

セキュリティ最前線 (2008年01月24日号)

目次:

1. 不正プログラムを蔓延させるツールキット..... P.1
2. 進化するツールキット..... P.4
3. どのようにして身を守ればよいのか..... P.6

1. 不正プログラムを蔓延させるツールキット

サイバー犯罪の初期の頃、ハッカーたちは自分たちの評判を高め目立たせるため、注目をひくような不正侵入や情報収集などを行っていました。こうして、Kevin Mitnick や Kevin Lee Poulson、Adrian Lamo といったハッカーたちが、いわば“カウンターカルチャーの有名人”として反抗的でアンダーグラウンドなイメージを高めていったのです。しかし最近では、そうした一匹狼的なハッカーたちに代わって、RBN(Russian Business Network)のような組織化された犯罪シンジケートが、違法コンテンツの掲載、フィッシング活動、スパム送信、不正プログラムの攻撃等を行う不正のサービスネット組織として台頭してきました。

初期のハッカーたちは、金銭だけでなく自分たちの“評判”も求めていました。他方、RBNやその他のシンジケートにとっての活動目的は、単に金銭的利益のみです。また、こうした組織的なサイバー犯罪も、他の一般のビジネスと似たような形で多様化の傾向を帯びてきました。サイバー犯罪活動に関する専門的な知識を、数多くの初心者ハッカーたちに有償で提供することで、自分たちの活動を“ビジネス”として価値を高めてきたのです。

たとえば、2005 年後半、「WebAttacker」というツールキットが、Windows 共通の弱点を利用するツールとして、技術的な知識が低い不正ユーザに販売されました。この「WebAttacker」を利用すれば、Web サイト訪問者にトロイの木馬型ウイルスを組み込む不正な Web サイトを作成することができます。他にも、「MPack」や「IcePack」、「WebAttacker II」、「NeoSploit」等は、さらに危険なツールキットです。これらを利用すれば、無防備な Web サーバや正規の Web サイトを改ざんすることができ、そうして改ざんされたサイトへの訪問者は、不正プログラムに感染してしまうことになります。

不正プログラム関連のツールキットといえば何も目新しいものではありませんが、いわゆる新世代のツールキット

の場合、その使用範囲の柔軟性や広さという点で特徴的です。トレンドマイクロのリサーチ・プログラム・マネージャである Ivan Macalintal は次のように説明します。

「不正プログラム関連のツールキットといえば、ずっと昔、DOS ウイルスのものまでさかのぼることができます。ただし、技術者しか利用できなかったそうした過去のツールキットとは異なり、最近のツールキットは、“スクリプトキディ”と呼ばれる十代のアマチュアプログラマーから専門的な知識を有したサイバー犯罪者まで誰もが利用できます。またこうしたツールキットは、Web 上で流布し、Web ブラウザを使用する誰もが入手できるため、あっという間に蔓延してしまうのです。実際、「WebAttacker」、「Mpack」、「NeoSploit」、「IcePack」、「FirePack」といった最も有名な5つのツールキットが、今日のインターネット上における「Webからの脅威」の主な原因となっていると言っても間違いはないでしょう。」

そうした犯罪用ソフトウェアの開発者たちは、自分たちが作成したツールキットが法的措置の目に留まらないよう注意深く隠してはいます。しかし、サイバー犯罪に関わる者たちにとっては、ハッカー関連の BBS やチャットルーム等から簡単に入手することができるのです。また、組織的に活動するサイバー犯罪者の場合などでは、あたかもオフィスで働く社員にワープロソフトが提供されるように、自分の“上司”からそうしたツールキットの提供を受けることさえあります。

Ivan Macalintal も、サイバー犯罪の内情をオフィス内の業務のように描写しています。「サイバー犯罪者たちは、それぞれ仕切られたデスクで“業務”を行い、あるツールキットが必要になれば、その要求は管理者と財務課へ送られ、今度はそこで目的のツールキットを購入するための“業務”が行われるわけです。」

