アナタの知識が会社を救う! セキュリティ強化塾

盗撮に盗聴…端末を"スパイ"に変える「クリープウェア」の恐怖

2014/05/20

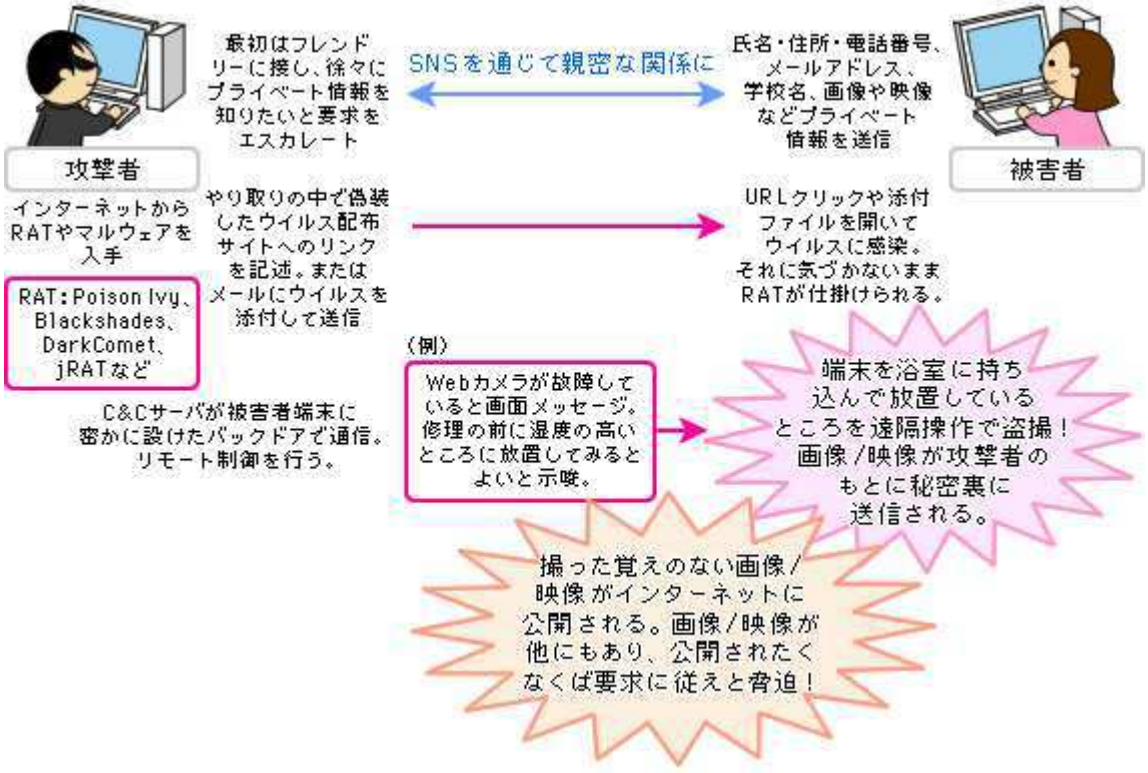
いつの間にか自分のPCやスマートデバイスが「スパイ」になり、カメラやマイクを使って行動を監視する……そんな不気味な出来事が現実のものになっている。こっそりと端末に忍び込み、潜伏しながら端末内やネットワーク上の情報をどこかの誰かに送信する「スパイウェア」が、端末のカメラやマイクを外部からリモート操作する機能を追加しているのだ。そんなウイルスについた名前が「クリープウェア」。その実体は、遠隔操作ウイルスの一種「RAT」だ。BYODが広まる中、個人所有端末がRATに感染すると、社内会議の内容など機密情報が外部に筒抜けになることも想像に難くない。今回は、クリープウェアの特徴とその対策について考えてみる。

