クライアントPCを狙う攻撃の最新動向と対応

Tokyo SOCが観測する日本国内企業の現状

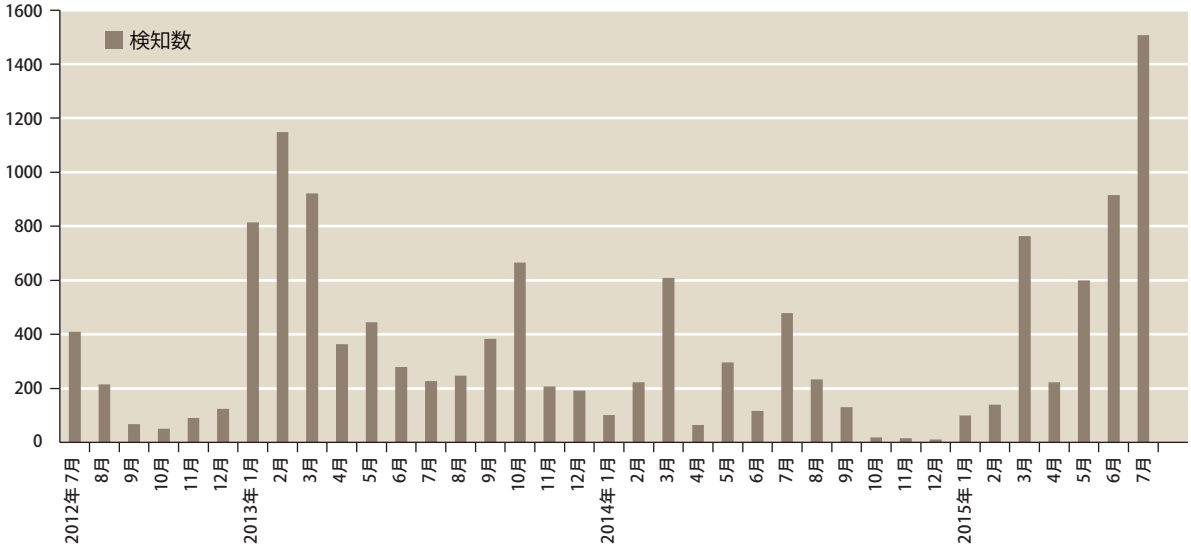
日本アイ・ビー・エム株式会社
セキュリティー事業本部
東京セキュリティー・オペレーション・センター
セキュリティー・アナリスト
窪田 豪史
Takeshi Kubota

2007年日本IBMに入社。セキュリティー機器の導入・機能検証業務担当を経て、2009年よりセキュリティー・オペレーション・センターにてセキュリティー監視に従事。IBMブログ「Tokyo SOC Report」や半期に1度発行する「Tokyo SOC情報分析レポート」で情報発信を行っている。日本セキュリティオペレーション事業者協議会（ISOG-J）会員、CISSP。

Webサイト閲覧やメールを介して発生するマルウェア感染

クライアントPCへのマルウェア感染は、企業や組織におけるセキュリティー上の重大な脅威の一つとなっています。遠隔操作型のマルウェア感染による情報漏洩事例や、ファイルを暗号化し、復元のためと称して金銭を要求するマルウェア（ランサムウェア）の被害事例が数多く報告されています[1][2]。

日本IBMの東京セキュリティー・オペレーション・センター（以下、Tokyo SOC）でも、マルウェア感染を狙う攻撃やマルウェアの活動を日々検知しています。本稿では、Tokyo SOCで近年特に多く検知しているドライブ・バイ・ダウンロード攻撃とメールを悪用する攻撃について、またそうしたインシデント発生時に求められる対応について解説します。



