マルウェアに感染しないための Windowsクライアント要塞化

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4月から6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。標的型攻撃による情報漏えいも国内外で発生しており、国内の大手旅行会社の事件では最大で約697万件の個人情報が漏えいした可能性があると発表されています。また過去に大手SNSサービスなどから大量のパスワード情報が漏えいしていたことが明らかとなり、この情報を悪用したと考えられる攻撃も複数観測されています。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4月から6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。

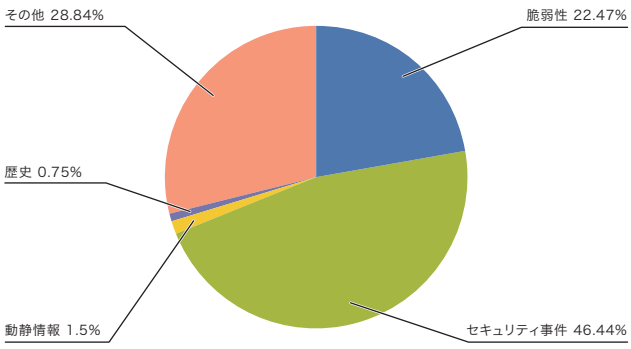


図-1 カテゴリ別比率(2016年4月〜6月)

■ 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、昨年9月から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が、この期間においても国内のサイトにおいて被害が継続して発生しています(OpKillingBay/OpWhales/OpSeaWorld)。ただし4月以降の国内への攻撃発生回数はかなり減少しており、理由ははっきりしませんが、攻撃者の興味が他の攻撃キャンペーンへと移っていったためではないかと考えられます。しかし、これが攻撃の終了を意味するとは限らず、他の攻撃者によって攻撃キャンペーンが今後も継続する可能性も考えられます。いずれにせよAnonymousなどのHacktivistによる攻撃活動は、一連の攻撃キャンペーンの終了や継続を判断するのは難しく、攻撃キャンペーンを契機として対応するのではなく、日頃からいつ攻撃が発生しても対応できるように備えておくべきです。

Anonymousによる世界中の主要な金融機関をターゲットとした攻撃キャンペーンOplcarusが2016年1月に開始され、断続的に攻撃活動が継続していましたが、5月になってギリシアの中央銀行やキプロス、フランス、フィリピンなどの多数の金融機関が被害に遭ったことで注目されました。その後6月まで更に多数の金融機関へと攻撃は拡大し、国内の一部の金融機関も攻撃ターゲットのリストに掲載されましたが、観測されるような被害は特に発生しませんでした。

2014年8月にGamma International、2015年7月にHacking Teamと、それぞれFinFisher、RCSという監視用ソフトウェアを開発する企業が相次いで侵入され、その内部情報がインターネット上に公開されたことで大きな話題となりました。その

*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。

攻撃を行った匿名のハッカーPhineas Fisher[*2]が、2016年4月になってHacking Teamへの侵入手口の詳細を公開しています。また5月にはイタリアの警察組織のWebサイトに侵入する様子をYouTubeで公開しました。また同時期にある銀行から1万ユーロ相当のBitcoinを盗み出し、Rojavaで活動するクルド人グループに送金したことも明らかにしました。彼(または彼女)は企業から盗んだ情報の公開や、銀行からお金を奪うこと、そしてこれらによって一般の人々のコンピュータのセキュリティ向上を手助けすることを"Ethical Hacking"だとして、自らの行為を擁護しています。しかし一方でこれらの行為の理由を"for the lulz"だとインタビューで述べており、2011年に世間を大きく騒がせたLulzSecなどのグループの活動に似た側面があると言えます。現在は個人としての活動に留まっているようですが、過去に起こした事件の影響などから今後も引き続き注目しています。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*3*4*5*6*7*8*9*10]、Internet Explorer[*11*12*13]、Edge[*14*15*16]、Office[*17*18*19]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提供され、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る更新が提供され、多くの脆弱性が修正されました。