端末を思いどおりに操る「クリープウェア」、その手口とは

「クリープウェア」という言葉は昨年から日本でも知られるようになったが、その契機となったのはミス・ティーンUSAとなった女性のプライベート画像をもとにした脅迫事件だった。この女性のFacebookアカウントがハッキングされ、成りすましログインによりパスワードが変更されてログインできなくなったことに気づいたのが事件の顕在化の始まりだった。やがて彼女は自分のアカウントのプロフィール写真が、撮影した覚えのない半裸の写真に変更されていることを発見した。その後しばらくすると「プライベートな画像や映像をばらまかれたくなければ要求を聞け」という脅迫メールが届いた。

ところが女性はこれを拒否、テレビ番組でこの事実を公表した。この勇気ある行動のおかげで、PCの遠隔操作を利用した覗き行為とそれで得た画像／映像による脅迫手口が広く知られることになった。これに類した脅迫行為はかねてから「Sextortion（性的なゆすり/SexとExtortionを意味する造語）」と呼ばれて米国で社会問題化していたが、それにWebカメラなどの遠隔操作の手口が加えられていることが大きな話題になったのだ。こうした端末遠隔操作機能を持つウイルスは「クリープウェア（Creepware）」と呼ばれている。クリープウェアの「クリープ（Creep＝這う）」は「気味の悪い／嫌らしい」といったニュアンスとともに「静かに這いよるもの」といった不気味さも漂わせている。クリープウェアを利用するSextortionは、だいたい図1に見るような構図だ。

図1 クリープウェアを利用するSextortionの手口の例



上図からおわかりのように、これは現在最大のセキュリティ上の脅威となっている「標的型攻撃」と類似している。利用されている不正プログラムは情報窃取用のウイルスおよびリモート操作ツール「RAT（Remote Access ToolまたはRemote Access Trojan）」と呼ばれるウイルスだ。これらを使い、ユーザの不審を呼ばないように慎重に情報窃取やリモート操作を行えば、対象者が決して公開したいとは思わないようなプライバシーに迫ることが可能だ。例えば次のような機能が発見されている。

〈端末機能の遠隔操作〉

- カメラ撮影（画像/動画録画）
- 音声録音
- メッセージの画面表示/音声メッセージ再生
- 端末エラーの発生、再起動
- ファイルやメールの送信
- ファイルのダウンロード

〈情報の窃取/送信〉

- スクリーンショット
- キー入力
- レジストリなどシステム情報
- 端末所有者情報、アドレス帳データなど
- パスワード
- Webアクセス履歴

こうした機能を組み合わせれば、端末内部および端末から手を広げて入手しうるありとあらゆる情報を窃取できてしまう。それだけで不足なら、図に示したように相手の無警戒や知識不足に乗じた「騙しの手口」による行動誘導と遠隔操作による撮影や録音などの能動的な情報窃取も可能だ。

目的がプライバシーの覗き見や個人の脅迫であるとはいっても、もしもウイルス感染した端末が会社に持ち込まれ、会議の場に置かれていたとすれば、機密情報が外部に筒

抜けになる可能性が懸念される。攻撃者はそんな情報を前に方針を変え、企業情報の窃取/売却に走るかもしれない。クリープウェアは従業員の安全だけでなく、企業の情報保護にとっても重大な脅威なのだ。いったいどのように対策していけばよいだろうか。

1 クリープウェアの侵入を防ぐための対策は？

1-1 米・FBIも呼びかけ！「New kid in town」「Justin Bieber」手口に注意

クリープウェアを仕込む動機の1つは強い性的な関心が挙げられる。実際の脅迫で要求されるのは金銭よりもさらに露骨なプライベート写真や映像であることが多いようだ。Sextortion被害を防ぐために、米国FBIは主に年少者に対して次のような事項（意訳）に注意するよう呼びかけている。

