PlugXの背後にいる攻撃者について

今回は、標的型攻撃に使われているマルウェア、PlugXの背後にいる攻撃者について、調査結果とその背景を紹介すると共に、最近のDDoS攻撃の傾向とその対策、総務省の電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会について解説します。

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2014年1月から3月までの期間では、前回の期間に続いてAnonymousなどのHacktivismによる攻撃が複数発生しています。また、NTPを悪用したDDoS攻撃が頻発し、1つの攻撃で400Gbpsもの攻撃の通信量が発生したと報告されています。ccTLDなど、国単位で影響を受けるドメインハイジャック事件も続いています。加えて、昨年より国内で被害が増加しているオンラインバンキングを悪用した金銭被害についても、本年も引き続き増加傾向にあります。昨年末に米国で発覚した、マルウェアにより小売店のPoSシステムから多くの情報を盗まれた事件では、その影響の大きさから対策に関する数多くの議論が行われました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

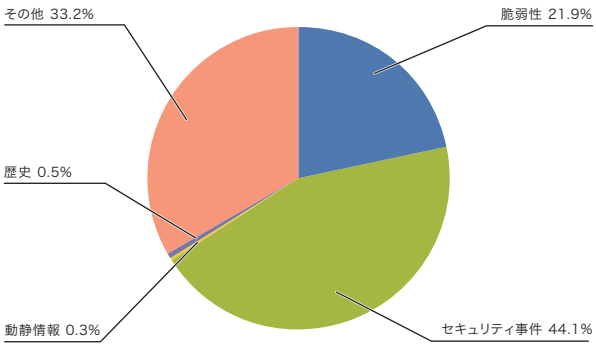


図-1 カテゴリ別比率(2014年1月〜3月)

1.2 インシデントサマリ

ここでは、2014年1月から3月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します*1。

■ Anonymousなどの活動

この期間においても、Anonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。1月には、ブラジルの複数の政府関連サイトに対してWeb改ざんの被害が発生しています。同じく1月には、昨年自殺した活動家にちなみ、マサチューセッツ工科大学(MIT)のWebサイトが改ざんされています(OpLastresort)。

ウクライナ情勢では、EUやウクライナとロシアやその周辺国のAnonymousなどによって、政府機関へのDDoS攻撃や野党議員のメールの漏えい、クレジットカード情報の漏えいやマスコミのWebサイトへの攻撃などが複数発生しています。更に、3月には、これに関連していると考えられる、北大西洋条約機構(NATO)へのDDoS攻撃が発生しました*2。

他にも、南米や欧州を中心に、世界各国の政府とその関連サイトに対して、Anonymousなどによる攻撃が継続して行われました。また、Syrian Electronic Armyを名乗る何者かによるSNSアカウントの乗っ取りや、Webサイト改ざんも継続して発生しており、被害を受けた企業にはMicrosoftやSkypeなどの著名な企業も含まれていました。

*1 このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットや利用者の環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェアなどの脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃など、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日などで、過去の史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策などの作業を示す。
セキュリティ事件:ワームなどのマルウェアの活性化や、特定サイトへのDDoS攻撃など、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中など、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

*2 この攻撃についてはNATO報道官であるOana Lungescu氏のTwitter(@NATOpress)で確認できる"(https://twitter.com/NATOpress/statuses/445112624578306048)。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*3][*4][*5][*6]、Internet Explorer[*7][*8]、などで修正が行われました。Adobe社のAdobe FlashPlayer、Adobe Reader及びAcrobat、Shockwave Playerなどでも修正が行われました。Oracle社のJava SEでも四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。なお、この更新ではセキュリティ機能の変更が行われ、署名の付いていないJavaアプレットについては実行が制限されるなど、初期設定でのセキュリティの強化が行われています[*9]。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で、四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。また、DNSサーバのBIND9では、NSEC3を用いてDNSSEC署名されたゾーンを保持している権威DNSサーバとして運用していた場合に、DNS問い合わせ受信時の処理の不具合によるnamedが異常終了する脆弱性が見つかり修正されました[*10]。時刻同期に利用されているNTPについても、サーバの管理機能を悪用して、他者へのDDoS攻撃に繋がる不具合が見つかり、修正が行われました。また、この不具合を悪用した攻撃が複数発生しており、注意喚起が行われています。詳細については「1.4.2 DrDoS攻撃とその対策」も併せてご参照ください。

3月には半年に1度行われるCisco Systems社のIOSで定例アップデートが行われ、システム停止の可能性のある脆弱性などが修正されています[*11]。CMSとして利用されるWordPressについてもPingback機能を悪用した他者へのDDoS攻撃に繋がる不具合が見つかっています。また、実際にこの不具合を悪用した攻撃が発生しています[*12]。

■ Webサービスに対する攻撃

この期間でも、昨年から多数発生しているユーザのIDとパスワードを狙った試みと、取得したIDとパスワードのリストを使用したと考えられる、なりすましによる不正ログインなどのWebサービスへの不正ログインや、Web改ざんによるマルウェア感染が継続しています。

ISPやゲームサイト、交通機関のサイトやクレジットカード会社、SNSなど様々なサイトでリスト型攻撃による不正なログインの試みが行われる事件が多く発生しています。この内、航空会社のマイレージサービスで発生した不正ログイン事件では、サイト上のポイントを他のギフトポイントに不正に交換されるなどの被害が発生しました。被害が発生した一部のサイトについては、ユーザが設定できるパスワードの文字列の長さが少ないことなど、仕様に問題があることが以前から指摘されていました。このように不正アクセス事件は継続して数多く発生しており引き続き注意が必要です。

また、この期間ではWebサイトの改ざんと、改ざんされたWebサイトからマルウェアへ誘導される事件が多く発生

＊3 「マイクロソフト セキュリティ情報 MS14-002 - 重要 Windows カーネルの脆弱性により、特権が昇格される」(https://technet.microsoft.com/library/security/ms14-002)。
＊4 「マイクロソフト セキュリティ情報 MS14-007 - 緊急 Direct2D の脆弱性により、リモートでコードが実行される」(https://technet.microsoft.com/library/security/ms14-007)。
＊5 「マイクロソフト セキュリティ情報 MS14-011 - 緊急 VBScript スクリプト エンジンの脆弱性により、リモートでコードが実行される」(https://technet.microsoft.com/library/security/ms14-011)。
＊6 「マイクロソフト セキュリティ情報 MS14-013 - 緊急 Microsoft DirectShow の脆弱性により、リモートでコードが実行される」(https://technet.microsoft.com/library/security/ms14-013)。
＊7 「マイクロソフト セキュリティ情報 MS14-010 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム」(https://technet.microsoft.com/library/security/ms14-010)。
＊8 「マイクロソフト セキュリティ情報 MS14-012 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム」(https://technet.microsoft.com/library/security/ms14-012)。
＊9 Oracle、「開発者 - ブラウザでのJavaコンテンツ - セキュリティ・マニフェストの変更」(https://www.java.com/ja/download/faq/signed_code.xml)。
＊10 株式会社日本レジストリサービス(JPRS)、「(緊急)BIND 9.xの脆弱性(DNSサービスの停止)について(2014年1月14日公開)」(http://jprs.jp/tech/security/2014-01-14-bind9-vuln-nsec3-handling.html)。
＊11 "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" (http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html)。
＊12 攻撃の詳細については、次のKrebs on Security Blogに詳しい。"Blogs of War: Don't Be Cannon Fodder" (http://krebsonsecurity.com/2014/03/blogs-of-war-dont-be-cannon-fodder/)。

1月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

脆 **1日**：Cisco社の複数のLinksys機器にリモートからルータのリセットや、adminパスワードの取得が可能なバックドアが見つかり、研究者が詳細を公開した。
詳細については次の研究者のGitHubを参照のこと。"elvanderb/TCP-32764"（https://github.com/elvanderb/TCP-32764）。

セ **2日**：US-CERTは、12月に発覚した大手小売り事業者の情報流出の原因となったPOS端末に感染するマルウェアについて、注意喚起を行った。
US-CERT、"Alert (TA14-002A) Malware Targeting Point of Sale Systems"（http://www.us-cert.gov/ncas/alerts/TA14-002A）。

セ **4日**：複数のオンラインゲームで、何者かによるDDoS攻撃が行われ、サービス停止などの影響が出た。この攻撃は特定の利用者に対する攻撃の可能性が指摘されている。

セ **6日**：独立行政法人日本原子力研究開発機構は、高速増殖炉もんじゅの事務処理用パソコン1台がウイルスに感染し、情報流出の可能性があることを公表した。
「コンピュータウイルス感染による情報漏えいの可能性について」（http://www.jaea.go.jp/02/press2013/p14010601/index.html）。

セ **6日**：米国Yahoo!は、年末年始の期間に欧州の自社サイトに配信した広告のいくつかで不正サイトからのマルウェアへの誘導が行われていたことを公表した。
詳細については例えば次のトレンドマイクロ社のSECURITY BLOGを参照のこと。「『Yahoo!』広告経由での感染事例、被害の分かれ目はパッチ管理とセキュリティ対策ソフト」（http://blog.trendmicro.co.jp/archives/8421）。

セ **8日**：韓国で、大手クレジットカード３社から延べ8,500万件のクレジットカード情報が、カード会社と契約していた信用情報会社の社員により流出していたことが発覚した。

セ **11日**：オンラインストレージサービスのDropboxでメンテナンス時の不具合により、2日間に渡るサービス障害が発生した。
この障害については、次のDropboxの公式blogに詳しい。"Outage post-mortem"（https://tech.dropbox.com/2014/01/outage-post-mortem/）。

脆 **15日**：ntpdのmonlist機能がDoSを引き起こす可能性のあるとして、注意喚起が行われた。
US-CERT、"Alert (TA14-013A) NTP Amplification Attacks Using CVE-2013-5211"（http://www.us-cert.gov/ncas/alerts/TA14-013A）。

脆 **15日**：Microsoft社は、2014年1月のセキュリティ情報を公開し、MS14-002を含む4件の重要な更新をリリースした。
「2014 年 1 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms14-jan）。

脆 **15日**：Adobe Reader及びAcrobatに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-01: Adobe ReaderおよびAcrobat用セキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/acrobat/apsb14-01.html）。

脆 **15日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-02: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-02.html）。

脆 **15日**：Oracle社はOracleを含む複数製品について、四半期ごとの定例アップデートを公開し、Java SEの36件の脆弱性を含む合計144件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - January 2014"（http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html）。

セ **15日**：Symantec社は、日本の大手出版社のWebサイトが改ざんされ、Toolkitによる不正サイトからのマルウェアへの誘導が行われていたことを発表した。
詳細については次のSymantec社のSecurity Response Blogを参照のこと。「日本の大手出版社の Web サイトが Gongda 悪用ツールキットに利用される」（http://www.symantec.com/connect/ja/blogs/web-gongda）。

他 **23日**：セキュリティ関連企業から、動画再生ソフトであるGOM playerの更新機能を不正利用したマルウェア感染について注意喚起が行われた。
1月6日に発表された、日本原子力研究開発機構で発生したウイルス感染事件の原因とされている。詳細については次の韓国GRETECH JAPAN Corp社のお知らせを参照のこと。「マルウェア（ウイルス）感染に関するお詫びと調査結果のご報告」（http://www.gomplayer.jp/player/notice/view.html?intSeq=300）。

他 **29日**：GMOグローバルサイン社のルート証明書が有効期限を迎え、更新されていない場合に接続ができなくなったり、クライアント側で警告が出るなどの影響が発生した。
GMOグローバルサイン社、「旧ルート証明書の有効期限切れに伴う影響範囲について」（https://jp.globalsign.com/support/faq/538.html）。

他 **30日**：IPAより、2012年10月から2013年12月までの標的型攻撃メールを分析した技術レポート「標的型攻撃メールの傾向と事例分析 ＜2013年＞」が公開された。
「標的型攻撃メールの傾向と事例分析　＜2013年＞」（http://www.ipa.go.jp/security/technicalwatch/20140130.html）。

セ **31日**：米国Yahoo!のYahoo! Mailで一部アカウントに対するリスト型攻撃による不正ログインが発生した。
Yahoo! Inc.、"Important Security Update for Yahoo Mail Users"（http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users）

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

しました。SNS関連サイトや出版・放送関連の複数の企業のWebサイト、交通機関や金融機関のWebサイトでも発生しています。誘導されたサイトでは、未修正の脆弱性を含むいくつかの脆弱性を悪用して、ドライブバイダウンロードによるマルウェアの感染活動が行われていました。これらのWeb改ざんは著名な企業のWebサイトでも発生しており今後も注意が必要です。

