Ursnif(gozi)の解析妨害とその回避手法

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2016年10月から12月までの期間では、依然としてAnonymousなどのHacktivismによる攻撃が複数発生しており、DDoS攻撃や不正アクセスによる情報漏えい、Webサイト改ざんなどの攻撃が多発しています。またIoT機器に感染するマルウェアから構成されたボットネットによるDDoS攻撃や、なりますしによる不正ログイン事件なども継続して発生しています。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。

1.2 インシデントサマリ

ここでは、2016年10月から12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。

日本で行われているイルカや小型クジラの追い込み漁への抗議活動として、2013年からAnonymousによると考えられるDDoS攻撃が断続的に行われています。今年も9月1日の漁解禁日に合わせて攻撃キャンペーンの継続が宣言され、10月以降も国内のWebサイトに対するDoS攻撃が続いています(OpKillingBay / OpWhales / OpSeaWorld)。一度攻撃されたWebサイトが何度も繰り返し攻撃される事例や、攻撃対象のリストに記載がないWebサイトへの攻撃事例も数多く発生しました。本稿執筆時点の1月において、攻撃頻度はやや減少したものの攻撃キャンペーンは継続しており、引き続き警戒が必要な状況です。

この期間ではほかにも国内のWebサイトがAnonymousによる攻撃を受けたり、攻撃対象リストに掲載される例が相次ぎました。動物の権利を主張する活動の1つ#OpCircusでは国内のサーカス団のWebサイトがDoS攻撃を受けました。また世界中の金融機関を攻撃対象としたOpIcarus Phase 4 OpBlackOctが10月1日から開始され、一部の国内の金融機関も対象リストに含まれていましたが、特に大きな被害は発生しませんでした。またタイでは12月に国内におけるインターネット利用規制を強化する法案が議会で可決されましたが、この法案改正については表現の自由の侵害などが懸念されるとして署名などの反対活動が行われていました。Anonymousもこの法案改正に抗議する活動#OpSingleGatewayを実施し、タイ政府関連サイトへの不正侵入やDoS攻撃などを行いました。タイ警察当局は12月末にこれらの攻撃活動に関わった9人を逮捕しています。OpSingleGatewayの攻撃対象にはタイ国内の金融機関も列挙されており、バンコクに支店をもつ日本の複数の金融機関も含まれていたため、注意喚起する動きがありました。

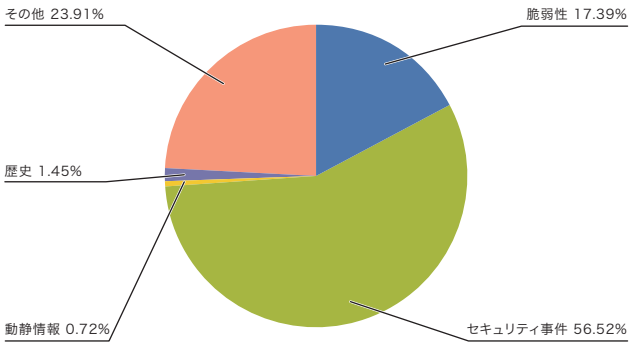


図-1 カテゴリ別比率(2016年10月～12月)

*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、過去に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。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2][*3][*4][*5][*6][*7][*8]、Internet Explorer[*9][*10][*11]、Edge[*12][*13][*14]、Office[*15][*16]などで多数の修正が行われました。Adobe社のAdobe Flash Player、Adobe Acrobat及びReaderでも修正が行われています。Oracle社のJava SEでも四半期ごとに行われている更新が行われ、多くの脆弱性が修正されました。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。DNSサーバのBIND9でも、DNAMEレコードがanswer sectionに含まれている応答を処理する際にnamedが異常終了する脆弱性が見つかり修正されています。またICMPパケットによって特定機種のFirewallのCPU負荷を上げる攻撃手法"BlackNurse"が公開され、該当ベンダーによる修正などが行われました。代表的なCMSの1つであるJoomla!では、外部からの不正なユーザ登録やユーザの権限昇格が可能となる脆弱性が見つかり修正されましたが[*17]、パッチ公開後まもなくこの脆弱性を悪用する攻撃が確認されています[*18]。PHPアプリケーション用のメール送信ライブラリであるPHPMailerやSwiftMailerなどにOSコマンドインジェクションにより任意のコードが実行可能な脆弱性が見つかり修正されました[*19]。

IT資産管理ツールのSKYSEA Client Viewのエージェントプログラムに、外部からの不正なTCPパケットによって任意のコード実行が可能な脆弱性が見つかり、攻撃事例も確認されていることから開発者による修正が行われました[*20]。

---

*2 「マイクロソフト セキュリティ情報 MS16-120 - 緊急 Microsoft Graphics コンポーネント用のセキュリティ更新プログラム（3192884）」(https://technet.microsoft.com/ja-jp/library/security/ms16-120)。
*3 「マイクロソフト セキュリティ情報 MS16-122 - 緊急 Microsoft ビデオ コントロール用のセキュリティ更新プログラム（3195360）」(https://technet.microsoft.com/ja-jp/library/security/ms16-122)。
*4 「マイクロソフト セキュリティ情報 MS16-130 - 緊急 Microsoft Windows 用のセキュリティ更新プログラム（3199172）」(https://technet.microsoft.com/ja-jp/library/security/ms16-130)。
*5 「マイクロソフト セキュリティ情報 MS16-131 - 緊急 Microsoft ビデオ コントロール用のセキュリティ更新プログラム（3199151）」(https://technet.microsoft.com/ja-jp/library/security/ms16-131)。
*6 「マイクロソフト セキュリティ情報 MS16-132 - 緊急 Microsoft Graphics コンポーネント用のセキュリティ更新プログラム（3199120）」(https://technet.microsoft.com/ja-jp/library/security/ms16-132)。
*7 「マイクロソフト セキュリティ情報 MS16-146 - 緊急 Microsoft Graphics コンポーネント用のセキュリティ更新プログラム（3204066）」(https://technet.microsoft.com/ja-jp/library/security/ms16-146)。
*8 「マイクロソフト セキュリティ情報 MS16-147 - 緊急 Microsoft Uniscribe 用のセキュリティ更新プログラム（3204063）」(https://technet.microsoft.com/ja-jp/library/security/ms16-147)。
*9 「マイクロソフト セキュリティ情報 MS16-118 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム（3192887）」(https://technet.microsoft.com/ja-jp/library/security/MS16-118)。
*10 「マイクロソフト セキュリティ情報 MS16-142 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム（3198467）」(https://technet.microsoft.com/ja-jp/library/security/ms16-142)。
*11 「マイクロソフト セキュリティ情報 MS16-144 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム（3204059）」(https://technet.microsoft.com/ja-jp/library/security/ms16-144)。
*12 「マイクロソフト セキュリティ情報 MS16-119 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム（3192890）(https://technet.microsoft.com/ja-jp/library/security/ms16-119)。
*13 「マイクロソフト セキュリティ情報 MS16-129 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム（3199057）」(https://technet.microsoft.com/ja-jp/library/security/ms16-129)。
*14 「マイクロソフト セキュリティ情報 MS16-145 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム（3204062）」(https://technet.microsoft.com/ja-jp/library/security/ms16-145)。
*15 「マイクロソフト セキュリティ情報 MS16-121 - 緊急 Microsoft Office 用のセキュリティ更新プログラム（3194063）」(https://technet.microsoft.com/ja-jp/library/security/ms16-121)。
*16 「マイクロソフト セキュリティ情報 MS16-148 - 緊急 Microsoft Office 用のセキュリティ更新プログラム（3204068）」(https://technet.microsoft.com/ja-jp/library/security/ms16-148)。
*17 "Joomla! 3.6.4 Released"(https://www.joomla.org/announcements/release-news/5678-joomla-3-6-4-released.html)。
*18 "Joomla Exploits in the Wild Against CVE-2016-8870 and CVE-2016-8869"(https://blog.sucuri.net/2016/10/joomla-mass-exploits-privilege-vulnerability.html)。
*19 "Security notices relating to PHPMailer"(https://github.com/PHPMailer/PHPMailer/blob/master/SECURITY.md)。
*20 「【重要】グローバルIPアドレス環境で運用されている場合の注意喚起(CVE-2016-7836)｜SKYSEA Client View｜Sky株式会社」(http://www.skyseaclientview.net/news/161221/)。

10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 **6日：Adobe Acrobat及びReader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見つかり、修正された。**
「Adobe Acrobat および Reader に関するセキュリティアップデート公開」(https://helpx.adobe.com/jp/security/products/acrobat/apsb16-33.html)。

セ **6日：株式会社優良住宅ローンの電子メールの管理サーバに外部から不正アクセスがあり、役職員のメールが外部に転送されたことによって、これらのメールに含まれる顧客情報が外部に流出した。**
「弊社電子メールの管理サーバへの不正アクセス及びお客様の個人情報漏えいの可能性について」(http://www.yuryoloan.jp/wp/wp-content/uploads/2016/10/20161005_YJL_release.pdf)。「弊社お客さまの個人情報漏えいの可能性について」(http://www.yuryoloan.jp/wp/wp-content/uploads/2016/10/20161026news_topics.pdf)。

セ **6日：米司法省は、国家安全保障局(NSA)の契約職員を、国家機密の情報を盗んだ疑いで8月に逮捕していたことを発表した。容疑者は自宅や車に最高機密に区分される書類のデータなどを持ち帰って保存していた。**
"Government Contractor Charged with Removal of Classified Materials and Theft of Government Property"(https://www.justice.gov/usao-md/pr/government-contractor-charged-removal-classified-materials-and-theft-government-property)。

セ **8日：関西学院大学の職員がフィッシングサイトにアクセスし、学生や卒業生らの個人情報が漏えいした。他の複数の大学関係者にも似たような文面のフィッシングメールが届いており、注意喚起が行われていた。**
「フィッシングサイトへのアクセスによる個人情報漏えいについて」(http://www.kwansei.ac.jp/notice/2016/notice_20161007_013525.html)。

セ **10日：富山大学の水素同位体科学研究センターの職員が使用するPCが2015年11月にマルウェアに感染し、学生や研究期間などの個人情報が流出していたことが分かった。研究に関する情報も流出していたが公知の内容であり、機密情報に該当するものはなかった。**
「富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について」(https://www.u-toyama.ac.jp/news/2016/1011.html)。

脆 **11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見つかり、修正された。**
「Adobe Flash Player に関するセキュリティアップデート公開」(https://helpx.adobe.com/jp/security/products/flash-player/apsb16-32.html)。

脆 **12日：Microsoft社は、2016年10月のセキュリティ情報を公開し、MS16-118など7件の緊急と3件の重要な更新を含む合計11件の修正をリリースした。**
「2016年10月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-jp/library/security/ms16-oct.aspx)。

セ **13日：鳥取県が運営する海外向けの観光情報サイトで外部からの不正アクセスがあり、約50万件のメールが不特定多数に送信された。**
「鳥取県海外向け観光情報発信サイトにおける第三者による不正アクセス案件の発生／報道提供資料／とりネット／鳥取県公式ホームページ」(http://db.pref.tottori.jp/pressrelease.nsf/5725f7416e09e6da492573cb001f7512/8948346D7BCF82434925804B0018D682?OpenDocument)。

脆 **18日：Oracle社は 四半期ごとの定例アップデートを公開し、Java SEやOracle Database Serverなどを含む複数製品について、合計253件の脆弱性を修正した。**
"Oracle Critical Patch Update Advisory - October 2016"(http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html)。

セ **18日：株式会社マーケティングアプリケーションズが運営する「アンとケイト」のサイトで、なりすましによる不正ログインが発生し、メールアドレスの改ざんと不正なポイントの交換が行われた。**

セ **21日：米Dyn社のDNSサービスがMiraiボットによる DDoS攻撃を受けて障害が発生し、Twitterや Spotifyなど多数の顧客のサービスが影響を受けた。**
"Dyn, Inc. Status - DDoS Attack Against Dyn Managed DNS"(https://www.dynstatus.com/incidents/nlr4yrr162t8)。
"Dyn, Inc. Status - Update Regarding DDoS Event Against Dyn Managed DNS on October 21, 2016"(https://www.dynstatus.com/incidents/5r9mppc1kb77)。

セ **21日：Weebleから約4,343万人分のユーザ情報が流出したことが分かった。**

脆 **24日：Apple社はiOS 10.1、macOS Sierra 10.12.1及びOS Xのセキュリティアップデートをリリースし、リモートの攻撃者によって任意のコードを実行される可能性があるなどの複数の脆弱性を修正した。また、併せてtvOS 10.0.1とwatchOS 3.1もリリースされた。**
「iOS 10.1 のセキュリティコンテンツについて - Apple サポート」(https://support.apple.com/ja-jp/HT207271)。「macOS Sierra 10.12.1、セキュリティアップデート 2016-002 El Capitan、セキュリティアップデート 2016-006 Yosemite のセキュリティコンテンツについて - Apple サポート」(https://support.apple.com/ja-jp/HT207275)。「tvOS 10.0.1 のセキュリティコンテンツについて - Apple サポート」(https://support.apple.com/ja-jp/HT207270)。「watchOS 3.1 のセキュリティコンテンツについて - Apple サポート」(https://support.apple.com/ja-jp/HT207269)。

セ **27日：マツモトキヨシのWebサイトでなりすましによる不正ログインが発生し、一部のアカウントでポイントが不正に利用された。**
「当社ウェブサイトへの不正ログインに関するご報告」(http://www.matsukiyo.co.jp/online/html/info/info20161027.html)。

