レポート

McAfee®
An Intel Company

McAfee® Labs 2014 年の脅威予測

目次

1: モバイルマルウェアがマルウェア市場全体の技術革新および攻撃件数の増加を牽引

2013 年の新しいモバイルマルウェアの出現数の増加率は、PC をターゲットにした新しいマルウェアの増加率をはるかに上回り、その大半は Android プラットフォームを標的としていました。過去直近の 2 四半期（2013 年 7 月～ 12 月）の新しい PC マルウェアの増加はほぼ横ばいでしたが、新しい Android マルウェアのサンプルは 33% 増加しました。

McAfee Labs では、この傾向が 2014 年も継続すると予測しています。増加率だけではなく、被害の面でも大きな話題となるでしょう。Android を狙った全く新しいタイプの攻撃が見られると予測しています。モバイルデバイスを狙い、重要なデータを暗号化する最初の本格的なランサムウェア攻撃が見られる可能性が高いです。この攻撃では、人質になった情報を解放する条件として、通常の通貨や Bitcoin などの仮想通貨による支払いが要求されます。また、多くのデバイスに搭載されている近距離無線通信（NFC）機能の脆弱性が狙われる可能性もあります。この攻撃が実行されると、正規のアプリが破壊され、ユーザーに気づかれることなくデータが盗み出されます。

また、企業のインフラを狙うモバイルデバイスへの攻撃も登場するでしょう。モバイルセキュリティ技術が相対的に未熟であるだけでなく、BYOD（Bring-Your-Own-Device）の普及も攻撃に拍車をかける結果となっています。知らないうちにダウンロードされたマルウェアが会社のネットワークに侵入し、機密データを盗み出す可能性があります。BYOD が今後も増加することを考えると、企業は被害者にならないよう、包括的なデバイス管理ポリシーとソリューションを配備し攻撃を回避する必要があります。

2: 仮想通貨により、世界中ランサムウェアによる攻撃が悪質化

被害者のデバイスにあるデータを暗号化するランサムウェアによる攻撃は以前からありましたが、これまでは、犯罪者が利用する決済機関に対する捜査や法的措置で攻撃の阻止に成功してきました。

CryptoLocker のダイアログボックス

仮想通貨の普及は経済活動に恩恵をもたらしていますが、サイバー犯罪者も同様の利益を得ています。被害者から金銭を盗み出すための決済インフラには何の規制もなく、匿名での利用が可能です。メリットがある限り、CryptoLocker のような攻撃は今後も増加すると予想されます。また、重要な会社のデータ資産を暗号化すると騙し、企業を脅迫する新しいランサムウェアによる攻撃も見られることでしょう。

個人や企業にとって幸いなことに、ランサムウェアのペイロードは固有ですが、配布方法（スパム、ドライブバイダウンロード、感染アプリなど）はそうではありません。エンドポイントとネットワークの両方で常に最新のマルウェア対策を利用していれば、このような攻撃を受ける可能性はかなり低くなります。個人でも企業でも、バックアップシステムを効果的に使用することで、ランサムウェアがもたらす被害を回避することができます。

3: スパイ対スパイの攻防が続くサイバー犯罪およびサイバー戦争の世界では、犯罪者集団と政府関係者が、これまで以上に特定・阻止が困難な新しいステルス攻撃を仕掛けるように

情報セキュリティソリューションの進化に伴い、これらの防御を回避しようとするサイバー犯罪者の動きも複雑さを増しています。企業のデータセキュリティ戦争の最前線では、高度な回避技術を駆使した攻撃が発生しています。2014 年は、サンドボックスに対応した回避技術が広まる可能性があります。サンドボックス技術を回避するために、保護されていないデバイス上でのみ攻撃プログラムを全面的に展開する攻撃など、セキュリティに対する高度な回避方法が幅広く採用されるようになるでしょう。

その他にも、正規のアプリケーションに悪意のある動作をさせる目的のプログラミング攻撃、標的を壊滅した後に証拠を隠蔽する自己削除型のマルウェア、官民のインフラを標的にして専用の産業用制御システムを狙う高度な攻撃が含まれます。

政治的動機に基づく攻撃が、特に、2014 年ソチ冬季オリンピック（2 月）やブラジルで開催される FIFA ワールドカップ（6 月～ 7 月）を中心に引き続き増加し、ハクティビストは政治的信念を広める好機と利用するでしょう。

企業の IT 部門はこのような新たな攻撃手法に対して対応し、世界的な犯罪者集団によって容易に打破されないセキュリティ対策を講じる必要があります。

4: 2014 年末までに「ソーシャル攻撃」が一般化

ソーシャルプラットフォームを狙う攻撃は、Facebook、Twitter、LinkedIn、Instagram などの大規模なユーザーベースが標的となります。Koobface などの以前のマルウェアと同様に、これらの攻撃ではソーシャルプラットフォームを配布手段として利用することになるでしょう。ただし、2014 年には、ソーシャルプラットフォーム独自の機能を利用して、ターゲット広告や仮想世界または実世界の犯罪に利用可能なユーザーの連絡先、位置情報、またはビジネスに関するデータを収集する攻撃も見られるようになると予測されます。