■ ccTLDへの攻撃

ccTLDを含むドメインレジストリに対しての攻撃と、それによるドメインハイジャックや情報の漏えいも継続して複数発生しています。1月には、モンテネグロのドメインである.meが何者かによる不正アクセスを受け、約3,500ドメインがハイジャックされる事件が発生しました。GoogleやYahoo、AmazonやFacebookなどのドメインの管理を行っているドメイン管理サービスのMarkMonitor社では、Syrian Electronic Armyを名乗る何者かによる管理ツールへの不正なアクセスによって、これらのドメイン情報の一部が書き換えられる事件が発生しています。

3月には、ベネズエラのISPが、Google Public DNS (8.8.8.8)の経路情報を広報したことから、ベネズエラとブラジルのネットワークでGoogle Public DNS宛の通信に影響が出ています。Google Public DNSについては、トルコで本来のサーバとは異なるサーバと通信している可能性があることが分かり、政府による検閲の可能性が指摘されています[*13]。また、トルコでは、これ以外にもTwitterやYouTubeへのアクセスが禁止されていて、政府によるインターネットへの制限が強化されていることが伺えます。

■ Bitcoin

仮想通貨であるBitcoin[*14]についても、その取引が拡がるにつれて、様々な事件が発生しています。この期間では、2月にBitcoin取引所の1つであるMt.Goxが、技術的な問題が発生したとして一時的に取引を中止する措置を発表しました。この数日後には、同じくBitcoin取引所の1つであるBitstampでも問題が発生したとして取引を一時的に停止しました。これらの取引所では、BitcoinのTransaction Malleabilityの問題を悪用したDoS攻撃を受けていたことを公表しています[*15]。この問題は、Bitcoinの取引に使われる固有の番号であるトランザクションIDを書き換えて広報することで、取引の妨害や多重取引を行える可能性があるものでした。Bitstampは、その後、対応を行ったとして取引を再開しましたが、Mt.Goxについては、この問題により、預かっていたBitcoinが盗まれたとして、約65億円の負債により経営破たんし、日本の民事再生法の適用を申請しました。しかし、破たん前から不透明な取引が指摘されていたことから、事業内容が明らかでないとして申し立ては棄却され、破産手続きが開始されています[*16]。

Mt.Goxについては、この問題が2011年から指摘されていたにも関わらず、システム改修を行わず放置していたことが明らかとなっています。さらに、盗まれたとされた資産の一部が古いBitcoinウォレットから見つかったことを公表したり[*17]、第三者による調査結果が公表され、問題によって盗まれた可能性のある約74万XBTのBitcoinのうち、この問題によって盗まれたのは、約386XBTだけである可能性が指摘されています。

これ以外にも、仮想通貨交換所や口座管理サービスに対する攻撃も相次いでおり、Webサイトへの DDoS攻撃や、不正侵入によりBitcoinそのものが盗まれたり、サイトのアカウント情報が盗まれるなどの事件が多く発生しています。また、米国の複数の報道機関でBitcoinの作者とされるSatoshi Nakamoto氏が見つかったとの報道がされましたが、Nakamoto氏とされた本人は否定しています。更に、現在Bitcoinの取り扱いに関する議論が各国で活発に行われています。日本でも3月に通貨に該当しないとの見解について閣議決定が行われています。

＊13 Google Online Security Blog、"Google's Public DNS intercepted in Turkey" (http://googleonlinesecurity.blogspot.jp/2014/03/googles-public-dns-intercepted-in-turkey.html)。
＊14 Bitcoinについては、本レポートのVol.21 (http://www.iij.ad.jp/development/iir/pdf/iir_vol21.pdf)の「1.4.3 仮想通貨Bitcoin」で紹介している。
＊15 Bitstamp、"BITCOIN WITHDRAWAL PROCESSING SUSPENDED"(http://www.bitstamp.net/article/bitcoin-withdraws-suspended/)。
＊16 株式会社MTGOX、「破産手続開始決定のお知らせ - 基本的なご質問に対する回答」(http://www.mtgox.com/img/pdf/20140424_announce_qa_ja.pdf)。
＊17 株式会社MTGOX、「当社保有ビットコインの残高に関するお知らせ」(http://www.mtgox.com/img/pdf/20140320-btc-announce.pdf)。

2月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

セ **3日**：航空会社の会員向けWebサイトで不正アクセスが発生し、通信販売サイトのポイントに交換される事件が発生した。

セ **3日**：東京大学 国際高等研究所 カブリ数物連携宇宙研究機構で、スーパーコンピュータシステムが外部からの不正アクセスを受けたことを公表した。この事件では侵入されたシステムを通じて、共同研究を行っていた国立天文台など、外部の研究機関への不正アクセスも確認されたことから各研究機関で対応が行われた。
詳細については次の東京大学国際高等研究所 カブリ数物連携宇宙研究機構（Kavli IPMU）の発表を参照のこと。「カブリ数物連携宇宙研究機構の研究用計算機への不正アクセスについて」（http://www.ipmu.jp/ja/node/1831）。

脆 **5日**：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-08: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-06.html）。

他 **5日**：経済産業省と一般社団法人JPCERTコーディネーションセンターは、制御システムにおける国内外の技術動向の紹介を通じ、制御システムのセキュリティ向上に向けた検討を行う「制御システムセキュリティカンファレンス 2014」を開催した。
JPCERTコーディネーションセンター、「制御システムセキュリティカンファレンス 2014開催のご案内」（https://www.jpcert.or.jp/event/ics-conference2014.html）。

セ **6日**：独立行政法人 国立がん研究センターは、国立がん研究センター東病院のパソコン2台がウイルス感染し、患者情報などが漏えいした可能性があることを公表した。
詳細については次の国立がん研究センターの発表を参照のこと。「国立がん研究センター東病院における動画再生ソフトアップデートプログラムによるコンピュータウイルス感染について」（http://www.ncc.go.jp/jp/information/20140206.html）。

セ **7日**：Bitcoinの取引所の1つであるMt. Goxは、技術トラブルを修正するためとしてビットコインの払い出しを一時停止した。この後、2月28日にサイバー攻撃によるBitcoinと銀行預金の流出のため、債務超過に陥ったとして、民事再生手続きを申請した。

セ **12日**：Bitcoin取引所のMtGoxやBitStampなどが、トランザクション展性を悪用した取引妨害攻撃を受けたとして口座からの引き出しを一時停止した。この影響でBitcoinの対ドルレートが一時急落するなどの影響が出た。
この問題については、チューリッヒ大学の研究者チームによってMt.GOXに対する検証が行われており、この問題による影響は限定的だったとの反論も行われている。Christian Decker and Professor Roger Wattenhofer、"Bitcoin Transaction Malleability and MtGox"（http://arxiv.org/pdf/1403.6676v1.pdf）。

脆 **12日**：Microsoft社は、2014年2月のセキュリティ情報を公開し、MS14-007やMS14-010、MS14-011を含む4件の緊急と3件の重要な更新をリリースした。
「2014 年 2 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms14-feb）。

脆 **12日**：Adobe Shockwave Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-06: Adobe Shockwave Player用セキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/shockwave/apsb14-06.html）。

他 **12日**：一昨年発生したパソコン遠隔操作ウイルス事件で、昨年逮捕された容疑者の初公判が東京地裁で行われた。

他 **13日**：米国立標準技術研究所（NIST）は重要インフラ分野の組織や企業が情報セキュリティ対策を行う上で指標となる"Framework for Improving Critical Infrastructure Cybersecurity"を公表した。
NIST、"NIST Releases Cybersecurity Framework Version 1.0"（http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm）。

脆 **17日**：米国 Cisco Linksys社の複数のルータに、CGIスクリプトの脆弱性があり、これを悪用したTheMoonと呼ばれるマルウェアの感染が複数発生していることが報告された。
詳細については次の米国SANS ISCのInfoSec Diaryを参照のこと。"Linksys Worm "TheMoon" Summary: What we know so far"（https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633）。

他 **17日**：日本発の情報セキュリティ国際会議としてCODEBLUEが2日間の日程で開催された。
詳細については次のCODEBULE公式サイト（http://codeblue.jp/）を参照のこと。

セ **18日**：検索サイトの検索連動型広告を悪用し、複数の金融機関の偽サイトへの誘導が行われていたことが発覚し、対応が行われた。
この事件については次の発表を参照のこと。「検索連動型広告の悪用に関する続報と対策について」（http://advertisingblog.yahoo.co.jp/2014/02/post_33.html）。

脆 **20日**：Microsoft社は、Internet Explorerに未修正の脆弱性があり、悪用されるとリモートでコードが実行される可能性があるとしてアドバイザリを公開した。この脆弱性については公開された時点で既に悪用が確認されていた。
「マイクロソフト セキュリティ アドバイザリ (2934088) Internet Explorer の脆弱性により、リモートでコードが実行される」（http://technet.microsoft.com/ja-jp/security/advisory/2934088）。

脆 **21日**：Adobe Flash Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-07: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-07.html）。

セ **24日**：はてなは、提供しているサービスに対して、外部から不正ログインされた可能性があるとしてパスワード変更や登録内容の確認を行うよう注意喚起を行った。
株式会社はてな、「不正ログイン防止のため、パスワードと登録情報のご確認をお願いします」（http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701）。

他 **27日**：IPAは、オフィス機器や家電製品のインターネット接続に伴う新たな脅威や、不用意な外部公開を確認する手順をまとめた「増加するインターネット接続機器の不適切な情報公開とその対策」を公開した。
「IPAテクニカルウォッチ『増加するインターネット接続機器の不適切な情報公開とその対策』」（http://www.ipa.go.jp/security/technicalwatch/20140227.html）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

■ 業務システムへの攻撃

昨年11月に発生した、米国の大手小売業者による顧客のカード情報の漏えい事件では、その後の調査で4000万人分のカード情報と、それ以外に7000万人分の顧客データが盗まれた可能性があることが判明しています。また、その手口についてはカードリーダーとレジを狙う特殊なマルウェアであるPOSマルウェアが利用されたことが分かりました。更に、この企業以外にも高級百貨店など複数の企業が同様の攻撃を受けていたことを発表しています[*18]。

これらの攻撃で使われたマルウェアは、暗号化してやりとりされているクレジットカードなどのデータを、支払処理の際に、レジで復号したタイミングを狙って情報を盗み出すようになっており、盗んだデータは外部のサーバに送信されていました[*19]。

今回の事件では、被害にあった事業者の取引業者に貸与したIDが不正に盗まれて悪用されたため、この事業者のネットワークに侵入した上で、攻撃が行われていたとされています。この事業者では、設備の管理システムと顧客情報の管理システムがネットワークで繋がっていたことなどが伝えられており、情報セキュリティ対策に不備があったことも、大規模な情報漏えいに繋がった原因とされています。

産業用システムやPOSシステムなどの業務用端末は、インターネットに直接つながっていなかったりすることから、企業で利用しているPCでは行われているセキュリティ上の対策やソフトウェア更新などが行われていないなど、適切な管理が行われていない場合が多く見受けられます。そのような状況から、POS端末などの業務システムに対する攻撃は今後も継続することが考えられ、注意が必要です。

■ 正規のソフトウェアを介した攻撃

1月には、独立行政法人日本原子力研究開発機構の高速増殖原型炉もんじゅで、従業員が共同で使用しているPCからウイルスが見つかったとの発表が行われました[*20]。また、2月には国立がん研究センター東病院で同じくPC2台がウイルスに感染していたことが公表されています[*21]。これらのウイルス感染は、動画再生ソフトの正規のアップデート機能を悪用したものでした。この事件ではユーザがインストールしていた正規のソフトウェアが利用しているアップデートサーバが不正アクセスを受けて、改ざんされていました。このため、ソフトウェアのアップデートの際に、本来のアップデートサーバから意図しない外部の第三者のサイトに誘導され、該当ソフトウェアのアップデートプログラムを装ったマルウェアがダウンロード、実行される可能性がありました[*22]。

このように正規のソフトウェア管理の仕組みを悪用された事例としては、2013年3月に韓国の複数の放送局や金融機関で多数のPCでシステム停止が発生した事件があります。この事件では被害企業内の更新管理サーバ(Patch Management System)が不正アクセスを受け、これを介してシステム破壊を行うマルウェアが企業内の端末に配布されていました[*23]。また、最近では正規のアプリやブラウザの拡張機能などを入手し、正規のソフトウェアに不正な機能を組み込んでアップデートとして配布する事件も発生しています[*24]。

これらの問題に対処するためには、インストール済みのソフトウェアのアップデートが正当なものであるかどうかを検証する仕組みの導入や、企業内のソフトウェアアップデートサーバのセキュリティの強化などを行う必要があります。