- 画像/映像を含めプライベート情報をオンラインサービスに投稿する時は、それが様々なPCや携帯電話、タブレットなど多くの端末に行き渡る可能性があり、取り返しがつかないことに留意して、慎重に行う。
- パスワードは大小文字・数字・記号を組み合わせて推測が困難なものにする。
- アンチウイルスツールを導入して適切に定義ファイルやバージョンを更新する。ただし、その上でも不正侵入されることはあり得るので、安心しすぎてはいけない。
- 端末を使わないときには電源を切る（多くのSextortion被害者はSNSやチャットのためにラップトップ端末を常にONにしている）。
- 知り合いからのメールであることをチェックする前に添付ファイルを開いてはいけない。そこには個人情報や画像などを勝手に盗み出すウイルスが含まれているかもしれない。
- 見知らぬ人とインターネットで会話したり個人情報や画像などを送ったりしない。
- Webカメラを使わないときには覆いをつけて、遠隔操作されても撮影できないようにする。
- 常識外れの時間帯（深夜など）に届くメールやメッセージは、それが親族や友人からのものでも疑う。

●端末が攻撃を受けたことを発見したり、脅迫を受けたりした時には、両親または法的に対応してくれる窓口（日本では警察）に相談する。

またFBIによるSextortion手口の分析によると、犯人は被害者へのアプローチに一種のシナリオを用意し、SNSなどで型どおりにやり取りすることで多くの犯行を成功させているようだ。その典型例の1つは「最近近所に引っ越してきた者だが友達になってほしい」と言って接近する「New kid in town手口」、もう1つは「歌手活動をしている者だが、無料チケットやバックステージパスと写真を交換しよう」と言ってそそのかす「Justin Bieber（動画投稿がきっかけで大成功した歌手。不正行為とは無関係）手口」だ。

これは実際に31歳の男が1人で数百人の若い女性を騙したアプローチ法だ。これを夢見がちな少女相手だから成功した「ベタ」な手口だと笑えようか。恐らく最初のコンタクトに好意的に反応するのは子どもだけではあるまい。その後の会話のエスカレートの仕方が巧みであれば、分別ある大人でも騙されてプライベート情報を渡してしまったり、不用意な行動でウイルスに感染したりすることがないとは言えない。残念なことではあるが、SNSなどで見知らぬ人相手に簡単に個人情報を明かしたり、ファイルのやり取りを行うことは厳に慎まなければならない。そのことを自分の家族、特に子どもには、十分に認識させる必要がある。またISPによるURLフィルタなどが利用できる場合には利用すべきだし、端末を利用する家族は1人ひとりが個別にIDを持ち、安全で堅牢なパスワードを利用するといった対策も大事だ。

このような話題はなかなか企業内研修の場にはなじみにくいが、従業員の家庭を守るためにも、また家庭と会社の両方で利用される可能性があるタブレットなどの端末にクリープウェアが仕込まれることがないようにするためにも、あらゆる機会を捉えて知識を広める努力が望まれる。

1-2　クリープウェアの侵入手口と対策

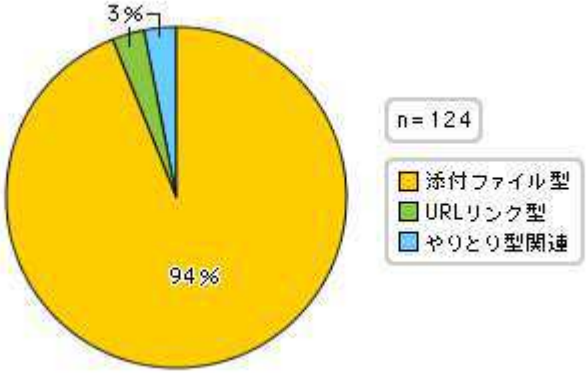
■クリープウェアの侵入手口

クリープウェアが端末に侵入する経路は、メールの添付ファイル、メール本文やSNSメッセージに記載されたURLのクリックが主なものだ。これは「標的型攻撃」の発端となる侵入手口とまったく同様だ。標的型攻撃については本コーナーでたびたび取り上げているので、バックナンバーを参照していただきたい。

【怪しいメールの見分け方】

ここでは標的型攻撃に使われたメールについてのIPAによる分析結果の一部を紹介しよう。まずウイルス感染の種別の割合は、図2に見るように圧倒的に添付ファイルによるものが多い（94%）。URLリンクのクリックを誘い、ウイルス配布サイトに接続させて、アプリケーションなどの脆弱性を悪用して感染させる手口は3%、事前に1～複数回の一般的な問合せなどの内容のメールをやり取りして信用させておいてからウイルス入り添付ファイルを送る「やりとり型」が3%となっている。