このプラットフォームに対する攻撃でよく見られる手口の一つは、ユーザーの認証情報を盗み出し、無警戒な友人や同僚の個人データを収集するものです。Facebook、Google、Yahoo などから 200 万を超えるパスワードを盗み出したボットネット「Pony」[1] は氷山の一角にすぎません。Facebook の推計によれば、5,000 万件から 1 億件の MAU（月間アクティブユーザー数）のアカウントが複製され、登録済みの MAU のうち最大 1400 万件は無効なアカウントと見ています。Stratecast の最近の調査によると、ソーシャルメディアユーザーの 22% はセキュリティ関連の被害を受けています [2]。

民間企業も公的機関も、直接あるいは第三者を介して競合他社や競争相手を対象としたソーシャルプラットフォームへの攻撃を利用するようになるでしょう。2013 年は、官民を問わず知名度の高い組織がこのような攻撃の標的にされました。2014 年はこのような攻撃の頻度や被害が増加すると予想されます。

2014 年はユーザーを騙して個人情報や認証情報を開示させる攻撃も増加するでしょう。よくある手口は、パスワードのリセットを指示する緊急の依頼です。実際にはパスワードをリセットすることはなく、ユーザー名とパスワードを入力させて、その情報を利用してアカウントにログインし、ユーザーや連絡先などの個人情報を収集するものです。

ソーシャルプラットフォームに対する攻撃やなりすましを阻止するには、個人も企業も、ソーシャルメディアプラットフォームでの利用で個人情報が盗まれないように、ポリシーやソリューションを配備して警戒する必要があります。

5: OS の脆弱性をターゲットにする新たな PC およびサーバー攻撃が登場

多くの犯罪組織がモバイルデバイスに目を向ける一方で、PC やサーバープラットフォームを狙う犯罪者も引き続き存在します。2014 年に見られる新しい攻撃は、単に OS を攻撃するだけでなく、OS の上位層や下位層に存在する脆弱性を利用します。

2014 年、PC に対する攻撃の多くは HTML5 対応アプリケーションの脆弱性を利用します。HTML5 は対話機能、パーソナライズ機能、プログラマー用のリッチ機能を Web サイトに組み込むことが可能ですが、新たな攻撃を受ける可能性もあります。研究者の多くは、HTML5 でブラウザーの履歴を監視し、ユーザー固有の広告を表示する方法をすでに確認しています。HTML5 で作成するアプリケーションの多くはモバイルデバイス向けのため、ブラウザーのサンドボックスを回避し、デバイスやサービスに直接アクセスできるようにする攻撃が見られると予測されます。また、業務用のアプリケーションを HTML5 で作成している企業も少なくありません。これらのアプリが使用するデータの流出を防ぐには、新しいシステムに最初からセキュリティを組み込む必要があります。

記憶域スタックといった OS に関連する脆弱性や BIOS を狙ったサイバー攻撃が増えるでしょう。企業環境でこのような下位層の攻撃を回避するには、ハードウェア支援型のセキュリティ対策を導入し、OS の下位層で保護対策を実行する必要があります。

6: 脅威の進化により、検出と性能の要件を満たすビッグデータセキュリティ分析の導入が進む

これまで、ほとんどの情報セキュリティソリューションは、悪質なペイロードの特定（ブラックリスティング）や既知のアプリケーションの追跡（ホワイトリスティング）に依存してきました。現在、情報セキュリティの専門家が直面している課題は、「グレー」のペイロードを特定し、適切に処理することです。この課題を解決するには、複数のセキュリティ技術を実装し、堅牢なスレットレピュテーションサービスと併用する必要があります。

スレットレピュテーションサービスはマルウェア、不正なサイト、スパム、ネットワーク攻撃の検出で成果を挙げています。2014 年、ステルス攻撃や APT 攻撃を迅速かつ正確に検出するために、新たな脅威評価サービスと解析ツールがセキュリティベンダーから提供されるでしょう。たとえば、ビッグデータ分析により、洗練された回避技術や基幹業務を妨害する APT の検出が可能になります。

7: クラウドベースの企業アプリケーションの採用により、新たな攻撃対象領域が発生

20 世紀初めに 100 の銀行を襲ったとされるウィリー・サットン（Willie Sutton）は「銀行を狙うのはそこに金があるからだ」と述べたと言われています[3]。21 世紀のサイバー犯罪者がクラウドベースのアプリケーションやデータリポジトリを狙うようになるのは、そこにデータがある、あるいは間もなく存在するようになるからです。犯罪者が狙うビジネスアプリケーションは IT 部門が会社のセキュリティポリシーで保護していないことが多く、最近の報告によると、80% を超えるビジネスユーザーが、会社の IT 部門が認識していない、あるいはサポートしていないクラウドアプリケーションを使用しています[4]。