TLSのAES-GCMに対して初期ベクトル(IV)が再利用されると実用的な攻撃が可能であることが研究者によって示され、IBM

＊2 "Hack Back!(@GammaGroupPR)"(https://twitter.com/GammaGroupPR)。
＊3 「マイクロソフト セキュリティ情報 MS16-039 - 緊急 Microsoft Graphics コンポーネントのセキュリティ更新プログラム(3148522)」(https://technet.microsoft.com/ja-jp/library/security/MS16-039)。
＊4 「マイクロソフト セキュリティ情報 MS16-040 - 緊急 Microsoft XML Core Services 3148541 用のセキュリティ更新プログラム(3148541)」(https://technet.microsoft.com/ja-jp/library/security/MS16-040)。
＊5 「マイクロソフト セキュリティ情報 MS16-053 - 緊急 JScript および VBScript 用の累積的なセキュリティ更新プログラム(3156764)」(https://technet.microsoft.com/ja-jp/library/security/MS16-053)。
＊6 「マイクロソフト セキュリティ情報 MS16-055 - 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(3156754)」(https://technet.microsoft.com/ja-jp/library/security/MS16-055)。
＊7 「マイクロソフト セキュリティ情報 MS16-056 - 緊急 Windows Journal 用のセキュリティ更新プログラム(3156761)」(https://technet.microsoft.com/ja-jp/library/security/MS16-056)。
＊8 「マイクロソフト セキュリティ情報 MS16-057 - 緊急 Windows Shell 用のセキュリティ更新プログラム(3156987)」(https://technet.microsoft.com/ja-jp/library/security/MS16-057)。
＊9 「マイクロソフト セキュリティ情報 MS16-069 - 緊急 JScript および VBScript 用の累積的なセキュリティ更新プログラム(3163640)」(https://technet.microsoft.com/ja-jp/library/security/MS16-069)。
＊10 「マイクロソフト セキュリティ情報 MS16-071 - 緊急 Microsoft Windows DNS Server のセキュリティ更新プログラム(3164065)」(https://technet.microsoft.com/ja-jp/library/security/MS16-071)。
＊11 「マイクロソフト セキュリティ情報 MS16-037 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3148531)」(https://technet.microsoft.com/ja-jp/library/security/MS16-037)。
＊12 「マイクロソフト セキュリティ情報 MS16-051 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3155533)」(https://technet.microsoft.com/ja-jp/library/security/MS16-051)。
＊13 「マイクロソフト セキュリティ情報 MS16-063 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3163649)」(https://technet.microsoft.com/ja-jp/library/security/MS16-063)。
＊14 「マイクロソフト セキュリティ情報 MS16-038 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3148532)」(https://technet.microsoft.com/ja-jp/library/security/MS16-038)。
＊15 「マイクロソフト セキュリティ情報 MS16-052 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3155538)」(https://technet.microsoft.com/ja-jp/library/security/MS16-052)。
＊16 「マイクロソフト セキュリティ情報 MS16-068 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3163656)」(https://technet.microsoft.com/ja-jp/library/security/MS16-068)。
＊17 「マイクロソフト セキュリティ情報 MS16-042 - 緊急 Microsoft Office 用のセキュリティ更新プログラム(3148775)」(https://technet.microsoft.com/ja-jp/library/security/MS16-042)。
＊18 「マイクロソフト セキュリティ情報 MS16-054 - 緊急 Microsoft Office 用のセキュリティ更新プログラム(3155544)」(https://technet.microsoft.com/ja-jp/library/security/MS16-054)。
＊19 「マイクロソフト セキュリティ情報 MS16-070 - 緊急 Microsoft Office 用のセキュリティ更新プログラム(3163610)」(https://technet.microsoft.com/ja-jp/library/security/MS16-070)。

4月のインシデント

1 セ 1日：NTTグループ持株会社のWebサイトに対し、AnonymousによるDDoS攻撃が行われ、一時閲覧できなくなるなどの影響が出た（OpKillingBay）。

2

3 セ 1日：DeNA社が運営している「Mobage」で、第三者のなりすましによる不正ログインが発生し、最大で約10万件のユーザ情報が閲覧された可能性があることが分かった。

4 セ 4日：パナマの法律事務所Mossack Fonsecaから、企業の租税回避の実態を示す大量の内部文書が流出し、その内容が公開された。
Süddeutsche Zeitung、"Panama Papers：This is the leak"（http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/）。

5 セ 5日：トルコの政府機関から全人口の2/3にあたる約5,000万人分の個人情報が流出し、インターネット上に公開された。

6

7 脆 7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/apsb16-10.html）。

8

9 脆 12日：Windows及びSambaに複数の脆弱性が見つかり、修正プログラムがそれぞれリリースされた。
"Badlock Bug"（http://badlock.org/）。

10 脆 13日：Microsoft社は、2016年4月のセキュリティ情報を公開し、MS16-037など6件の緊急と7件の重要な更新を含む合計13件の修正をリリースした。
「2016年4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-apr.aspx）。

11

12 脆 14日：Apple社のQuickTime for Windowsに複数のヒープバッファオーバフローの脆弱性が見つかったが、Apple社は製品のサポートを終了し、修正は行われないことになった。
「QuickTime 7やQuickTime 7 Proについて分からないことがある場合 - Appleサポート」（https://support.apple.com/ja-jp/HT201175）。
「JVNTA#92371676: QuickTime for Windowsに複数のヒープバッファオーバフローの脆弱性」（https://jvn.jp/ta/JVNTA92371676/）。