*18 Krebs on Security、"Hackers Steal Card Data from Neiman Marcus"(http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/)。
*19 詳細については、次のKaspersky Lab社のBlogに詳しい。「レジやPOSを狙うマルウェア」(http://blog.kaspersky.co.jp/ram-scrapers-and-other-point-of-sale-malware/)。
*20 独立行政法人日本原子力研究開発機構、「コンピュータウイルス感染による情報漏えいの可能性について」(http://www.jaea.go.jp/02/press2013/p14010601/index.html)。
*21 独立行政法人国立がん研究センター、「国立がん研究センター東病院における動画再生ソフトアップデートプログラムによるコンピュータウイルス感染について」(http://www.ncc.go.jp/jp/information/20140206.html)。
*22 株式会社グレテックジャパン、「マルウェア(ウイルス)感染に関するお詫びと調査結果のご報告」(http://www.gomplayer.jp/player/notice/view.html?intSeq=300&page=1)。
*23 この事件については、本レポートのVol.19(http://www.iij.ad.jp/development/iir/pdf/iir_vol19.pdf)の「1.4.1 韓国3.20大乱」で解説している。
*24 この事件については、例えば、実際に3万人のユーザがいたchrome拡張機能を売却した際の顛末を、作者であるAmit Agarwal氏がブログで報告している。"Selling a Google Chrome Extension is Easy but Monetizing is Tricky"(http://www.labnol.org/internet/sold-chrome-extension/28377/)。

3月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

脆 **5日**：フランス国立情報学自動制御研究所(INRIA)のセキュリティ研究者によって、中間者攻撃によりクライアント証明書が盗まれる可能性のあるTLSへの新たな攻撃手法が公表された。
詳細については次の発表を参照のこと。"Triple Handshakes Considered HarmfulBreaking and Fixing Authentication over TLS"(https://secure-resumption.com/)。

脆 **6日**：GnuTLSに、特定の条件における証明書の検証に不具合があり、正規のWebサイトを装った中間者攻撃を仕掛けることが可能な脆弱性が見つかり修正された。
US-CERT、"GnuTLS Releases Security Update"(http://www.us-cert.gov/ncas/current-activity/2014/03/05/GnuTLS-Releases-Security-Update)。

他 **7日**：日本政府は、ビットコインに関する質問主意書に対し、日本においては通貨に該当しないなどの政府見解をまとめ、閣議決定を行い公表した。
参議院、「ビットコインに関する質問主意書」(http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/meisai/m186028.htm)。

セ **10日**：別の航空会社の会員向けWebサイトで不正ログインが発生し、マイレを別のポイントに交換される事件が発生したことを公表した。

他 **10日**：IPAは、脆弱性の発見方法、対策について実習形式で体系的に学習できる脆弱性学習ツール「AppGoat」について、新しい演習テーマと脆弱性の修正演習を追加したウェブアプリケーション版を公開した。
「脆弱性体験学習ツール AppGoat」(http://www.ipa.go.jp/security/vuln/appgoat/index.html)。

脆 **12日**：Microsoft社は、2014年3月のセキュリティ情報を公開し、MS14-012とMS14-013の2件の緊急と3件の重要な更新をリリースした。
「2014 年 3 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms14-mar)。

脆 **12日**：Adobe Flash Playerに、情報漏えいの可能性がある脆弱性を含む複数の脆弱性が発見され、修正された。
「APSB14-08: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-08.html)。

脆 **12日**：Adobe Shockwave Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-08: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-08.html)。

セ **12日**：CMSであるWordPressで投稿にリンクが張られたことを知らせるPingback機能を悪用した大規模なDDoS攻撃が発生した。
Sucuri Blog、"More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack"(http://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html)。

脆 **13日**：Samsung Galaxyシリーズに、リモートからファイルの操作を実行可能な機能が含まれていることが公表された。
詳細については次のFree Software FoundationのBlogを参照のこと。"Replicant developers find and close Samsung Galaxy backdoor"(http://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor)。

セ **17日**：ブラジルとベネズエラでGoogle Public DNSの経路が一時的にBGPハイジャックされる事件が発生した。
この事件については次のBGP Monのtwitterのつぶやきで確認できる。(https://twitter.com/bgpmon/status/445266642616868864/photo/1)。

脆 **18日**：メッセージアプリのIP電話機能に発信者番号の偽装ができる不具合が見つかり、話題となった。

他 **18日**：全府省庁や内閣官房情報セキュリティセンター、重要インフラ事業者などの担当者約100人が参加し、府省庁をまたがる情報の収集や共有、緊急対応の訓練を行った。
内閣官房情報セキュリティセンター、"全府省庁等の参加による 大規模な政府サイバー攻撃対処訓練を初実施 ～【3・18訓練】～"(http://www.nisc.go.jp/active/kihon/pdf/318.pdf)。

脆 **19日**：Apache HTTP ServerにDoS攻撃可能な脆弱性を含む複数の脆弱性が見つかり修正された。
The Apache Software Foundation、"Apache HTTP Server 2.2.27 Released"(http://www.apache.org/dist/httpd/Announcement2.2.html)。

他 **19日**：2002年に開設され、脆弱性情報の公開や論議の場として活用されてきたFull Disclosure MLが終了した。なお、3月25日に別の管理者によって、同名のFull Disclosure MLとして再開されている。
seclists.org、"Administrivia: The End"(http://seclists.org/fulldisclosure/2014/Mar/332)。
seclists.org、"Administrivia: A Fresh Start"(http://seclists.org/fulldisclosure/2014/Mar/333)。

他 **20日**：一般社団法人インターネットコンテンツセーフティ協会は、4月1日よりファイル共有ソフトを悪用した児童ポルノ流通防止対策の取り組みとして、当該ユーザに対する連絡メールの送信を実施することを発表した。
「ファイル共有ソフトを悪用した児童ポルノ流通への対策について」(http://www.netsafety.or.jp/p2p/index.html)。

脆 **25日**：Microsoft社は、Microsoft Wordに任意のコード実行が可能な未修正の脆弱性があり、この脆弱性を悪用した標的型攻撃が確認されたとして、アドバイザリーを公開した。
「Microsoft Wordの脆弱性により、リモートでコードが実行される」(https://technet.microsoft.com/library/security/2953095)。

他 **26日**：防衛省は、高度化・複雑化するサイバー攻撃の脅威に対応するため、サイバー防衛隊を新編した。
防衛省、「サイバー防衛隊の新編について」(http://www.mod.go.jp/j/press/news/2014/03/25d.html)。

他 **27日**：警察庁は、サイバー犯罪の検挙状況についてまとめた「平成25年中のサイバー犯罪の検挙状況等について」を公表した。検挙件数は8,113件で前年比10.6%増となっており過去最高を記録している。
警察庁、「平成25年中のサイバー犯罪の検挙状況等について」(https://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf)。

他 **31日**：IPAより、「2014年版 情報セキュリティ10大脅威」が公表された。
「2014年版 情報セキュリティ10大脅威」(https://www.ipa.go.jp/security/vuln/10threats2014.html)。

[凡例] 脆 脆弱性　セ セキュリティ事件　動 動静情報　歴 歴史　他 その他

※日付は日本標準時

■ 政府機関の取り組み

政府機関のセキュリティ対策の動きとしては、1月に「第38回情報セキュリティ政策会議」が開催され、昨年6月に決定した「サイバーセキュリティ戦略」[*25]とそれを受けて、2013年度の各府省庁の取り組みを定めた「サイバーセキュリティ 2013」[*26]について、評価指標に基づくデータの把握と評価に関する基本方針が取りまとめられました。また、政府機関の情報セキュリティ対策のための統一規範などについても検討されています。更には深刻化・高度化するサイバー空間の脅威やその対応策等について理解を深めるため、2月の最初のワーキングデーを「サイバーセキュリティの日」と定め、サイバー空間の安全に資する取り組みを重点的に行うことを決定しています。また、2月には「IT利活用セキ ュリティ総合戦略推進部会」が開催され、今後のIT利活用を見据えた情報セキュリティ政策の総合的・戦略的推進について、検討が行われています。3月18日には、複数の政府機関を同時に狙うサイバー攻撃が発生したことを想定し、内閣官房情報セキュリティセンターと各府省庁及び重要インフラ事業者等との間の情報収集・共有訓練とCYMAT要員による緊急対処訓練が実施されました。

■ その他

1月にはICANNより新しいgTLDとして「TOKYO」と「NAGOYA」が承認されました。また3月には「OKINAWA」も承認されています[*27]。これは2012年1月からICANNが進めているgTLDの新規承認プロセス[*28]によるものです。現在、世界中から二千近い新gTLDの申請が行われており、今後も次々と新たなgTLDが承認されていくことになります。

警察庁から、「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」[*29]が発表され、平成25年中の発生状況は、1,315件となり、被害金額も約14億600万円と過去最大の被害であったことが報告されました。また、特に6月以降に発生件数が急増しており、IDやパスワードの入手手段として、ウイルスにより表示された不正画面に入力を促して盗むものが多くみられたことや、11月以降には、メールによるフィッシングサイトへの誘導が多発していることが報告されています。

2月には不正に入手したIDとパスワードを用いてISPへのアクセスを行ったとして、プロキシサーバを運営していた会社の社長他2名が、不正アクセス禁止法違反容疑で逮捕されています。この会社で運営していたプロキシサーバは、記録を取っておらず、利用者の追跡ができない状態で運用されていたことから、ネットバンキングの不正送金や標的型攻撃のメール送信に利用されていたとされています。

同じく2月には、一昨年話題となった、遠隔操作ウイルスに関連する一連の事件で逮捕され、威力業務妨害罪などに問われた容疑者の初公判が行われました。容疑者は無罪を主張しています。

3月には総務省から、ISPやインターネットエクスチェンジ及び研究者の協力を得て実施している、インターネットにおけるトラヒックの定期的な集計・試算の2013年11月の集計結果が公表されました[*30]。これによると2013年11月時点のブロードバンドサービス契約者の推定総ダウンロードトラヒックは、約2.6Tbpsとなり、前年同月に比べ35.6％増加となっています。また、総アップロードトラヒックは、推定で約834Gbpsとなっており、こちらも前年同月に比べて25.2%増加しています。

＊25 内閣官房情報セキュリティセンター、「情報セキュリティ政策会議　第３５回会合（平成２５年６月１０日）」（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku35）。
＊26 内閣官房情報セキュリティセンター、「情報セキュリティ政策会議　第３６回会合（平成２５年６月２７日）」（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku36）。
＊27 承認されたgTLDについては次のICANN"DELEGATED STRINGS"（http://newgtlds.icann.org/en/program- status/delegated-strings）で確認できる。
＊28 ICANN、"New gTLDs Update: Applications Accepted Today; New Guidebook Posted; Financial Assistance for Qualifying Applicants"（http://www.icann.org/en/news/announcements/announcement-11jan12-en.htm）。
＊29 警察庁、「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」（http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf）。
＊30 総務省、「我が国のインターネットにおけるトラヒックの集計・試算」（http://www.soumu.go.jp/menu_news/s- news/01kiban04_02000077.html）。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は、状況により多岐にわたります。しかし、攻撃の多くは、脆弱性等の高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2014年1月から3月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。ここでは、IIJ DDoSプロテクションサービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*31]、サーバに対する攻撃[*32]、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、495件のDDoS攻撃に対処しました。1日あたりの対処件数は5.5件で、平均発生件数は前回のレポート期間と比べてほとんど変わりません。DDoS攻撃全体に占める割合は、サーバに対する攻撃が61%、複合攻撃が20.8%、回線容量に対する攻撃が18.2%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大60万1千ppsのパケットによって2.86Gbpsの通信量を発生させる攻撃でした。攻撃の継続時間は、全体の90.5%が攻撃開始から30分未満で終了し、9.5%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃はありませんでした。なお、今回もっとも長く継続した攻撃は、サーバに対する攻撃に分類されるもので10時間55分にわたりました。また、この期間中に話題となったNTPによる攻撃では、最大で51万7千ppsのパケットによって1.8Gbpsの通信量を発生させる攻撃が発生しています。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*33]の利用や、DDoS攻撃を行うための手法としてのボットネット[*34]の利用によるものと考えられます。

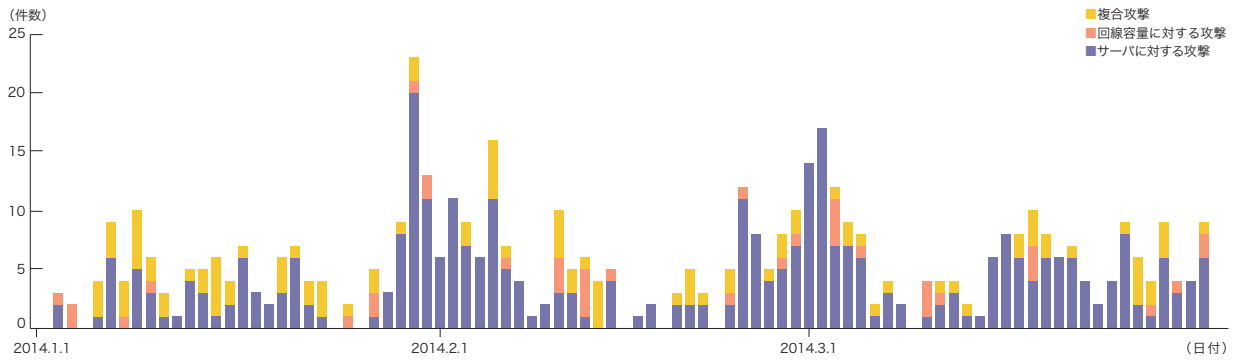


図-2 DDoS攻撃の発生件数

*31 攻撃対象に、本来不必要な大きなサイズのIPパケットやその断片を大量に送りつけることで、攻撃対象の接続回線の容量を圧迫する攻撃。UDPパケットを利用した場合にはUDP floodと呼ばれ、ICMPパケットを利用した場合にはICMP floodと呼ばれる。