実際、サイバー犯罪者たちは、不正プログラムのツールキットを用いて、過去に数多くの攻撃を行っています。「イタリアンジョブ」では、6,000 に及ぶ Web サイトが影響を受けましたが、この場合、「Mpack」というツールキットとリモートコンソールプログラムが使用されたと言われています[*1]。サイバー犯罪者は、イタリアの観光関係の Web サイトを改ざんし、「IFRAME」を組み込みました。これにより、サイト訪問者は、まず、トロイの木馬型ウイルスに感染します。このトロイの木馬型ウイルスが実行されると、別のプログラムがダウンロードされます。こうしてダウンロードされた不正プログラムは、感染コンピュータから情報収集を行うわけです。

昨年8月、「The Bank of India」の Web サイトを改ざんしたケースでは、「IcePack」が使用されたと言われています。このケースでは、Web サイトの修復が完了するまでの丸一日の間、サイト訪問者は複数の不正プログラムに感染する状態が続きました[*2]。また、つい最近、2008年1月、「FirePack」というツールキットを利用して、アメリカ NFL チーム、ニューヨーク・ジェッツのファンサイトを改ざんしたケースが発生しました。この場合、アメリカでの NFL シーズン到来に伴うファンサイトへの訪問者数の急増を見越した犯罪でもあります[*3]。

こうしたツールキット利用の大部分は、何も目新しいものではありませんが、そこに潜む危険性は甚大です。それほど巧妙ではなかったサイバー犯罪のほとんども、こうしてツールキットが簡単に入手できることに伴い、巧妙な犯罪が大量に出現することとなります。またその巧妙さゆえ、ほんの僅かの成功率が、甚大な数の Web サイトに被害を与えることになってしまいます。こうして感染した Web サイトは、広範囲に被害を広めるため、無数のコンピュータに存在するセキュリティホールも直ぐに利用され、スパイウェアや不正プログラム、ボット等が組み込ま

れてしまいます。

参照:

*1. Trend Micro, "A Long and Winding Road: Tracking Down the LINKOPTIM Attack,"
<http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VName=A+Long+and+Winding+Road%3A+Tracking+Down+the+LINKOPTIM+Attack>.

*2. Larry Dignan, ZDNet, "Bank of India Site Hijacked, Launching Exploits,"
<http://blogs.zdnet.com/security/?p=487>, August 30, 2007.

*3. Paul Ferguson, Trend Micro, "A Spear in my Heart: Jets Fan Sites Compromised,"
<http://blog.trendmicro.com/a-spear-in-my-heart-jets-fan-sites-compromised/>, January 4, 2008.

2. 進化するツールキット

不正プログラム関連のツールキットが広く蔓延することで、甚大なダメージが引き起こされます。そうしたツールキットが有する潜在能力については十分に認識されていますが、サイバー犯罪に携わる開発者たちは、その潜在能力をさらに引き出そうと努力しています。トレンドマイクロのリサーチ・プログラム・マネージャである Ivan Macalintal は、以下のように述べます。

「こうしたツールキット類は、簡単に修正を加えることができます。そのため、ネットを潜り抜けながら多くの人の手で修正が加えられることによって、ますます強力なものへと成長させることができるのです。器用なハッカーが一人、そこに不正コードを少し追加し、さらにもう一人、それを強化していく。こうして“ネット上のコラボレーション”を通してツールキットは、どんどん巧妙化していき、ついには、誰もが簡単にいつでもサイバー犯罪に利用できる“優れたツールキット”ができあがるというわけです。」

こうした「コラボレーションによる強化」や、「ゼロデイ・ツールキット」、「ロックフィッシング・ツールキット」により、不正リモートユーザたちにとってますます強力な武器となりつつあるのです。

ゼロデイ・ツールキット

最近まで不正プログラムのツールキットといえば、「既に古くなったセキュリティホールへのアクセス方法をサイバー犯罪者に知らせる」というものがほとんどでした。もちろんその場合でも、しっかりとセキュリティホールの修正管理が行われていないコンピュータへの感染には有効ですが、そうでない場合、つまり、正しく修正パッチがほどこされ、セキュリティソフトウェアが更新されているコンピュータに対しては、こうしたツールキットはあまり役に立ちません。しかしながら 2007 年後半、ツールキットは進化を遂げ、極めて危険なツールキットが多くのサイバー犯罪者の手に渡ることとなったのです。

