセキュリティ低下状態に持ち込むために必要となるツールに投資することができます。投資額の膨大さと、検出されずに残ることの重大性により、ルートキットは過小評価してはならない脅威となります。

攻撃者は、セキュリティを低下させ、標的のシステム上での存在を確立した後、攻撃者が使用する可能性のあるマルウェアやその他のツールの存在だけでなく、そのセキュリティ低下状態の症状も隠す必要があります。攻撃者が検出を回避するための最も効果的な方法の 1 つは、セキュリティ低下状態の兆しをまったく示さないことです。マルウェアなどに感染した組織が、潜入されたことに気付いていない場合、さらなる調査や、より厳重なセキュリティ対策によって、攻撃を察知したり、改善策や強化策を実施したりする可能性は低くなります。

ルートキットが検出されなければ、何年間もとどまり、感染したシステムからデータやリソースを盗み続ける可能性があります。一般に、ウイルス対策技術は、多くのタイプのマルウェアを包括的かつ先手を打って検出することは非常に得意ですが、実際問題として新しいマルウェアを検出する能力は、そのマルウェアに関する情報を効果的に収集することにかかっています。ルートキット作成者が、自分たちの成果物が検出されないように多大な努力を払っているため、必要な情報を収集するのは簡単ではありません。その結果、組織が取り組む必要のある難しい問題が持ち上がっています。たとえば、組織は情報のない仮説的な脅威からユーザーをどのように有意義な方法で保護することができるでしょうか。脅威の広がりに関する正確な情報がない状態で、問題の範囲をどのように正確に判断することができるでしょうか。ルートキットがどのように機能するのか、どのタイプの既知のマルウェアがルートキットを利用するのかをより深く理解することで、これらの質問により効果的に答えることができます。

ルートキットが機能するしくみ

ルートキットは基本的に、自己をシステムに挿入してオペレーティング システムへの要求を操る、つまりフィルタリングすることによって機能します。ルートキットは情報要求を操ることで、偽のデータ (不完全なデータ) を提供して、感染したシステムの完全性を徹底的に破壊することができます。これがルートキットの主要な機能であり、ルートキットが重大な脅威であることの理由です。ルートキットがいったんインストールされると、感染したコンピューターから報告される情報を信頼することはできなくなります。

たとえば、ルートキットに感染したコンピューター上のプロセスのリストを要求した場合、実行中のすべてのプロセスからそのルートキットまたはそれが保護するその他のコンポーネントに関係するプロセスが除外されたリストが返される可能性があります。一般に、マルウェアはルートキット機能を使用して、ファイル、レジストリ改変、ネットワーク接続の証拠、および各種プロセスだけでなく、マルウェアの存在を示す可能性があるその他のものを隠します。

ルートキットが自己を挿入してフィルタリング機能を実行できる場所は、オペレーティング システム内にいくつかあります。ルートキットの「タイプ」は、ルートキットが実行パスの破壊を実行する場所で判定されます。これらの理由により、ルートキットは従来、「ユーザー モード ルートキット」または「カーネル モード ルートキット」のいずれかに分類されてきました。

- **ユーザー モード ルートキット**: このタイプのルートキットは、アプリケーション プログラミング インターフェイス (API) 機能を「フッキング」することで、ユーザー モード アプリケーションから行われた情報の要求をフィルタリングします。フッキングは、ソフトウェア コンポーネント間でやり取りされる関数呼び出し、メッセージ、またはイベントを傍受することで、アプリケーションの動作を改変または拡充するために使用されるさまざまな手法に適用されます。このような傍受された関数呼び出し、メッセージ、またはイベントを処理するコードは、「フック」と呼ばれます。このルートキット機能は、マルウェア開発者にとってより利用しやすいものとなっています。一般に、有用なユーザー モード コードを書くことは、有用なカーネル モード コードを書くことより簡単だからです[2]。ただし、一般には、ユーザー モード フックの方が簡単に検出できます。

---

[2] Kasslin, K. et al (2005) *Hide n' seek revisited – Full stealth is back*. Virus Bulletin Conference October 2005