*32 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃など。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリなどを無駄に利用させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立した後、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

*33 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、送出すること。

*34 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*35]によるDDoS攻撃のbackscatter観測結果を示します[*36]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2014年1月から3月の期間中に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものはWebサービスで利用される80/TCPで、対象期間における全パケット数の33.1%を占めています。またDNSに利用される53/UDP、リモートデスクトップで利用される3389/TCPやSSHで利用される22/TCPなどへの攻撃、通常は利用されない8010/TCPや8000/TCPなどの攻撃が観測されています。

図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、米国の15.2%が最も大きな割合を占めていました。その後にチリの9.6%、ドイツの9.0%といった国が続いています。前回に引き続きチリのIPアドレスを多く観測していますが、これは複数のIPアドレスから複数のハニーポットの445/TCPに対するパケットを当期間中、合計で7万2千回以上観測したためです。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、Webサーバ(80/TCP)への攻撃としては、1月2日から4日にかけて米国のホスティング事業者、2月18日にはドイツのホスティング事業者、また、2月23日から24日にかけて香港のホスティング事業者がベリーズ国内に持つIPアドレスに対する攻撃をそれぞれ観測しています。1月23日には中国国内のサーバに対する8400/TCPへの攻撃が、3月24日にはドイツにあるロシア語サイトに対する8000/TCPへの攻撃が、また、3月26日から27日にかけて英領バージン諸島のISPが持つIPアドレスに対する8010/TCPへの攻撃が観測されています。

今回の期間では、2月4日からDNS(53/UDP)のbackscatterが増加傾向にあります。そのほとんどは、多数のIPアドレス

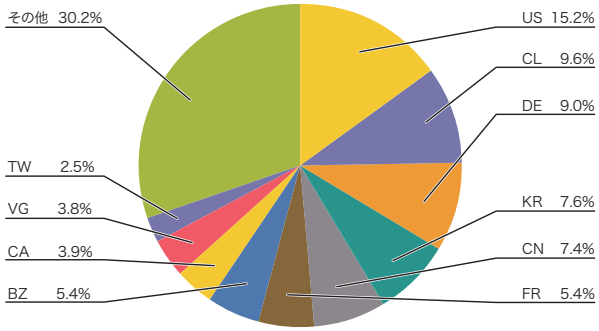


図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

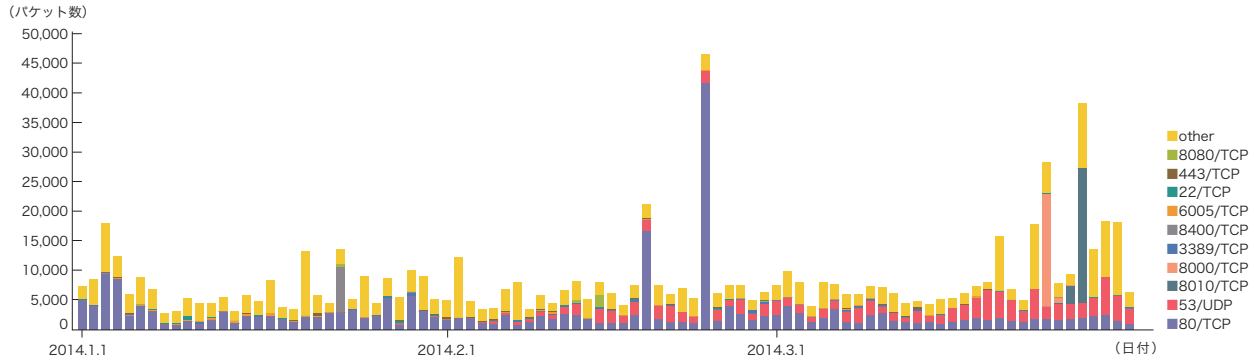


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*35 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。「1.3.2 マルウェアの活動」も参照。

*36 この観測手法については、本レポートのVol.8(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

に、ランダムな文字列を含むドメイン名を問い合わせた結果と考えられるパケットでした。これらのパケットと直接に関連するかどうかは不明ですが、4月15日にJPRSからキャッシュポイズニング攻撃の危険性増加に対して注意喚起が発せられています[*37]。DNSサーバの設定を再確認すると共に、今後の動向に注意していく必要があります。

また、1月4日にオンラインゲーム関連のサーバに対する攻撃を観測しましたが、これは複数のゲーム関連や技術関連のニュースサイトで報じられた攻撃の一部でした。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*38]による観測結果を示します。MITFでは、一般利用者と同様にインターネットに接続したハニーポット[*39]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

■ 無作為通信の状況

2014年1月から3月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量（到着パケット数）の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類（上位10種類）ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPやWindowsのリモートログイン機能である、RDPで利用される3389/TCP、SSHで利用される22/TCP、HTTPで利用される80/TCP、ICMP Echo Request、DNSで利用される53/UDP、Telnetで利用される23/TCPによる探査行為も観測されています。

期間中、SSHの辞書攻撃の通信も散発的に発生しており、例

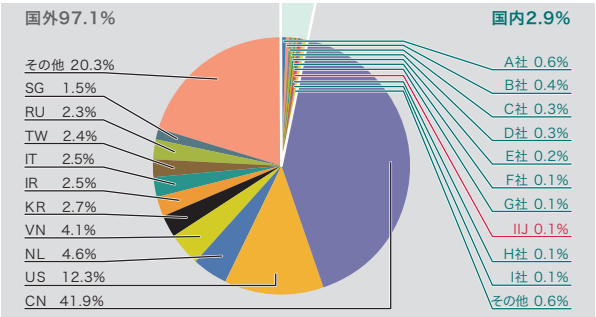


図-5 発信元の分布（国別分類、全期間）

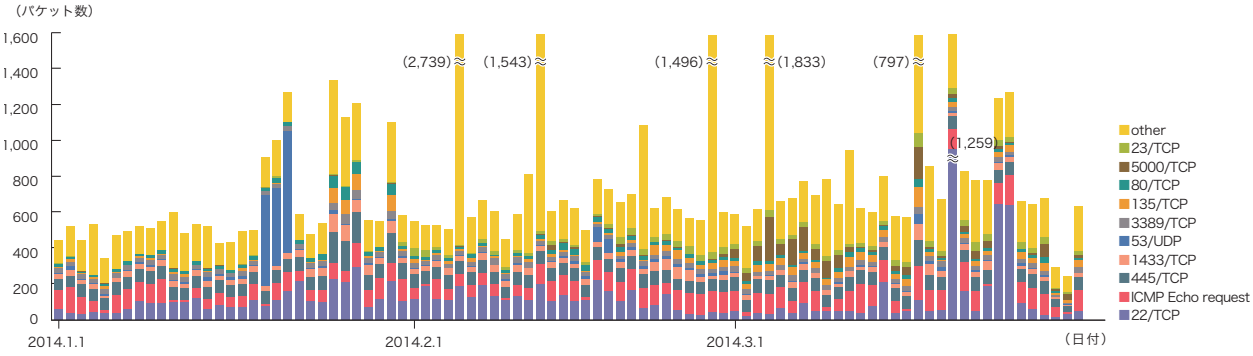


図-6 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊37 JPRS、「（緊急）キャッシュポイズニング攻撃の危険性増加に伴うDNSサーバーの設定再確認について（2014年4月15日公開）」(http://jprs.jp/tech/security/2014-04-15-portrandomization.html)。

＊38 Malware Investigation Task Forceの略。MITFは2007年5月から開始した活動で、ハニーポットを用いてネットワーク上でマルウェアの活動の観測を行い、マルウェアの流行状況を把握し、対策のための技術情報を集め、対策につなげる試み。

＊39 脆弱性のエミュレーションなどの手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

えば3月20日に発生している通信はシンガポールと韓国、3月24日から3月25日にかけて発生している通信は、イタリアに割り当てられたIPアドレスからのものです。また、1月中旬から2月にかけて、SSHの通信が前回の期間中に比べて増加しています。これは主に中国に割り当てられたIPアドレスからの通信が増加したためです。

1月19日から1月21日にかけて、DNSの通信が増加しています。通信内容を確認したところ、オランダに割り当てられたIPアドレスが28ドメインに対し、ANYレコードの問い合わせを繰り返し試行していました。詳細に調査したところ、28のドメインはいずれも応答として比較的大きなサイズの応答をしていることから、攻撃者がこのオランダのIPアドレスを詐称して問い合わせを繰り返すことで、そのIPアドレスに対するDNSAmp攻撃の試行をしていたとIIJでは考えています[*40]。

また、2月5日にベトナム、2月12日、2月27日、3月4日に中国に割り当てられた1つのIPアドレスから、広範囲に繰り返し探査行為が行われています。対象となるポートは1000から9999までのTCPと一部のUDPでした。

■ 組み込み機器（NAS、DVR）に対する探査と攻撃

期間中、2月中旬以降から5000/TCPに対する探査行為が増加し始め、3月に大幅に増加しました。ハニーポットに到着した5000/TCP通信の送信元IPアドレスの総量（到着パケット数）の推移（ハニーポット1台あたりの平均値）を図-7に示します。

これは、Synology社のNASやHikvision社のDVR（Digital Video Recorder）製品への脆弱性の探査もしくは攻撃であると考えています。この製品に対する任意のコード実行が可能な脆弱性が2013年に発見されており、Exploitも既に公開されています。警察庁やSANS ISCもブログで同様の事象と思われる内容を複数回に渡って報告[*41]しており、攻撃を受けたと思われる製品からこの製品には本来存在しないマルウェアと思われるプログラムが検出されたと報告しています。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち図-9と図-10では、1日あたりに取得した検体[*42]の総数を総取得検体数、検体の種類をハッシュ値[*43]で分類したものを

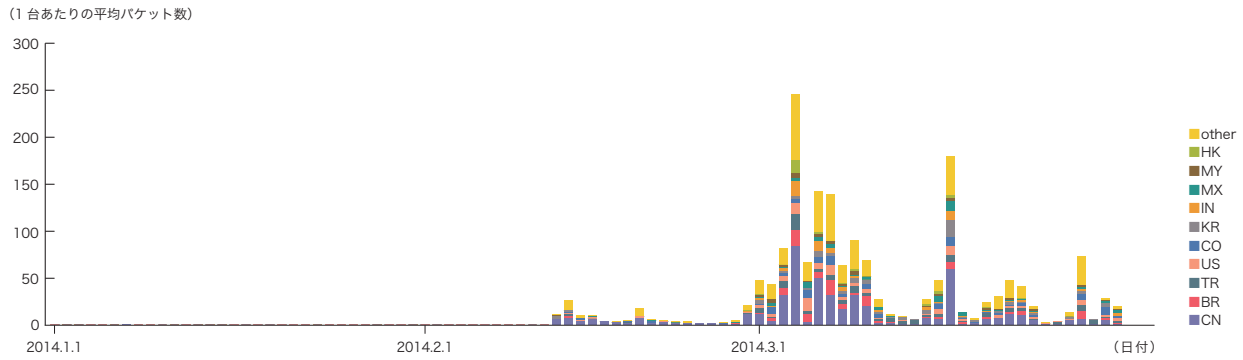


図-7 ハニーポットに到着した5000/TCPの通信の発信元IPアドレスの国別推移（ハニーポット1台あたりの平均値）

＊40 ハニーポットはDNSの問い合わせを拒否するため、当該IPアドレスには増幅された応答は届いてはいない。

＊41 警察庁の発表は以下のとおり。「脆弱性が存在するNASの探索と考えられる宛先ポート5000/TCPに対するアクセスの急増について（http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf）」。SANS ISCでは、次の4つのブログエントリで本事象に関するハニーポットのデータやマルウェアの調査結果を報告している。"TCP/5000 - The OTHER UPNP Port"（https://isc.sans.edu/diary/TCP5000+-+The+OTHER+UPNP+Port/17763）。"Port 5000 traffic and snort signature"（https://isc.sans.edu/diary/Port+5000+traffic+and+snort+signature/17771）。"Let's Finally "Nail" This Port 5000 Traffic - Synology owners needed."（https://isc.sans.edu/diary/Let%27s+Finally+%22Nail%22+This+Port+5000+Traffic+-+Synology+owners+needed./17859）。"More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!)"（https://isc.sans.edu/diary/More+Device+Malware%3A+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+%28and+now+with+Bitcoin+Miner!%29/17879）。

