エクスプロイトキットは消え行く運命にあるのか？
エフセキュアの最新「脅威レポート」の答えは「YES」

「脅威レポート
2015年」は、Flashエクスプロイトの終焉を予想/マクロマルウェア復活をはじめとする、2015年におけるグローバルなトレンドとイベントを解説

エフセキュア株式会社（本社： 東京都千代田区、カントリーマネージャ
キース・マーティン）は、エフセキュア（F-
Secure、本社：ヘルシンキ）の新しい「脅威レポート 2015年」を公開しました。
同レポートは、2015年中に消費者や企業を襲ったグローバルなサイバー脅威のトレンドおよびイベントについて詳述されており、最も目立った脅威であるエクスプロイトキットは、ビジネスモデルの崩壊に直面しています。

◆エクスプロイト破滅のシナリオ

昨年のマルウェアにおいて目立ったのは、AnglerおよびNuclearエクスプロイトキットでした。いずれも、主流となっている他のエクスプロイトキット同様、主にFlashの脆弱性を悪用して不正行為をするものです。しかし、エフセキュアのセキュリティ研究所であるF-Secure
Labsにおいてセキュリティ・アドバイザーを務めるショーン・サリバンは、このレポートの中で、Google ChromeブラウザはFlashのサポートを打ち切り、Mozilla
FirefoxとMicrosoft
Edgeも後に続くだろうと予想しています。サリバンは、2017年の春までには、エクスプロイトキット作者にとって、Flashはもはや、不正行為の成果を産むものではなくなると予想します。

この10年間、最も一般的なマルウェアの媒体の1つであったエクスプロイトは、セキュリティホールをすり抜けるという目的を達成するために、古いバージョンのソフトウェアを必要とします。しかし、そうしたソフトウェアは、見つけるのがますます難しくなるだろう、とサリバンは述べます。たとえば、HTML 5の「do it

all」機能により、サードパーティのブラウザプラグインは、ほとんどその必要性がなくなりつつあります。また、最近のブラウザは、ユーザーが何もしなくても自動的にアップデートされるため、ユーザーは常に最新バージョンを使うようになっています。
他のプログラムからも、あまり多くの不正行為の成果は望めません。マイクロソフトのソフトウェアは以前と比べてはるかにセキュアになっており、パッチの公開も非常に迅速です。アドビのソフトウェアは、個々のマシンにローカルに置かれるのではなく、クラウドベースへと着々と変わっています。また、ブラウザ開発者は、Javaの使用に制限を加えました。不正行為者にとって、もはや新たな成果が見当たらないとしたら、エクスプロイトキットはどうなるのでしょうか。サリバンは述べます。「うまくいけば、滅びます。マルウェアにおいて、ビジネスモデルが崩壊する最初のケースとなるかもしれません。そうでなければ、ブラウザにターゲットを絞るかもしれません。しかし、そのためにはゼロデイ脆弱性を見つける必要があります。」

◆マクロマルウェアの復活

エクスプロイトキットはやがては衰退に向かっていくようですが、コモディティ化されたマルウェアサービスによって、メール添付ファイルをベースにしたマルウェアスキームが利用されるケースは増えるだろうとレポートは予想しています。そのようなスキームの1つがマクロマルウェアであり、それは2000年代前半から長らく影を潜めていましたが、2015年に復活しました。
マルウェア作者は、Officeのマクロ機能を使って、メールに添付したドキュメントに悪意のあるコードを埋め込みます。マイクロソフトはOffice
2003で、マクロを自動実行できないようにデフォルト設定を修正しました。そのため、攻撃はかなり難しくなっています。しかし、最近のマクロマルウェアは、マイクロソフトのデフォルト設定をかいくぐるために、ドキュメントを開いたときに、ユーザーがマクロを有効化する必要がある「保護された」ドキュメントであると主張する文言を表示するようになっています。

◆エフセキュアの「脅威レポート 2015年」における、
その他の注目すべき重要項目

*
警察を装ったランサムウェアは減少したものの、暗号化型ランサムウェアは活動の増加が見られる
* マルウェア全体のうち、ワームの占める割合は、前年の10%から18%へと増加
* The
Dukesというサイバー諜報組織が、幾年間も、マルウェアを使用してロシア連邦のために機密情報を収集している件に関する報告
* 様々な国および地域がそれぞれに直面している最も顕著な脅威
* Windows、Mac、およびAndroidオペレーティングシステムに対する上位の脅威
*
サイバー攻撃がどのようにしてデバイスおよびネットワークを侵害するかを説明する、ユーザー中心モデル、CoC（Chain of Compromise：脅威の連鎖）を通して見た最近の脅威
* 2015年の上位エクスプロイトキットに利用された上位の脆弱性

.....
※「脅威レポート
2015年」の全文を、エフセキュアのウェブサイトから無料でダウンロードできます。
英文レポートhttps://business.f-secure.com/threat-report-malware-the-dukes-and-how-

systems-become-compromised/
和文レポートhttp://jp.business.f-secure.com/「脅威レポート」：-マルウェア、the-dukes、システムは/

※同レポートに関連するF-Secure Labsセキュリティ・アドバイザーのブログもご参照ください。
「マルウェア、The Dukes、システムはどのようにして侵害されるか」
As Cyber Threats Die, Old Attacks Re-emerge
http://safeandsavvy.f-secure.com/2016/03/10/as-cyber-threats-die-old-attacks-re-emerge/
.....

■エフセキュアについて

https://www.f-secure.com/ja_JP/
エフセキュアは、オンラインセキュリティおよびプライバシー保護を提供するフィンランドの企業です。エフセキュアの製品は数多くの受賞実績があり、クライムウェアから企業へのサイバー攻撃にいたる全ての脅威から人々と企業を守ってきました。現在、世界40か国以上、6,000以上のパートナーが販売しており、また、200以上のクラウドサービスでも提供されています。「Switch on
freedom」をスローガンに掲げ、全世界の人々が安全に“つながる”ことができるよう支援することを使命としています。エフセキュアは、1988年に創業し、NASDAQ OMX Helsinki Ltdに上場しています。エフセキュア株式会社は、エフセキュア社100%出資の現地法人として1999年に設立され、以降、増収を続けながら順調に企業規模を拡大しています。