図2 標的型攻撃メールで感染を図る手口の割合

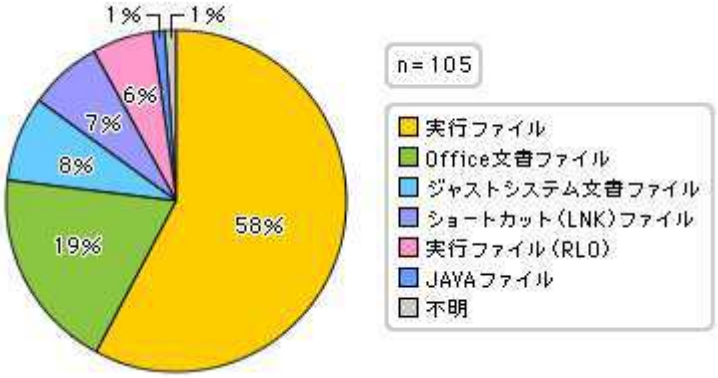


「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

添付ファイルの中味は、図3に見るように、拡張子が「.exe」などになっている実行ファイル形式のものが過半を占め、「.docx」などのOffice文書ファイル形式、「.jtd」などのジャストシステム製オフィスソフトのファイル形式、さらにショートカットファイル形式のもの（後述）が多い。こうした形式のファイルは開く前にウイルススキャンして、さらに差出人に確認してみるとよいだろう。

図3 標的型攻撃メールに添付された不審ファイルの種別割合



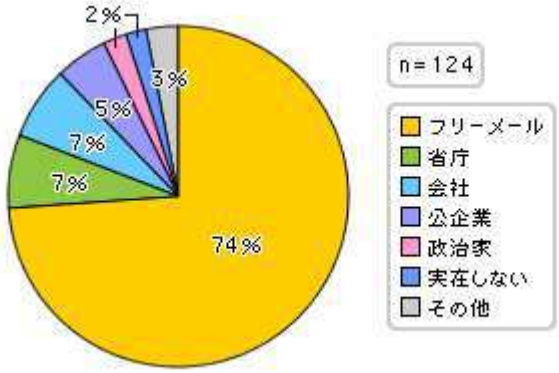
「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

なお、図3で「実行ファイル（RLO）」としているのは、ファイル名の文字並びを右から左に変更する特殊文字（RLO）を挿入して、本来の拡張子を隠蔽／偽装した実行ファイルのことだ。例えば「samplefdp.exe」というファイル名の「sample」の後にRLO文字を入れると「sampleexe.pdf」となる。PDF形式だから大丈夫だろうと開かせることを狙った手口だ。アイコンが通常と違っていたり、プロパティを開いてみるとそのタイトルの文字並びが逆順になっていたりするので、怪しいと思ったら開く前に確認するとよい。

さらにメールヘッダの「From」項に注目したい。メールの差出人として表示されるのは「特定の会社名」「省庁名」「社団法人などの公的機関」「実在する個人名」などが多いが、「From」には差出人や件名、本文内の署名などとは無関係のドメインが表示されているケースが多数を占める。図4に見るように、「hotmail」や「yahooメール」などのようなフリーメールのドメインが74%を占めている。フリーメールで得意先や省庁からのメールが送信されるケースはほぼないので、このような特徴をもつメールの添付ファイルを開いたり、記載URLをクリックしたりする前には、差出人に確認をとることが望ましい。