＊42 ここでは、ハニーポットなどで取得したマルウェアを指す。

＊43 様々な入力に対して一定長の出力をする一方向性関数（ハッシュ関数）を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディングなどにより、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮した上で指標として採用している。

ユニーク検体数としています。また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-9と図-10は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行いConfickerと認められたデータを除いて集計しています。

期間中での1日あたりの平均値は、総取得検体数が114、ユニーク検体数が21でした。1月25日と3月17日にotherが増加しています。これらは、それぞれブラジルと台湾に割り当てられたIPアドレスからのAllaple[*44]ファミリが増加したことによります。Allapleはポリモーフィックマルウェアであることが知られており、図-10により顕著に表れていることが確認できます。

未検出の検体をより詳しく調査した結果、インドなど、複数の国に割り当てられたIPアドレスからワーム[*45]が観測されました。また、未検出の検体の約71%がテキスト形式でした。これらテキスト形式の多くは、HTMLであり、Webサーバからの404や403によるエラー応答であるため、古いワームなどのマルウェアが感染活動を続けているものの、新たに感染させたPCが、マルウェアをダウンロードしに行くダウンロード先のサイトが既に閉鎖させられていると考えられます。

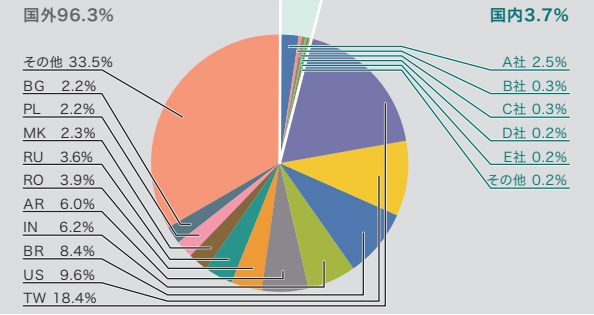


図-8 総取得検体数の分布

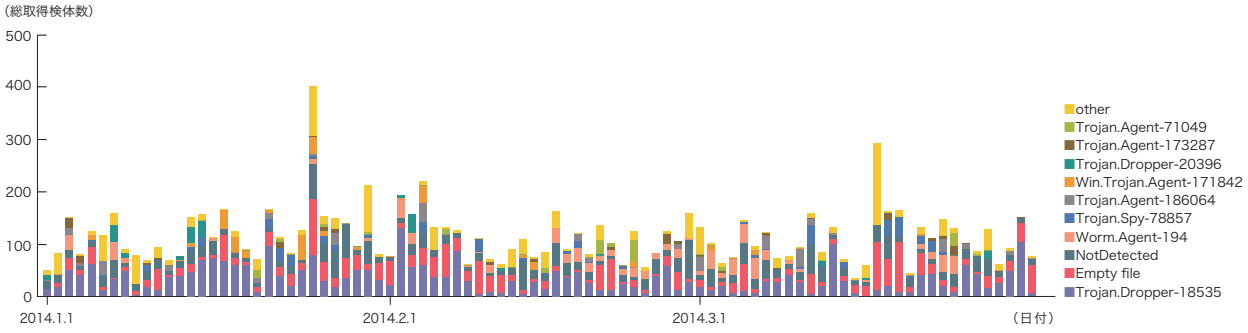


図-9 総取得検体数の推移(Confickerを除く)

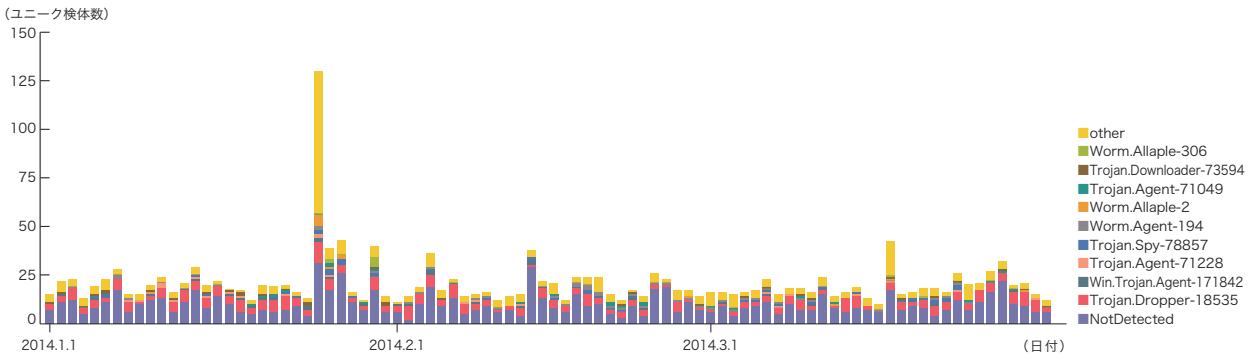


図-10 ユニーク検体数の推移(Confickerを除く)

*44 Win32/Allaple(http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Win32%2fAllaple)。
*45 WORM_ATAK(http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D)。

MITF独自の解析では、今回の調査期間中に取得した検体は、ワーム型92.4%、ボット型4.6%、ダウンローダ型3.0%でした。また解析により、16個のボットネットC&Cサーバ[*46]と7個のマルウェア配布サイトの存在を確認しました。

■ Confickerの活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が35,739、ユニーク検体数は787でした。短期間での増減を繰り返しながらも、総取得検体数で99.7%、ユニーク検体数で97.3%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerを含む図は省略しています。本レポート期間中の総取得検体数は前号の対象期間中と比較し、約2%減少しています。また、ユニーク検体数は前号から約4%増加しました。Conficker Working Groupの観測記録[*47]によると、2014年3月31日現在で、ユニークIPアドレスの総数は1,277,911とされています。2011年11月の約320万台と比較すると、約40%に減少したことになりますが、依然として大規模に感染し続けていることが分かります。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*48]について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2014年1月から3月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-11に、攻撃の推移を図-12にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、中国65.4%、日本20.8%、米国7.4%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回に比べて大幅な増加が見られましたが、これはこの期間中、中国からの大規模な攻撃が複数発生したためで、これを除いた検知傾向はそれほど変化していません。

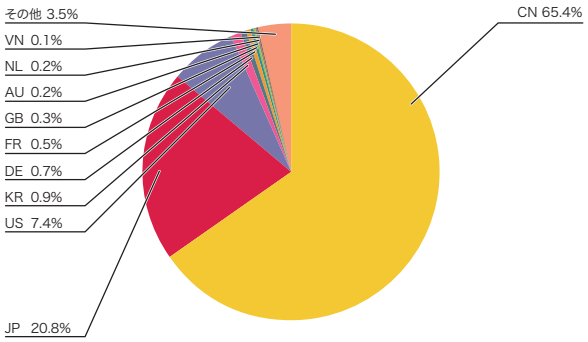


図-11 SQLインジェクション攻撃の発信元の分布

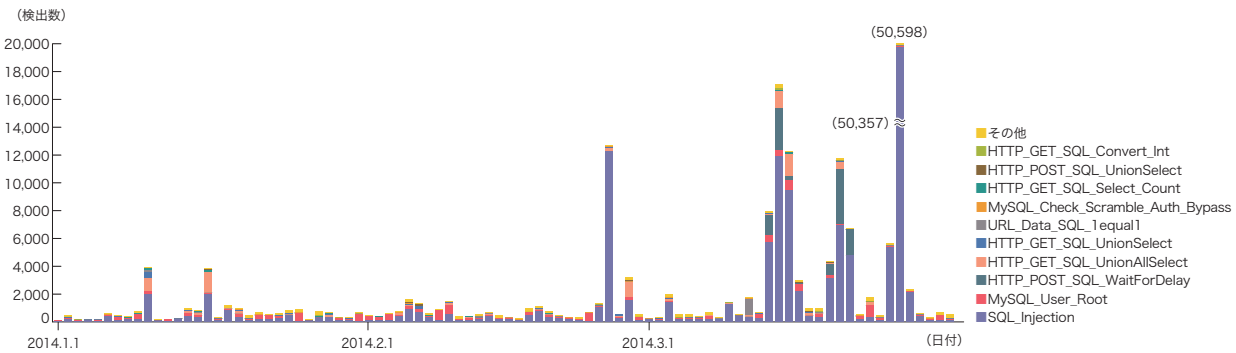


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*46 Command&Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。
*47 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking)。
*48 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

この期間中、2月25日には、中国の特定の攻撃元より特定の攻撃先への攻撃が発生していました。3月13日から15日にかけては、別の中国の複数の攻撃元より別の特定の攻撃先に対する攻撃が発生していました。この攻撃は3月19日から21日にかけても、中国の同じ特定の攻撃元を含む複数の攻撃元より同じ特定の攻撃先に対する攻撃が発生しています。3月25日から27日にかけては、別の中国の特定の攻撃元より別の特定の攻撃先に対する大規模な攻撃が発生しています。これらの攻撃はWebサーバの脆弱性を探る試みであったと考えられます。

ここまでに示したとおり、各種の攻撃はそれぞれ適切に検出され、サービス上の対応が行われています。しかし、攻撃の試みは継続しているため、引き続き注意が必要な状況です。

1.3.4 Webサイト改ざん

ここでは、MITFのWebクローラ(クライアントハニーポット)によって調査したWebサイト改ざん状況を示します*49(図-13)。このWebクローラは、国内の著名サイトや人気サイトなどを中心とした数万のWebサイトを日次で巡回しており、更に、巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなども観測対象に加えています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

2014年1月から2月の中旬ごろまでは、Sweet Orange Exploit Kit及びRamayana Exploit Pack(別名DatkaChefまたはDotCacheF Exploit Kit)による攻撃が多くを占めていました。これは、昨年末から続いている傾向で、改ざんされ攻撃に悪用されているのも、中小企業やネットショップなど、比較的小規模なWebサイトが多くを占めていました。これらの攻撃は、Exploit Kitの傾向から、主に古いバージョンのJREの脆弱性などを攻撃対象にしているものと考えられます。

一方、2月後半以降は、攻撃の総数が激減し、Sweet Orange Exploit Kitを用いた攻撃はまったく観測されなくなりました。代わりに、Infinity Exploit Kit(別名Red Kit v2またはGoon Exploit Kit)による攻撃が増加しており、2月20日に公開され、当時パッチが未公開であったMicrosoft Internet Explorerの脆弱性(CVE-2014-0322)を悪用する攻撃が観測されました。この時期は、比較的知名度の高い大手企業のWebサイトの改ざんが複数発生しており、それらのほとんどのケースで前述のInternet Explorerの脆弱性を悪用する攻撃が行われていました。

3月下旬には、攻撃はほぼ収束傾向となり、国内でのドライブバイダウンロード攻撃が減少傾向にあるものと推測される状況となっています。ただし、このような傾向は攻撃者の意図によって急変する可能性があるので、Webサイト運営者、訪問者共に、引き続き注意が必要です。

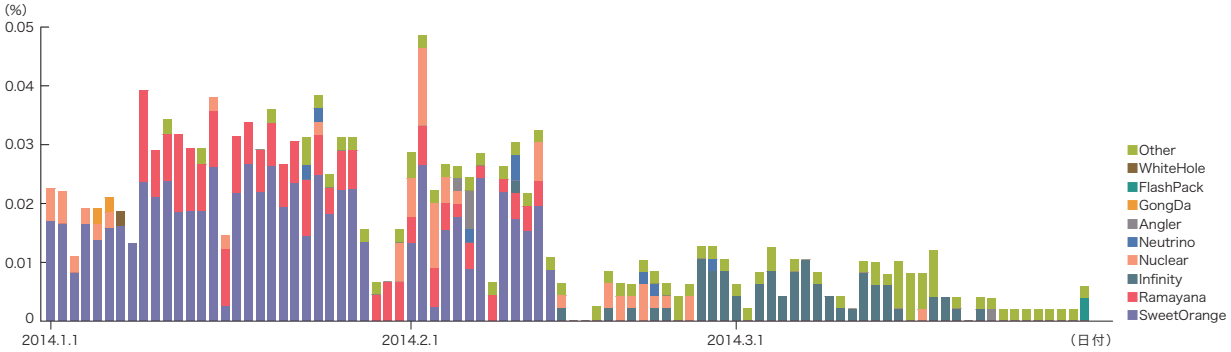


図-13 Webサイト閲覧時のドライブバイダウンロード発生率(%)(Exploit Kit別)

※ 調査対象は日本国内の数万サイト。
近年のExploit Kitでは、クライアントのシステム環境やセッション情報、送信元アドレスの属性、攻撃回数などのノルマ達成状況などによって攻撃内容や攻撃の有無が変わるよう設定されているため、試行環境やクロールタイミングなどの状況によって異なる結果が得られる場合がある。
※ 2月15日及び16日はWebクローラを停止していたため、攻撃を検知していない。

*49 Webクローラによる観測手法については本レポートのVol.22(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf)の「1.4.3 Webクローラによる Webサイト改ざん調査」で仕組みを紹介している。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、PlugXの背後にいる攻撃者について、DrDoS攻撃とその対策、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会、の3つのテーマについて紹介します。