セ **31日：一般社団法人ICT-ISACの名前を騙り、「マルウェアに感染しているので、除去ツールをダウンロードし、マルウェアを除去するよう促すメール」が配信されていることが確認された。またこのメールの指示に従うとランサムウェアに感染することが分かった。**
「[注意喚起]当法人になりすました偽メールについて | 一般社団法人ICT-ISAC」(https://www.ict-isac.jp/news/news20161031.html)。

※ 日付は日本標準時

【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

■ IoTボットネットによる攻撃活動

前号でも紹介したMiraiなどのIoT機器に感染したボットネットによるDDoS攻撃は、この期間においても継続して観測されています。

10月21日には米国の大手DNSサービスプロバイダDyn社のDNSサーバがMiraiボット[*21]からのDNS水責め攻撃[*22]を受け、2度にわたって障害が発生しました[*23]。この障害によりTwitter、Spotify、Redditなどの多数のサービスにおいて数時間接続できないなど広範囲にわたる影響が出ました。Miraiボットは9月20日にBrian Krebs氏のブログ"Krebs on Security"に対して約623Gbpsという大規模なDDoS攻撃を発生させ、その後に作者がソースコードを公開して話題となりました。そのKrebs氏は今回のDyn社への攻撃に関して、NANOGで報告[*24]された、Dyn社の研究者と共同で行ったDDoS攻撃対策サービスの会社によるBGPハイジャックに関する調査結果が引き金となったのではないかと推測しています[*25]。なお一部の記事では攻撃規模が1.2Tbpsと過去最大級だったと伝えていますが、この数字はDyn社自身が確認したものではなく不確実な情報で、攻撃規模がここまで大きかったのかどうかははっきりしません。

11月末にはドイツテレコムの通信サービス利用者およそ90万のルータで障害が発生し、インターネットにつながらなくなるなどの影響が出ました[*26]。これはマルウェアがルータの管理インタフェースを利用して繰り返し感染を試み、これに失敗した結果引き起こされたものです[*27]。この感染活動を行ったマルウェアはMiraiの亜種の1つで、TR-064：LAN-Side DSL CPE Configurationとよばれる管理プロトコルを利用し、特定の機器がもつ実装上の脆弱性[*28]を悪用して感染を試みていました。TR-064は通信回線の利用者宅内に設置されるルータなどのCPE（Customer Premises Equipment）をPCから設定するための管理プロトコルで、本来は宅内LAN側で使われるべきものがインターネット側からも利用可能であったことが脆弱性を悪用される一因となりました。この脆弱性はアイルランドやイギリスなど他の地域の通信会社で利用されているルータにも存在しており、これらの地域でも同じ時期に影響があったことが確認されています。また警察庁による観測では、この管理プロトコルが利用するポート7547/tcpと5555/tcpへのアクセスがこの時期に急増したことが報告されています[*29]。12月には、この他にも37777/tcp、23231/tcp、6789/tcpなどのポートをスキャンして感染を試みるMirai亜種の活動が世界的に観測されています[*30]。各ポートのスキャン状況については、「1.3.2 マルウェアの活動」も参照してください。

10月5日に米国の司法省は、Lizard Squad及びPoodleCorpと名乗るハッカーグループの主要メンバー2人を米国とオランダで9月に逮捕したと発表しました[*31]。Lizard Squadはbooter/stresserなどとも呼ばれるDDoS-for-hireサービス（DDoS攻撃代行サービス）の1つShenronを提供しており、同様にPoodleCorpもPoodle Stresserというサービスを提供

*21 Miraiボットの詳細については、本レポートVol.33（http://www.iij.ad.jp/company/development/report/iir/033.html）のフォーカスリサーチ「1.4.1 Mirai Botnetの検知と対策」を参照。
*22 DNS水責め攻撃については、株式会社日本レジストリサービス 森下氏による次の資料が詳しい。「DNS水責め（Water Torture）攻撃について」（http://2014.seccon.jp/dns/dns_water_torture.pdf）。
*23 "Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog"（https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/）。
*24 "BackConnect's Suspicious BGP Hijacks"（https://www.nanog.org/sites/default/files/20161016_Madory_Backconnect_S_Suspicious_Bgp_v2.pdf）。
*25 "DDoS on Dyn Impacts Twitter, Spotify, Reddit — Krebs on Security"（https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/）。
*26 "Deutsche Telekom: Information on current problems"（https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862）。
*27 "WERE 900K DEUTSCHE TELEKOM ROUTERS COMPROMISED BY MIRAI? - Comsecuris Security Research & Consulting Blog"（https://comsecuris.com/blog/posts/were_900k_deutsche_telekom_routers_compromised_by_mirai/）。
*28 この脆弱性は11月7日にセキュリティ研究者によって最初に報告されPoCも公開されていた。"Eir's D1000 Modem Is Wide Open To Being Hacked. - Reverse Engineering Blog"（https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/）。
*29 「海外製ルータの脆弱性を標的としたアクセスの急増等について（平成28年11月期）」（警察庁）（https://www.npa.go.jp/cyberpolice/detect/pdf/20161221.pdf）。
*30 「「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について（平成28年12月期）」（警察庁）（https://www.npa.go.jp/cyberpolice/detect/pdf/20170120.pdf）。
*31 "American and Dutch Teenagers Arrested on Criminal Charges for Allegedly Operating International Cyber-Attack-For-Hire Websites | USAO-NDIL | Department of Justice"（https://www.justice.gov/usao-ndil/pr/american-and-dutch-teenagers-arrested-criminal-charges-allegedly-operating）。

11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

脆 **2日：BIND9に、DNS応答の処理に不具合があるため、外部からDoS攻撃可能な脆弱性が見つかり、修正された。**
"CVE-2016-8864: A problem handling responses containing a DNAME answer can lead to an assertion failure | Internet Systems Consortium Knowledge Base"（https://kb.isc.org/article/AA-01434）。

セ **2日：キヤノンマーケティングジャパン株式会社が運営する「キヤノンオンラインショップ」において、なりすましによる不正ログインが発生し、不正な商品購入が行われた。**
「キヤノン：「キヤノンオンラインショップ」での会員ID・パスワード不正使用による取引発生のご報告とパスワード変更のお願い」（http://cweb.canon.jp/caution/161102.html）。

セ **7日：英国のTesco Bankにおいて、不正ログインによって約9,000人の顧客の口座から250万ポンドが引き出された。**
"Tesco Bank announces full service has resumed for customers（8 November, 2016） - News releases - News - Tesco Bank"（http://corporate.tescobank.com/25/news/news-releases/tesco-bank-announces-full-service-has-resumed-for-customers/?newsid=291）。

脆 **8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見つかり、修正された。**
「Adobe Flash Player に関するセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb16-37.html）。

他 **8日：中国で全国人民代表大会が開催され、サイバーセキュリティに関する新たな法案が可決された。ユーザに実名登録を求めることや、ユーザの個人情報などを中国国内に保管することなどを企業に要求している。**

脆 **9日：Microsoft社は、2016年11月のセキュリティ情報を公開し、MS16-129など6件の緊急と8件の重要な更新を含む合計14件の修正をリリースした。**
「2016年11月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms16-nov.aspx）。

セ **10日：ロシアの銀行大手少なくとも5行がDDoS攻撃を受けた。DDoS-for-hireサービスを利用したものとみられる。**
"DDoS attack on the Russian banks: what the traffic data showed - Securelist"（https://securelist.com/blog/incidents/76728/ddos-attack-on-the-russian-banks-what-the-traffic-data-showed/）。

脆 **11日：ICMPパケットによって特定機種のFirewallのCPUに負荷をかけるDoS攻撃手法"BlackNurse"が公開された。**
"BLACKNURSE it can bring you down"（http://www.blacknurse.dk/）。

セ **14日：出会い系サイトなどを運営する Friend Finder Networksから約4億1,200万件のアカウント情報が漏えいしていたことが発覚した。**

セ **15日：東北電力のWebサービス「よりそうeねっと」で、なりすましによる不正ログインが発生し、一部のアカウントでポイントが不正に利用された。調査のためにサービスが停止されたが、ログインIDの変更などの対応を行い、12月1日よりサービスを再開した。**
「「よりそうeねっと」への不正アクセスに伴うサービス停止について| 東北電力」（http://www.tohoku-epco.co.jp/news/normal/1193122_1049.html）。「「よりそうeねっと」のサービス再開とログインIDの変更について」（https://www3.zf1.tohoku-epco.co.jp/terms/announce.html）。

セ **18日：m3.comのサイトでなりすましによる不正ログインが発生した。**
「m3.com サイトへの不正ログイン発生のご報告とパスワード変更のお願い」（https://corporate.m3.com/2016/11/18/m3.com-20161118.pdf）。

セ **21日：ローソンの会員向けWebサイトで、なりすましによる不正ログインが発生し、一部のアカウントでポイントが不正に利用された。**
「ローソンWEB会員向けサービスサイトご利用のお客様に向けたパスワード再設定のお願いを実施いたします｜ローソン」（http://www.lawson.co.jp/company/news/detail/1284326_2504.html）。

セ **22日：徳島市や千葉市など、全国の多数の市で、市役所と市内の施設に爆弾を仕掛けたとの同じ内容の爆破予告メールが届いたが、特に不審物などは発見されなかった。**
「徳島市役所本庁舎等の爆破予告を受けての対応：徳島市公式ウェブサイト」（https://www.city.tokushima.tokushima.jp/anzen/shoubo_bousai/kikikanrijyoho/anzen_20161121.html）。「千葉市：市施設の爆破予告について不審物や爆発は確認されませんでした」（http://www.city.chiba.jp/somu/kikikanri/bakuhayokoku.html）。

セ **28日：San Francisco Municipal Transportation Agency（SFMTA）がランサムウェアの被害に遭い、約900台のコンピュータに影響した。被害の拡大を防ぐために、地下鉄の駅の料金システムが一時停止された。**
"Update on SFMTA Ransomware Attack | SFMTA"（https://www.sfmta.com/about-sfmta/blog/update-sfmta-ransomware-attack）。

セ **29日：ドイツテレコムの通信サービス利用者およそ90万でルータに障害が発生し、インターネットに接続できないなどの影響が出た。Mirai亜種のマルウェアによる感染活動が原因とみられる。**
"Deutsche Telekom: Information on current problems"（https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862）。

セ **29日：サイバーエージェントが運営する「Ameba」で、なりましによる不正ログインが発生し、被害を受けた約59万アカウントのパスワードをリセットする対応が行われた。**
「「Ameba」への不正ログインに関するご報告とパスワード再設定のお願い｜株式会社サイバーエージェント」（https://www.cyberagent.co.jp/newsinfo/info/detail/id=12977）。

※ 日付は日本標準時

【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

していました。これらのサービスはいずれもIoTボットネットであるLizardStresserを利用してDDoS攻撃を実施していたと考えられています。LizardStresserは2015年にソースコードが公開されたため、様々な攻撃者によって多数のボットネットが構築されDDoS攻撃に使用されています。逮捕された2人はいずれも19才の青年で、これらのサービスを利用して大手ゲーム会社などに繰り返しDDoS攻撃を行っていました。

IoTボットネットは、telnetなどの管理用ポートが開いているIoT機器に対して、初期パスワードなどでログインし感染を試みます。IoT機器の中には管理用アカウントの初期パスワードが変更できない、telnetなど管理用ポートの開閉を設定できない、などの問題があるものも存在しています。Miraiボットなどの感染拡大によってこれらの問題を認識し、製品の出荷を停止した上で、問題点を修正するファームウェアを公開する製品ベンダーなども出ています[*32]。こうした現状をふまえて、IPA[*33]やJPCERT/CC[*34]はIoT機器の利用者に対して、利用前の初期パスワードの変更やファームウェアのアップデートなど、適切な対応を行うよう注意を促しています。

■ 米大統領選挙に関連するロシアからのサイバー攻撃

2016年は4年ぶりの米大統領選挙の年でしたが、サイバー攻撃による選挙活動への影響が大きな話題となりました。

6月には民主党全国委員会(DNC)が外部から不正に侵入され、選挙活動に関連する内部情報が漏えいしていたことが明らかとなりました。またその後、DNCから漏えいしたとみられる情報を含め、メールやドキュメントなど主に民主党関連の情報がWikiLeaks、GUCCIFER 2.0、DCLeaksなどから相次いで公開される事態となりました。これらの民主党にとって不利な内容が、選挙結果にどのような影響を与えたのかは定かではありませんが、結果的に11月の大統領選挙では共和党候補のトランプ氏が大統領に選出されることになりました。

5月に国家情報長官室(ODNI)は大統領選挙に関連する米国内の複数の組織に対するサイバー攻撃が発生していると警告していましたが、こうした一連の事件に対する政府内の調査結果を受けて、10月には国家安全保障省(DHS)とODNIは大統領選挙のセキュリティに関して共同声明を発表しました[*35]。この中で、DNCなど関連組織への侵入やメールのリークなどをロシア政府によるものとして名指しで非難しました。更に大統領選挙後の12月、オバマ大統領は過去の大統領令(Executive Order 13694)の内容を改正し[*36]、米大統領選挙へのロシア政府の介入に対して、35人のロシア外交官の国外退去などの制裁を発動すると発表しました。また一連の攻撃活動をGRIZZLY STEPPEと呼称したDHSとFBIによる共同分析レポートも同時に公開されています[*37]。このように米政府はロシアからのサイバー攻撃と断定した上で様々な対応を行っていますが、公開された情報からは明確な証拠と言えるものが不十分なため、その内容に関して批判的なセキュリティ専門家も少なくありません[*38]。

