



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

Integrity Anti-Spyware

企業活動を脅かすスパイウェアの無効化



Intelligent Security

チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

Contents

本書の内容

概要	3
スパイウェアの台頭	3
スパイウェアとは	3
企業内のスパイウェアの検出	4
スパイウェアの無効化	4
解決策：Check Point Integrity	4
企業をスパイウェアから保護するためのステップ	5
結論	6

概要

企業ネットワーク内におけるスパイウェアの蔓延は、企業に金銭的に多大な損失をもたらし、法規制を遵守するうえで深刻な脅威となるなど、企業活動に大きな影響を及ぼしています。企業が直面しているスパイウェアの脅威に対処するためには、スパイウェアを無効化し、デスクトップPCおよびモバイルPC上のスパイウェアを一貫した方法で検出および削除できる統合セキュリティ・ソリューションを導入する必要があります。アンチスパイウェア・ソリューションは、第1に、企業データの消失やネットワークへの不正侵入を防止できなければなりません。第2に、絶対にバイパスすることのできない一貫したスパイウェアの仕組みを備え、ネットワーク帯域およびPCのシステム・リソースを本来あるべき状態に回復させることができる必要があります。最後に、エンドポイントの全体的なセキュリティ状態を継続的に管理し、スパイウェアの存在しないPC環境を維持できる必要があります。これらすべての条件を満たすためには、統合型のソリューションと、エンドポイントの全般的なセキュリティ・ポリシーを調整し、エンドポイントのセキュリティ問題を診断するためのレポート作成および分析を継続的に実行できる一元的な管理インタフェースが必要になります。

スパイウェアの台頭

巧みな宣伝文句や巧妙な手口、および最新の技術を駆使してPCに侵入するスパイウェアは、すでに企業全体に広まっており、今や最も危険な脅威の1つとなっています。スパイウェアは多くの場合、サードパーティ製アプリケーションやWebサイトを閲覧中のWebブラウザ、さらにはインスタント・メッセージング (IM)、ストリーミング・ビデオなどを通じてPCに侵入します。Hewlett Packard (HP) が発表した資料によれば、スパイウェアが企業に与える金銭的な被害は、控えめに見積もってインシデント1件あたり138ドルにもなっています。全PCの約8割がスパイウェアに感染しているというNational Cyber Security Allianceの調査結果とこの数字を掛けてみれば、自社内でスパイウェアにどれだけのコストがかかっているかを大まかに知ることができます。これだけでもすでに膨大なコストと言えますが、この数字には、ネットワーク・セキュリティの侵害や知的財産の漏洩などによって生じる財政的な損害は含まれていません。スパイウェアに関しては、単にスパイウェアの脅威を認識するだけでなく、脅威の特性を理解することが極めて重要です。なぜならスパイウェアの脅威は、企業活動に重大な影響を与えうる問題であるからです。

スパイウェアとは

今日のスパイウェアの主たる目的は金銭を得ることです。ホストからインターネットにデータを送信することができ、企業ネットワークへのリモート・アクセスが行えるのであれば、ハッカーにとって、機密文書や顧客データを盗み出す準備ができたことになります。さらに厄介なのは、データの転送や企業ネットワークへのリモート・アクセスが暗号化されているケースが多いことです。境界でフィルタを使用して不正なデータ転送を制御しようとしても、暗号化されたトラフィックを復号化できないのです。またスパイウェアは、自らが感染しているホストに、勝手に悪意あるソフトウェアを追加インストールする機能も備えています。不穏な傾向は、CSI/FBIが2004年に発表したレポートですですに明らかとなっていました。サイバー・セキュリティ侵害を原因とする損失額 (米ドル) のランキングにおいて、機密データの盗難は、ウイルスとサービス妨害 (DoS) 攻撃に次いで第3位にランクされていたのです。

¹ HP. "Spyware - The business cost" <http://h71028.www7.hp.com/eNewsletter/cache/110968-0-0-224-121.aspx>

² "AOL/NCSA Online Safety Study." http://www.staysafeonline.info/pdf/safety_study_v04.pdf

企業内のスパイウェアの検出

企業にスパイウェアが侵入しているかどうかの判断も、一筋縄では行かない場合があります。PCの処理速度の低下や、ネットワークトラフィックの急増は、スパイウェアが侵入している証と言えます。しかしながら、より危険性が高いのは、スパイウェアが何の兆候も見せない場合です。トロイの木馬は、ハッカーがネットワークに不正に侵入することを可能にし、重要な顧客データや知的財産を危険にさらします。キーロガーは、ユーザ・パスワードや内部WebサイトのURLといった機密データの情報をキャプチャし、ハッカーに送信します。これらのスパイウェア・ツールは、PC内に存在していても、感染の症状を示さない場合があります。また、PCをスキャンしてスパイウェアを削除したとしても、最近のスパイウェア・プログラムは自動的に自分自身を再インストールできるため、また元の状態に戻ってしまうこともあります。このように、最近のスパイウェアは狡猾で非常に洗練されているため、エンドポイントPCでは、プロアクティブ（事前対応的）なセキュリティ対策が必要になります。

