ASIS INTERNATIONAL
Advancing Security Worldwide®
055 JAPAN

ISSA 東京支部長　米澤　一樹

ASIS インターナショナル日本支部便り

月次セミナー　6月度　「PowerShell と Windows セキュリティ」

6月の月次セミナーは、Tyson Kopczynski（タイソン・コプチェンスキー）氏による「PowerShell と Windows セキュリティ」です。

（講演中の Kopczynski 氏）

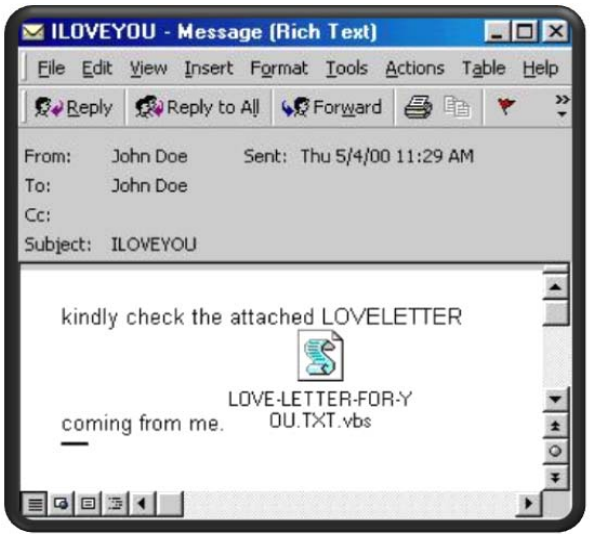
Tyson Kopczynski 氏は、情報セキュリティの専門家であり、特に Windows 関連では「Windows PowerShell Unleashed」の著書もあります。また、「Microsoft Internet Security and Acceleration (ISA) Server 2006Unleashed」、「Microsoft Windows Server2008 Unleashed」への寄稿もしています。

現在は Convergent Computing にてコンサルタントの仕事をする傍ら、マイクロソフトの次世代セキュリティ技術・自動化技術へのフィードバックなども積極的に行っています。

講演では、マイクロソフト製品に使用されていた自動実行の仕組みである Windows Script Host が、Windows の脆弱性を構成してきた経緯と、それを解決するために開発された PowerShell の仕組み、及び、Windows の最新バージョンにおけるセキュリティ対策について詳細に触れました。以下はその概要です。

■I love you ウイルスの与えた衝撃

I love You ウイルスは全世界の 5000 万台以上の PC に感染するという広範囲な被害をもたらし、それゆえに、マスメディアを騒がせた史上初のウイルスとなりました。



（I love you ウイルスを送信してきたメール）

マスメディアがウイルスに注目したことは、一般の方々の関心をひきつけたことにおいて非常に大きな意味を持ちますが、このウイルスは同時に、次の特記すべき事柄を引き起こしました。

それは、インシデント・レスポンスやマネジメント

への取り組みを後押ししたことと、そして、それまでは潜在的脅威であった Windows Script Host の欠陥を明示したことです。

特に後者はマイクロソフト社に大きな衝撃を与え、後に同社がセキュリティ対策に真剣に取り組むきっかけとなりました。

■Windows Script Host の問題点

Windows Script Host(以 下「 WSH 」) は 、Windows 上での自動実行機能を実現するためにWindows98 以降のバージョンに実装されましたが、利便性を追求した結果としてセキュリティがなおざりにされた形になっていました。

最も端的な例として、アプリケーションが素早く簡単に他のアプリケーションのコンポーネンツを使用できたことが挙げられます。これは、I love you ウイルスだけではなく、それ以外の不正プログラムが侵入する際に悪用されました。さらには、WSH によるスクリプト実行を限定したり WSH の機能そのものを使えなくすることが、簡単にはできなかったことなどが挙げられます。ちなみに、ユーザのダブルクリックによるスクリプト実行が限定できなかったことも、I love you ウイルスが蔓延した要因の一つです。

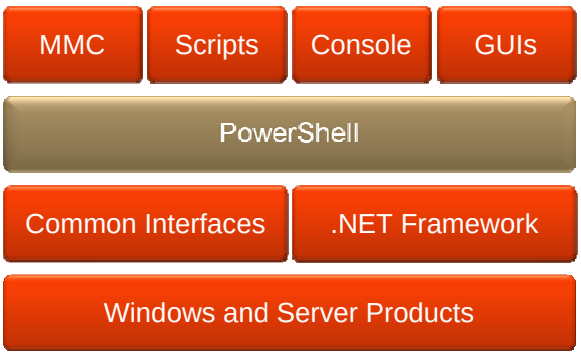
講演者は当時の状況を「ドッコムにおける西部開拓時代（の無法地帯）」と表現していました。

WSH の機能を使えなくすることで一定レベルのセキュリティが確保できたのは事実ですが、それは、同時に、使えなくてはならない機能が使えなくなるリスクをともなっていました。そして、当時は、システム管理者ですら WSH の機能を OFF にする方法を一般には知りませんでした。当時、講演者は「WSH を OFF にする方法」についての質問をシステム管理者からしばしば受けていたそうです。