1.4.1 PlugXの背後にいる攻撃者

2014年3月、IIJではBlack Hat Asia 2014[*50]において、PlugX[*51]に関する講演を行いました。この講演は、PlugXの検体からC&Cサーバなどの設定情報を抽出して解析することで、PlugXの検体群から共通項を見つけてグループ化し、それらPlugXグループの背後にどのような標的型攻撃のグループが関与しているかを調査したものです。本章では、その結果を共有すると共に、なぜこの調査を行ったのかを併せて解説します。

■ PlugXの亜種

PlugXは、2012年3月に発見されたRAT[*52]であり、標的型攻撃での利用が度々確認されています。IIJでは、PlugXの亜種が本稿執筆時点で大きくわけて3タイプ存在することを確認しています。ここでは、それらをType I、II、IIIと呼ぶことにします。Type Iは、PlugXが発見されてから今まで一番多く発見されている検体であり、以前、本レポートのVol.21[*51]で解説しています。Type IIは、IIJ-SECT Security Diaryで新型PlugX[*53]として報告したとおり、2013年の第3四半期に発見された亜種です。PlugXの特徴であった"GULP"というシグネチャを含むヘッダを取り除き、Basic認証付きのProxyを通過する機能を持つなど、Type Iよりも大きく進化しています。Type IIIはType Iより前から存在しており、PlugXの前身[*54]として過去の事件に使用されたことが報告されています。C&Cサーバからの命令を処理するコマンドや、通信の特徴はTypeIやIIとほぼ同一でありながら、コードの特徴は大幅に異なり、耐解析機能もより強化されています。また、Type IやIIと同様に、現在でもアップデートされ続けています。

■ 各PlugX検体からの設定情報の抽出

PlugXの各亜種は、それぞれコードの特徴が大きく異なります。そこで、IIJでは各亜種に対応する抽出スクリプトをそれぞれ作成することで、すべての亜種から有用な設定情報（C&Cサーバや、サービス名、レジストリ値といった自動実行に関する情報など）の抽出を可能にしました。Type IとIIに関しては、多くの処理を共通化することができたため、1つのImmunity Debugger[*55]用のスクリプトとして実装しています。Type IIIは、PlugXのコードを特定するための特徴が、難読化などの耐解析機能によって正規化できなかったため、半自動で抽出を行うIDA Python[*56]スクリプトとして実装しました。これらのスクリプトを利用して、150のユニークハッシュ値を持つPlugXの検体から設定情報の抽出を試みました。このうち、27検体については設定情報を持たない、デモバージョン[*57]でした。よって、残りの123検体について分類の対象としています。

---

*50 Black Hat (https://www.blackhat.com/) は米国、ヨーロッパ、アジアの主に3地域で毎年開催されている世界最大規模のITセキュリティのカンファレンス。IIJでは今回アジア地域で行われたBlack Hat Asia 2014にて講演を行った。

*51 PlugXはIIR vol.21（http://www.iij.ad.jp/company/development/report/iir/021.html）で詳しく解析している。

*52 Remote Administration Toolの略で、主にホストを遠隔から操作するためのマルウェアの一種。標的型攻撃ではこの種のマルウェアを起点に攻撃が行われることから、IIJでもこのマルウェアに注目して解析を行っている。専門家によってはRemote Access ToolやRemote Access Trojanの略であると定義する場合もある。

*53 IIJ Security Diary「新型PlugXの出現（https://sect.iij.ad.jp/d/2013/11/197093.html）」。Type IIやType IIIの亜種についてそれぞれ触れている。

*54 「SK Hack by an Advanced Persistent Threat（https://www.commandfive.com/papers/C5_APT_SKHack.pdf）」によると、2011年の攻撃で、Destory RATと呼ばれるRATが使用されていることが報告されている。これはPlugX Type IIIとほぼ同一であることをIIJでは確認している。

*55 Immunity DebuggerはImmunity社が提供しているWindows用のデバッガ（https://www.immunityinc.com/products-immdbg.shtml）。OllyDbgを基に作成されており、Python拡張が特徴の1つ。プラグインやスクリプトをPythonで記述できる。

*56 IDA PythonはHex-Rays社が提供する逆アセンブラ、デバッガであるIDA Pro（https://www.hex-rays.com/products/ida/）で処理を自動化するためのPython拡張。

*57 PlugXのデモバージョンに関する詳細は次のサイトが詳しい「An Analysis of PlugX（http://lastline.com/labs/plugx）」。デモバージョンの場合、設定情報は文字列 "XXXX" でパディングされることが多いため、情報を抽出することはできない。ただし、一部の検体ではデモバージョンのフラグが立っているにも関わらず、設定情報を持ち、パディングがされない検体が存在することも確認している。そのような検体は解析対象に含めている。

■ PlugXの分類

図-14は、PlugXの分類手法を図示したものです。前述のスクリプトを用いて設定情報を抽出後、各検体の共通項を見つけて分類しています。

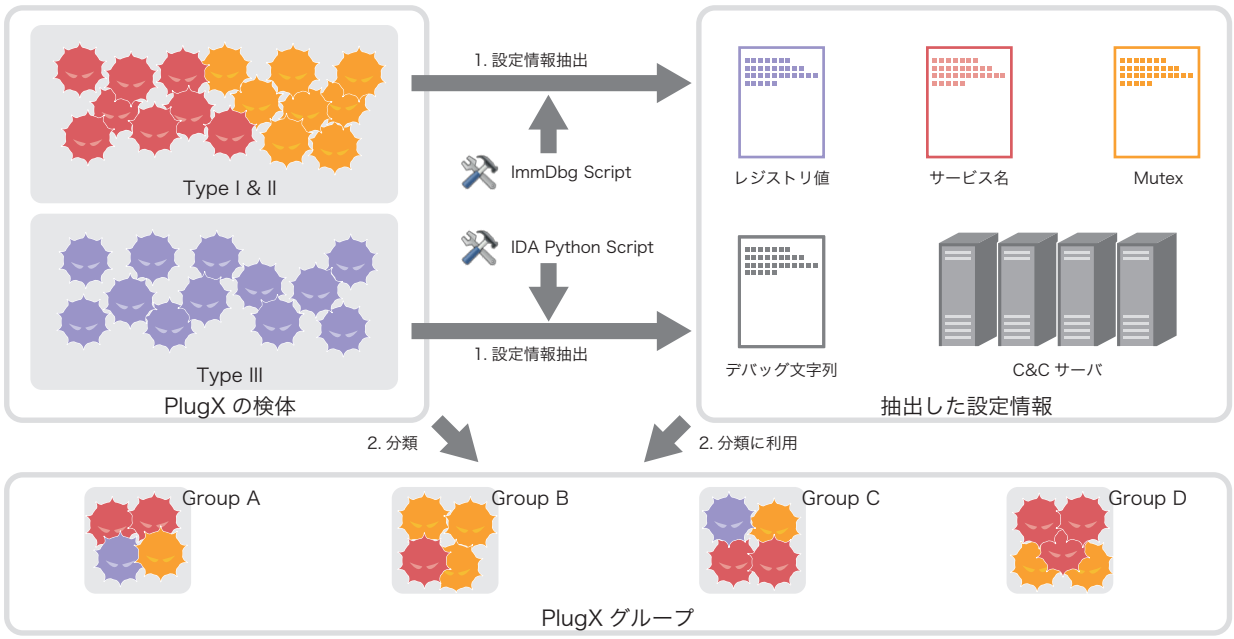
第一段階としてサービス名を基に分類しました。PlugXは、感染ホストが再起動した場合でも継続的に活動できるよう、感染時にサービスやレジストリのRunキーに登録を行います。これらの値で特徴的なものをグルーピングしました[*58]。第二段階では、C&Cサーバの情報(FQDN、IPアドレス[*59]、ドメイン名、ドメイン所有者のメールアドレス)や、コード内のデバッグ文字列[*60]を基に更なるグルーピングを行いました。

これらの作業を繰り返してできたグループを表-1に示します。全PlugX検体の約3分の2を7グループに分類することができました。なお、今回は、最低4つの検体が属しているものを1グループとしています。

表-1 PlugX検体の分類結果

PlugXグループ名	Type I	Type II	Type III	グループの合計	
*Sys	15	0	5	20	全検体の約3分の2(67%)
*Http	12	3	0	15	
Starter	13	7	4	24	
Graphedt	8	0	0	8	
WS	6	1	0	7	
360	4	0	0	4	
cochin	0	0	4	4	
- (Others)	30	8	3	41 ※注	

※注 : 内8検体は標的型攻撃者グループと関連が確認された。



1. 各PlugXの検体からそれぞれのタイプに応じたスクリプトを用いて設定情報を抽出する。
2. 抽出した設定情報を基に、各検体間で設定情報の値が一致、もしくは整合性があるものを同じグループとして分類する。

図-14 PlugXの分類方法

＊58 サービス名でグルーピングする際「SxS」、「XXX」、「TVT」といった、デフォルト値はグルーピングのキーから除いた。一方、サービス名で同一グループとして分類された検体の多くは、その検体間でC&Cサーバの情報が一致するか、類似性が見られた。このことからも、一定の時期もしくは攻撃者ごとに独自のサービス名をつけている可能性が高いと考えられる。

＊59 FQDNを名前解決したものも含む。

＊60 PlugXの検体の多くは現在も開発が頻繁に行われている。そのためかデバッグを有効にしてコンパイルされている検体が多く存在する。PlugXで何らかの処理中にエラーが発生した場合、そのエラーの内容と共に、どのバージョンで不具合が発生したかを示すバージョン情報や中国語圏の文字列を含むパス情報を併せてログとして記録するルーチンが存在する。このパス情報の文字列は数多くのパターンが存在するため、この情報も同一攻撃主体を示すものの1つとして利用できると考えられる。次のWebサイトでは、多くのデバッグ文字列例が紹介されている。「CASSIDIAN CyberSecurity Blog PlugX: some uncovered points (http://blog.cassidiancybersecurity.com/post/2014/01/plugx-some-uncovered-points.html?2014/01/plugx-some-uncovered-points.html)」。

■ 既知の標的型攻撃者グループとの比較

最後に、前項で生成したPlugXグループが、既知の標的型攻撃者グループとの関係があるかを調査しました。具体的には、標的型攻撃の外部レポートに記載されている検体のハッシュ値や、C&Cサーバの情報が一致しているかを調査しました。図-15は、それらの関係性をまとめたものです。今回の調査では7つのPlugXグループのうち、5グループが何らかの既存の事件に関連していることが分かりました。特に、5グループ中4グループが、APT1 [*61]と呼ばれる攻撃者グループと関連していることが今回の調査で分かりました。これは、多くのPlugXを使う攻撃者がAPT1に属している、もしくは、少なくとも異なる攻撃者グループ間でインフラを共有していることを示しています。また、今回グループに分類しきれなかったPlugXのうち、8検体についてはAPT1やWinnti [*62]など、何らかの既知の標的型攻撃者グループに関わりがあることが判明しました。

■ 新たな対策手法の検討

今回は、PlugXを例にしてこのような調査を行いました。標的型攻撃では、少数の特定組織が狙われるため、攻撃者の意図、組織の規模、攻撃に使うツール、インフラ設備などの全貌が見えにくいという側面があります。各組織が入手できる検体数も限られており、少数の検体から得られた情報を頼りに対策を行うことになりがちです。それに対して、もし多くの検体を集められた場合、今回のように、多くのPlugXグループがAPT1との関連が見つかるなどの新たな事実が判明する可能性があります。もしそのようなことが分かれば、例えば、APT1の攻撃者がRATを経由して組織内に侵入した後に使用する攻撃手法や、攻撃ツールの特徴を基にした検出や対策が行えるなど、攻撃の進行状況に応じた多角的な対策を取ることができる可能性があります。

Black Hat ASIAにおける発表では、講演資料や設定情報抽出スクリプトに加え、各PlugXの検体と既知の標的型攻撃者グループとの相関図も併せて配布[*63]しています。これはSVGと呼ばれる画像フォーマットになっています。SVGは、画像でありながら実際にはXML形式でもあるため、これを解析することでC&Cサーバなど、今回開示した情報をすべて取り出すことができます。そのため、このデータを利用して出口対策などが可能になります。