図4 標的型攻撃メールの「From」欄に表示されるドメイン種別の割合

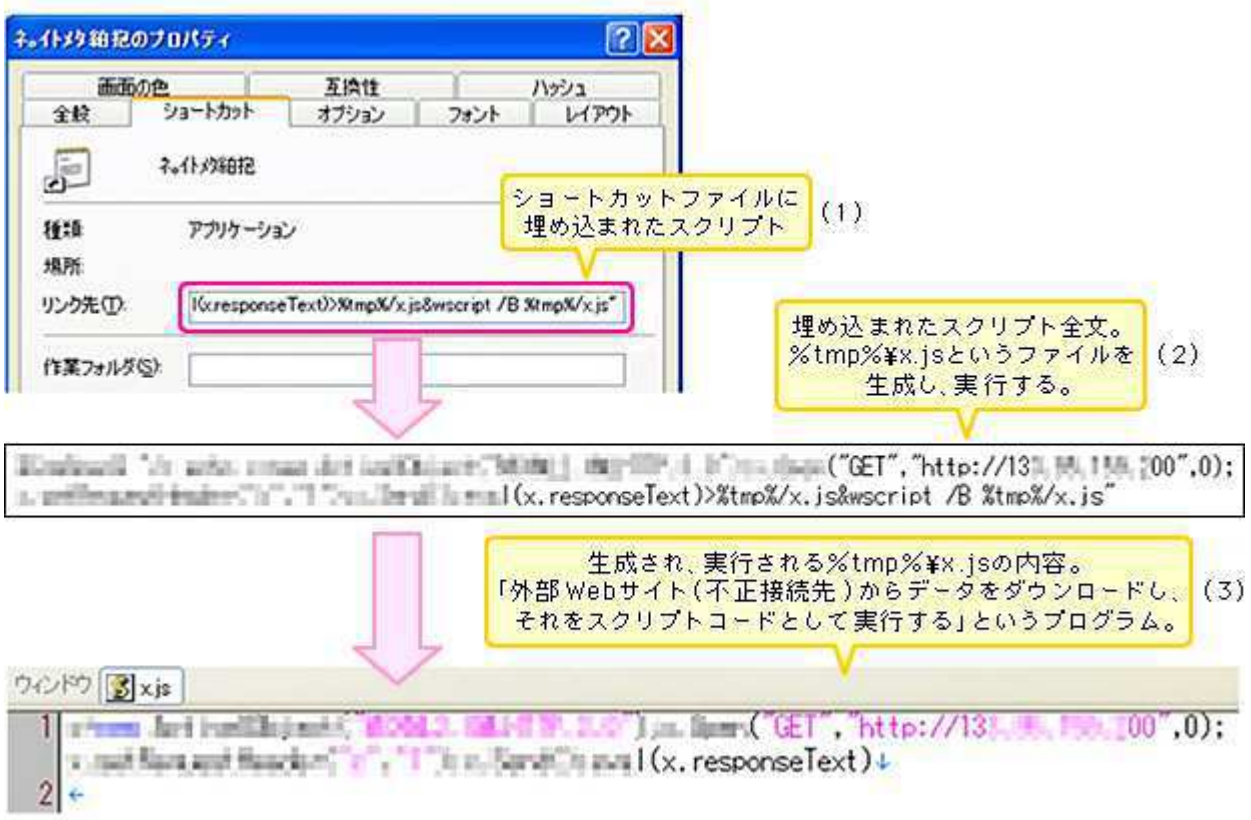


「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

最近はショートカット（LNK）ファイルが使われるケースが目立つ。これはその形式（.lnk形式）のまま、またはzipで圧縮した形式で届く。ショートカットファイルには図5の(1)のようにスクリプトが埋め込まれていて、これを開くと(2)のようにスクリプトが実行され、(3)のようにウイルス配布サイトにウイルスを取りに行くといった一連のウイルス活動が始まる。図6にはショートカットファイルからの感染～RATインストールなどに至る仕組みの一例を示すので、参考にしていただきたい。