これらの事柄が明らかになった時、マイクロソフト社は設計段階からセキュリティを考慮に入れた自動実行の環境を作る必要性を認識し、PowerShell の開発に着手しました。

■PowerShell

PowerShell は、Windows における自動実行の統合環境として開発されました。2006 年に最初のバージョンがリリースされ、NET フレームワークに組み込まれました。セキュリティだけではなく、使用や学習が容易にできるように考慮されているのも特徴です。



（PowerShell の概念図）

統合自動実行環境として、Windows 上のあらゆる処理について GUI を使用せずに行うことができるようになっています。PowerShell がリリースされるまでは、処理によって異なるインターフェースを使い分ける必要があり、これがシステム管理者の負担を増やすと共に、見落としなどによる脆弱性を作りこむ原因にもなっていました。PowerShell では、全ての処理を PowerShell のライブラリを呼び出して行うことができるので、開発者やシステム管理者は複数のインターフェースを使いこなす必要が無くなり、作業の管理が容易になりました。

PowerShell は、既に Exchange Server 2007・2010、System Center Operations Manger 2007、SQL Server 208、そして、Windows Server 2008 に組み込まれています。また、多くのソフトウェアベンダーも PowerShell を用いて製品の開発を行っています。そして、現在開発中の PowerShell Version 2 は、Windows 7 と Windows Server 2008 にはアン・インストールが不可能な必須コンポーネンツとして組み込まれます。

■PowerShell におけるセキュリティ対策

セキュリティを設計段階から考慮に入れた PowerShell には、様々なセキュリティ対策が組み込まれています。代表的なものとして、講演者は、1)ダブルクリックによるスクリプト実行が行えなくなったこと、2)信頼できる発行元からの電子証明書によって署名されていることがスクリプト実行の条件とできること、そして、3)実行にあたっては同一ディレクトリのスクリプトを呼び出さなくてはならないこと、の 3 点を挙げていました。以下に各々の詳細を説明していきます。

ダブルクリックによるスクリプト実行が行えなくなったことにより、I love you ウイルスのような不正プログラムをユーザがうっかり実行して侵入させてしまうことがなくなりました。

また、信頼できる発行元からの電子証明書によって署名されていることを実行の条件とすることで、当該のスクリプトが署名された時点からは変更されていないことが証明できます。そして、電子証明書によって発行元、ひいては、作成者を特定することができ、それによってスクリプトが安全なものかどうかを実行する人が判断することができます。ここで、講演者はスクリプトに対する署名が簡単にしかし確実に行えることを実際にデモで見せてくれました。

最後に、同一ディレクトリからスクリプト呼び出さなくてはならなくなったことにより、不正プログラムが行っていた相対パスを使用した不正なスクリプト実行を防ぐことができるようになりました。

■Windows 最新版のセキュリティ

2008 年の RSA カンファレンスでマイクロソフト社は「End-to-End Trust」という概念を提唱しました。これは、信頼できるコンピューティング環境の実現のためには、ソフトウェアだけではなくハードウェアやデータ、そして、人々までも然るべき環境において認証される必要があるというものです。そのような環境を実現するためには、技術的な要件だけでなく、社会的、政治的、経済的、その他の要件が必要ですが、それゆえに新たな前進を行うことができると主張しています。

講演者は、上記の提唱と最新版の Windows におけるセキュリティ技術との関係を Windows Vista と Windows 7 ベータ版における技術的な実装例を挙げて解説しました。そして、特に、Windows Vista での極度にコンセプトに忠実な実装がもたらした弊害が Windows 7 では大幅に改善されていることを強調しました。

講演後の質疑応答では、SE Linux などの他の OS との比較や、上記の提唱がもたらす社会的影響などについて活発な議論が行われ、それは、懇親会の場でも続きました。

以上、Tyson Kopczynski 氏によるセミナーでした。

7月のセミナーでは、ハネウェルジャパンの岩ヶ谷弘明氏に話していただきます。

■ ASIS インターナショナル日本支部の月次セミナーへのお誘い

ASIS インターナショナル日本支部は、月次セミナーを開いています。産業セキュリティに興味がある方ならどなたでも参加できます。お申し込みはホームページから！

■ 開催日

毎月第三火曜日 午後 6 時半より

■ 場所

国際文化会館（六本木）

東京都港区六本木 5-11-16

TEL: 03-3470-4611

http://www.i-house.or.jp/jp/ihj/access.html

■ 参加費

2,000 円（ASIS 会員・非会員同一料金）

このコーナーへのお問い合わせや入会お申込みは
ASIS インターナショナル日本支部 事務局まで

〒101-0021 東京都千代田区外神田 2-2-17
日本保安人事株式会社内
TEL 03-3255-3468 FAX 03-3258-7630
E-Mail info@asis-japan.org
www.asis-japan.org