13

14 他 15日：「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」が参議院で可決され成立した。この改正により「情報処理安全確保支援士」の資格が新設されることとなった。

15

16 脆 19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136件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - April 2016"（http://www.oracle.com/technetwork/jp/topics/ojkbcpuapr2016-2995215-ja.html）。

17

18 セ 21日：日本テレビ放送網株式会社のWebサイトに不正アクセスがあり、約43万人分の個人情報が流出した可能性があることが分かった。攻撃者は「ケータイキットfor Movable Type」の未知の脆弱性を悪用して、OSコマンドインジェクション攻撃を行った。
「弊社ホームページへの不正アクセスによる個人情報流出の可能性について」（http://www.ntv.co.jp/oshirase/index_20160421.html）。

19

20 セ 22日：メキシコの有権者情報9,340万人分のデータがインターネット上に公開されていたことが、セキュリティ研究者によって判明した。MongoDBの設定ミスによるもの。
"BREAKING：Massive Breach of Mexican Voter Data"（https://mackeeper.com/blog/post/217-breaking-massive-data-breach-of-mexican-voter-data）。

21

22 セ 23日：株式会社J-WAVEのWebサイトに不正アクセスがあり、約64万人分の個人情報が流出した可能性があることが分かった。攻撃者は「ケータイキットfor Movable Type」の未知の脆弱性を悪用して、OSコマンドインジェクション攻撃を行った。
「J-WAVE WEBサイトへの不正アクセスによる個人情報流出の可能性に関するお知らせ：J-WAVE 81.3 FM RADIO」（http://www.j-wave.co.jp/topics/1604_info.htm）。「不正アクセスによる個人情報流出の可能性に関する特別調査委員会による調査結果のお知らせ：J-WAVE 81.3 FM RADIO」（http://www.j-wave.co.jp/topics/1606_info.htm）。

23

24

25 セ 26日：2月に発生したバングラデッシュ中央銀行の不正送金事件で、SWIFTの送金システムにマルウェア感染があったことをBAE Systemsの研究者が報告した。SWIFTも顧客に注意喚起を出した。

26

27 脆 27日：Apache Struts2にDynamic Method Invocation（DMI）を有効にしている場合に任意のコード実行の可能性がある脆弱性（S2-032）が見つかり、修正された。また、この脆弱性を標的としたアクセスが観測されているとして、警察庁から注意喚起された。
Apache Software Foundation、"S2-032"（https://struts.apache.org/docs/s2-032.html）。警察庁、「Apache Struts 2の脆弱性を標的としたアクセスの観測について」（https://www.npa.go.jp/cyberpolice/detect/pdf/20160427.pdf）。

28 セ 27日：株式会社NETSEAのB2B卸プラットフォームサイト「NETSEA」において、外部からの不正アクセスによりクレジットカード情報を含む顧客情報が流出した可能性があることが分かった。
「不正アクセスについてのお詫び | 株式会社NETSEA」（http://netsea.co.jp/press/20160427.php）。

29

30 セ 29日：栄光ゼミナールのWebサイトに不正アクセスがあり、2,761人分の個人情報が流出した可能性があることが分かった。攻撃者は「ケータイキットfor Movable Type」の未知の脆弱性を悪用して、OSコマンドインジェクション攻撃を行った。
株式会社 栄光、「お客様情報の流出に関するお詫びとお知らせ」（http://www.eikoh.co.jp/news/pdf/20160429.pdf）。

※ 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

Domino WebserverやRadwareなど一部の実装においては影響を受けることが確認され、脆弱性が修正されています。

Webアプリケーションフレームワークの Apache Struts2に Dynamic Method Invocation(DMI)を有効にしている場合に任意のコード実行の可能性がある脆弱性(S2-032)や、REST Pluginを有効にしている場合に任意のコード実行の可能性がある脆弱性(S2-037)が見つかり、修正されています。画像処理を行うソフトウェアImageMagickには細工されたコンテンツを開いた場合に任意のOSコマンドが実行される脆弱性が見つかり、修正されています。また、CMSのMovable Typeのプラグインで、携帯電話向けコンテンツの製作に利用されるケータイキットfor Movable Typeに、OSコマンドインジェクションの脆弱性が見つかり、修正されています。これらの脆弱性では修正版のリリース後すぐに攻撃が観測されており、JPCERT/CCや警察庁などから注意喚起が出されました。特にケータイキットfor Movable Typeの脆弱性については、開発元からの修正版のリリース前に既に攻撃が行われており、複数のWebサイトから多数の個人情報が流出する事件が発生しています。