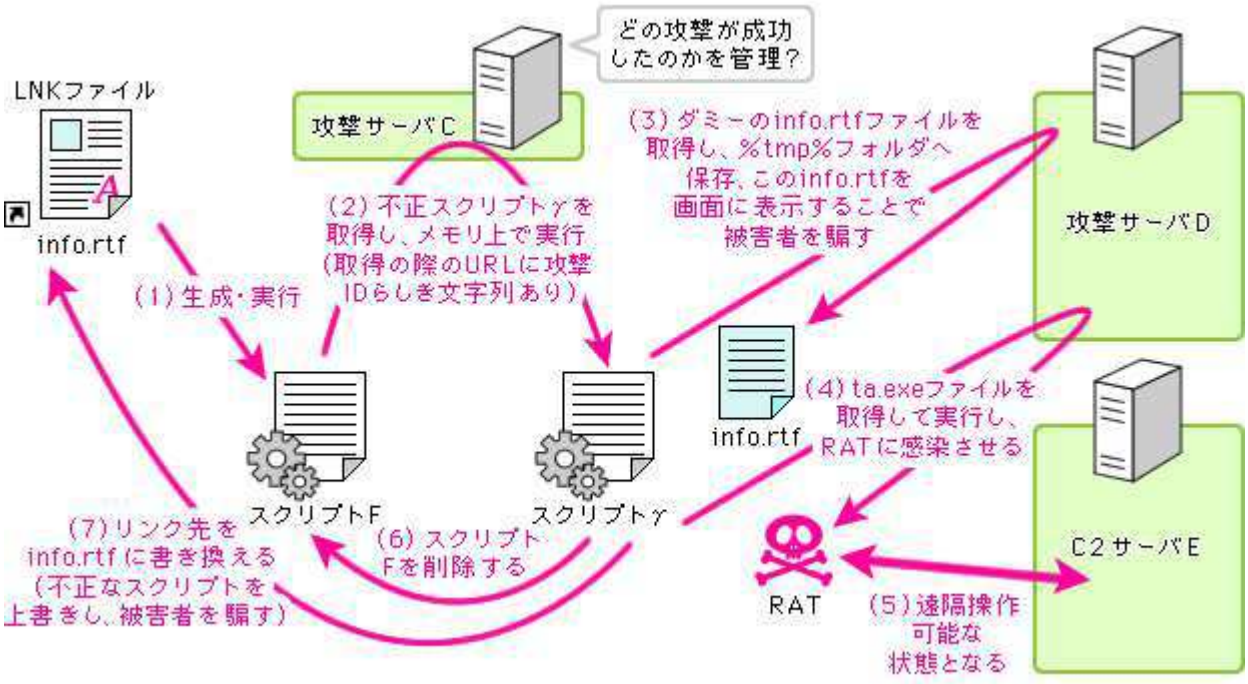
図5 ショートカットファイルを用いたウイルス感染の例



「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

図6 ショートカットファイルからの感染～RATインストールまでの流れの一例



「標的型攻撃メールの傾向と事例分析」2013

資料提供：IPA

SNSメッセージからの感染を防ぐために

メールと同等以上に注意が必要なのがSNSメッセージだ。mixiやFacebookなどで不正サイトへのURLを含むメッセージ投稿例が見つかっている。メッセージの投稿者は「友達」である場合が多いだろうが、実際にはウイルス感染して遠隔操作されている可能性がある。しかし表面上は本当の「友達」からのメッセージと区別がつかない。そこに例えば「ビデオを見てください」「あなたがビデオに映っています」と書かれていたら、その動画の視聴／ダウンロード先として記載されたURLをクリックするのは自然な行動だ。特にyoutubeなどの著名な動画サイトのURLに偽装したものだと、何の疑いも抱かないだろう。

しかしいったんURLをクリックすると「この動画の再生にはプログラムのインストールが必要です」などとメッセージが表示され、その操作をするとウイルスがインストールされてしまう。実際に情報窃取や遠隔操作が可能なウイルスに感染したケースがある。ゲームや動画など、いかにも一般に興味が持たれそうなコンテンツの提供を謳うURLリンクは、まずは疑ってみる慎重さが必要だ。

Webのターゲティング広告からの感染可能性

またWebサイトによく設けられるようになった、ユーザの行動履歴に基づいた「ターゲティング広告」もウイルス感染の原因になりかねない。Webサイトの運営者とは異なる広告業者や広告主がウイルス感染した場合、運営者も気づかないままウイルス配布を行ってしまうことになり、ページ訪問者が感染してしまう。ユーザとしてはターゲティング広告からは可能ならオプトアウトし、リスクを避けることが薦められる。また自社Webサイトでターゲティング広告が必要か否かをよく考え、必要なら、信頼できて損害賠償契約も結べるような業者と契約したいものだ。