- **カーネル モード ルートキット**: このタイプのルートキットは、フィルタリングとフッキングをカーネル レベルで実行します。このレベルでフィルタリングする方がより効果的なのですが、感染したシステムを破壊することなく首尾良く目的を達成することは難しくなります。カーネルにコードを埋め込むための 1 つの方法は、デバイス ドライバーを利用することです。このレベルでフッキングするために使用される方法はいくつかあります。たとえば、「インライン フッキング」ではコードが埋め込み先で改変され、「System Service Dispatch Table へのパッチ適用」では特定のイベントをフッキングします。

「MBR ルートキット」または「ブートキット」と呼ばれることもある最近のいくつかのルートキットでは、マスター ブート レコード (MBR) を改変してシステムを掌握し、ブート シーケンス内のできるだけ早い段階でルートキットを読み込むプロセスを起動します[3]。

少なくとも概念的には、実行パスのさらに深部に潜り込むことができ、この点を例証するルートキットの概念証明がいくつかあります。“Blue Pill”[4] の概念では、薄いハイパーバイザーを使用して、影響を受けるユーザーとの間のインターフェイスとなるオペレーティング システムの仮想インスタンスを作成するという考え方を重視します。「ハイパーバイザー」とは、プロセッサー固有の仮想化プラットフォームであり、複数の独立したオペレーティング システムが 1 つのハードウェア プラットフォームを共有できるようにします。ハイパーバイザーは、要求の発生元にかかわらずほとんどあらゆるデータ要求を傍受して改変できますが、これは「ベアメタル」オペレーティング システムとユーザーの仮想オペレーティング システムとの間に位置しているためです。実行パスのさらに深部に入り込むことができるため、セキュリティの低下したファームウェアがネットワーク レベルでデータを傍受することもできます[5]。

ルートキットがオペレーティング システムへの要求を傍受してフィルタリングするために自己を埋め込む実行パスが深ければ深いほど、ステルス性も高くなります。ただし、ルートキットの潜入先が深くなればなるほど、気付かれずに実装することも難しくなり、そのようなルートキットを開発することはさらに複雑かつ高コストになります。同様に、ルートキット

---

[3] MMPC Malware encyclopedia DOS/Alureon description
www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=DOS%2fAlureon
[4] http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
[5] Presentation at Hack.lu:Reversing the Broadccom NetExtreme's firmware – Sogeti Esec Lab Blog, http://esec-lab.sogeti.com/dotclear/index.php?post/2010/11/21/Presentation-at-Hack.lu-%3A-Reversing-the-Broacom-NetExtreme-s-firmware