*32 例えば、アイ・オー・データ機器の「WFS-SR01」やプリンストンの「PTW-WMS1」などがこうした対応を行っている。「Wi-Fiストレージ「WFS-SR01」セキュリティの脆弱性につきまして | IODATA アイ・オー・データ機器」(http://www.iodata.jp/support/information/2016/wfs-sr01/)。「PTW-WMS1をルーター機能の無いモデムに接続してご使用されているお客様へ　ファームウェアアップデートのお知らせ | 対応情報 | お知らせ一覧 | 株式会社プリンストン」(http://www.princeton.co.jp/news/2016/12/201612271100.html)。

*33 「ネットワークカメラや家庭用ルータ等のIoT機器は利用前に必ずパスワードの変更を 安心相談窓口だより:IPA 独立行政法人 情報処理推進機構」(https://www.ipa.go.jp/security/anshin/mgdayori20161125.html)。

*34 「インターネットに接続された機器の管理に関する注意喚起」(https://www.jpcert.or.jp/at/2016/at160050.html)。

*35 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security"(https://www.odni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement)。

*36 "Executive Order -- Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities | whitehouse.gov"(https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency)。

*37 "GRIZZLY STEPPE – Russian Malicious Cyber Activity"(https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity)。

*38 例えば次のような批判記事がある。"Critiques of the DHS/FBI's GRIZZLY STEPPE Report – Robert M. Lee"(http://www.robertmlee.org/critiques-of-the-dhsfbis-grizzly-steppe-report/)。"FBI/DHS Joint Analysis Report: A Fatally Flawed Effort"(https://medium.com/@jeffreycarr/fbi-dhs-joint-analysis-report-a-fatally-flawed-effort-b6a98fafe2fa)。

12月のインシデント

1

セ **2日：ロシアの中央銀行及び民間銀行の口座から、今年1年間にサイバー攻撃によって不正に20億ルーブル（約3,100万ドル）が盗まれていたことが、報告書によって明らかとなった。**

2

セ **2日：pixivの一部のアカウントで、なりすましによる不正ログインが発生し、該当ユーザのパスワードはリセットされた。**
「[pixiv] Announcements -【重要】pixivの一部アカウントに対する「なりすましログイン」の報告とパスワード変更のお願い」（http://www.pixiv.net/info.php?id=3897）。

3

4

セ **2日：欧州刑事警察機構（Europol）や米司法省などの連携により、マルウェア感染などに利用されていたAvalancheネットワークが摘発され、5人のメンバーの逮捕やサーバの押収などが行われた。**
"'Avalanche' network dismantled in international cyber operation | Europol"（https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation）。

5

6

脆 **5日：Newcastle Universityの研究者がVISAの決済ネットワークの問題を発表した。"Distributed Guessing Attack"によって、カード番号、有効期限、CVVによる認証を数秒で突破できることを示した。**
"Cyber attack - Press Office - Newcastle University"（http://www.ncl.ac.uk/press/news/2016/12/cyberattack/）。

7

8

セ **6日：ココカラファインが運営する「ココカラクラブ」「ココカラ公式アプリ」において、なりすましによる不正ログインが発生し、一部のアカウントでポイントが不正に利用された。**
「当社「ココカラクラブ」「ココカラ公式アプリ」への不正アクセスについて ｜【ココカラクラブ】ドラッグストアのココカラファイン」（http://www.cocokarafine.co.jp/info/CSfViewNews.jsp?sort=1&no=24）。

9

10

セ **6日：フランスの動画共有サービスDailymotionから約8,500万件のアカウント情報が流出していたことが発覚した。**
"Dailymotion accounts security update - Dailymotion Official Blog"（http://blog.dailymotion.com/en/dailymotion-account-security-update/）。

11

12

セ **8日：韓国国防部は、韓国軍内部のネットワークである国防網に接続された PCがマルウェアに感染し、軍の機密情報などが流出していたことを発表した。**
「국방망 해킹 관련 설명자료」（http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=I_42745&boardSeq=I_4009863&mcategoryId=&id=mnd_020500000000）。

13

他 **8日：経済産業省から「サイバーセキュリティ経営ガイドライン Ver1.1」が公開された。またIPAからはガイドラインの内容を補足し、実施方法を具体的に解説する「サイバーセキュリティ経営ガイドライン解説書」が公開された。**
「サイバーセキュリティ経営ガイドライン（METI/経済産業省）」（http://www.meti.go.jp/policy/netsecurity/mng_guide.html）。「サイバーセキュリティ経営ガイドライン解説書：IPA 独立行政法人 情報処理推進機構」（https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html）。

14

15

16

17

他 **8日：内閣サイバーセキュリティセンター（NISC）が、重要インフラにおける分野横断的演習を実施した。**
「重要インフラにおける分野横断的演習の実施概要について ～【2016 年度分野横断的演習】～」（http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2016gaiyou.pdf）。

18

19

脆 **12日：Apple社はiOS 10.2、macOS Sierra 10.12.2及びOS Xのセキュリティアップデートをリリースし、リモートの攻撃者によって任意のコードを実行される可能性があるなどの複数の脆弱性を修正した。また、併せてtvOS 10.1もリリースされた。**
「iOS 10.2 のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT207422）。「tvOS 10.1 のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT207425）。「macOS Sierra 10.12.2、セキュリティアップデート 2016-003 El Capitan、セキュリティアップデート 2016-007 Yosemite のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT207423）。

20

21

22

脆 **13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見つかり、修正された。**
「Adobe Flash Player に関するセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb16-39.html）。

23

24

脆 **14日：Microsoft社は、2016年12月のセキュリティ情報を公開し、MS16-144など6件の緊急と6件の重要な更新を含む合計12件の修正をリリースした。**
「2016年12月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms16-dec.aspx）。

25

26

セ **18日：ウクライナの電力会社Ukrenergoが、サイバー攻撃の影響により電力供給が一時停止したと発表した。**
"Щодо аварійної ситуації на підстанції 330 кВ "Північна"（http://www.ukrenergo.energy.gov.ua/Pages/ua/DetailsNew.aspx?nID=3387）。

27

28

他 **20日：改正個人情報保護法の施行期日を2017年5月30日とする政令が閣議決定された。**

29

30

動 **30日：米国のオバマ大統領が大統領令（Executive Order 13694）により、米大統領選挙へのロシア政府による介入に対して、外交官の国外退去などの制裁を発動した。**
"Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment"（https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity）。

31

※ 日付は日本標準時

【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

■ 政府機関の取り組み

2016年4月に「サイバーセキュリティ基本法」の改正案が国会で可決され成立しましたが、その第13条で規定されたサイバーセキュリティを確保すべき対象として、中央省庁だけでなく独立行政法人や特殊法人にまで拡大されました。2016年10月に開催されたサイバーセキュリティ戦略本部 第10回会合において、この第13条の規定にもとづいて新たに9法人が指定されました[*39]。この中には2015年に情報漏えい事件を起こした日本年金機構も含まれています。この指定により、これらの法人では中央省庁と同様に、国による監査や情報システムに対する不正な活動の監視、インシデントの原因究明調査などの対象組織として扱われることになります。

12月7日に内閣サイバーセキュリティセンター(NISC)は、重要インフラ事業者およそ2,000名の参加を得て、11回目となる分野横断的演習を実施しました。この演習により、IT障害が発生した場合における関係者との情報共有、連携をはじめ、重要インフラ事業者における対応策、体制の実効性が確認されました。

■ その他

2016年は、MySpaceやLinkedInなど過去に発生した大量のパスワード情報の漏えいが多くのサービスで発覚しました。12月には、2013年時点のユーザ情報少なくとも10億件が漏えいしていたと、米Yahoo!が発表しました[*40]。これは現在までに分かっている情報漏えい事件の中では過去最大の規模です。Yahoo!は9月にも2014年時点のユーザ情報少なくとも5億件が漏えいしていたと発表したばかりですが、これとは別に更に大規模な漏えい事件を起こしていたことが分かりました。

このようなパスワード情報の漏えい事件が国内外で常態化していることから、同じパスワードを複数のサービスで使い回しているユーザを狙ったなりすましによる不正ログイン、いわゆるリスト型攻撃も多く発生しています。この期間では、会員向けのWebサイトでなりすましによる不正ログインが発生し、ポイントが不正に利用されるという被害が国内の複数のサイトで確認されています。ユーザは自分のパスワード情報が漏えいして悪用される可能性をあらかじめ考慮して、複数のサービスで同じパスワードを使い回さないようにするなどの自衛策が求められます。

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、多岐にわたります。しかし、攻撃の多くは、脆弱性など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、2016年10月から12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、攻撃の実態を正確に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。

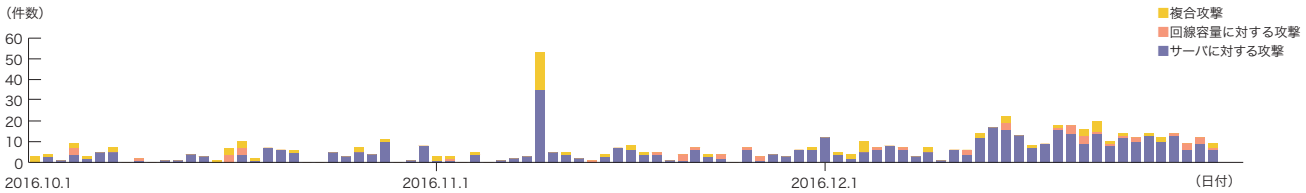


図-2 DDoS攻撃の発生件数

*39 内閣サイバーセキュリティセンター(NISC)、「サイバーセキュリティ基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人」(http://www.nisc.go.jp/conference/cs/pdf/shiteihojin.pdf)。
*40 "Important Security Information for Yahoo Users | Yahoo"(https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users)。

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、その影響度合いが異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*41]、サーバに対する攻撃[*42]、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、620件のDDoS攻撃に対処しました。1日あたりの対処件数は6.74件で、平均発生件数は前回のレポート期間と比べて増加しています。DDoS攻撃全体に占める割合は、サーバに対する攻撃が78.39%、複合攻撃が13.23%、回線容量に対する攻撃が8.39%でした。

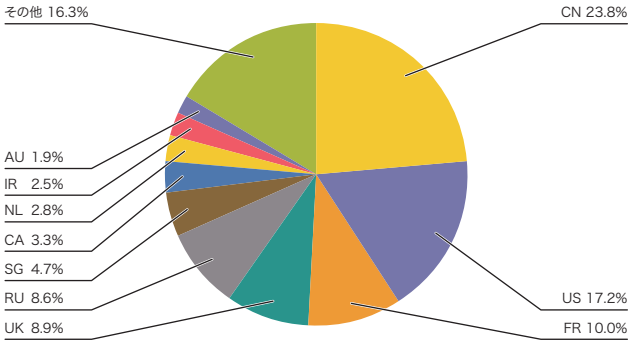


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

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761万ppsのパケットによって15.25Gbps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90.97%が攻撃開始から30分未満で終了し、9.03%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観測されませんでした。なお、今回最も長く継続した攻撃は、複合攻撃に分類されるもので16時間53分にわたりました。

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[*43]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[*44]の利用によるものと考えられます。

■ 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[*45]によるDDoS攻撃のbackscatter観測結果を示します[*46]。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。

2016年10月から12月の間に観測した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。

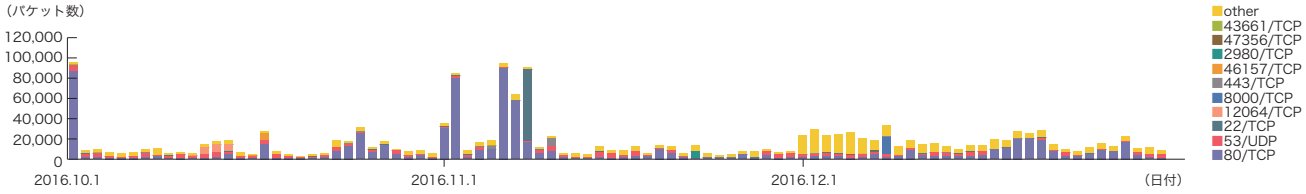


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*41 攻撃対象に対し、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。

*42 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。

*43 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。

*44 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。

*45 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。

*46 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。

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、全パケット数の47.6%を占めています。また、DNSで利用される53/UDP、SSHで利用される22/TCP、HTTPSで利用される443/TCPへの攻撃、通常は利用されない12064/TCP、8000/TCP、46157/TCP、2980/TCPなどへ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、中国の23.8%が最も大きな割合を占めています。その後に米国の17.2%、フランスの10.0%といった国が続いています。

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及び443/TCP)への攻撃としては、10月1日には前回期間に引き続き中国にある電気街の公式サイトへの攻撃、11月1日から5日にかけて英国ブックメーカーへの攻撃、11月6日にロシアのホスティング事業者への攻撃、11月6日から7日にかけては特定のロシア語のサイトへの攻撃、11月10日にはジブラルタルのオンラインカジノへの攻撃を観測しています。他のポートへの攻撃としては、10月11日から14日にかけて中国の特定のIPアドレスに対する12064/TCPへの攻撃、10月16日から17日にかけて中国の特定のIPアドレスに対する46157/TCPへの攻撃、11月8日にシンガポールのISPが持つIPアドレスに対する22/TCPへの攻撃、11月22日に中国のCDN事業者のサーバに対する2980/TCPへの攻撃、12月8日にフランスのホスティング事業者のサーバに対する8000/TCPへの攻撃を観測しています。