■アンチウイルスツールは「統合型」にし、適切な更新を心がける

上掲のFBIの「呼びかけ」が「アンチウイルスツールが効かない侵入がありうる」ことに言及していることに注意したい。現在のウイルスは非常に多様化しており、亜種や新種が大量

に生み出されている状況にあるため、パターンマッチングを利用する従来型のアンチウイルスツールではすべてのパターンを登録・配布することができず、複数のツールを利用していてもいくつかは網をすり抜けてしまうのだ。また脆弱性を狙って感染するウイルスは脆弱性の公開前または公開後間を置かずに発生するものもあり（ゼロデイ攻撃）、パターンファイルが更新される前に感染してしまう危険性もある。

最新のアンチウイルスツールにはパターンマッチング以外に「ヒューリスティック検知」「ふるまい検知」と呼ばれる、怪しい動作をするプログラムを検知して隔離する機能が盛り込まれているものが多くなっている。またウイルスか否かという判断だけでなく安全性を点数で評価する「レピュテーションサービス」も多くのアンチウイルスツールベンダが採り入れ、製品の一部としてサービス提供を行っていて、ウイルスのデータベースにまだ登録されていないウイルスも検知可能だ。古いアンチウイルスツールを利用している場合は、こうした統合型の最新ツールにリプレースするとリスクを低減できる。

またアンチウイルスベンダはインターネットで利用できるオンラインウイルススキャンサービスを提供してもいる。端末へのインストールをせずにそのベンダのウイルス検知能力を使えるので、普段は端末に導入したアンチウイルスツールを適切に更新しながら利用しつつ、定期的に他の複数のベンダのオンラインスキャンを行うのも有効な手立てとなる。

2 クリープウェアの活動の発見と対応

上述のように対策をとってもクリープウェアの侵入は100%は防げない。例えば端末の動作がいつもより遅くなったと感じたら、クリープウェアの活動の影響なのかもしれない。クリープウェアが侵入しているか否か、何か気になることがあった時に、または定期的にチェックしておくとよい。

2-1 端末ではレジストリ、スタートアップ、保管フォルダをチェック

主にチェックするのはOSのレジストリ情報、スタートアップ時の起動プログラム、データ保管用のフォルダだ。これらが正常時、あるいは前回チェック時から書き替えられていたら、その内容を精査し、ウイルス活動の痕跡か否かを判断、もしそうなら、端末を初期化してクリーンインストールすればよい。BIOSにまで感染が拡大している場合にはそれでも退治したことにならない場合はあるものの、メモリやハードディスク内に存在しているクリープウェアなら、巧妙に隠蔽されていたとしてもたいていは退治できる。

以下にウイルスが頻繁に利用するレジストリ、スタートアップ登録先、保存先フォルダの例を上げる。こうした情報は各セキュリティベンダも発表しているので、内容の差分を調べるスクリプトを作成すれば一定の検知効果が期待できる。また変更/追加の有無を追跡できる差分チェックツールも市販または無償提供されているので利用するとよい。

表1 ウイルスが改変/追加するレジストリの例

レジストリ（HKLMまたはHKCU以下）
SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
SOFTWARE¥Microsoft¥Active Setup¥Installed Components¥
SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Winlogon¥Notify¥WPF
SOFTWARE¥SYSTEM¥CurrentControlSet¥Services¥mspool¥Parameters
SOFTWARE¥SYSTEM¥CurrentControlSet¥Services¥mspool¥sdeweggs
SOFTWARE¥rar¥ActiveSettings

「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

表2 ウイルスが改変/追加するスタートアップ登録先

スタートアップフォルダ（Windows7）
%APPDATA%¥Microsoft¥Windows¥Start Menu¥Programs¥Startup
%ALLUSERSPROFILE%¥Microsoft¥Windows¥Start Menu¥Programs¥Startup