の実行パス内の位置が深くなればなるほど、駆除も難しくなります。カーネル モード ルートキットによるセキュリティ低下の影響を次の図に示します。

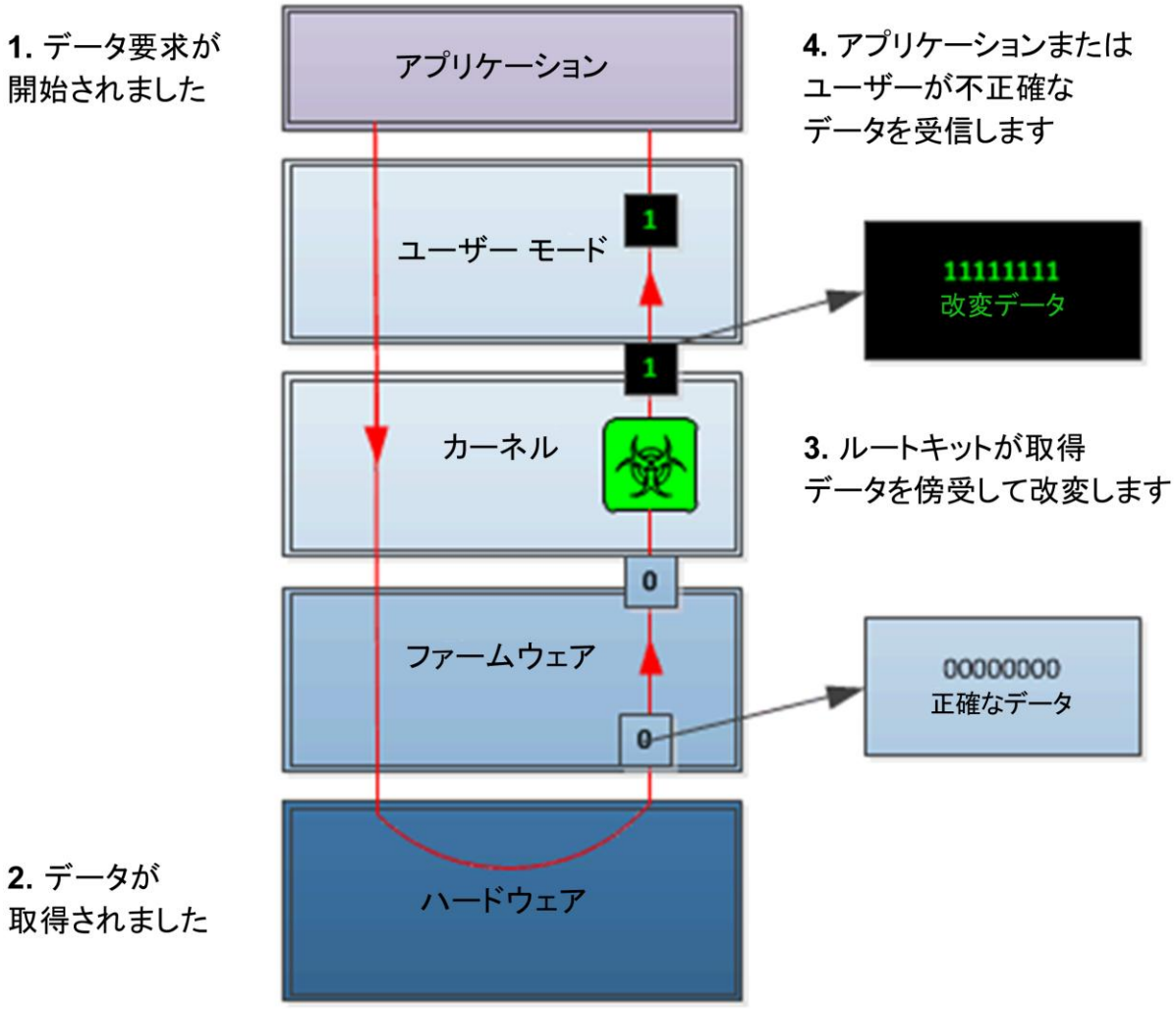

図 1。カーネル モード ルートキットによるセキュリティ低下の影響

ルートキット問題の範囲

多くの最新のマルウェア ファミリでは、ルートキット手法を使用して、影響を受けるユーザーから身を隠し、検出と駆除を回避します。マルウェアがステルス機能を使用することは、過去 10 年間でさらに増えてきています。このような手法の使用が増えているにもかかわらず、MMPC はこのような脅威の多くに関する情報を収集してきており、テクノロジー ユーザーをこれらの脅威から保護するのに役立つ研究に相当な時間と労力を費やしてきました。

もっとも、特定の組織を特に標的とするために開発され、したがって一般的な脅威の状況には蔓延しないために検出されにくいタイプのルートキットやその他のマルウェアもいくつかあります。この特定のタイプのマルウェアやルートキットという脅威の範囲や、脅威にさらされている組織の件数を判断することは、困難な課題です。これらの理由により、最新の情報にもかかわらず、このような脅威が重大であり、貴重なデータを保有しているどの組織も適切な予防措置を講じる必要があることを示す証拠は十分にあります。

ルートキットを使用する有名なマルウェア ファミリ

今日最も蔓延しているマルウェア ファミリのいくつかは、一貫してルートキット機能を使用しています。有名な例をいくつか次のリストで説明します。

Win32/Alureon[6]。オンラインでの広範囲に及ぶ破壊活動に関与する、トロイの木馬のマルチコンポーネント ファミリ。さまざまなソースからコントローラーに収益をもたらします。Win32/Alureon はほとんどの場合、攻撃者の利益となるように、影響を受けるユーザーのオンラインでの活動を操ることと関係があります。このマルウェア ファミリのさまざまなコンポーネントは、次のことを実行するために使用されてきました。

- 影響を受けるユーザーの検索結果を改変します (「検索ハイジャック」とも呼ばれます)。
- 影響を受けるユーザーが攻撃者の指定するサイトにアクセスするよう仕向けます (「ブラウザー ハイジャック」とも呼ばれます)。
- 影響を受けるユーザー本人が気付かずに攻撃者の指定するサイトにアクセスするよう DNS 設定を変更します。
- 任意のファイルをダウンロードして実行します。これには、追加コンポーネントや他のマルウェアも含まれます。
- 違法な広告を表示します。
- 悪質なセキュリティ ソフトウェアをインストールします。
- バナー クリックを実行します (ペイパークリック広告で)。