スパイウェアの無効化

スパイウェアにプロアクティブに対処するには、すべてのエンドポイント（デスクトップPCとモバイルPCの両方）に、スパイウェアの多様な進入経路と活動内容に対応できる強力な防御ソリューションが必要となります。アンチスパイウェア・ソリューションは、第1に、スパイウェアの活動を食い止めるための基礎となる環境を確立できなければなりません。PCによる不正な通信を内向き/外向き共にブロックすることにより、既存のスパイウェアが、企業の機密データを外部に送信したり、内部ネットワークへの無許可のリモート・アクセスを可能にする不正サーバとして機能したりすることを防止できます。第2に、既知の脅威に対するシグネチャと、未知の脅威に対するヒューリスティックを使用してスパイウェアを検出できなければなりません。そして、可能な場合にはスパイウェアを削除し、削除ができない場合には少なくとも隔離する必要があります。このプロセスにおいては、アンチスパイウェア・ソフトウェアを無効にしようとするスパイウェアまたはユーザの操作を防止するクライアント保護の機能が重要になります。最後に、成長を続けるスパイウェアの常に一歩先を行くために、アンチスパイウェア・ソフトウェアは、定期的にスキャンを実行し、自動的に新しいエンジンおよび定義ファイルを手に入れる必要があります。

企業環境においては、スパイウェアの活動を確実に停止するため、これらに加えて、一元的な管理機能および統合されたレポート機能も必要です。管理者は、一元的な管理コンソールを使用することで、アンチスパイウェア・ポリシーを定義および配布したり、統合されたレポート機能にアクセスしてすべてのエンドポイントPCに対するポリシーを調整したりできます。

しかしながら、企業にはすべてのPCに新しいセキュリティ・クライアントを追加する余裕はなく、管理者には新しい管理コンソールの使用方法を学習する余裕がないのが実情です。そのため企業は、エンドポイント・セキュリティ・ソリューションの1コンポーネントであるようなアンチスパイウェア・ソフトウェアを必要としています。このようなソリューションであれば、エンドポイントに導入するセキュリティ・クライアントは1つだけで済み、アンチスパイウェア・ポリシーを含むすべてのエンドポイント・セキュリティ・ポリシーを1つの一元的な管理コンソールで管理できるため、ITコストの負担を軽減できます。

解決策：Check Point Integrity

Check Point Integrity™ Anti-Spywareは、業界をリードするZoneAlarm®のアンチスパイウェア技術をベースにした製品で、スパイウェアをブロックし、セキュリティ環境の継続的な強化を可能にします。Integrity Anti-Spywareは、Integrity製品に統合されたモジュールの1つであり、独立したクライアントをインストールすることなく導入可能です。統合Integrityクライアントのアンチスパイウェア機能は、Integrityのサーバ・コンソールから一元的に管理され、スパイウェアのスキャンは、管理者が指定したスケジュールに従って、ユーザの生産性に影響を与えることなくバックグラウンドで透過的に実行されます。

スパイウェアの検出を行うためのスキャンは、シグネチャとヒューリスティックの両方が使用されるため、効率的かつプロアクティブにスパイウェアを検出することができます。シグネチャは、レジストリ・キーや既知の実行可能ファイル名に対応します。ヒューリスティックは、キーボード入力をモニタするなどの悪意ある振舞いに基づいてスパイウェアを検出するプロアクティブな手法です。スキャンによりPC上で検出されたスパイウェアは、すべて削除または隔離されます。またIntegrityクライアントは、ユーザやスパイウェアによってスキャン機能が無効にされないよう自分自身を保護して、PC上で確実にスキャンが行われるようにします。管理者は、スパイウェアのスキャン・レベルを指定することが可能で、例えばスパイウェアによって使用されることの多い場所をクイック・スキャンしたり、あるいはPC全体にわたってスパイウェアの痕跡を完全にスキャンしたり選択できます。さらに、例外リストを作成することもできるため、正規のモニタリング・ツールやリモート・アクセスによるトラブルシューティング・ツールをスキャンの対象から除外できます。

十分なセキュリティを確保するためには、最新の脅威の常に一步先に行くことが非常に重要です。チェック・ポイントのセキュリティ・サービス・チームは、独自のスパイウェア・リサーチを行っており、数百万人のZoneAlarm®ユーザで構成されるZone Labs® DefenseNetコミュニティからリアルタイムでデータを受け取っています。これらのユーザからは、スパイウェアのMD5チェックサムやOS固有のスパイウェア・ファイルの格納場所といった重要情報が自動的に送られてきます。こうしたリアルタイム情報を利用することで、企業へのセキュリティ侵害が発生する前に、検出および削除のルールを作成することが可能となっています。IntegrityサーバとIntegrityクライアントはどちらも、定期的にSmartDefense™ Anti-Spywareサービスに自動接続して最新の定義ファイルとヒューリスティック技術を入手するように設定できます。