■ 標的型攻撃による情報漏えい

この期間でも、組織内部の端末へのマルウェア感染とそれによる情報漏えいなどの事件が国内外で相次いで起きました。6月には国内の大手旅行会社において、個人情報約697万件(有効なパスポート番号4,000件余りを含む)が外部に流出した可能性があると発表されました。この事件では、送信元として取引先の大手航空会社を装ったメールを受信し、メールに添付されていたファイルを実行したことによって社内の端末がマルウェアに感染しました。その後、攻撃者は社内の他の端末やサーバへと侵入範囲を徐々に拡大し、大量の個人情報を含むデータファイルを作成して外部に送信しようとしていたことが分かっています。

またこの他にも6月中旬以降、市役所などの地方自治体の組織において端末がマルウェアに感染し、外部に対して不正な通信が発生したことが相次いで発表されました。これらの一連の事件に関連があるのかはっきりしませんが、地方自治体に送られた攻撃メールの内容などから、不特定多数の組織宛てにばらまかれたものである可能性が高いと考えられます。

米国でも6月に民主党全国委員会Democratic National Committee(DNC)のシステムに対して、外部から不正アクセスがあり、大統領予備選挙に関する内部情報などが流出していたことが分かりました。事件を調査したセキュリティベンダーのCrowdStrikeは、ロシアの2つの異なる攻撃グループCOZY BEAR(APT29)とFANCY BEAR(APT28)によるものだと断定し、2015年から既にDNCの内部システムに侵入していたと発表しました。これより前に米国家情報長官(DNI)のJames Clapper氏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おり、DNCへの侵入事件も米国の政治システムに対するロシアからの諜報活動の一環ではないかと考えられています。

しかしその後、GUCCIFER 2.0を名乗るハッカーがDNCへの侵入は自らの仕業であるとブログで公表し、DNCから取得したとする文書の公開などを行いました[*20]。GUCCIFER 2.0はロシアのハッカーグループとの関連を否定し、単独での犯行であるとブログやメディアなどで主張しましたが、その内容には不可解な点も多く、ロシアによる欺瞞工作の可能性も考えられます。いずれにせよ今回の事件では、近年その重要性が指摘されている、サイバー攻撃における犯人の特定、いわゆるアトリビューション(Attribution)が極めて難しいことを改めて印象付ける結果となりました。

■ 大量のパスワード情報漏えい

この期間では、SNSなどのサービスから過去に大量のパスワード情報が漏えいしていたことが相次いで発覚しました。これはロシア人ハッカーグループが2011～2013年頃に侵入して取得したデータが元になっていると考えられ、今年になってからロシアの掲示板サイトやDark Web上の販売サイトで一般に売り始められたことによって情報流出が分かったものです。MySpaceから約3億6,000万件、LinkedInから約1億6,700万件、Badooから約1億2,700万件、VKから約1億件、Tumblrから約6,500万件など、いずれも漏えい件数がかなり大規模でし

*20 "GUCCIFER 2.0"(https://guccifer2.wordpress.com/)。

5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

セ **4日：ギリシアの中央銀行のWebサイトに対し、AnonymousによるDDoS攻撃が行われ、一時閲覧できなくなるなどの影響が出た（Oplcarus）。**

脆 **5日：ImageMagickに、コンテンツを開いた場合に任意のOSコマンドが実行される脆弱性が見つかり、修正された。**
"ImageMagick Security Issue - ImageMagick"（https://www.imagemagick.org/discourse-server/viewtopic.php?f=4&t=29588）。"ImageTragick"（https://imagetragick.com/）。

脆 **5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/apsb16-14.html）。

脆 **11日：Microsoft社は、2016年5月のセキュリティ情報を公開し、MS16-051など8件の緊急と8件の重要な更新を含む合計16件の修正をリリースした。**
「2016年5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-may.aspx）。

セ **11日：株式会社サイバーエージェントが運営する「Ameba」で、第三者のなりすましによる不正ログインが発生し、5万905件のユーザ情報が閲覧された可能性があることが分かった。**
株式会社サイバーエージェント、「『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」（https://www.cyberagent.co.jp/newsinfo/press/detail/id=11977）。

セ **11日：通っていた大阪市内の中学校のWebサイトにサイバー攻撃をかけたとして、高校1年の男子生徒が電子計算機損壊等業務妨害の疑いで書類送検された。**

脆 **12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/apsb16-15.html）。

セ **13日：2013年の初めにTumblrからユーザのメールアドレスとパスワード情報が漏えいしていたことが分かった。また、後にDark Web上のマーケットで約6,500万件の情報が販売されていることが確認された。**
"Tumblr Staff"（https://staff.tumblr.com/post/144263069415/we-recently-learned-that-a-third-party-had）。