2007 年 9 月、「IcePack」というツールキットがリリースされました。これは、ゼロデイ攻撃、すなわち、まだセキュリティ業界でも知られていないセキュリティホールを暴く機能を有したツールなのです[*4]。ゼロデイ攻撃は、まだ知られていないセキュリティホールを狙った攻撃です。セキュリティ関連企業やソフトウェア開発企業から修正措置が提供されていないため、サイバー犯罪者たちはここを利用して不正活動を行うことができます。

このときのゼロデイ攻撃は、「DirectX SDK」のセキュリティホールを利用したものでした。幸い、最小限のダメージですみましたが、「IcePack」の開発者は声明を発表しています。こうしたことから、この種のツールキットも「修正パッチを施しておけば大丈夫」という“たいしたことのない脅威”などと言って無視することができなくなりました。実際、2007 年 11 月、「Quicktime 7.3」の「RealTime ストリーミングプロトコル」のセキュリティホールを利用した攻撃でも、ゼロデイ・ツールキットが使用されました[*5]。

ロックフィッシング・ツールキット

2007 年 8 月、アメリカ国税庁 (IRS: Internal Revenue Service) から多くの消費者にメールが送信されました。内容は、メール内のオンラインフォームに記入すれば税金の払い戻しができるというものでした。実際、メール内の

リンクをクリックすると、アメリカ国税庁とは何の関係もない偽のオンラインフォームにリダイレクトされ、そこに記入した情報が収集されるというものでした。

一見すると、これは、特定の権威を装ったフィッシング行為の典型的な例のようにも見えます。信頼のおける相手からのメールと見せかけて偽のサイトで情報を入力させるという手口です。さらに詳しく見てみると、アメリカ国税庁を装ったこのサイバー犯罪の場合、いわゆる“ロックフィッシング”というツールキットを利用していることが分かります。

他の不正プログラム関連のツールキットと同じく、この「ロックフィッシング・ツールキット」も、技術が低いサイバー犯罪者たちに低価格(約 1,000 米ドル以下)で提供され、大いに利用されているのです。「ロックフィッシング (Rock-phishing)」とは、偽サイトのドメイン名を次々に作成していき、矢継ぎ早に URL リンクを提供していくことで、アンチ・フィッシングの対抗策を逃れようとする手口のことです。今回のアメリカ国税庁の場合、16 の異なった URL やドメインによるリンクが使用されました。そのいくつかは以下のようなものです[*6]。

- ・ <http://www.<省略>ton.com/bridge/feedback.php>
- ・ <http://<省略>tack.net/catalog/images/awstats/.stats/.secure/.server/.refund/login.html>
- ・ <http://<省略>ab.hoseo.ac.kr:8080/Refund.html>
- ・ <http://www.<省略>ho.ch/Tcho.chindex/jpg/not.php>
- ・ <http://www.<省略>-let-go.net/gallery/include/help.php>

たった 1 つのフィッシングで 16 もの URL を識別してアクセスを終了させなければならないことで、セキュリティ企業の対応は遅れてしまいます。このため、セキュリティ製品のアップデートのみに頼っている個人ユーザや企業も、その分いつもより長く危険にさらされることになるわけです。

このロックフィッシングは新しい手口というわけではありませんが、この手口が低価格のツールキットで何千というサイバー犯罪者の手に簡単に渡ることができるという点で、トレンドマイクロもこのケースがこれからの数ヶ月の間に増加するだろうと予想しています。

参照:

*4. Gregg Keizer, InfoWorld, "Hackers update malware tool kit with zero-day code,"
http://www.infoworld.com/article/07/09/11/Hackers-update-malware-tool-kit_1.html,
September 11, 2007.

*5. Rommel Garcia, Trend Micro, "QuickTime Player Gets Exploited Via RTSP,"
<http://blog.trendmicro.com/quicktime-player-gets-exploited-via-rtsp/>, November 28, 2007.

*6. Roderick Ordoñez, Trend Micro, "PhishIRS Cast Their Net Anew,"
<http://blog.trendmicro.com/phishirs-cast-their-net-anew/>, November 15, 2007.