Tokyo SOC調べ：2012年7月1日～2015年7月31日

図1. ドライブ・バイ・ダウンロード攻撃の月別検知数推移（日本国内）

1 Webサイト閲覧をきっかけとする攻撃（ドライブ・バイ・ダウンロード攻撃）

ドライブ・バイ・ダウンロード攻撃は、Webサイトの閲覧を通じてクライアントPCへマルウェアを感染させる攻撃手法です。攻撃者は、一般のWebサイトの改ざんや悪意ある広告コンテンツを表示することで、それを閲覧したユーザーを自動的に攻撃サーバーへ接続させ、クライアントPCの脆弱性を悪用してマルウェアに感染させようとします。Tokyo SOCでは**図1**のとおり、時期による増減はあるものの継続した攻撃を検知しています。また**図2**に示すように、Tokyo SOCでクライアントPCによる通信を監視している組織のうち、2015年1月から6月の間にドライブ・バイ・ダウンロード攻撃が検知された組織は40.5%に上り、現在ドライブ・バイ・ダウンロード攻撃発生のリスクは高い状態にあると言えます。

ドライブ・バイ・ダウンロード攻撃の対策として重要となるのが脆弱性への対応です。クライアントPCに脆弱性が存在しなければ、ドライブ・バイ・ダウンロード攻撃によるマルウェア感染の被害は生じません。しかし現実には、ドライブ・バイ・ダウンロード攻撃によるマルウェア感染の事例が後を絶ちません。その主な要因として、次々と新しい脆弱性が発見され攻撃に悪用されていることが挙げられます。過去にはAdobe ReaderやOracle JREの脆弱性が狙われていましたが、2015年以降はAdobe Flash Playerの脆弱性を狙うケースが増えています（**図3**）。

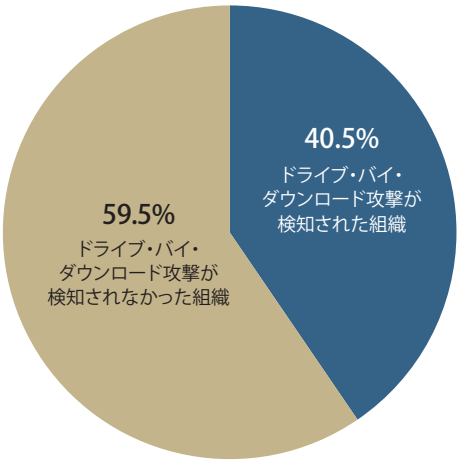
Adobe Flash Playerには2015年1月から7月にかけて毎月新たな脆弱性が公表されましたが、修正プログラムが公表される前に悪用が確認された事例（ゼロデイ攻撃）も7件に及びました。このような状況において、多数存在するクライアントPCすべてに対して最新版へのアップデートや回避策のタイムリーな適用が困難であることが、ドライブ・バイ・ダウンロード攻撃への対策の難しさにつながっています。

2 メールを悪用する攻撃

メールを悪用する攻撃では、攻撃者は不正なファイルを添付したメールを送信し、それらを開かせることでマルウェアに感染させようとします。標的を特定の組織や個人に絞って行われる攻撃（標的型攻撃）や、不特定多数に対して行われる攻撃（ばらまき型攻撃）があり、いずれも多くの被害が確認されています。

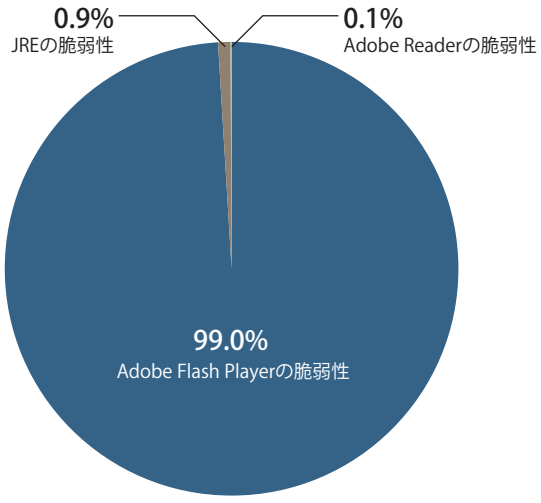
（1）標的を絞って行われる攻撃

2015年6月に発表された日本年金機構における情報漏洩事件をきっかけとして、主に日本の組織を対象とした遠隔操作型マルウェアへの感染を狙う攻撃が注目されました。Tokyo SOCでも同様の攻撃を検知しており、ある事例では国内の実在する組織をかたった巧妙に作り込