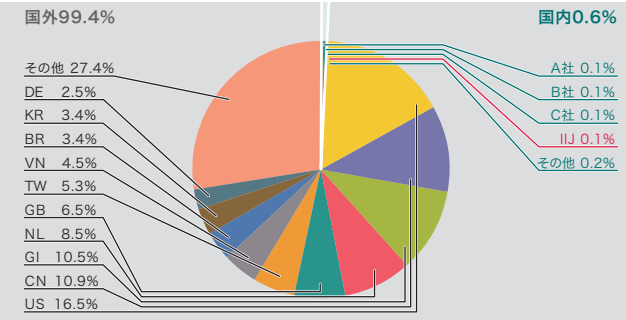


図-5 発信元の分布(国別分類、全期間)

また、今回の対象期間中に話題となったDDoS攻撃のうち、IIJのbackscatter観測で検知した攻撃としては、10月24日にSyrian Cyber Armyを名乗るグループによるベルギーの複数の新聞社サイトへの攻撃、12月22日にSNSサイトTumblrに対する攻撃をそれぞれ検知しています。

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[*47]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[*48]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

2016年10月から12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に示します。また総量(到着パケット数)に関して、本レポートの期間中に最も接続回数の多かった23/TCP、3番目に接続回数の多かった1900/UDP、4番目に接続回数の多かった2323/TCPはその他の通信よりも突出して多かったため、それぞれ図-6から図-8に別途記載し、残りの推移を図-9に示します。期間中、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。

本レポートの期間中にハニーポットに到着した通信の多くは、Telnetで使われる23/TCP、SSDPで使われる1900/UDP、FTPで使われる21/TCP、SSHで使われる22/TCP、Web Proxyで使用される8080/TCP、ICMP Echo Request、Microsoft社の

*47 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。
*48 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。

OSで利用されているSQL Serverで利用される1433/TCP、同社のRemote Desktopで使用される3389/TCPなどでした。

前回のレポートに引き続き、Telnetで使われる23/TCP宛ての通信が本レポート期間中でも引き続き高い値を示しており、更に10月後半から11月中旬までと12月中旬以降はより増加しています。これは前回レポートしたとおり、Miraiボット[*49]及びその亜種、Bashlite、KaitenやhajimeなどといったIoT機器のLinuxをターゲットにしたボットの感染が拡がっているためです。この通信は台湾、中国、ベトナム、韓国、ブラジルなどに割り当て

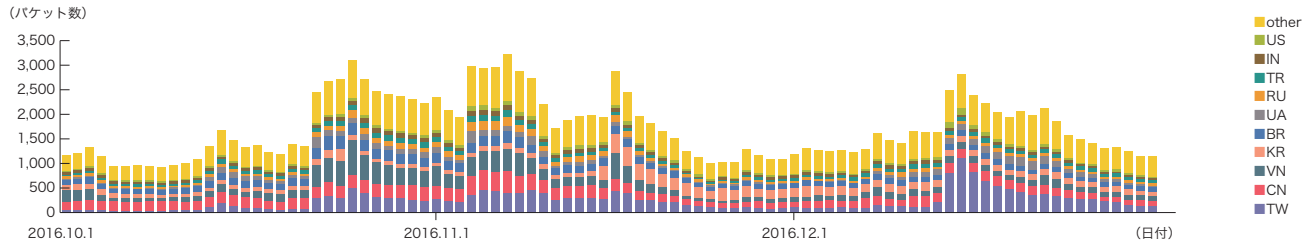


図-6 ハニーポットに到着した23/TCP通信の推移(日別・23/TCP、国別・1台あたり)

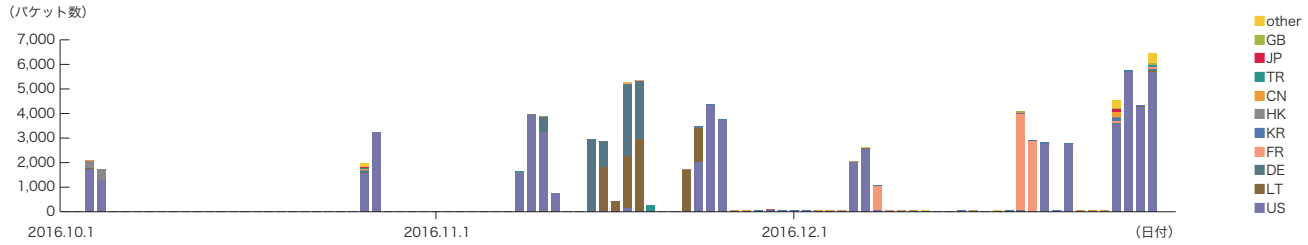


図-7 ハニーポットに到着した1900/UDP通信の推移(日別・1900/UDP、国別・1台あたり)

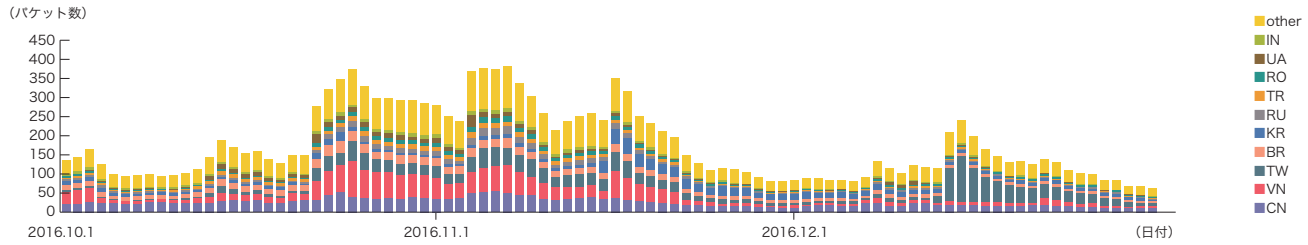


図-8 ハニーポットに到着した2323/TCP通信の推移(日別・2323/TCP、国別・1台あたり)

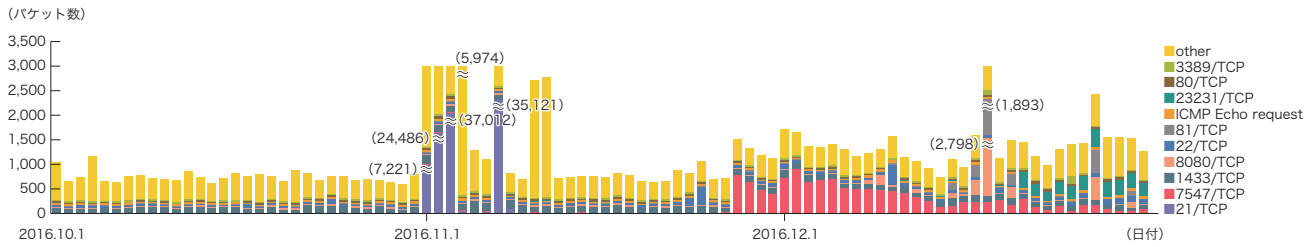


図-9 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*49 Mirai Botnetについては、前回のレポートで詳しく解説している。「Internet Infrastructure Review (IIR) Vol.33 1.4.1 Mirai Botnetの検知と対策」(http://www.iij.ad.jp/company/development/report/iir/033.html)。

られた多数のIPアドレスからの通信でした。また2323/TCP、7547/TCP、23231/TCPなどについてもMiraiボットやその亜種の影響であり、本レポートの期間中、大幅に増加しています。

本レポートの期間中、SSDPプロトコルである1900/UDPが断続的に増加しています。主に米国、リトアニア、ドイツ、フランスなどに割り当てられたIPアドレスからSSDPの探査要求を受けています。これらは、SSDPリフレクターを使ったDDoS攻撃に利用可能な機器を探査する通信であると考えられます。また11月の後半から1900/UDPの通信回数がそれまでの定常時より10倍程度に増加しており、ボットなどによって定常的にスキャン活動が行われるようになった可能性が考えられます。

■ Miraiボットの通信

Miraiボットは感染活動を行う前に、インターネット上に存在するIoT機器のスキャンを行いますが、そのパケットはTCPのシーケンス番号と宛先IPアドレスが同一であるという特徴を持っていることが、解析結果から分かっています。23/TCPの通信において、この特徴に合致する通信の割合を調査したものが図-10になります。調査したところ、2016年8月1日からこのパターンに合致する通信が出現したことが分かったため、それ以降の通信を示します。23/TCPの約80%がMiraiボット、もしくはそれに準ずるアルゴリズムを持つマルウェアによる通信であることが分かりました。また、図-11は、このアルゴリズムに合致する通信をプロトコル別に並べたものになります。2323/TCPは9月6日、80/TCP及び8080/TCPが11月2日、7547/TCP[*50]が11月26日、5555/TCP[*51]が11月28日、23231/TCP[*52]、37777/TCP[*53]が12月10日、6789/TCPが12月18日、22/TCP[*54]が12月19日、2222/TCPが12月20日にそれぞれ初めて観測されています。ソースコードがリリースされたことも影響しているためか、特に11月以降は活発に開発が行われていることが分かります。

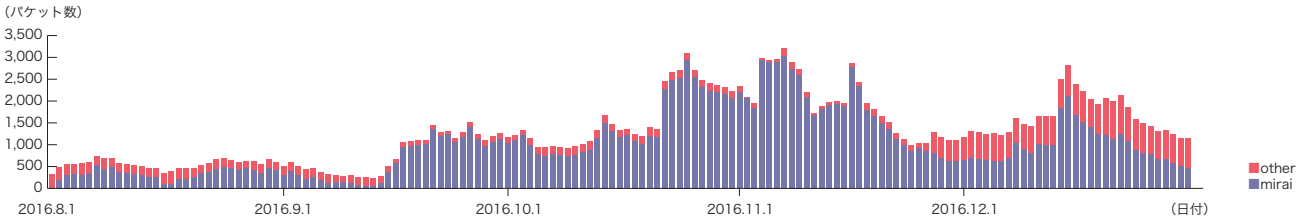


図-10 ハニーポットに到着した23/TCP通信の推移(日別・23/TCP、Miraiボットの割合・1台あたり)

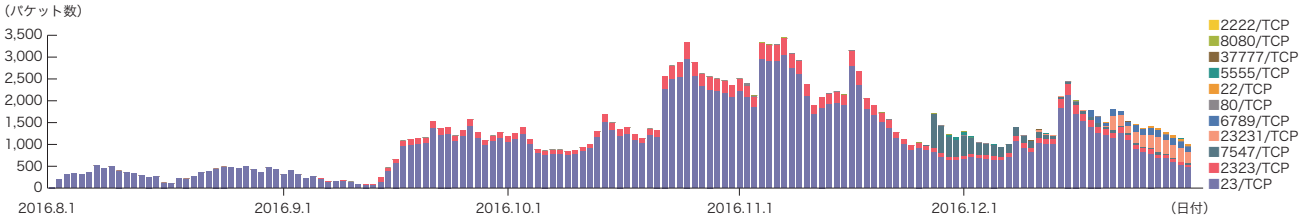


図-11 ハニーポットに到着したMiraiボットと推定される通信の推移(日別・宛先ポート別・1台あたり)

*50 "Port 7547 SOAP Remote Code Execution Attack Against DSL Modems"(https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759/)。

*51 5555/TCPのMiraiボット亜種によるスキャンは次のURLで解説されている。"Now Mirai Has DGA Feature Built in"(http://blog.netlab.360.com/new-mirai-variant-with-dga/)。

*52 23231/TCP及び6789/TCPをスキャンするMiraiボット亜種は以下で言及されている。"UPDATED x1: Mirai Scanning for Port 6789 Looking for New Victims / Now hitting tcp/23231"(https://isc.sans.edu/diary/UPDATED%2Bx1%3A%2BMirai%2BScanning%2Bfor%2BPort%2B6789%2BLooking%2Bfor%2BNew%2BVictims%2B%2BNow%2Bhitting%2Btcp23231/21833)。

*53 「JPCERT/CC Alert 2016-12-21 インターネットに接続された機器の管理に関する注意喚起 - インターネットにつながったあらゆる機器が脅威にさらされています -」(https://www.jpcert.or.jp/at/2016/at160050.html)。

*54 22/TCP、2222/TCPのスキャンは次のURLで紹介されている。「「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について」(https://www.npa.go.jp/cyberpolice/detect/pdf/20170120.pdf)。

■ ネットワーク上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-12に、マルウェアの総取得検体数の推移を図-13に、そのうちのユニーク検体数の推移を図-14にそれぞれ示します。このうち図-13と図-14では、1日あたりに取得した検体[*55]の総数を総取得検体数、検体の種類をハッシュ値[*56]で分類したものを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ウェアで判別し、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、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。

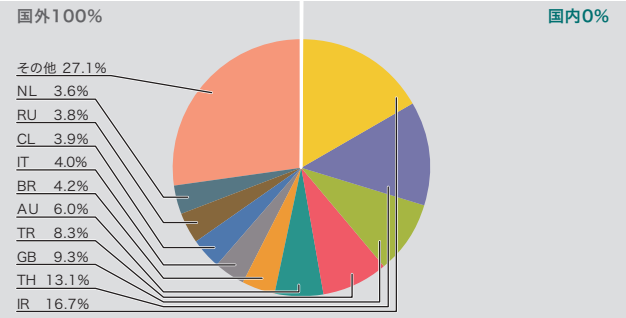


図-12 検体取得元の分布（国別分類、全期間、Confickerを除く）

期間中の1日あたりの平均値は、総取得検体数が280、ユニーク検体数が21でした。図-13において、12月初旬に未検出の検体が急増していますが、これはMITFハニーポットの改修を行い、5555/TCP及び7547/TCPをスキャンするマルウェアを取得できるようにしたためです。それらのポートから取得した検体は、調査の結果、Miraiボットの亜種であることが分かりました。また、そのほかの未検出の検体をより詳しく調査した結果、ベトナム、インド、米国、中国などに割り当てられたIPアドレスで複数のSDBOTファミリ（IRCボットの一種）やビットコインマイニングツールのダウンローダなどが観測されています。