「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

表3 ウイルスがよく使う保存先フォルダ

保存フォルダ（%で囲ったものは環境変数を示す）
%TEMP%(%TMP%)
%ALLUSERSPROFILE%
%ALLUSERSPROFILE%¥DRM¥（ランダムな文字など）
%ALLUSERSPROFILE%¥Starter¥（ランダムな文字など）
%APPDATA%
%WINDIR%
%WINDIR%¥system32
%PROGRAMFILES%
%PROGRAMFILES%¥Common Files¥System¥Library
%USERPROFILE%
添付ファイルの保存先や解凍先フォルダ

「標的型攻撃メールの傾向と事例分析」2013年

資料提供：IPA

ただしチェックは一定以上のOS知識がないと難しい。会社支給でIT部門の管理下にある端末の場合、あるいはBYODユーザであっても了解が得られるなら、IT資産管理ツールなどにより端末レジストリ内容やプログラムリストなどをできるだけ自動収集してIT部門で分析するとよい。それが無理なら、せめて業務部門のサーバ管理担当者などにはチェック方法をガイドし、リテラシを上げてもらうことはしておきたい。社内のリテラシ向上が何よりの対策となるからだ。

2-2 サーバやネットワークの監視と安全な設計・運用

サーバの動作状況やファイルアクセスのログ、ネットワークのトラフィックや通信先のログの監視はウイルス活動の証拠をつかむ決め手の1つになる。またDLPツールによる機密情報のポリシーによる利用制限は非常に有効な対策だ。

また本コーナーの今年1月の記事（最新サイバー攻撃と対策）ではシステム設計と運用にかかわる対処法をまとめている。詳細はIPA発行の「標的型攻撃メールの傾向と事例分析〈2013年〉」および「『標的型メール攻撃』対策に向けたシステム設計ガイド」が参考になる。

2-3　不審なプログラムや不正活動の痕跡を見つけたら

攻撃の事実に気づき、ウイルスそのものや活動痕跡を特定したら、まずはIPAに届け出るとともに相談してみるとよい。IPAには個人からの相談を受け付ける「安心相談窓口」と、企業の標的型サイバー攻撃に関する相談を受け付ける「標的型サイバー攻撃の特別相談窓口」がある。メールと電話で相談できるので、クリープウェアなどの発見後の対処法や再感染防止策などのアドバイスを求めてみるとよい。また感染や被害の事実やクリープウェアそのもの（検体）を届け出ることは、自分/自社のみならず日本および世界のセキュリティに対する貢献になる。単一のセキュリティベンダに検体を提供してもそのベンダに利用されるだけで対策が広がらない可能性があるので、公的機関への提出が望ましい。

3　国家資格、情報セキュリティスペシャリスト試験問題にチャレンジ！

Question 1:

送信元を詐称した電子メールを拒否するために、SPF（Sender Policy Framework）の仕組みにおいて受信側が行うことはどれか。

平成22年秋期午前II問題

- ア Resent-Sender:、Resent-From:、Sender:、From：などのメールヘッダ情報の送信者メールアドレスを基に送信メールアカウントを検証する。
- イ SMTPが利用するポート番号25の通信を拒否する。
- ウ SMTP通信中にやり取りされるMAIL FROMコマンドで与えられた送信ドメインと送信サーバのIPアドレスの適合性を検証する。
- エ 付加されたディジタル署名を受信側が検証する。

解答を表示する

取材協力

独立行政法人情報処理推進機構（IPA）　企業サイトへ

この記事を読んだアナタにおすすめします

セキュリティ情報局の最新特集

日本のPOS端末が狙われる？組込みシステムのセキュリティ対策【セキュリティ強化塾】 2015/02/17

セキュリティ面では放っておかれがちなPOS端末や複合機を狙ったウイルス感染が日本でも増加…組込みシステムに潜むリスクとは…

» セキュリティ情報局一覧へ

(C) Recruit Marketing Partners Co.,Ltd.
印刷日：2015/02/24