Tokyo SOC調べ：2015年1月1日～2015年6月30日

図2. ドライブ・バイ・ダウンロード攻撃発生状況（日本国内）



Tokyo SOC調べ：2015年1月1日～2015年6月30日

図3. ドライブ・バイ・ダウンロード攻撃で悪用された脆弱性の割合（日本国内）

まれたメールが利用されていました（**図4**）。

攻撃対象を絞って行われる攻撃は、攻撃発生時点では多くのセキュリティー製品が検知できないという特徴があります。上記の事例でも、検知時点では主要アンチウイルス・ソフトウェアの1製品でしかマルウェアであるとの判定がなされませんでした。このため、感染直後に被害の発生に気付くことは難しく、この攻撃の被害を受けた組織の多くは外部からの通報によりマルウェア感染に気付いたと言われています。

(2)不特定多数に対して行われる攻撃

標的を絞って行われる攻撃とともに、不特定多数に対して広く行われる攻撃（ばらまき型攻撃）の動向にも注意が必要です。2014年の後半から、不正なマクロを含むMicrosoft Officeファイルを添付する攻撃の増加が目立ち、2015年10月末には国内の実在の組織をかたる攻撃が確認されるなど、手口の巧妙化の兆しもあります[3]。Tokyo SOCでは、不正なマクロを含むファイルが添付されたメールを継続して検知しており、それらのメールに添付されたマクロを開き実行してしまった事例も確認しています（**図5**）。

時期により検知数に変動はあるものの、1カ月に1万～3万件程度の攻撃メールが対象組織の業種や規模を問わず送信されています。

不特定多数に対して広く送信される攻撃メールは、セキュリティー・ベンダーもその動向を把握しやすいために対応は比較的早く、スパム・フィルターなどで自動的に排除されやすい特徴があります。また、最近のMicrosoft Officeの標準設定ではマクロの実行にはユーザーによる明示的な許可が必要になります。しかしこうした対策にも関わらず、ばらまき型攻撃によるマルウェア感染事例はゼロにはならず、Tokyo SOCでは毎月数件の感染を確認しています。これは、届いたメールや添付ファイルが不正なものか否かを最終的に人が判断するため、被害の発生を完全に防ぐのは難しいということを示しています。

インシデント発生時に求められる対応

Tokyo SOCでは、お客様環境において攻撃の成功やインシデントを検知した場合、お客様に発生した攻撃の概要や対処・対策を即座にご連絡しています。その際にご支援する対応内容には以下の項目があります。

- ●該当クライアントPCの特定
- ●関連する他のログの調査（Proxyやアンチウイルスなど）
- ●対処および根本対策の実施

これらの対応をスムーズに実施するためには、インシデント発生を前提とし、必要な対応がとれるよう準備しておくことが重要となります。

図4. マルウェアへの感染を狙う不正なメール例

被害の疑いのあるクライアントPCを特定するには、検知されたIPアドレスなどの情報と該当通信を発したクライアントPCを紐付ける必要があります。被害を最小限にするためには可能な限り迅速に特定することが望まれますが、IPアドレスとクライアントPCを紐付ける情報がなかったり、DHCPを利用しているためにIPアドレスが変わっていたりする場合、特定に時間がかかる可能性があります。通信の情報からクライアントPCを特定できるかをあらかじめ確認しておくことで、インシデント発生時にも素早い対応が可能となります。