標的型攻撃を受けた各組織が、もっと広く詳細に情報を開示

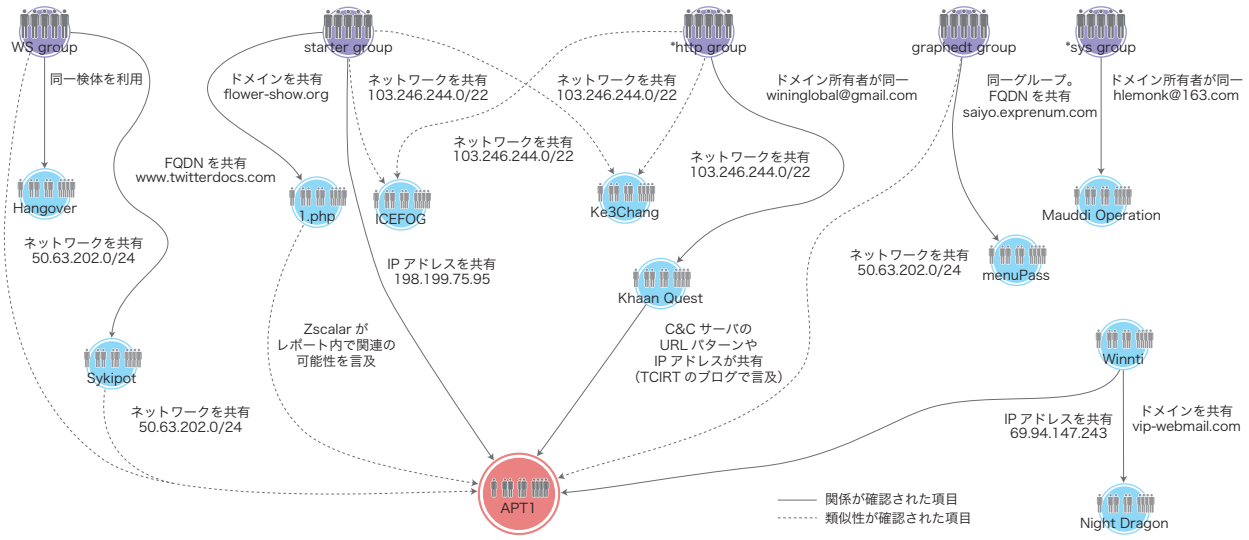


図-15 PlugXグループと標的型攻撃者グループとの相関図

*61 APT1はMandiant社が報告した標的型攻撃を行うグループの1つ(http://intelreport.mandiant.com/)。

*62 WinntiはKaspersky Lab社が報告した、ゲーム業界を標的とする標的型攻撃(https://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf)。

*63 今回の講演資料、抽出スクリプト及び相関図はBlack Hatのアーカイブサイトから入手できる(https://www.blackhat.com/asia-14/archives.html#Haruyama)。スクリプトは更新版を以下でも配布している(http://takahiroharuyama.github.io/blog/2014/03/27/id-slash-idapython-scripts-extracting-plugx-configs/)。

し合うことが標的型攻撃の対策につながります。IIJではこの様な解析や調査活動を継続し、積極的に情報を開示することによって、標的型攻撃の対策に向けた活動を行っていきます。

1.4.2 DrDoS攻撃とその対策

2013年3月に、DNSのオープンリゾルバを悪用したDDoS攻撃が問題となりました[*64]。この攻撃は、外部からの再帰的な問い合わせを許可しているDNSキャッシュサーバを悪用し、攻撃対象のIPアドレスに送信元IPアドレスを偽装した問い合わせを行うことで、その応答を攻撃対象のサーバに対するDDoS攻撃として送りつけるものでした。

10月頃には、NTPによるDDoS攻撃が観測されており[*65]、12月には米国Symantec社がブログで、NTPによるDDoS攻撃に関する報告を行いました[*66]。これらのNTPによるDDoS攻撃では、NTPの管理機能の1つであるmonlistを悪用しており、DNSによる攻撃と同様に送信元IPアドレスを偽装した問い合わせを行うことでDDoS攻撃を行っていました。この問題については2014年1月に入り、DDoS攻撃に悪用される可能性が高いとして、日本でもJPCERTコーディネーションセンターなど複数の組織から注意喚起が行われており[*67]、実際に、この攻撃によると考えられる被害や、踏み台となった事件が複数確認されています。更に、欧米では2013年12月頃から何者かによるゲーム関連サイトなどに対するNTPによるDDoS攻撃が複数発生しており、最大で80Gbpsにも達したことが、米国のDDoS対策事業者の1つであるStaminus社によってブログで報告されています[*68]。また、クラウド事業者であるCloudFlare社のブログでは、同社の顧客に対して、攻撃規模としては最大で400Gbpsの攻撃があったことを報告しており[*69]、更に、ArborNetworks社からは、同社の複数ISPネットワークにおける観測情報として、NTPによる通信量が最大で800Gbpsにも上ったと報告されています[*70]。

これらの攻撃は、Distributed Reflection Denial of Service attacks（以下、DrDoS攻撃）と呼ばれ、その攻撃の容易さと増幅率による影響の大きさから問題となっています。本稿では、DrDoS攻撃について解説すると共にその対策について検討します。

■ DrDoS攻撃の仕組み

DrDoS攻撃はその名のとおり、ある通信の応答（反射）を悪用した攻撃です。DNSやNTPなど、UDPのサービスが悪用されることが多いですが、これはUDPがコネクションレスのプロトコルであることに起因しており、攻撃の容易さに繋がっています。攻撃は踏み台となった脆弱な機器のIPアドレスからの攻撃に見えるため、被害者からは本当の攻撃者が分かりません。このため、攻撃元からの通信を遮断するなどの対処を行ったとしても、新たな踏み台を見つけて攻撃が継続できることから、被害者側での対策が攻撃の根本対処にはつながらない場合もあります。

更に、攻撃先を直接攻撃する場合に比べ、DrDoS攻撃では、問い合わせに対する応答のデータ量が多いことを利用して、その攻撃規模を数倍から数十倍に増幅させます。例えば、DNSの場合では理論上の増幅率は70倍まで増幅される可能性があります[*71]。今回問題となった、NTPのmonlist機能を悪用した攻撃の場合、1つの問い合わせに対し、理論上の最大値で返答した場合、約200倍のデータが送られることになります。このように、NTPの場合には増幅率が非常に

---

*64 DNSオープンリゾルバ問題については、本レポートのVol.21「2. インターネットオペレーション DNS オープンリゾルバ問題 」も参照のこと、(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol21.pdf)。

*65 リトアニアの研究教育機関のネットワークであるLITNETのCERTチームの報告で確認できる。LITNET CERT、"NTP DoS reflection attacks" (https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks)。

*66 Symantec Cyber Readiness & Response Blog、"Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks" (http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks)。

*67 JVN、「JVNVU#96176042　NTP が DDoS 攻撃の踏み台として使用される問題」(https://jvn.jp/vu/JVNVU96176042/index.html)。

*68 Staminus Communications、"Mitigating 80 Gbps Attacks – NTP Amplification Attacks on the Rise"　(https://blog.staminus.net/mitigating-80-gbps-attacks-ntp-amplification-attacks-on-the-rise)。

*69 CloudFlare、"Technical Details Behind a 400Gbps NTP Amplification DDoS Attack"　(http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack)。

*70 ArborNetworks、"NTP attacks continue – a quick look at traffic over the past few　months" (http://www.arbornetworks.com/asert/2014/03/ntp-attacks-continue-a-quick-look-at-traffic-over-the- past-few-months/)。

*71 実際にはキャッシュDNSサーバの設定などにより増幅率が律速されるため、最大で8倍から40倍程度となる。

高いことが分かります[*72]。DrDoS攻撃では、これにより、攻撃先の回線容量を超える通信量を発生させています。

■ NTPによるDrDoS攻撃とその影響

今回、問題となったNTPのmonlistによるDrDoS攻撃の可能性については、NTPの実装に関する開発者のコミュニティで2010年に指摘されており、同年5月には修正が行われていました[*73]。しかしながら、この修正はDevelopment（開発版）のみに反映され、Stable（安定版）は4.2.6p5のまま、本修正は反映されていませんでした。このため、一部のntpdの実装を使っていたルータなどの機器やUNIX系OSでは、この修正が反映されていませんでした[*74]。

図-16に今回問題となったNTPによるDrDoS攻撃について示します。ntpdなど一部のNTPの実装では、管理のために、参照しているクライアントのIPアドレスの一覧を返すmonlistコマンドが実装されています。外部からのこの問い合わせに応答するルータやサーバなどの機器があった場合、送信元を攻撃先のIPアドレスに偽装した問い合わせを送ることで、返答が攻撃先に返ることになります。攻撃者は、このような通信を多数の機器に対して行うことで攻撃を行います。ntpdでは、参照しているクライアントのIPアドレスを、最大で600までリストとして持つことから、今回の攻撃では、攻撃者は外部から詐称したIPアドレスで連続して問い合わせを行うことで、リストを最大値まで増やした後に、実際の攻撃先を詐称して攻撃を行っていたと考えられます。

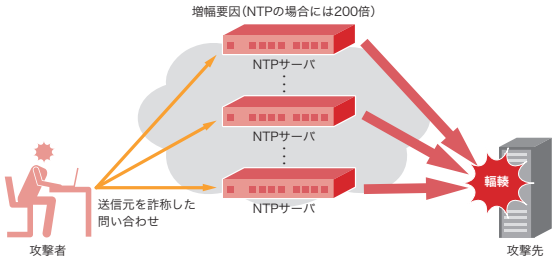


図-16 DrDoS攻撃の概要（NTPの場合）

今回のNTPの問題について、NTPサーバにおいて2つ注意する点があります。1つは、DrDoS攻撃の踏み台として悪用される可能性です。これらの攻撃の踏み台となってしまった場合には、攻撃の被害者であると同時に加害者となってしまうことになります。もう1つは、情報漏えいの可能性です。今回の問題では、管理機能として参照しているクライアントのIPアドレスの一覧を返すmonlistコマンドが使われています。このため、外部からの問い合わせに答えることで、このNTPサーバを利用しているネットワーク上のクライアントのIPアドレスなどの情報が外部に漏れる可能性があります。

■ ハニーポットによる観測状況

図-17に昨年10月初めから今年3月末の期間で、ハニーポットに到着したNTP（123/UDP）の通信について、発信元IPア

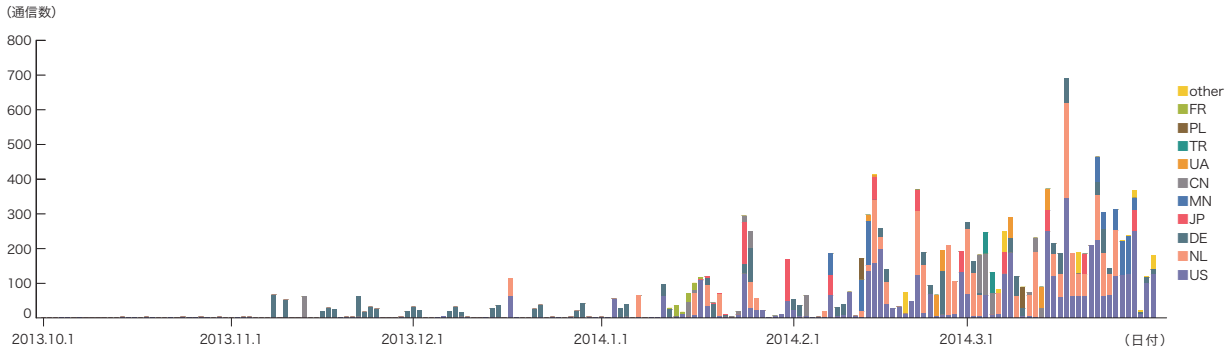


図-17 ハニーポットに到着したNTP（123/UDP）の通信

＊72 攻撃に使われるプロトコルの増幅率については、CERT/CCのアドバイザリでも注意喚起が行われている。"Alert (TA14-017A) UDP-based Amplification Attacks" (https://www.us-cert.gov/ncas/alerts/TA14-017A)。

＊73 4.2.7p26以前のntpdが本脆弱性の影響を受ける。修正については次のntp.orgのBugレポートなども参照のこと。"Bug 1532 - remove ntpd support for ntpdc's monlist (use ntpq's mrulist)"(http://bugs.ntp.org/show_bug.cgi?id=1532)。

＊74 例えば、FreeBSDなどが該当している。The FreeBSD Project、"ntpd distributed reflection Denial of Service vulnerability" (http://www.freebsd.org/security/advisories/FreeBSD-SA-14:02.ntpd.asc)。

ドレスの国別分類を示します。ここに示したとおり、11月中旬よりドイツを発信元とした通信が行われていたことが確認できます。この後、今年の1月中旬にCERT/CCなどから脆弱性情報が公表[*75]された時期から継続的に通信が発生していることが確認できます。国別で見ると、米国が36.8%と最も多く、オランダの25%、ドイツの14.3%と続いており、欧米からの通信が多いことが確認できます。日本からの通信も4位で5.9%ありました。このことから、この問題が公表されてから問題の確認を行ったり、攻撃の試みを行う活動が増加したことが推測できます。また、DrDoS攻撃では、送信元を偽装した問い合わせを問題のあるサーバなどに対して行いますが、この期間に確認された通信では、総数があまり多くないため、外部からの問い合わせを許可しているサーバやルータなどを探索する活動なのか、送信元に対する攻撃なのか判断することはできませんでした。しかしながら、送信元の一部がゲーム関連のサービスを提供していると考えられるIPアドレスであったことなどから、攻撃と探査活動の両方が行われていたと考えられます。