未検出の検体の約97%がテキスト形式でした。前号より大幅に割合が増加していますが、これはMiraiボット亜種のダウンロード先がほとんど閉鎖されており、Webサーバからのエラーが出力されていたためであるのと、従来通り、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

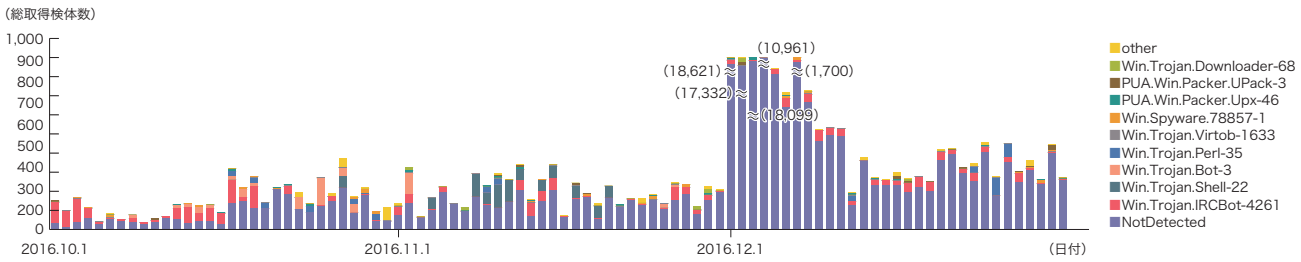


図-13 総取得検体数の推移（Confickerを除く）

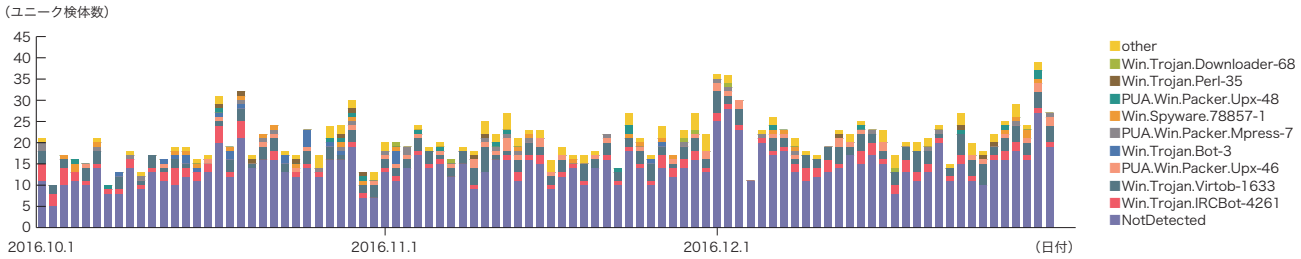


図-14 ユニーク検体数の推移（Confickerを除く）

＊55 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。

＊56 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。

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れているためであると考えられます。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5.1%、ボット型78.4%、ダウンローダ型16.5%でした。また解析により、74個のボットネットC&Cサーバ[*57]と87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3,961、ユニーク検体数は303でした。総取得検体数で75.8%、ユニーク検体数で93.1%を占めています。総取得権対数の割合が前回のレポート期間中より4分の1程度減少していますが、これはMiraiボットの亜種が取得できるようになったことによるものです。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回の対象期間と比較し、約5%減少し、ユニーク検体数は前号から約19%減少しており、本レポート期間中は全体的に緩やかに減少しています。Conficker Working Groupの観測記録[*58]によると、2017年1月現在で、ユニークIPアドレスの総数は45万台とされています。2011年11月の約320万台と比較すると、約14%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[*59]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。

2016年10月から12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-15に、攻撃の推移を図-16にそれぞれ示します。これらは、IIJマネージドIPS/IDS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、日本24.8%、米国18.1%、ロシア14.9%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合計値は前回と比べて増加傾向にあります。特に日本とロシアが大幅な増加傾向にあります。

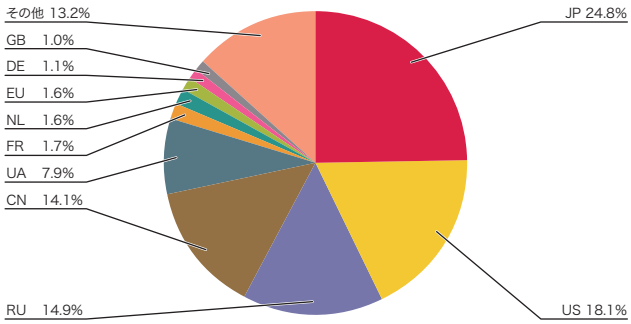


図-15 SQLインジェクション攻撃の発信元の分布

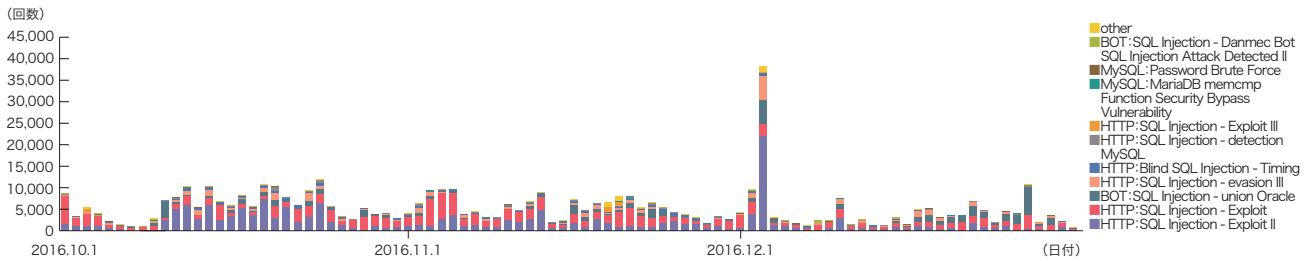


図-16 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*57 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。
*58 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking)。本レポート期間中、数値のデータが2016年1月7日以降表示されていないため、2017年1月前半の最高値をグラフから目視で確認して採用している)。
*59 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、12月3日に日本の特定の攻撃元から特定の攻撃先に対する攻撃が発生しています。また、ロシアの複数の攻撃元から複数の攻撃先に対する攻撃が連日発生した結果、大幅に攻撃検知件数が増加しました。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

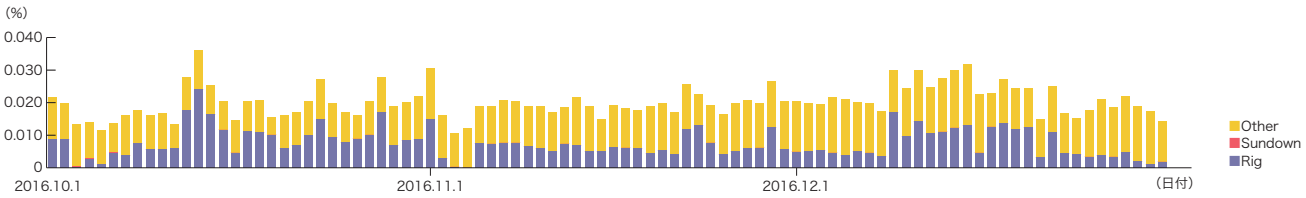
MITFのWebクローラ（クライアントハニーポット）によって調査したWebサイト改ざん状況を示します[*60]。

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十万の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サイトなどを対象に、一時的な観測も行っています。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。

2016年10月から12月までの期間は、検知したドライブバイダウンロード攻撃のほぼすべてがRig Exploit Kitでした（図-17）。2016年9月末にNeutrinoが観測されなくなって以降、継続している傾向です[*61]。Rigのペイロードとして、Cerber、Ursnifなどを確認しています。また、10月の上旬にSundownを観測しました。確認したケースではInternet Explorer、Flash、Silverlightの脆弱性を悪用する機能を備えていました。

なお、これらのExploit Kitへの誘導元となっているWebサイトにmacOSクライアントでアクセスした場合は、Landing pageへ誘導されない、あるいはLanding pageが応答を返さないことを確認しています。本期間中、macOSを対象としたドライブバイダウンロード攻撃は観測していません[*62]。

PUA[*63]のインストールや偽のサポートセンターへの電話を促す目的で、ブラウザ画面にマルウェア感染などを仄めかす偽のダイアログなどを表示する詐欺サイトへの誘導が継続しています。また、このような詐欺サイトへの誘導では海外のTDS[*64]が利用されているケースが複数確認されました。例えば、ある欧州のTDSについては2016年9月中旬から2017年1月現在まで、複数の種類の詐欺サイトへの誘導に継続して利用されていることを観測しています。業務利用端末などでは、用途を踏まえて、TDSの遮断を検討



※調査対象は日本国内の数十万サイト。
※近年のExploit Kitによるドライブバイダウンロード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、試行環境や状況によって大きく異なる結果が得られる場合がある。
※詐欺サイトや実行ファイルへの直リンクなど、Exploit Kit以外の受動的攻撃による脅威はOtherに分類している。

図-17 Webサイト閲覧時の受動的攻撃発生率（%）（Exploit Kit別）

*60 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。
*61 2016年9月末から10月中旬までのRig Exploit Kitの観測状況については、IIJ-SECT「Rig Exploit Kit 観測数の拡大に関する注意喚起」（https://sect.iij.ad.jp/d/2016/10/178746.html）で速報している。
*62 MITF Webクローラシステムでは、Windowsクライアント環境で巡回した際に受動的攻撃の兆候が観測されたWebサイトを対象に、macOSクライアント環境を用いた追加調査（ブラウザによるWebアクセス）を行っている。
*63 Potentially Unwanted Applicationの略。一般的な業務に不要と思われたり、用途によってはPCユーザやシステム管理者にとって不適切な結果を招く可能性があると考えられたりするアプリケーションの総称。
*64 Traffic Distribution Systemsの略。Webサイトのトラフィックを売買するシステム。通常、Webサイト所有者がリンクなどの形でトラフィックをTDSベンダーにリダイレクトし報酬を、受け取る。更にTDSベンダーはこのトラフィックを販売し、最高額入札者へリダイレクトする。TDSを悪用したマルウェア拡散についてはシマンテック社のセキュリティレスポンスブログ「Web ベースのマルウェア拡散経路：トラフィック流通システムの概要」（https://www.symantec.com/connect/blogs/web-1）で紹介されている。

してもよいかもしれません。なお、TDSや類似するシステムの多くではインフラとして著名なクラウドサービスを利用していることが多いため、IPアドレスベースでの制御は有効に機能しません。ドメインベースでトラフィックを制御する仕組みが必要です。

また、これらの詐欺サイトではダイアログを表示する主体として被害者の利用しているOSメーカーやISPを仄めかすものがあります。IIJのインターネット接続サービスをご利用いただいているお客様の環境では、IIJの名前が表示される場合がありますが、弊社の関与したものではないのでご注意ください[*65]。

Rigを用いたドライブバイダウンロード攻撃が継続しています。ブラウザ利用環境ではOS、アプリケーションやプラグインのバージョン管理やEMET導入などの脆弱性対策の徹底しておくことを推奨します[*66]。Webサイト運営者は利用しているWebアプリケーションやフレームワーク、プラグインの脆弱性管理による脆弱性対策に加え、TDSを経由したトラフィック、広告や集計サービスなど外部から提供されるマッシュアップコンテンツの管理が必須です。

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、Ursnif（gozi）の解析妨害とその回避手法について紹介します。

1.4.1 Ursnif（gozi）の解析妨害とその回避手法

Ursnif（別名gozi、snifula、ISFB、Papras、Dreambot）は、Banking Trojanに分類される、金融機関などのアカウント情報をWebブラウザから盗み出し、その情報を不正に利用することで金銭を窃取するマルウェアです。近年、Ursnifを使う攻撃者は日本の金融機関のアカウント情報を標的にしていることが確認されています[*67]。感染源は複数確認されており、Exploit Kit経由でのWeb感染、SPAMメールやURLZone（別名 BEBLOH、Shiotob）が追加ダウンロードする場合が報告されています[*68]。そのため、このマルウェアの名前はITセキュリティに関するニュースでも頻繁に取り上げられています。

*65 このような詐称は繰り返し行われており、IIJ-SECT「ISP情報を表示して偽のサポート窓口へ誘導する詐欺サイトに関する注意喚起」（https://sect.iij.ad.jp/d/2015/12/258504.html）でも紹介した。

*66 例えば管理者権限の分離やアプリケーションホワイトリストの適用などが考えられる。詳細は本レポートのVol.31（http://www.iij.ad.jp/company/development/report/iir/031.html）の「1.4.3 マルウェアに感染しないためのWindowsクライアント要塞化」参照。

*67 2016年以降は特に日本国内でのUrsnifの感染事案が多く、各ベンダーや組織から注意喚起がなされている。「インターネットバンキングマルウェア「Gozi」による被害に注意」（https://www.jc3.or.jp/topics/gozi.html）。「Ursnif（別名：Gozi他）が3月以降猛威を振るっています。」（http://www.lac.co.jp/blog/category/security/20160615.html）。トレンドマイクロセキュリティブログ「国内ネットバンキングを狙う「URSNIF」が新たに拡散中」（http://blog.trendmicro.co.jp/archives/13471）。トレンドマイクロセキュリティブログ「2017年もマルウェアスパムの攻撃は継続中、新たな「火曜日朝」の拡散を確認」（http://blog.trendmicro.co.jp/archives/14296）。"2017-01-24 - ONGOING JAPANESE MALSPAM CAMPAIGN SPREADING URSNIF VARIANT"　（http://www.malware-traffic-analysis.net/2017/01/24/index3.html）。中でもDreambotと呼ばれる亜種は頻繁に更新がなされており、Tor上に存在するC&Cサーバにアクセスを行う場合がある。"Nightmare on Tor Street: Ursnif variant Dreambot adds Tor functionality" (https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality)。このレポートの中では2016年7月の日本国内の事案が紹介されている。更に2017年1月末にもDreambotによる不正送金事案が発生していることをJC3が報告している（https://www.jc3.or.jp/info/malware.html#pl05）。また、次のレポートでは2016年8月から9月のDreambotの事案も紹介されている（https://www.cyber.nj.gov/threat-profiles/trojan-variants/dreambot）。