Win32/Alureon は長年、作成者たちによって活発に開発され、強引に配布され、専門的に管理されてきました。そのコンポーネント (他のマルウェア ファミリから利用されることがよくあります) がコンピューターの使用現場に蔓延し、ステルス機能を使用することで、このマルウェア ファミリは有名な脅威となっています。

---

[6] MMPC malware encyclopedia Win32/Alureon description
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fAlureon

Alureon は、さまざまな方法で自己のプロセスやシステムの変更内容を隠してきました。たとえば、次のとおりです。

- 悪意のあるデバイス ドライバーをインストールします。これにより、Alureon は System Service Dispatch Table (SSDT) と Windows API をフッキングすることができます。その目的は、名前に特定の文字列を含んでいるファイル、レジストリ エントリ、およびプロセスへのアクセスを隠したり防止したりできるファイル システム要求を傍受することです[7]。
- 既存のシステム デバイス ドライバーに悪意のあるコードを感染させます。これにより、Alureon はディスク操作を処理するカーネルの一部に自己を挿入して、ファイルおよびディスク セクターを隠すことができます[8]。Alureon のより最近の亜種では、これらの動作をシステム ファイルに感染することなく実行するものもあります。
- マスター ブート レコード (MBR) に感染します。これには、64 ビット版 Windows オペレーティング システムの MBR にうまく感染して、オペレーティング システムのカーネル モードのコード署名ポリシーと PatchGuard 保護をすり抜けることができるようにすることも含まれます。

Win32/Rustock[9] – (Rustock ファミリの詳細については、go.microsoft.com/?linkid=9777699 からダウンロードできる『セキュリティ インテリジェンス レポート スペシャル エディション – Rustock の脅威との闘い』を参照してください)。ルートキット対応バックドア トロイの木馬のマルチコンポーネント ファミリは当初、「ボットネット」による「スパム」メールの配信を支援するために発達しました。ボットネットとは、セキュリティが低下したコンピューターで構成される、攻撃者の制御下にある大規模なネットワークのことです。Rustock が初めて検出されたのは 2006 年初期であり、その後発展して、広く蔓延した脅威の 1 つとなりました。何件かのレポートによると、ピーク時には兵力 100 万の Rustock ボットネットが、スパム トラフィックの約 80% を占めており、1 秒あたり 2,000 通を超えるスパム メッセージを送信していたとのことです。

---

[7] MMPC malware encyclopedia Trojan:WinNT/Alureon.C description
www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3aWinNT%2fAlureon.C
[8] MMPC malware encyclopedia Virus:Win32/Alureon.A
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus:Win32/Alureon.A
[9] MMPC malware encyclopedia Win32/Rustock description
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fRustock

Rustock は、複雑な方法でドライバーをインストールして、検出と駆除を困難にしていました[10]。さらに、これらのルートキット ドライバーはシステム関数をフッキングして、自己とそのコンポーネントを隠していました。これは、SSDT をパッチ適用してイベント ZwCreateEvent、ZwCreateKey、および ZwOpenKey をフッキングすることで、達成されていました。この方法により、これらのルートキット ドライバーは、各ドライバーの名前を含んでいる要求をフィルタリングし、一致する場合には STATUS_UNSUCCESSFUL を返すことで、検出を免れることができました。また、Rustock はネットワーク操作とディスク I/O 操作も隠そうとしました。そのため、このルートキットのあるドライバーが、ntoskrnl.exe と ntdll.dll API のセットをフッキングし、NTFS ファイル システム (NTFS) と TCP/IP デバイス (NTFS、IP、TCP、UDP、RawIP、IPMULTICAST など) と直接通信していました。

Microsoft は、業界と教育界のパートナーと連携して法的措置と技術的措置の画期的な組み合わせを活用して、Project MARS (Microsoft Active Response for Security) の一部として 2011 年 3 月に Rustock ボットネットを鎮圧することに成功しました[11]。この措置の結果、進行中の犯罪捜査資料の一部となる証拠が集まりました[12]。