また、フル構成のIntegrityエンドポイント・セキュリティ・ソリューションでは、管理者は、エンドポイントによる企業ネットワークへのアクセスを制御することができます。Integrityは、ネットワーク・アクセスを許可する前に、エンドポイントがセキュリティ・ポリシー（アンチウイルス、アンチスパイウェア、およびパーソナル・ファイアウォールの機能が最新の状態かどうかなど）を遵守しているかどうかを検証します。セキュリティが充分でないPCは隔離され、自動的にポリシーを遵守した状態に修正されます。Integrityは、この状態から不正な通信をブロックすることにより、スパイウェアを無効化するための基礎となるセキュアな環境を確立します。Integrityクライアントは、自動スキャンによってスパイウェアを削除した場合、中央の管理コンソールにレポートを送信します。管理者は、このレポートを使用してアンチスパイウェアによる全般的なセキュリティ効果を分析し、スパイウェアが継続して見つまっている場合には、ユーザ教育や企業ポリシーの見直しを図ることができます。

企業をスパイウェアから保護するためのステップ

- 一元管理可能なエンドポイント・セキュリティ・ソリューションであるCheck Point Integrity™を導入し、PC内のアプリケーションによって行われる内向き/外向きの通信を制御します。プログラム・イベントは一元的にログに記録されるため、ネットワーク・アクセスを試みるプログラムをまとめた管理レポートを作成できます。
- Integrity Anti-Spywareモジュールを有効にし、スパイウェアのタイプごとに自動処理方法を定義した基本的なスパイウェア・セキュリティ・ポリシーを導入します。自動処理（監視、隔離、削除）により、エンド・ユーザの関与を最小限に抑えながら、セキュリティを向上させることが可能になります。
- 定期スキャンをスケジューリングして、新しいスパイウェア・アプリケーションやサービスを検出し、隔離、削除、または監視できるようにします。Integrityは、確実にスキャンを実行し、結果を記録してレポートを管理者に送信します。管理者は、このレポートを使用して分析を行うことができます。
- チェック・ポイントのSmartDefense™ Anti-Spywareサービスを利用して、アンチスパイウェア・エンジンおよび定義ファイルを自動アップデートします。これにより、スパイウェアに対する防御メカニズムを常に最新の状態に保つことができます。
- 最後に、スパイウェアを定期的にスキャンするようにIntegrityを設定します。これにより、ネットワーク・アクセスを許可する時点でスキャンが実施済みであることを保証でき、スパイウェアに対する防御をより確実にすることができます。

結論

企業のネットワーク環境において、スパイウェアを無効化するためには、総合的なエンドポイント・セキュリティ・ソリューションによる複合的な対策が必要です。Integrityは、企業のPCを保護し、機密情報の漏洩を防ぎ、ハッカーによる侵入をブロックすることによって、スパイウェアの主な影響を確実に無効化します。そして、クラス最高のスパイウェア検出および削除機能により、感染マシンからスパイウェアを取り除き、ネットワーク帯域およびPCのシステム・リソースを本来あるべき状態にまで回復させます。最新のスパイウェアの常に一步先を行くためには、アンチスパイウェア・サービスは、リアルタイムのスパイウェア情報を（理想的には信頼できる数百万規模のソースから）入手できる必要があります。Integrityエンドポイント・セキュリティ・ソリューションは、一元的な管理機能、リアルタイムのモニタおよびレポート機能、そしてネットワーク・アクセス・ポリシーの実施機能を提供することにより、スパイウェアの存在しないPC環境を維持できるようネットワーク管理者を支援します。Integrity Anti-Spywareは、スパイウェアの問題を解決するための、エンタープライズ・クラスの統合された防御機能を提供する現在唯一のソリューションです。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおける世界トップ企業として、特に企業向けファイアウォール、パーソナル・ファイアウォール、およびVPNの市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースを保護する、広範な境界、内部、Webおよびエンドポイントに対するセキュリティ・ソリューションのための統一されたセキュリティ・アーキテクチャを提供しています。チェック・ポイントのZoneAlarm製品群は、インターネット・セキュリティの分野で高い信頼性を誇るブランドとして、数々の賞に輝くエンドポイント・セキュリティ・ソリューションを提供し、何百万台ものコンピュータをハッカーやスパイウェア、データの盗難などから保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security)により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界88ヶ国、2200社を超えるパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客にはFortune 100社の全社を含む、何万ものあらゆる規模の企業や組織が含まれています。

©2003-2006 Check Point Software Technologies Ltd. All rights reserved.
Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, NGX, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標、サービス・マーク又は登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の 特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Integrity Anti-Spyware

P/N:501931-J 2006.1

※記載された製品仕様は予告無く変更される場合があります。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500