*68 Exploit kit経由では、Angler Exploit kitやNeutrino Exploit kit、Rig Exploit　kitからドライブバイダウンロードされていたことをIIJでは確認している。また、メールに関しては2017年1月現在、添付ファイルとして「.svg」や「.js」などが添付され、これを実行することでUrsnifがダウンロードされ、実行されることが多い。またメールの文章は日本語である。特に「.svg」は画像ファイルであるにも関わらず、その実態はXML形式であり、かつJavaScriptが動作することから、メールゲートウェイやサンドボックスをすり抜けるために悪用された。「.svg」の事例は次のレポートが詳しい。「さまざまな件名でマルウェア（ウイルス）付き日本語メール拡散中　[ウィルス/不正アクセス]」（http://security-t.blog.so-net.ne.jp/2017-01-23）。また、URLZone経由での感染は次のレポートが詳しい。「バンキングマルウェア「URSNIF」解析レポート」（https://www.nttsecurity.com/-/media/nttsecurity/files/resource-center/what-we-think/ursnif_20161215.pdf）。「2016年をサイバー攻撃で振り返る--「ばらまき型」「40ドル汎用マルウェア」」（https://japan.zdnet.com/article/35093731/）。

Ursnifは複数の手法を使って解析を妨害しており、解析環境上では正常に解析結果が得られないことがあります。そこで、本稿ではUrsnifが使う解析妨害手法を紹介すると共に、それをどのように回避してC&Cサーバへの通信を出力させ、インシデント対応に有効な情報を得るかを解説します。なお、本稿で紹介している手法は、必ず仮想マシンなど、解析が終わったらすぐに戻せる環境で行い、ネットワークからも隔離した状態で行ってください。

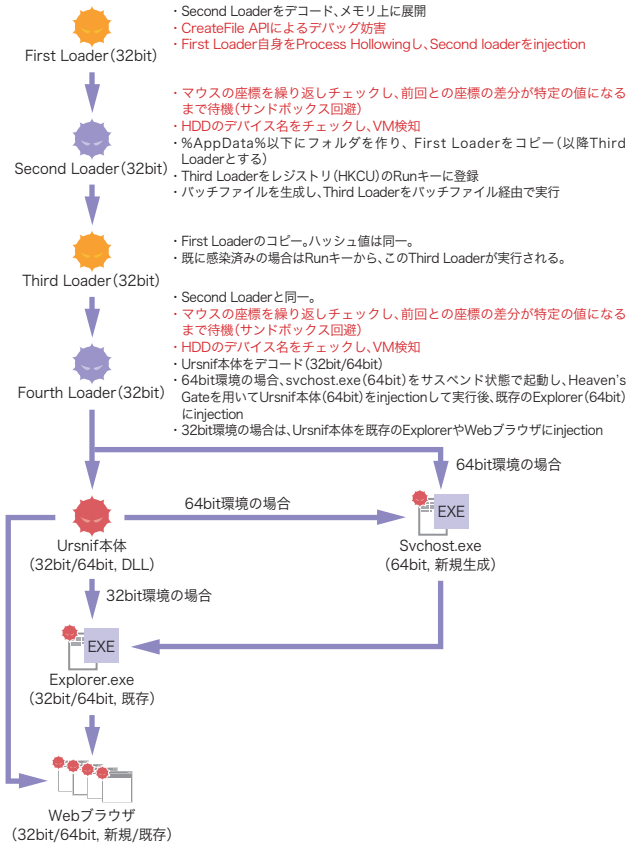


図-18 Ursnifの感染時の挙動

■ 概要

図-18はUrsnifの感染時の挙動を示したものです。図のとおり、Ursnifは複数回にわたってコードインジェクション*69を行い、その中で解析妨害を行っています。First Loaderの実行ファイル内にはメモリ上にしか展開されないSecond Loaderや、Ursnif本体がエンコードされて入っています。図-18中の赤文字で書かれた部分が、今回主に解説を行う妨害手法です。

■ CreateFile APIによるデバッグ*70妨害

UrsnifのFirst Loaderは「CreateFileA」*71というAPIを使用してファイルを開き、自分自身を読み込みます。その際、「dwShareMode」を0にして呼び出すため、排他モードで読み込もうとします。一方で、デバッガも解析対象をCreateFile APIを使用して開きます。しかし、多くのデバッガは開いた際に生成されるファイルハンドル*72を閉じないため、UrsnifのCreateFile APIが排他モードでファイルを読み込もうとした際、既にデバッガによってファイルが開かれており、同一ファイルをオープンしようとして失敗します。筆者がよく使うデバッガを調査したところ、表-1のような結果でした。

*69 コードインジェクションとは、実行中のプロセスとは異なるプロセスにコードを挿入し、実行させる手法。

*70 デバッグとは、一般的にソフトウェアのバグを発見し、そのバグを除去することをいい、その際に使うツールのことをデバッガという。マルウェア解析においてはバグの発見が目的ではなく、デバッガ上でマルウェアを動作させつつ、解析者が一時停止させたい部分でピンポイントで一時停止させ、その周辺のコードやメモリの状態を調査するために利用する。

*71 本稿では、CreateFile APIと記述した個所と、「CreateFileA」と記述した箇所がある。これには明確な理由がある。Windowsでは、引数や戻り値に文字列へのポインタが含まれる場合、ほとんどのAPIの末尾にANSI形式を扱うA、もしくはWindowsの内部表記であるUNICODE形式を扱うWがつく。例えば、CreateFile APIはCreateFileA(ANSI)とCreateFileW(UNICODE)の2つのAPIが存在する。CreateFile APIと表現した場合、その両方を指す。コードを書くときは単純に「CreateFile」と記述しておけば、コンパイル時にコンパイラが設定に応じて適切なAPIを自動で選択するため、プログラマはこの点を気にする必要はない。しかし、厳密に言えばWindows内部に「CreateFile」というAPIは存在せず、存在するのはCreateFileA、もしくはCreateFileWであり、解析者はこれらを区別して扱わなければならない。例えば、ブレークポイントの設定時、「CreateFile」にはブレークポイントを設定できない。あくまでAとWのいずれか、もしくは両方に設定しなければならない。一方で、マルウェアがどちらを使っているかはマルウェア作者の開発環境に依存するか、単に作者の好みであり、解析開始時点では不明であるため、筆者はとりあえずAにまず設定して停止するかを確認し、停止できなかった場合はWを試すようにしている。そのため、本稿では、CreateFile APIと表現した場合はCreateFileAとCreateFileWの両方を指し、「CreateFileA」とカギ括弧付きで記述した場合は、API名を厳密に指し示すものとする。ちなみに、Windowsには、CreateFile APIの低レイヤー版である「ZwCreateFile」というAPIが存在する。CreateFileAやWは、最終的にKernelに渡される前に「ZwCreateFile」が実行されるようになっており、一部のマルウェアはこのAPIを直接使用する場合もある。これも作者の好みで異なるため、状況に応じて解析者もブレークポイントを設定するAPIを使い分ける必要がある。

*72 ファイルハンドルとは、読み書きなどのファイル操作を行う際、事前にOSから取得しておく許可証のようなもの。現実世界でハンドルというと、車のハンドルを思い浮かべる人も多いと思うが、車のハンドルは車を操作するためのものであるのと同様に、ファイルのハンドルはファイルを操作(読み書きなど)するためのものである。

表-1中でxとなったデバッガでこの妨害を回避するには、デバッガ上に読み込み終えた後にファイルハンドルを手動で閉じます。例として、x32dbg[*73](x64dbgの32bit版)を用いた解析例を記載します。

1. x32dbgにUrsnifをロードする(x32dbgを起動後、Ursnifをドラッグ&ドロップすることで可能)。
2. Process Hacker[*74]を起動し、x32dbg.exeプロセス上で右クリックし(図-19(1))、「Properties」を選択する。
3. 「Handles」タブをクリックし(図-19(2))、Nameが解析対象のファイル名で、かつTypeが「File」となっているものを選択し(図-19(3))、右クリックして「Close」を選択する(図-19(4))。

表-1 解析対象のファイルハンドルのクローズの有無

デバッガ	クローズ
OllyDbg 1.10 / 2.01	○
Immunity Debugger 1.85	○
x64dbg / x32dbg(Jan 27 2017)	×
WinDbg 6.2 / 6.3	×
IDA Pro 6.95(Local Win32 Debugger)	×

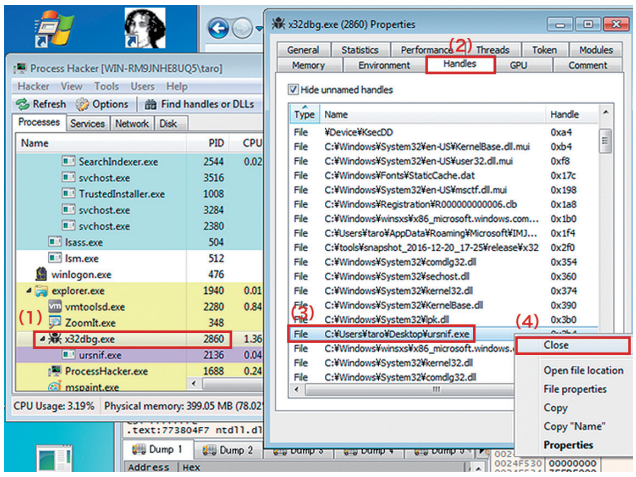


図-19 デバッカ内の解析対象のファイルハンドルのクローズ

図-20は、この対策を行わなかった場合(図-20上)と行った場合(図-20下)のUrsnifによるCreateFile APIの実行直後の状態を示したものです。対策済み(図-20下)の場合はEAX[*75]が0x74という値で正常にファイルハンドルが作られているのに対し、未対策の場合(図-20上)はEAXが0xFFFFFFFF(INVALID_FILE_HANDLE)になっています。つまりこれはファイルのオープンに失敗したことを意味します。よって、その後の処理が正常に行われず、Ursnifは途中で存在しないメモリ領域(正常であればSecond Loaderが格納されるはずの領域)を読み込もうとして異常終了します。

■ Process Hollowing

Process Hollowingはコードインジェクション手法の一種で、インジェクション対象のプロセスを新規で立ち上げ、対象プロセスに関連するコードやデータをメモリ上から削除し、その場所に悪意のあるコードやデータをインジェクションして実行する手法です。近年のマルウェアは、この手法や類似のインジェクション手法を多用しています。

この手法は、Personal FirewallやHost型IDSなどをすり抜けるために使われています。例えば、IEなどのWebブラウザにインジェクションすると、Webブラウザは通信が許可されているため、C&Cサーバへのアクセスが可能になります。また、

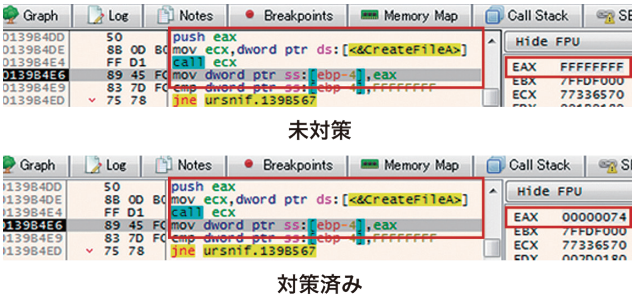


図-20 CreateFileAの結果

*73 x32dbg は、x64dbgに同梱される32 bitの実行ファイル用のデバッガで、長らく解析者の間でデファクトスタンダードであった、OllyDbgとほぼ同様の操作感を持つ。OllyDbgとの差異として、64 bit用の実行ファイル(PE32+フォーマット)をデバッグすることが可能である点と、Memory Breakpoint on Executionを設定できる点が優れている。また、数日に一度のペースで改良が行われている点も魅力である。次のURLから入手可能(http://x64dbg.com/)。

*74 Process Hackerは、高機能版のタスクマネージャと言えるもので、SysinternalsのProcess Explorerと類似する機能を持つ。Process Explorerと比較して、今回紹介するような任意のメモリ領域の書き換え機能などを持つ。次のURLから入手可能(http://processhacker.sourceforge.net/)。

*75 EAXとは、x86アーキテクチャにおける、汎用レジスタ(CPU専用の変数のようなもの)の1つで、Windowsの実装では関数の実行後、戻り値が格納されている。CreateFileでは戻り値にファイルハンドルが入るため、ここをチェックすることで、ファイルハンドルの取得の成否が分かる。

例えばタスクマネージャ上でプロセス一覧を見た場合、正規なプロセスが動作しているようにしか見えないため、インシデント対応者にマルウェアの存在を一目で認識させないようにするという効果もあります。