Win32/Sinowal[13]。機密データを盗み出そうとするマルウェアのマルチコンポーネント ファミリ。データとしては、さまざまなシステムのユーザー名やパスワードなどがあります。これには、さまざまな FTP、HTTP、および電子メール アカウントの認証詳細以外に、オンライン バンキングやその他の金融取引に使用される資格情報を盗もうとする行為も含まれます。Sinowal は特に、影響を受けるユーザーが暗号化された Secure Socket Layer (SSL) トランザクション中に使用するデジタル資格情報を標的とし、差し替えることで、このような通信の完全性を破壊しようとすることがあります。また、Sinowal はリモート攻撃者にバックドア機能を提供して、感染コンピューターに不正にアクセスして制御下に置き、攻撃者が後で任意のファイルをダウンロードして実行するために悪用できるようにします。Sinowal がキャプチャした機密データは、攻撃者が入手できるように Web サイトにアップロードされることもあります。

---

[10] Uprooting Win32/Rustock – MMPC Threat Research & Response blog
http://blogs.technet.com/b/mmpc/archive/2008/10/18/uprooting-win32-rustock.aspx
[11] Operation b107 – Rustock botnet takedown – MMPC Threat Research & Response blog
http://blogs.technet.com/b/mmpc/archive/2011/03/17/operation-b107-rustock-botnet-takedown.aspx
[12] http://blogs.technet.com/b/microsoft_blog/archive/2011/09/22/rustock-civil-case-closed-microsoft-refers-criminal-evidence-to-fbi.aspx
[13] MMPC malware encyclopedia Win32/Sinowal
www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fSinowal

Sinowal のデータ窃盗ペイロードでは、感染コンピューター上にどれほど長期間とどまることができるのかが、マルウェアの成功判定基準です。そのため、Sinowal はステルス機能を使用して検出を回避しながらとどまり続けようとする一方で、密かにデータを収集してリモート攻撃者に送信します。Sinowal も Rustock と同様に、複雑な方法でドライバーをインストールします。このような策謀の最終的な結果として、MBR が悪意のあるコードで上書きされ、メイン ドライバーが物理ドライブの末尾に書き込まれます[14]。これらの変更が実施されると、Sinowal は感染システムを掌握して、起動プロセスの初期に自己のドライバーを読み込ませることができます。

Win32/Cutwail[15]。任意のファイルをダウンロードして実行するトロイの木馬の一種。ダウンロードされたファイルは、ディスクから実行させることも他のプロセスに直接挿入させることもできます。ダウンロードされたファイルの機能はさまざまですが、Cutwail はスパムを送信する他のコンポーネントをダウンロードするのが一般的です。また、Cutwail はルートキットやその他の保護手段を使って、検出と駆除を回避します。

Cutwail では、カーネル モード ルートキットを使用します。Cutwail は、デバイス ドライバーをいくつかインストールして、影響を受けるユーザーからコンポーネントを隠します。ただし、Cutwail は自己を隠せるだけでなく、そのファイルとレジストリ エントリの削除を防止することもできます。Cutwail は自己のレジストリ エントリを隠して保護するために、SSDT の関数 ZwDeleteValueKey()、ZwEnumerateKey()、ZwEnumerateValueKey()、ZwOpenKey()、および ZwSetValueKey() をフッキングします。また、ディスク上のファイルを保護するために、ファイル システム フィルター ドライバーを実装します。

---

[14] MMPC malware encyclopedia VirTool:WinNT/Sinowal.A
www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=VirTool%3aWinNT%2fSinowal.A
[15] MMPC malware encyclopedia Win32/Cutwail
www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fCutwail

ルートキットからの保護

ルートキット感染を防ぐ最善の方法は、ルートキットのインストールを防止することです。ルートキットがいったんインストールされると、ステルス機能のために、ルートキットとそのコンポーネントおよびダウンロードされる可能性があるその他のファイルの検出と駆除は、非常に困難になります。そのため、セキュリティ低下を回避するためにありとあらゆる予防措置を講じることは、理にかなっています。

この目的を達成するために、仮想境界領域を確実に強化し、セキュリティで保護することをお勧めします。具体的には、ウイルス対策製品やファイアウォール製品など、保護技術に投資します。組織のセキュリティ保護の詳細なガイダンスと情報については、「Microsoft Security Intelligence Report」(www.microsoft.com/security/sir/strategy/default.aspx#!section_1) の「Managing Risk」を参照してください。