■ DrDoS攻撃への対処

DrDoS攻撃では、IPアドレスを詐称することで比較的容易に攻撃が行えるため、悪用できる脆弱性や新たな攻撃手法が公表されると、すぐに悪用の試みが行われる傾向があります。DrDoS攻撃の発生情報に注意し、自分の管理するシステムが攻撃に悪用される可能性について検討し、対処する努力が必要です。

また、今回の事件では、NTPが問題となりましたが、DrDoS攻撃に利用されるプロトコルはNTPだけではなく、DNSやSNMP、ECHO、Chargenなども悪用される可能性があります。サーバやルータなどの機器をインターネットに接続する場合には、まず、機器の脆弱性情報に注意し、ファームウェアなどについてセキュリティの問題のないバージョンを利用することが必要です。更に、機器において初期状態から動作しているサービスについて、利用者が認識していない状況で、踏み台として悪用されてしまうような場合も見受けられます。このような状況にならないために、機器の導入時には不要なサービスを停止し、適切にアクセス制御を設定します。導入後においても、動作するサービスについてインターネット側から継続的に調査することで、設定ミスを早期に発見することができ、外部から第三者に悪用される可能性を減らすことができます。

また、DrDoS攻撃では、送信元を詐称して攻撃を行うため、適切な通信制御を行うことでその影響を低減することができます。例えば、送信元検証(Source Address Validation)[*76]のような、詐称した通信がネットワークに流入することを防ぐ技術を利用することで、このような送信元のIPアドレスを詐称した攻撃を防ぐことが可能となります。

更に、ISPのネットワーク網において、これを遮断することについて、総務省の研究会などで検討されています。この議論については、「1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」も併せて参照してください。

■ まとめ

これまで解説したとおり、DrDoS攻撃は、攻撃の容易さに比べるとその攻撃の影響が非常に大きいことから、注意すべき脅威の1つです。一方で、攻撃としては比較的古くから知られていたものの、具体的な脅威があまりなかったことから、これまで十分な対策が行われているとはいえませんでした。
今後も、同様の手法を用いた新たな攻撃が出現することが考えられます。これに備えるためにも、日頃から利用している機器の管理を適切に行う必要があります。IIJとしても、業界団体などを通じて、適切な対策に向けた活動を今後も継続して行っていきます。

1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会[*77]

ここでは2013年11月から2014年3月までの期間に実施された、総務省の研究会「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の検討内容について解説します。この研究会は有識者や通信関連団体

*75 CERT/CC、"Vulnerability Note VU#348126 NTP can be abused to amplify denial-of-service attack traffic"(http://www.kb.cert.org/vuls/id/348126)。
*76 送信元検証については次の弊社解説も参照のこと。「送信元検証『Source Address Validation』」(http://www.iij.ad.jp/company/development/tech/activities/sav/)。
*77 総務省、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html)。

により構成されていますが、技術的な内容を検討するためのワーキンググループが組織され、また各関連団体においても検討の場が設けられるなど、短い期間に多くの人が関わる複数の場で、数々の議論がなされました。研究会の議事は要旨のみの公開となっていますが、ここでは公開された「第一次とりまとめ」を元に、検討のポイントについて紹介します。

■ 5つの課題と検討

この研究会では、最近の攻撃に関連する課題として次の5つについて検討を行っています。

・マルウェア配布サイトへのアクセス防止[*78]
・C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大
・新たなDDoS攻撃であるDNSAmp攻撃の防止
・SMTP認証の情報を悪用した迷惑メールへの対処
・攻撃の未然の防止と被害拡大の防止

これらのような攻撃の多くは通信を媒介として発生します。また通信インフラ自体も攻撃にさらされることから、攻撃への対処の機能を通信の過程で実現することは、ある程度必要になることです。加えて、通信事業を行うISPにおいて攻撃に対処することで、数多く発生する被害を効果的に防ぐことも可能です。一方で、通信の過程において攻撃に対処することは、通信すべてについて情報（通信内容や、誰がいつどこに通信を行ったのかなどの外延情報も含む）を取得し、その情報を利用することで攻撃の有無やその様態を判断し、適切に攻撃の通信を止めることを意味します。これは電気通信事業法にある通信の秘密を犯す行為、つまり違法行為にあたります。

そこで、通信事業において攻撃への対処を行うために、攻撃それぞれについて、その発生の原因や影響と、取りうる対処法に関して、違法性が阻却されるかどうかを確認する必要があります。まず、通信の情報を利用した攻撃への対処は、通信の当事者である利用者が同意したうえで実施することができますが、どのように有効な同意を得るかが大きな論点となります。また、利用者の同意の有無に関わらず、攻撃への対処として行う行為が、通信事業者にとっての正当防衛、緊急避難、正当業務行為などに該当する場合も考えられます。この研究会においても、5つの課題について、これらの検討を行っています。以下にそれぞれの検討の概要を示します[*79]。

■ マルウェア配布サイトへのアクセス防止

総務省施策ACTIVEで実施している、Web感染型マルウェアなどへの感染防止の試みのうち、通信に介在する装置などを用いて、すべての利用者に包括的に実施するURLフィルタリングの可能性について検討されています。利用者の通信に関わる情報を利用した対策については、将来契約者の不利益に繋がる可能性のあることから、従来は個別同意が必要とされていました。この課題の検討では、約款に基づく包括同意において、

・利用者が契約約款に同意したあとでも同意内容を変更できる（設定変更できる）こと
・同意内容の変更の有無に関わらず、その他通信サービスの提供条件が変わらないこと
・必要最小限の通信の秘密の検知で実施すること
・注意喚起画面などを表示すると共に、同意内容を変更できることとその方法を説明すること

などの条件を満たす場合については、有効な同意と見なすことができるとしています。また、併せて契約約款に記載すべき事項や注意喚起画面の例を示しています。

■ C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大

マルウェア対策を行う様々な組織の活動の結果、マルウェアを制御するサーバが差し押さえられる場合が増えてきています。そのサーバに蓄えられた情報を元に、感染に気づいていない利用者を特定し、感染の事実や駆除の方法を伝える注意喚起を実施することが検討されました。この場

*78 マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト、ACTIVEの普及展開策の一つとして検討された。ACTIVE(Advanced Cyber Threats response InitiatiVE)、「ACTIVE について」(http://www.active.go.jp/active/index.html)。総務省、「「ACTIVE」の実施及び「ACTIVE推進フォーラム」の開催」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000059.html)。
*79 この研究会における事例の検討は、多くの条件を設定したもとでの法解釈の検討であり、正確な検討内容については研究会の一次とりまとめを参照のこと。

合においては、C&Cサーバに蓄積された通信に関わる情報のうち、接続元のIPアドレスやタイムスタンプを元に、ISPにおいて顧客情報を検索し、利用者を特定することが通信の秘密（外縁情報）の侵害にあたります。この検討では、C&CサーバにIPアドレスなどの記録が残っている端末は、実際に当該サーバを利用するマルウェアに感染しており、そのマルウェアによる被害を受けるとしたうえで、C&Cサーバに残った記録を用いた対処方法について議論しています。結果として、当該IPアドレスから特定した利用者の情報を、注意喚起以外の用途で利用しない場合には、緊急避難として違法性が阻却されるとしています。

■ 新たなDDoS攻撃であるDNSAmp攻撃の防止

設定の緩いDNSリゾルバを踏み台とし、大きな通信量をともなうDDoS攻撃（DNSAmp攻撃）が、2013年に多く発生しました。DNSAmp攻撃は、攻撃者からDNSリゾルバに向かう通信、DNSリゾルバからISPのDNSサーバに向かう通信、インターネット上のサーバからの増幅された応答といった、複数の通信により構成されます。ここでは、それぞれの通信の状況や、その通信で対処を行うことによる効果について議論を行った上で、攻撃者から踏み台になるDNSリゾルバに向かった、増幅を誘発するための通信をブロックする対処について検討しています。また、通常の状況では利用者が特定できない、動的IPアドレスの範囲に多数のDNSリゾルバが存在するために、包括的にブロックを行う必要がある状況を想定しています。

この検討では、動的IPアドレスの空間に対するDNSのクエリの通信をブロックすることについて、宛先のIPアドレス及びポート番号を確認した結果がDNSAmp攻撃の防止以外の用途で利用しない場合に、正当業務行為として違法性が阻却されるとしています。

■ SMTP認証の情報を悪用したスパムメールへの対処

迷惑メール送信対策として広く利用されているSMTP認証ですが、最近は利用者によるパスワードの使いまわしなどに起因して、リスト型攻撃などの不正アクセスの対象となり、第三者にメール送信機能を悪用される場合が発生しています。ここでは、この課題への対策として、

・接続元が瞬時に外国に移動するなど、SMTP認証のID・パスワードの不正利用の蓋然性が高いものへの対策。一時的に利用停止すると共に、利用者にパスワード変更を依頼する。
・SMTP認証の接続の過程において、特定のIDに対して多くのパスワードを試すような辞書攻撃により、ID・パスワードを盗み取ろうとする試みの防止。特定のIPアドレスからの通信で発生する大量のSMTP認証失敗の検出と、そのIPアドレスからのSMTP認証を一時的に停止する。

の2つについて検討しています。いずれの場合も、サーバに対する通信状況に関する情報を元に判断し、一時的に通信を行わせなくする行為ですが、利用者によるパスワード変更などで不正利用が解消するまでの期間、もしくは攻撃が継続する期間に限って行う場合には、正当業務行為として違法性が阻却されるとしています。

■ サイバー攻撃の未然の防止と被害の拡大防止

この課題としては、システムの脆弱性を悪用する内容を含む通信を検出し、通信先に届けないことで攻撃を未然に防ぐ対策と、同時多発的なDDoS攻撃や国内のISPの利用者同士が攻撃をしあっている状況などに対する、ISP間の連携による対策について検討が行われました。しかし、前者は通信内容を直接判断する行為であり、また脆弱性を保有するシステムに依存する問題でもあること、後者は検討の前に連携が必要となる場面に関する整理が必要であることから、この一次取りまとめでは今後更に検討を進める必要があるとしています。

以上のように、この研究会では設定した5つの課題に関する検討を実施し、特に、いくつかの対策について、約款に基づく包括同意をもって利用者による有効な同意と解釈することや、従来攻撃の発生後に正当防衛や緊急避難として許容されてきた攻撃への直接的な対策について、正当業務行為として認められる検討結果を得ています。これらの結果は、今後ISPにおける攻撃対策を検討する上で、大きな影響を及ぼす成果であると考えることができます。

■ 今後の活動

インターネット上の攻撃の状況は日々変化しており、今回具体的に検討された範囲においても、例えばNTPサーバを踏み台としたDDoS攻撃の発生については、その発生の事実を認識していることを言及するのみにとどまってい

ます。このことからも研究会自体は今後も継続し、新しい攻撃とその対策について検討を進めるべきだと考えます。

また、今回検討された課題についても、ISPなどの通信事業者において実際に適用する場面では、より詳しく指針を示す必要があります。例えば、C&Cサーバをテイクダウンした場合において、どのような組織からの情報を信用して良いのか検討を要します。また、SMTP認証に関わる通信の異常についても、可能な限り多くの利用者や事業者が納得できる定量的な基準づくりを試みる必要があります。

このため、この研究会の検討結果を通信事業の実務上の状況に適用させるためのガイドラインづくりを、インターネットの安定的運用に関する協議会などの場で進めていきます[*80]。

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、PlugXの背後にいる攻撃者についての調査の概要と、DrDoS攻撃とその対策、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会について紹介しました。IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続してまいります。

執筆者:

齋藤 衛(さいとう まもる)
IIJ サービスオペレーション本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発に従事の後、2001年よりIIJグループの緊急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、複数の団体の運営委員を務める。

土屋 博英(1.2 インシデントサマリ)
永尾 禎啓、土屋 博英、鈴木 博志、梨和 久雄(1.3 インシデントサーベイ)
鈴木 博志、春山 敬宏(1.4.1 PlugXの背後にいる攻撃者)
土屋 博英(1.4.2 DrDoS攻撃とその対策)
齋藤 衛(1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会)
IIJ サービスオペレーション本部 セキュリティ情報統括室

協力:
加藤 雅彦、須賀 祐治、根岸 征史、小林 直、桃井 康成、小林 稔 IIJ サービスオペレーション本部 セキュリティ情報統括室

*80 インターネットの安定的運用に関する協議会は、通信関連団体である社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本インターネットプロバイダー協会、社団法人日本ケーブルテレビ連盟、財団法人日本データ通信協会テレコム・アイザック推進会議による協議会で、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」の策定を行っている。JAIPA、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について」(http://www.jaipa.or.jp/topics/?p=400)。