Process Hollowingは以下のような流れで実行されます。

1. 新規にプロセス(例えばsvchost.exeやiexplore.exeなどのWindowsの正規プロセスが多い[*76])をサスペンド状態で生成する(以下プロセスB)。これは、CreateProcess APIの引数にCREATE_SUSPENDEDが使われる(図-21)。
2. プロセスBの実行ファイルに関わる領域をZwUnmapViewOfSection APIを用いて削除する(図-21)。
3. マルウェアのコードやデータをプロセスBの領域にコピーする(図-22)。これにはZwCreateSection及びZwMapViewOfSection API、もしくはVirtualAllocEx及びWriteProcessMemory APIが使われることが多い。
4. プロセスBのエントリポイント[*77]をマルウェアのものに書き換える。これにはGetThreadContext及びSetThreadContext APIが用いられる。
5. ResumeThread APIを用いて、サスペンドされたプロセスBの実行を再開することで、コピー先で悪意のあるコードが実行される。

CreateProcess APIが実行された後、すぐにデバッガで生成されたプロセスをアタッチ[*78]すればよいのではないかと考える方もいるかもしれませんが、実はWindowsの仕様により、プロセスBの実行が項番5で再開されるまで解析者はデバッガなどで対象プロセスをアタッチすることができません。これはCREATE_SUSPENDEDで起動された場合、この実行ファイルのエントリポイントのはるか手前でコード実行が一時停止しているからです。そのため、OSが様々な準備処理を実行してからでないとアタッチできません。そこで、解析者は項番5に至る前までに何らかの手法を使い、デバッガでアタッチが可能になるまで対象プロセスの実行を進め、かつ悪意のあるコードが実行される前にコード実行を一時停止させることが要求されます。

筆者はこのような場合、以下の手法を用いて回避します。

1. SetThreadContext API(前述の項番4)まで実行を進め、悪意のあるコードのエントリポイントのアドレスを確認する。
2. 悪意のあるコードのエントリポイントを無限ループに書き換える。
3. ResumeThread APIを実行させ、プロセスBの実行を開始させる。
4. 無限ループしているプロセスBをデバッガでアタッチし、無限ループを元のコードに書き戻して解析を行う。

これにより、悪意のあるコードのエントリポイントまでは実行されますが(OSが行う準備処理のコードで、悪性コードではない)、その時点で無限ループするため、悪意のあるコードはまだ実行されていません。またエントリポイントまで到達していればデバッガでのアタッチが可能になるため、前述の要件を満たすことができます。

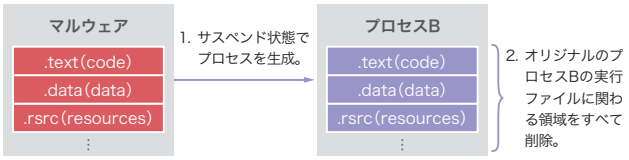


図-21 Process Hollowing(サスペンド状態での起動)

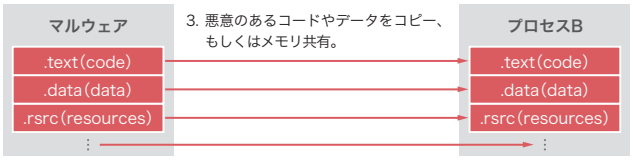


図-22 Process Hollowing続き(悪意のあるコードやデータのコピー)

*76 ただしUrsnifのFirst Loaderは、First Loader自身を子プロセスとして生成し、その子プロセスに対してProcess Hollowingを行う。よってパーソナルファイアウォールをすり抜けるためではなく、一種のデバッグ妨害として使用していると筆者は考えている。
*77 エントリポイントとは、実行ファイルにおいて最初に実行されるコードのアドレスのこと。
*78 アタッチとは、デバッガで既存のプロセスをデバッグすること。

例として、x32dbgとProcess Hackerを併用したProcess Hollowingの対処法を紹介します。Ursnifにおいては、前述のCreateFile APIによる妨害を回避したものとして話を進めます。

1. x32dbgの画面左上の逆アセンブル領域をクリックし、「Ctrl+G」を押します。
2. 出てきたポップアップウィンドウに「CreateProcessA」と入力(図-23(1))し、OKをクリックします(図-23(2))。
3. 「CreateProcessA」に移動したことが確認できたら(図-23(3))、ファンクションキーの「F2」を押してブレークポイント[*79]を設定します。設定されると、アドレス部分が赤く反転します(図-23(4))。
4. F9でコードを実行するとブレークポイントによって、「CreateProcessA」の先頭コードでコード実行が一時停止し、EIP[*80]が「CreateProcessA」をポイントします。ブレークポイントで停止した際、アドレス部が黒地でかつ、文字列が赤くなります(図-24(1))。スタック領域(図-24右下)を見ると、CreateProcess APIの第6引数「dwCreationFlags」にあたる部分[*81]に「4」が入っており(図-24(2))、これは「CREATE_SUSPENDED」を意味します。これがProcess Hollowingのサインであると言えます。
5. 次に、同じ要領で「SetThreadContext」にブレークポイントを設定し、実行します。「SetThreadContext」で停止したことを確認したら(図-25(1))、第2引数「lpContext」の部分をクリックし(図-25(2))、右クリックメニューから「Follow DWORD in Dump」を選択します。
6. 「Dump 1」タブのAddress部分がスタック領域の「lpContext」にあたるアドレスと一致していることを確認します(図-25(3))。このアドレスはCONTEXT構造体

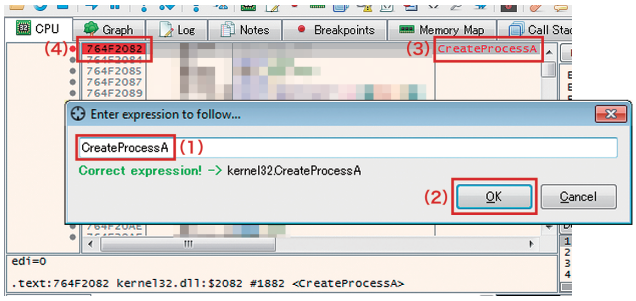


図-23 CreateProcessAへのブレークポイントの設定

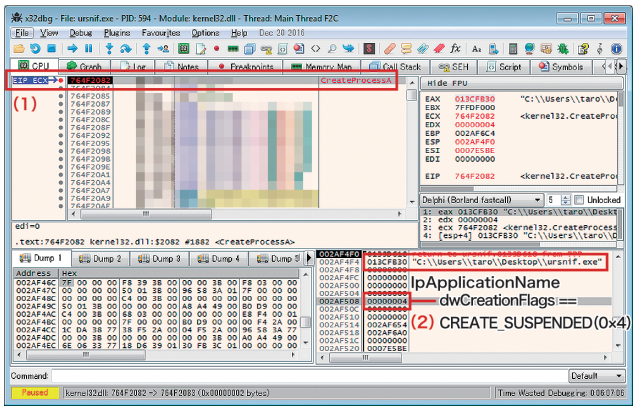


図-24 CREATE_SUSPENDEDでUrsnif自身を生成することを確認

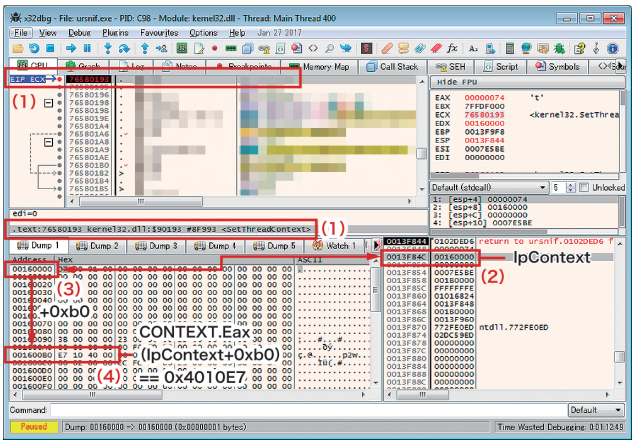


図-25 SetThreadContextで停止させて状態を確認

*79 ブレークポイントとは、デバッグ対象プロセスのコード実行を一時停止し、デバッガに処理を戻すための仕組みで、停止させたいコードの先頭バイトをデバッガ内部でint 3(0xcc)命令に変更し、例外を発生させて停止させるソフトウェアブレークポイントと、CPUのデバッグレジスタを使って停止させるハードウェアブレークポイント及び後述のメモリブレークポイントが存在する。今回設定しているのはソフトウェアブレークポイントである。どれも一長一短あるので、状況に応じて使い分ける。

*80 EIPはx86アーキテクチャにおける専用レジスタで、次に実行されるコードのアドレスを常にポイントしている。

*81 MSDNのCreateProcess APIのWebページ(https://msdn.microsoft.com/ja-jp/library/windows/desktop/ms682425 (v=vs.85).aspx)を参照すると、第6引数がdwCreationFlagsであることが分かる。一方、図-24は、「CreateProcessA」の先頭アドレスで実行を一時停止させている。その時のスタックの状態は、一番上(ESPレジスタが指している値)がリターンアドレス(CreateProcessAの呼び出し元に復帰するためのコードのアドレスが格納されている)で、その次から4バイト単位で引数が格納されている(今回は32 bitのWindows上で解析しているため、1つの引数が4バイト(= 32 bit)になる)。例えば図-24において、ESPは0x2af4f0であり、第1引数(lpApplicationName)は0x2af4f4、第2引数(lpCommandLine)は0x2af4f8となっている。つまり、第6引数はESP+6*4 = 0x2af4f0 + 24 (0x18) = 0x2af508と計算することができる。

の先頭を指しています。そこから「+0xb0」の位置にある4バイトはEAXにセットする値です。CREATE_SUSPENDEDで起動した場合、最終的にEAXに格納されているアドレスがエントリポイントとして扱われます[*82]。今回の検体は、「0x4010E7」という値であることが分かります（図-25(4)）[*83]。この値を書き留めてください。このアドレスにある命令を無限ループに書き換えてしまえば、Ursnifの悪意のあるコードが実行される前にプログラムを一時停止できます。

7. Process Hackerを起動し、子プロセス側のUrsnifをダブルクリックします（図-26(1)）。「Properties」ウィンドウが開くので、「Memory」タブに切り替え（図-26(2)）、先程書き留めたアドレスが属する領域を見つけます。今回のアドレスは「0x4010e7」であり、「0x400000」から396KBの領域内にあるため、「0x400000」をダブルクリックして開きます（図-26(3)）。「0x400000」のダンプウィンドウが開くため、「Go to...」（図-26(4)）をクリックし、残りの「0x10e7」を入力し、「OK」をクリックします。0x10e7にジャンプするので、その2バイトを書き留めたあと、「eb fe」に書き換え、「Write」をクリックし、「Close」をクリックします。これで、エントリポイントを無限ループに書き換えられました（「eb fe」はx86のマシン語で無限ループの意味）。
8. x32dbgに戻り、F9を押してプログラムを最後まで実行させます。すると、親プロセスは終了しますが、子プロセスはエントリポイントで無限ループになるため、Process Hackerを確認するとCPUを高い割合で消費したまま残っているのが確認できます（図-27(1)）。このプロセスのPIDの値を控えたら、x32dbgで「Alt+A」を押し、PIDが一致するものをアタッチします。このとき、Process Hacker側は

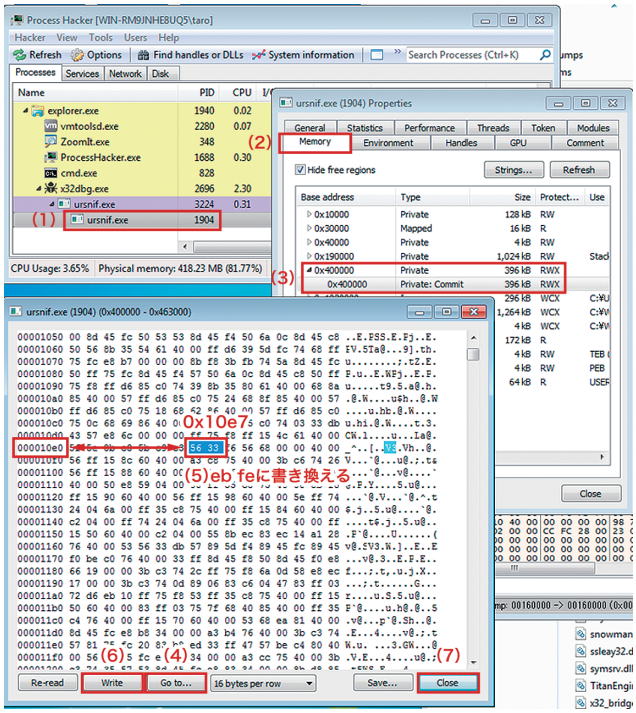


図-26 エントリポイントを無限ループに変更

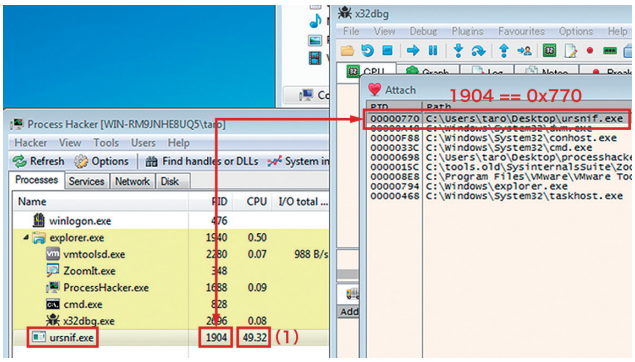


図-27 無限ループ中のUrsnifのプロセスをアタッチ

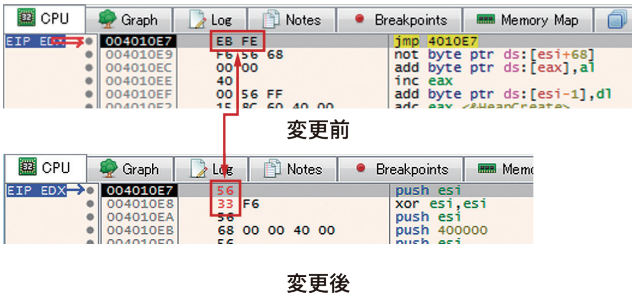


図-28 オリジナルのバイト列への書き戻し

*82 CONTEXT構造体内のEIPの部分を書き換えることも原理的には可能だが、CREATE_SUSPENDEDで起動したプロセスにコードインジェクションを行う場合、対象プロセスは実行するための準備ができていないため、EIPに直接悪意のあるコードのアドレスを渡しても正常には動かないことが多い。そのため、基本的にはEAXが使われる。ただし、既存のプロセスにインジェクションするケースはこの限りではないため、EIPも合わせてチェックする必要がある。また、SetThreadContext APIはGetThreadContext APIとセットで使われることが多い。もしどの部位を書き換えたのかが不明瞭である場合は、その差分をチェックすることで、マルウェアが書き換えた箇所が分かる。