クラウドベースのアプリケーションは機能的にも経済的にも非常に魅力的ですが、犯罪者はこれらのアプリケーションを攻撃するための新しい手口を探しています。たとえば、どのデータセンターでも使用されているハイパーバイザー、クラウドサービスが備えるマルチテナントの通信インフラ、大規模なクラウドサービスの準備と監視に使用される管理インフラなどが新しい攻撃領域になります。企業のセキュリティ担当者にとって厄介なことは、会社のアプリケーションがクラウドに移行するとセキュリティプロファイルの管理が難しくなる点です。

境界のセキュリティを直接管理できないため、クラウドプロバイダーの利用規約と操作手順を考慮してセキュリティ対策を配備し、脅威状況の変化に合わせて更新しなければなりません。セキュリティの責任者や管理者の負担は相当なものです。大企業であれば、自社のニーズに合ったセキュリティ対策を要求することも可能ですが、クラウドベースのサービスを利用する個人はプロバイダーの曖昧な利用規約をよく確認する必要があります。新しいクラウドサービスは、データの保護に必要な機器や対策が整備されるまで新しい攻撃に無防備な可能性があります。

筆者について

本レポートは、Christoph Alme、Cedric Cochin、Geoffrey Cooper、Benjamin Cruz、Toralv Dirro、Paula Greve、Aditya Kapoor、Klaus Majewski、Doug McLean、Igor Muttik、Yukihiro Okutomi、François Paget、Craig Schmugar、Jimmy Shah、Ryan Sherstobitoff、Rick Simon、Dan Sommer、Bing Sun、Ramnath Venugopalan、Adam Wosotowsky、Chong Xu が準備し、作成しました。

McAfee Labs について

McAfee Labs は、世界各地に存在する McAfee の研究機関で、マルウェア、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、世界各地に数百万台のセンサーを配備し、クラウド型サービスの McAfee Global Threat Intelligence™により情報収集を行っています。世界 30 か国に存在する McAfee Labs には、様々な分野を専門とする 500 名の研究者が在籍し、企業や一般のユーザーを保護するため、リアルタイムの脅威検出、アプリケーションの脆弱性特定、リスクの相関分析、迅速な問題解決に努めています。詳しくは、www.mcafee.com/labs をご覧ください。

マカフィーについて

マカフィーは、インテルコーポレーション（NASDAQ：INTC）の完全子会社であり、企業、官公庁・自治体、個人ユーザーが安全にインターネットの恩恵を享受できるよう、世界中のシステム、ネットワーク、モバイルデバイスを守るプロアクティブで定評あるセキュリティソリューションやサービスを提供しています。マカフィーは、Security Connected 戦略、セキュリティにハードウェアを活用した革新的なアプロ—チ、また独自の Global Threat Intelligence により、常に全力でお客様の安全を守ります。詳しくは、http://www.mcafee.com/jp/ をご覧ください。マカフィーでは、セキュリティに関する様々な研究成果や調査結果を web 上で公開しています。詳しくは下記ページをご覧ください。http://www.mcafee.com/japan/security/report/default.asp

マカフィー株式会社
www.mcafee.com/jp

東京本社　〒 150-0043 東京都渋谷区道玄坂 1- 12- 1
渋谷マークシティウェスト 20F
TEL 03-5428-1100（代）FAX 03-5428-1480

名古屋営業所　〒 460-0002 愛知県名古屋市中区丸の内 3-20-17
中外東京海上ビルディング 3F
TEL 052-954-9551（代）FAX 052-954-9552

西日本支店　〒 530- 0003 大阪府大阪市北区堂島 2-2-2
近鉄堂島ビル 18F
TEL 06-6344-1511（代）FAX 06-6344-1517

福岡営業所　〒 810- 0801 福岡県福岡市博多区中洲 5-3-8
アクア博多 5F
TEL 092-287-9674（代）

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, “The Hidden Truth Behind Shadow IT”（シャドー IT の真実）、2013 年 11 月。
http://www.mcafee.com/jp/resources/reports/rp-six-trends-security.pdf

[3] Sutton 自身は、このような発言をしていないと否定し、銀行強盗の理由は「楽しいから」としている。

[4] Stratecast, “The Hidden Truth Behind Shadow IT.”（シャドーITの真実）、2013年11月。
http://www.mcafee.com/jp/resources/reports/rp-six-trends-security.pdf

60756rpt_threats-predictions_1213_fnl_ETMG