ウイルス対策ソリューションが、従来のシグネチャベース検出、ヒューリスティック検出、動的反応シグネチャ機能と動作監視の両方を活用することで、包括的な方法で保護していることを確認します。それらのシグネチャ セットが常に最新に保たれていることを確認します。自動更新機能の使用が望ましいと言えます。マルウェア対策技術の詳細については、go.microsoft.com/?linkid=9776701 から入手できる MMPC ドキュメント『Introducing Antimalware Technologies』を参照してください。

また、システム内に脆弱なポイントがないかどうかを調べて監視し、組織内のユーザーが高リスク技術を使用することを制限し、組織内のソフトウェアすべてにセキュリティ更新プログラムを適切なタイミングで適用することも必要です。

また、社員にマルウェアがもたらすリスクに対する意識を高めさせ、適切なセキュリティ啓発研修を施すことで社員を保護することも必要です。詳細な情報とガイダンスについては、www.microsoft.com/security/resources/powerpoint.aspx から入手できる『Internet Safety for Organizations Toolkit』を参照してください。

これらの推奨事項を効果的に実施するために、ネットワーク捜査システム (NIS) と侵入防止システム (IPS) を導入することには正当な根拠があります。

いったん保護を実施したら、システムを監視して常に警戒し、個別のホストとより大きいネットワークの両方でトランザクションと動作の変化を調べることが重要です。組織が中規模であっても、これは気の遠くなるような作業になることがあります。組織は、高価値資産 (主要な知的財産など) を特定し、このような資産に焦点を合わせた監視分析計画を策定する必要があります。

あるセキュリティ低下事例が検出された場合でも、他のスペシャリスト テクノロジを導入して対応することができます。多くのウイルス対策製品には、特殊なルートキット対策技術が搭載されています。Microsoft の各種ウイルス対策ソリューションには、ルートキットの被害を低減することに特化した技術がいくつか搭載されています。たとえば、ライブ カーネル動作監視機能では、感染システムのカーネルを改変しようとする試みを検出して報告します。ダイレクト ファイル システム解析機能は、潜んでいるドライバーの特定と駆除を促進します。

最後に、あるシステムのセキュリティが低下していると判断された場合は、別のツールを導入して、既知の良好なまたは信頼できる環境にブートし、適切な修正措置を施せるようにすることが必要な場合があります。この場合、Microsoft Standalone System Sweeper ツール (Microsoft Diagnostics and Recovery Toolset (DaRT) の一部) または Windows Defender Offline が役に立つことがあります。既知の良好な、セキュリティの低下していないオペレーティング システムを使用してセキュリティの低下したシステムを起動することで、ウイルス対策技術やその他のツールが、マルウェア コンポーネントを特定することができます。このようなコンポーネントは、そうしなければルートキットによって隠されたままになっていたものです。これは、ルートキットに感染したセキュリティ低下状態の防止と回復に役立つ効果的な手法になることがあります。

全般的ガイダンス: 悪意のある望ましくない可能性のあるソフトウェアからの保護

ユーザーをマルウェアから効果的に保護するには、組織や個人が積極的に最新のマルウェア対策システムを維持し、ソーシャル エンジニアリングなどのマルウェア感染手法の最新情報を常に把握しておく努力が必要です。

詳細なガイダンスについては、 Security Intelligence Report Web サイトの「Mitigating Risk」セクションに記載の以下のリソースを参照してください。

- Promoting Safe Browsing

  http://www.microsoft.com/security/sir/strategy/default.aspx#!section_2_3

- Protecting Your People

  http://www.microsoft.com/security/sir/strategy/default.aspx#!section_4

その他の資料

次に示すリソースは、ルートキットの詳細およびマルウェア作成者がルートキット機能を利用する方法を学ぶための優れた入門書となります。

- Blunden. B., (2009) *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System.* Jones & Bartlett
- Hoglund, G. and Butler, J. (2006) *Rootkits – Subverting the Windows Kernel*. Upper Saddle River: Addison-Wesley
- Kasslin, K. et al, (2005) *Hide 'n seek revisited – Full stealth is back*. Virus Bulletin Conference October 2005

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/mmpc