*83 x86アーキテクチャはバイトオーダがリトルエンディアンであるため、int型の整数値として扱う場合、バイト単位で逆から読む必要がある。

10進数でPIDが表示されているのに対し、x32dbgは16進数で表示されている点に留意してください。

9. 子プロセスをアタッチできたら、F9を押して実行し、F12で一時停止してください。すると、EIPが以前に書き留めた0x4010e7で停止していることが分かります（図-28上）。そこで、このアドレスをクリックした後、「Ctrl+E」を押して、「eb fe」を元の2バイト（本例では「56 33」）に書き戻します（図-28下）。これで、インジェクション先のコードを解析する準備ができたことになります。Ursnifの場合、ここがSecond Loaderのエントリポイントになります。

■ マウス入力座標チェックによるサンドボックス回避

Second Loaderは、「.bss」セクション内にある重要な文字列をデコードして使いますが、デコードのための復号キーの一部にマウスカーソルの座標から生成した値を使います。図-29は該当するコードの付近です。ループ内でGetCursorInfo APIを繰り返し呼び出し、座標XとYを足し合わせたものと前回実行時の座標の差分を計算した上で、それを引数に「.bss」セクションをデコードするルーチンを呼び出します。デコードが終わった後、デコードの成否を判定するマーカーの値と比較し、一致しなければ、このループが終わりません。頻繁にマウスを動かして使用する一般ユーザの環境であれば繰り返しチェックしているうちに値が一致するので短時間のうちにこのループを抜けますが、サンドボックス環境の場合、マウスを自動でランダムに動かすような設定がされていないと、処理がこれ以上進まず、この検体が悪性であることを判定できません。最近のサンドボックスにはランダムでマウスカーソルを動かす機能がついているので問題ないと思われますが、設定により無効化されている場合は誤判定する可能性があるため、設定を見直したほうが良いでしょう。

■ HDDデバイス名によるVM検知*84

次はHDDデバイス名によるVM検知です。Ursnifは「SetupDiGetDeviceRegistryPropertyA」というAPIを特定のパラメータと共に使って行います。まずこのAPIにブレークポイントを設定して実行し、上記APIで一時停止させてください。実行後、マウスを小刻みに動かして、前述の「マウス座標チェックによるサンドボックス回避」を抜けなければこのAPIで停止しないことに注意してください。またこのAPIは、ほとんどの場合、2回1セットで呼び出されます。1回目の呼び出しでは、バッファ（第5引数、PropertyBuffer）をNULL（0）にして呼び出すことによって必要な文字長を取得します。その結果をもとに必要なバッファをHeapなどに確保してから第5引数にそのバッファのポインタをセットし、2度目の呼び出しを行います。よって、このAPIの2度目の呼び出しが終わった後にバッファに結果が格納されるため、2度目の呼び出しで一時停止させるためにもう一度F9を押し、かつCtrl+F9でこの関数の終了まで実行してください。すると、スタック領域のPropertyBuffer（図-30（1））にあたる部分に取得したHDD

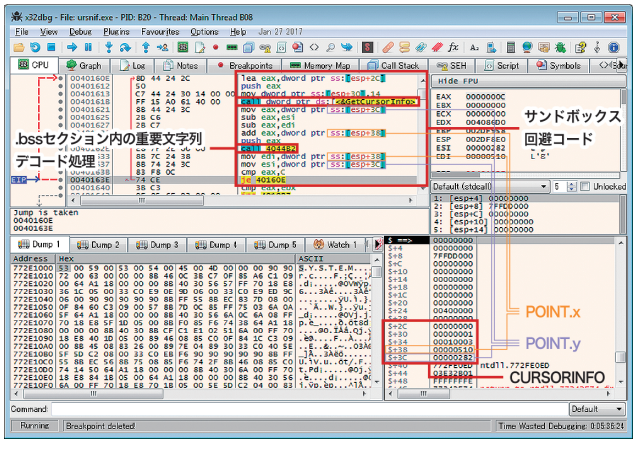


図-29 マウス座標監視によるサンドボックス回避

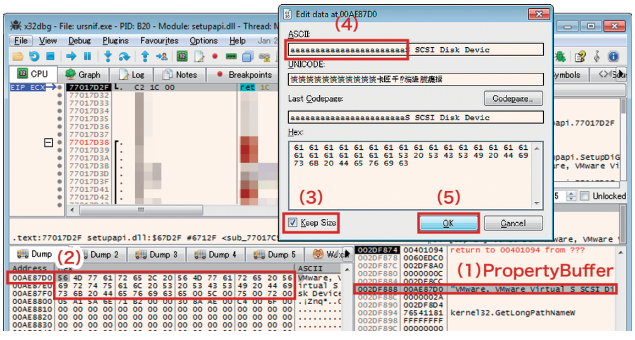


図-30 2度目のSetupDiGetDeviceRegistryPropertyAの実行後

*84 VM検知とは、VMwareやVirtualBoxなどの仮想マシンを検知する手法の総称。特殊な命令を発行することで検知するものや、特定のファイルやレジストリの値をチェックするもの、CPUの数をチェックするものなど、様々な手法が存在する。

のデバイス名が入ります。ここを右クリック(図-30(1))し、「Follow DWORD in Dump」をクリックすると、「Dump 1」タブにバッファが表示されるため、デバイス名の文字列部分をドラッグで選択し(図-30(2))、「Ctrl+E」を押すと、「Edit data」ウィンドウが現れます。「Keep Size」にチェックをつけ(図-30(3))、製品名やVirtualなど、検出されそうな文字列をすべて任意の文字列で潰してしまいます(図-30(4))。これで、マルウェアに検知されることなく、動作させることができます。ちなみに、F7を一度押してステップ実行し、APIから悪意のあるコードに戻ると、マルウェアが検知する文字列を確認することができます(図-31)。

■ C&Cサーバとの通信

このVM検知が終わると、Second Loaderは「%AppData%」以下にフォルダを作り、そこにFirst Loaderをコピー(以下、これをThird Loaderと呼ぶ)します(図-32)。また、Third Loaderをレジストリ(HKCUのRunキー)に登録し、次回マシンを起動時に自動起動するようにした上で、バッチファイルを生成して、Third Loaderを実行します。Third Loaderは、First Loaderと同一であり、Fourth LoaderもSecond Loaderと同一で、挙動が途中まで同じであるため、C&Cサーバと通信をさせるためには、Third Loader、Fourth Loaderの解析妨害も再度突破する必要があります。そこで、Second Loaderを最後まで実行させた後、生成されたThird Loaderをデバッガで読み込み、ここで記載したような解析妨害を再度回避します。これに成功すると、Fourth Loaderのプロセスは終了してしまいますが、数分後にExplorer.exe内にインジェクションされた悪性コードから、図-33のようにC&Cサーバへの通信が出るようになります[*85]。パス部に「/images/」や、長いパス部の文字列、「.gif」、「.bmp」、「.jpeg」など画像フォーマットの拡張子で終わっているといった特徴的な文字列があるため、パターンマッチングで検出できることが分かるかと思います。

また32bit環境では、Fourth LoaderからExplorerやIE、Firefox、Chrome、Operaに対してインジェクションを行います。その際、ZwCreateSection API、ZwMapViewOfSection APIを利用します。この付近までコードを進め、Explorerプロセスに新しいセクションが作られたらアタッチし、Memory breakpoint[*86]をその領域に設定することで、C&Cサーバとの通信を含む、Explorer内にインジェクションされた悪意の

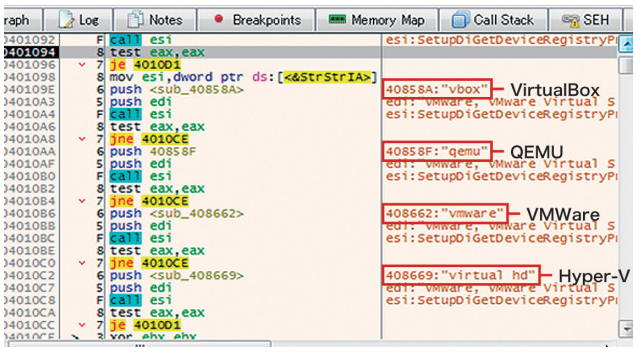


図-31 HDDデバイス名での検知キーワード

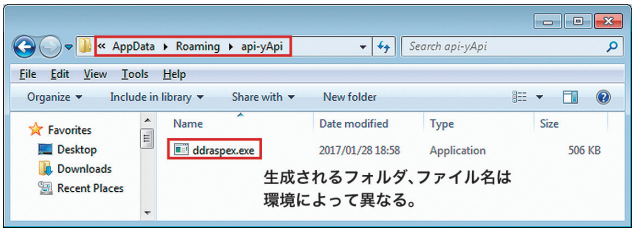


図-32 %AppData%以下にコピーされたUrsnif

*85 図-33はFakenet-NGと呼ばれるインターネットエミュレータを用いている。これを用いることで、クローズドな環境であってもマルウェアの通信をこのソフトウェアに転送し、観測することが可能。次のURLから入手可能(https://github.com/fireeye/flare-fakenet-ng)。

*86 Memory breakpointとは、ブレークポイントの一種である。ソフトウェアブレークポイントは任意の各命令の先頭アドレスに、ハードウェアブレークポイントは任意の1バイト、2バイト、4バイト単位でそれぞれ設定するのに対し、メモリブレークポイントはメモリ上の任意の領域全体に対して設定することが可能。また、ソフトウェアやハードウェアブレークポイントはアーキテクチャレベルで実装されているのに対し、このブレークポイントは各デバッガで独自実装されている。今回使用しているx32dbgや、OllyDbgなどはこの種のブレークポイント実装している。

あるコードの挙動を更に追うことができます。64bit環境では、svchost.exe(64bit) をCREATE_SUSPENDEDで生成し、Heaven's Gate[*87]という手法を多用してFourth Loader(32bitコード)から64bitプロセスにUrsnif本体をコードインジェクションした後、Explorerにインジェクションを行います。

今回はUrsnifを例に、このマルウェアが持つ解析妨害手法を紹介し、それらを回避する方法を紹介しました。見てのとおり、ほとんどの解析妨害はWindows APIを通して行われます。マルウェアの使う手法を事前に調べておくことで、解析妨害を突破し、多くの挙動を把握することができるでしょう。また、妨害手法は有限であるため、多くのマルウェアで似通った手法を使っています。例えば今回紹介したHDDデバイス名をチェックすることによる検知手法はURLZoneや、いくつかのアドウェアでも使われていることを確認しています。予め情報収集をしておけば、多くの場合で対処することが可能です。

ここで紹介した手法が適用可能であることを、以下sha-256のハッシュ値を持つ検体で確認しています。

```
5feeee23ecd310ed552b56c1992d5e7f6dbf4e656224a9f3073b83770768e994
```

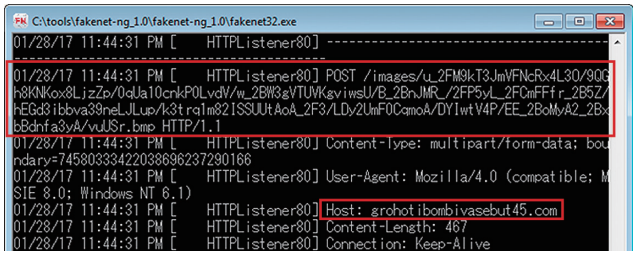


図-33 UrsnifによるC&Cサーバへの通信

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、Ursnif(gozi)の解析妨害とその回避手法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。

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

根岸 征史(1.2 インシデントサマリ)
小林 直、永尾 禎啓、鈴木 博志、小林 稔、梨和 久雄(1.3 インシデントサーベイ)
鈴木 博志(1.4.1 Ursnif(gozi)の解析妨害とその回避手法)
IIJ セキュリティ本部 セキュリティ情報統括室

協力:
須賀 祐治、桃井 康成、平松 弘行 IIJ セキュリティ本部 セキュリティ情報統括室

*87 Heaven's Gateとは、32 bitコードから64 bitコードを実行するための手法。通常利用の範囲内の場合、Windowsは64 bit環境において32 bitの実行ファイルを実行すると、WOW64(Windows on Windows)環境内で実行され、WOW64が32 bitと64 bitの橋渡しを行っているため、ユーザは特に意識せずに実行できる。しかし、Ursnifは32 bitコードから直接64 bitコードを64 bitプロセスにインジェクションするため、WOW64相当の処理を自分自身で担当することで解決しており、それがHeaven's Gateと名付けられている。"Heaven's Gate: 64-bit code in 32-bit file"(http://vxheaven.org/lib/vrg02.html)。"Knockin' on Heaven's Gate - Dynamic Processor Mode Switching"(http://rce.co/knockin-on-heavens-gate-dynamic-processor-mode-switching/)。