脆 **16日：Apple社はiOS 9.3.2とOS X El Capitan 10.11.5及びセキュリティアップデート2016-003をリリースし、アプリケーションにカーネル権限を取得され、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 9.2.1とwatchOS 2.2.1もリリースされた。**
「iOS 9.3.2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/HT206568）。「OS X El Capitan v10.11.5およびセキュリティアップデート2016-003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/HT206567）。「tvOS 9.2.1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/HT206564）。「watchOS 2.2.1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/HT206566）。

セ **18日：芸能人などのSNSやクラウドサービスのアカウントに不正アクセスしたとして、警視庁が長崎県の男性を不正アクセス禁止法違反容疑で逮捕した。名前や誕生日などからパスワードを推測してiCloudなどに不正にログインし、私的な画像を閲覧していた。**

セ **18日：DNSサービス事業者のNS1がDDoS攻撃を受け、Imgurなどの顧客サービスに影響が出た。**
"A Note From NS1's CEO：How We Responded To Last Week's Major, Multi-Faceted DDoS Attacks"（https://ns1.com/blog/how-we-responded-to-last-weeks-major-multi-faceted-ddos-attacks）。

セ **19日：2012年にLinkedInから漏えいしたメールアドレスとパスワード情報は当初発表された約650万人分ではなく、実は約1億6,700万人分だったことが分かった。また、Dark Web上のマーケットでアカウント情報が販売されていることが確認された。**
"Protecting Our Members | Official LinkedIn Blog"（https://blog.linkedin.com/2016/05/18/protecting-our-members）。

セ **19日：ランサムウェアのTeslaCryptのマスターキーが開発者から突如公開され、セキュリティベンダーから復号ツールが公開された。**
"ESET releases new decryptor for TeslaCrypt ransomware"（http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/）。

脆 **20日：TLSのAES-GCMに対して初期ベクトル（IV）が再利用されると実用的な攻撃が可能であることが研究者によって明らかにされた。**
"GitHub - nonce-disrespect/nonce-disrespect: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS"（https://github.com/nonce-disrespect/nonce-disrespect）。

セ **23日：全国17都府県のコンビニATM約1,400台から現金約14億4,000万円が不正に引き出された。南アフリカのスタンダード銀行から流出したカード情報を用いた偽造カードが使用された。**

脆 **26日：Cisco社のネットワーク製品に、細工されたIPv6 Neighbor Discovery（ND）パケットを受信することによってDoS状態となる脆弱性が見つかった。すべてのバージョンのIOS、IOS XR、IOS XEなどがこの脆弱性の影響を受ける。修正バージョンのリリースが準備されている。**
"Cisco Products IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability"（https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6）。

セ **28日：MySpaceから、2013年以前のユーザのメールアドレスとパスワード情報およそ3億6,000万人分が流出していたことが分かった。また、Dark Web上のマーケットでアカウント情報が販売されていることが確認された。**
"Myspace Blog"（https://myspace.com/pages/blog）。

※ 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

た。また、MySpaceやLinkedInではソルトなしのSHA1ハッシュによるパスワード情報が含まれていたため、パスワード解析が比較的容易であり、すぐに悪用される危険性が高いものでした。そのためこれらの流出に関連すると思われる事件がその後いくつか発生しました。

6月にはGitHubやGoToMyPCなどの複数のサービスにおいて、第三者のなりすましによる不正ログインが発生しました。これは別のWebサイトから漏えいしたパスワード情報を悪用して、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いわゆるリスト型攻撃であり、上記の大量のパスワード情報漏えいとの関連性が指摘されています。

また、Twitter社の共同創業者Biz Stone氏、Facebook社CEOのMark Zuckerberg氏、Google社CEOのSundar Pichai氏など、テクノロジー業界の著名人のSNSアカウントが5月以降相次いで乗っ取りの被害に遭っており、OurMine Teamを名乗るグループが犯行声明を出しています。これらの一連のアカウント乗っ取りもパスワード情報漏えいの影響の1つと考えられます。

こうしたパスワードを再利用しているユーザへのアカウント乗っ取り被害を見越して、事前に対応を取る企業も出始めています。例えばFacebook、Amazon、Netflixなどでは、他社サービスから漏えいしたユーザのパスワード情報を解析し、自社のサービスで同じパスワードを再利用しているユーザを見つけた場合、該当者のパスワードを強制的にリセットする対応をしています。このような対応は2013年のAdobe社からの約1億5,000万件のパスワード情報漏えいをきっかけに実施され始めた対策です。ユーザが複数のサービスでパスワードを再利用しないことが、このような乗っ取り被害を防ぐ根本的な対策ですが、実際には多数のユーザがパスワードを使い回しているために、こうした被害はなかなかなくならないのが実態です。