また攻撃内容や影響度の詳細調査のため、Proxyやアンチウイルスといった別のログ調査が必要となる場合があります。これらのログについても、調査に必要な情報を取得する設定になっていなかったり、ログの検索に想定以上に長い時間を要してしまったりする場合があります。

さらに、クライアントPC特定後の対応方法が定まっておらず、適切な対応が行えないといった問題が生じる場合もあります。該当クライアントPCから即座にネットワーク・ケーブルを抜線してよいのか、あるいはクライアントPC内の詳細調査（フォレンジック）のために定められた手順で対応する必要があるのかを事前に定めておく必要があります。加えて、実際に対応する要員に対応を実施するための適切な権限が与えられていることも重要です。

まとめ

ドライブ・バイ・ダウンロード攻撃では、次々に新しい脆弱性が狙われたり対策の徹底が困難であったりすることから、アップデートや回避策の適用のみによる対策が難しい状況が続いています。

メールを悪用する攻撃においても、対象を絞って行われる攻撃の成功率が高く、被害の発生に長期間気付けない状況が生じます。また、不特定多数に対して行われる攻撃の成功率は低いものの、受信したメールを最終的に人が扱うことの限界として影響をゼロとすることは困難と言えます。

このような脅威に対して、攻撃の影響を緩和するようなポリシーや教育、技術的な対策の実施は必須であり、攻撃の影響をゼロにすることは困難であるという事実も同時に受け入れる必要があります。その上で、影響の発生にいち早く気付き、適切に対処が行える体制を構築していくことが重要です。

[参考文献]
[1] IPA：【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！, https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html
[2] JPCERTコーディネーションセンター：ランサムウエア感染に関する注意喚起, https://www.jpcert.or.jp/at/2015/at150015.html
[3] IBM：日本国内の実在する企業を騙った不正なメールを広域で検知, https://www.ibm.com/connections/blogs/tokyo-soc/entry/mail_20151028

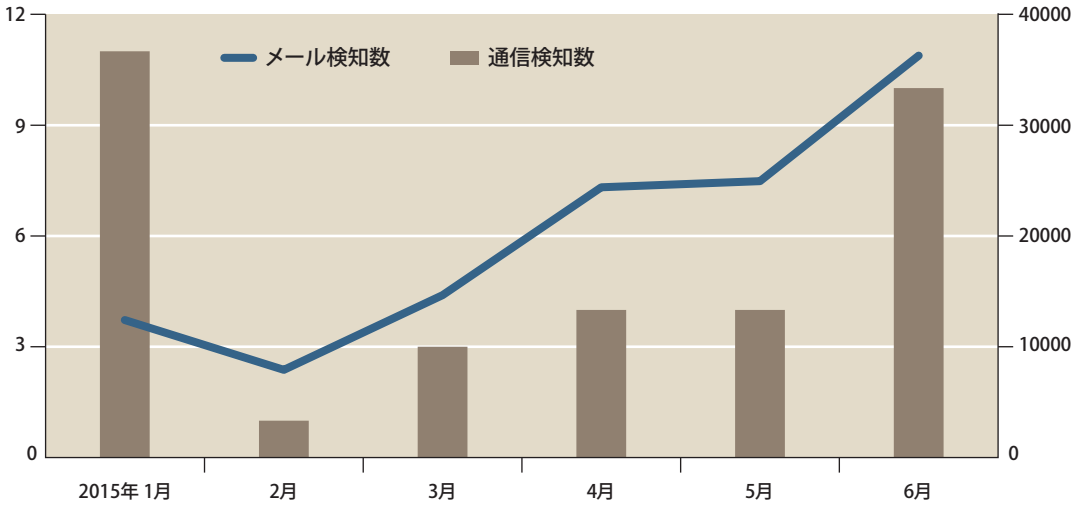


図5. 不正なマクロを含むファイルが添付されたメールの検知数および不正なマクロの実行を示す通信検知数の推移