3. どのようにして身を守ればよいのか

不正プログラムやロックフィッシング・ツールキット等の低価格化により、その利用範囲は明らかに拡大してきています。こうした点からもトレンドマイクロでは、2008 年は「ツールキット利用による攻撃」が確実に増加するだろうと予想しています。非常に多くの感染報告がなされている中、一般ユーザや企業において、感染を引き起こすセキュリティホールが確実に増大していることを念頭にセキュリティ管理に努めなければなりません。ゼロデイ攻撃が増加している今日、100%安全なコンピュータなどは無いとさえ言えるでしょう。そうした中でも、ちょっとした操作上の注意、防御に関するアプリケーションの適切な利用等により、被害を最小限に抑えることができます。

ツールキット自体は新しい脅威ではありませんが、それはむしろ、脅威を増大させ、セキュリティホールをどんどん暴いていく“先導者”といえるものです。このため、個人ユーザや企業にとって最も大事なことは、以下のようなセキュリティ対策を正しく継続的に怠らず取り組むということです。

各種ソフトウェアのアップデート

コンピュータにインストールされているソフトウェアのセキュリティパッチは常に最新化してください。また Web ブラウザに関しても旧バージョンを使用している場合は、直ちに IE (Internet Explorer) 7 や Mozilla Firefox 2 等の最新版にアップデートしてください。特にこの二種類のブラウザに関しては、最新バージョンにアップグレードすることでセキュリティ面も大幅に向上させることができます。

インスタント・メッセージやその他のインターネット関連のアプリケーションは、特にセキュリティホールに弱いものです。直ちにアップグレードを行うことです。また、Web ブラウザやオペレーティングシステムでも「自動更新」を有効にしておき、セキュリティアップデートも常に最新のものをダウンロードしてインストールしておくことです。また企業でも、使用中の各種アプリケーションを積極的に確認し、バージョンごとに準拠したセキュリティ対策を確認しておく必要があります。

ユーザとしては、コンピュータ内に入ってくる全てのファイルなどのスキャン機能等を備える、可能なかぎり総合的なスパム対策・ウイルス対策・スパイウェア対策機能を導入し、より積極的に「Web からの脅威」に対応した製品を利用すべきです。上述のようなフィッシング攻撃やゼロデイ攻撃が増加することを見越して、これらのプログラムを最新定義ファイルへアップデートさせることはたいへん重要です。

こうした様々な脅威がもたらされる“セキュリティホール”を閉じておくためにも、「ウイルスバスター2008」のようなセキュリティ対策製品の利用をお奨めします。最近のセキュリティ対策製品では、従来のような「ダウンロードによる最新化」を行うだけではなく、「オンラインデータベース」を利用します。ユーザは、ネットワークに接続して作業する機会が増えましたが、ネットワーク上には最新の脅威が待ちかまえています。オンラインデータベースの利用は、ユーザのアップデート状況に依存せずに、最新の脅威に迅速に対応することができるようになります。

セキュリティ関連情報に精通すること

トレンドマイクロのリサーチ・プログラム・マネージャである Ivan Macalintal は次のように説明します。「インターネッ

トとは安全な場所ではないと知ることが、何よりも大切な最初の一步です。同時に、どのように安全でないのか、なぜ安全でないのかを知ることも必要です。」

一般的な良識をもって信頼のおけるセキュリティ対策を行うことが最善策ではありますが、同時にこれらの関連情報に精通することで、「特にどの対策を行うべきか」を知る手助けにもなります。そのために、一般ユーザは、セキュリティ関連技術の雑誌類や、セキュリティ関連企業のブログやニュースにも目を通して、「既存の脅威は何か」、「新たに登場した脅威は何か」ということについても、よく知っておく必要があります。

「Trend プロテクト」による Web サイトの評価サービスも、一般ユーザが様々な Web サイトを閲覧する前にそれらのセキュリティ情報を知ることができ、こうした疑わしい Web サイトへのアクセスを回避することが可能になります。企業の場合、こうした情報に精通する機会を「社員必須のセキュリティ関連研修」等として実施することが有効でしょう。

- ※ セキュリティ最前線は、米国トレンドマイクロで発行しているニュースレター「*First Line Of Defense (FLOD)*」(英語)を元に翻訳したものです。
- ※ お申し込み:「*F.L.O.D. Threat Watch Newsletter Signup*」(英語)
<<http://us.trendmicro.com/us/newsletter/>>