なお、このように大量に漏えいしたパスワード情報を収集し、ユーザに注意喚起を促すWebサイトもあります。例えばセキュリティ研究者のTroy Hunt氏は2013年のAdobe社からの漏えい事件を契機に"Have I been pwned?"という無料サービスを立ち上げています[*21]。ユーザはこのWebサイトで自らのメールアドレスを検索してパスワード情報が漏えいしているか確認することができます。また、あらかじめメールアドレスを登録しておくと、今後の情報漏えい事件で対象となったときに知らせてくれるサービスも提供しています。しかし、同様のサービスを謳うものの中には、単にユーザからの情報収集を目的とするものもあるため、利用にあたっては十分注意することが必要です。

■ 政府機関の取り組み

2016年5月末に第42回先進国首脳会議（G7伊勢志摩サミット）が開催され、関係する府省庁を中心に民間企業も協力して、サミット開催に伴って発生する可能性のあるサイバー攻撃を警戒したセキュリティ確保の取り組みを推進しました。結果として、4月以降に行われたG7の関係大臣による各会合も含め、開催期間中に会合の運営に支障をきたすような事象は発生しませんでした[*22]。

■ その他

昨年後半からランサムウェアの感染による被害が国内外で拡大しており、この期間においても継続しています。中でも感染数が多いものとしてTeslaCryptがありますが、5月になって復号に使うマスターキーが開発者から突然公開され、セキュリティベンダーから復号ツールが公開されました。この前から既にTeslaCryptは活動の停滞が観測されており、何らかの理由により活動を中止したようです。

数年前から米国などでは、Business Email Compromise（BEC）と呼ばれるビジネスメールによる詐欺被害の拡大が懸念されています。攻撃者は企業のCEOなどのメールアカウントを乗っ取り、社内の担当者にメールで不正な送金を指示することによって金銭を騙し取る、というのが典型的なBECの手口です。FBIのInternet Crime Complaint Center（IC3）が発表した年次報告書[*23]によると、米国では2015年に7,838件の被害報告があり、2億6,300万ドルの被害が発生しています。また、今年に入って更に被害が拡大していることから、6月にも注

*21 "Have I been pwned? Check if your email has been compromised in a data breach"（https://haveibeenpwned.com/）。
*22 内閣サイバーセキュリティセンター、「G7伊勢志摩サミットにおける取組等」（http://www.nisc.go.jp/conference/cs/ciip/dai07/pdf/07shiryou0201.pdf）。
*23 FBI、"2015 Internet Crime Report"（https://pdf.ic3.gov/2015_IC3Report.pdf）。

6月のインシデント

1

2

3

セ **3日：不正送金マルウェアのLurkを使用していたサイバー犯罪グループがロシアで一斉に摘発された。LurkはAngler Exploit Kitを経由して感染活動が行われていたが、この摘発によってAngler Exploit Kitの活動も停滞した。**
"Cisco Talos Blog：Connecting the Dots Reveals Crimeware Shake-up"（http://blog.talosintel.com/2016/07/lurk-crimeware-connections.html）。"Locky, Dridex, and Angler among cybercrime groups to experience fall in activity | Symantec Connect"（http://www.symantec.com/connect/blogs/locky-dridex-and-angler-among-groups-experience-fall-activity）。

4

セ **3日：ソーシャルネットワークBadooから、ユーザのメールアドレスやパスワード情報およそ1億2,700万人分が流出していたことが分かった。また、Dark Web上のマーケットでアカウント情報が販売されていることが確認された。**

5

セ **6日：ロシアのSNSサイトVKから、2012年頃のユーザのメールアドレスやパスワード情報およそ1億人分が流出していたことが分かった。また、Dark Web上のマーケットでアカウント情報が販売されていることが確認された。**

6

7

セ **13日：既にサービスが終了しているファイル共有サービスiMeshから、2013年のユーザのメールアドレスやパスワード情報およそ5,100万人分が流出していたことが分かった。また、Dark Web上のマーケットでアカウント情報が販売されていることが確認された。**

8

9

10

11

12

セ **14日：株式会社ジェイティービー（JTB）の子会社i.JTBのサーバに外部から不正アクセスがあり、顧客情報およそ679万人分が流出した可能性のあることが分かった。また、関連してJTBの提携先である「dトラベル」「Yahoo! トラベル」「DeNAトラベル」などの顧客情報にも影響があった。**
JTB、「不正アクセスによる個人情報流出の可能性について」（http://www.jtbcorp.jp/jp/160614.html）。NTTドコモ、「ドコモからのお知らせ：提携先のJTB社のグループ会社サーバーへの不正アクセスに伴う『dトラベル』の個人情報流出の可能性について」（https://www.nttdocomo.co.jp/info/notice/page/160614_00_m.html）。Yahoo! Japan、「JTBの『個人情報流出の可能性』に関する発表について」（http://blogs.yahoo.co.jp/yjtravel_staff/20970682.html）。DeNAトラベル、「株式会社i.JTBへの不正アクセスによる個人情報流出の可能性に関するお知らせ」（http://www.skygate.co.jp/information/2016/information0614.html）。

他 **14日：FBI（IC3）が、Business Email Compromise（BEC）の被害拡大について注意喚起を行った。**
Internet Crime Complaint Center（IC3）、"Business E-mail Compromise：The 3.1 Billion Dollar Scam"（https://www.ic3.gov/media/2016/160614.aspx）。

13

脆 **15日：Microsoft社は、2016年6月のセキュリティ情報を公開し、MS16-063など6件の緊急と11件の重要な更新を含む合計17件の修正をリリースした。**
「2016年6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-jun.aspx）。

14

15

セ **15日：米国の民主党全国委員会Democratic National Committee（DNC）のシステムに対して、外部から不正アクセスがあったことが分かった。ロシアの2つの異なる攻撃グループによるものと、セキュリティベンダーのCrowdStrikeが報告した。**
CrowdStrike、"Bears in the Midst: Intrusion into the Democratic National Committee"（https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/）。

16

17

脆 **16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/apsb16-18.html）。

18

19

脆 **16日：Apache Struts2に、REST Pluginを有効にしている場合に任意のコード実行の可能性がある脆弱性（S2-037）が見つかり、修正された。**
Apache Software Foundation、"S2-037"（https://struts.apache.org/docs/s2-037.html）。

20

21

セ **17日：GitHubで第三者のなりすましによる不正ログインが発生したことが分かった。該当アカウントのパスワードはリセットされた。**
"GitHub Security Update：Reused password attack"（https://github.com/blog/2190-github-security-update-reused-password-attack）。

22

23

24

セ **18日：仮想通過の投資ファンド「The DAO」が攻撃者にコードの脆弱性を悪用されて、約364万ETH（Ethereum）の資金が不正に移動された。その後Ethereumの開発コミュニティはハードフォークの実施によって資金を元の状態に戻すことを決定した。**
"CRITICAL UPDATE Re：DAO Vulnerability - Ethereum Blog"（https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/）。"Update3：The DAO is under attack — but Vitalik saved us — DAOhub"（https://blog.daohub.org/the-dao-is-under-attack-8d18ca45011b?gi=ddf32dc5304a#.2kgccwfka）。

25

26

セ **20日：CitrixのGoToMyPCサービスで第三者のなりすましによる不正ログインが発生したことが分かった。すべてのアカウントのパスワードがリセットされた。**
"GoToMyPC® System Status Status - GoToMyPC Password Issues"（http://status.gotomypc.com/incidents/s2k8h1xhzn4k）。

27

セ **22日：パイプドビッツが提供するECプラットフォーム「スパイラルEC」で構築されたサイトにおいて、外部からの不正アクセスによる個人情報の流出が発生した。**
「『SPIRAL EC（R）』への不正アクセスによる個人情報流出について」（http://www.pi-pe.co.jp/pb/info/）。

28

29

セ **24日：米国の有権者情報1億5,400万人分のデータがインターネット上に公開されていたことが、セキュリティ研究者によって判明した。**
"Another US Voter Database Leak"（https://mackeeper.com/blog/post/239-another-us-voter-database-leak）。

30

セ **27日：佐賀県の教育情報システム（SEI-Net）及び県内の学校の校内LANに不正侵入したとして、不正アクセス禁止法違反容疑で17才の少年が再逮捕された。なお、この少年はB-CASの不正視聴プログラムを配布していたとして、6月6日に不正競争防止法違反容疑で逮捕されていた。**
佐賀県、「学校教育ネットワークに係る不正アクセス被害がありました」（http://www.pref.saga.lg.jp/kiji00348348/index.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

意喚起が出されました。それによると、2015年初めと比較してBECによる被害額が1,300%増加しています。国内では被害事例はまだあまり報告されていませんが、今後の被害拡大に十分注意する必要があります。

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4月から6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。

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[*24]、サーバに対する攻撃[*25]、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、267件のDDoS攻撃に対処しました。1日あたりの対処件数は2.93件で、平均発生件数は前回のレポート期間と比べて若干減少しました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が62.55%、複合攻撃が34.08%、回線容量に対する攻撃が3.37%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63万5,000ppsのパケットによって2.84Gbps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81.27%が攻撃開始から30分未満で終了し、17.23%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1.50%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2日と17時間15分（65時間15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[*26]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[*27]の利用によるものと考えられます。

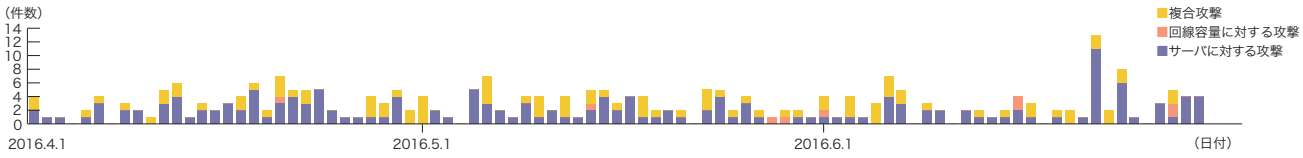


図-2 DDoS攻撃の発生件数

*24 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。

*25 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。

*26 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。

*27 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[*28]によるDDoS攻撃のbackscatter観測結果を示します[*29]。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4月から6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。

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40.3%を占めています。次いでDNSで利用される53/UDPが27.5%を占めており、上位2つで全体の67.8%に達しています。また、HTTPSで利用される443/TCP、SSHで利用される22/TCPへの攻撃、ゲームの通信で利用されることがある27015/UDPや25565/TCPへの攻撃、通常は利用されない42668/TCPや50401/TCP、44461/TCP、3306/UDPなどへの攻撃が観測されています。

2014年2月から多く観測されている53/UDPは、5月25日までは一日平均のパケット数で約4,900と高い水準が続いていましたが、翌日以降は一日平均で約20と、2014年2月以前の水準に戻りました。「1.3.2 マルウェアの活動」の無作為通信の状況においても同じ現象が見られています。これまで観測されていたDNS水責め攻撃[*30]の行為者が、この日を境に攻撃の手法を変えたか、あるいは攻撃を停止したものと考えられます。

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29.6%が最も大きな割合を占めています。その後に米国の25.0%、フランスの6.6%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、4月6日と12日に中国ホスティング事業者のサーバへの攻撃、4月26日に米国ソフトウェア開発企業によるブログホスティングサーバへの攻撃、5月27日に自動車関連の掲示板サイトへの攻撃、5月29日にカナダのホスティング事業

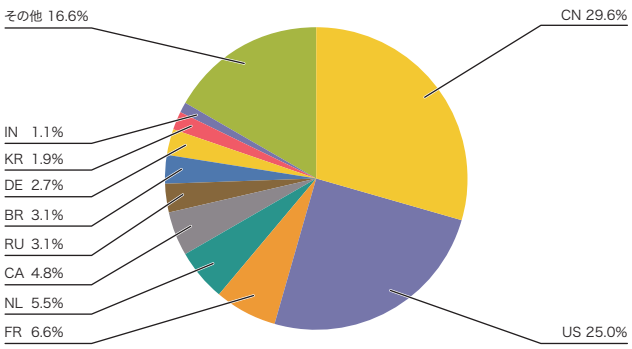


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

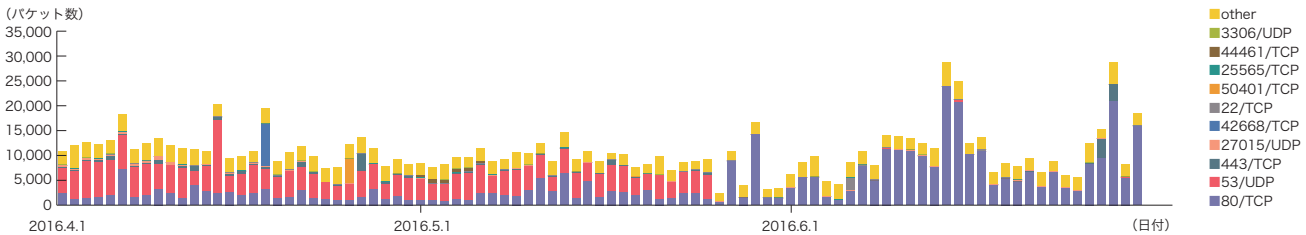


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*28 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。

*29 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。

*30 Secure64 Software Corporation、"Water Torture:A Slow Drip DNS DDoS Attack"(https://blog.secure64.com/?p=377)。日本語での解説としては、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)。

者が持つ複数のサーバへの攻撃、6月8日以降継続して米国ホスティング事業者のサーバへの攻撃、6月27日から28日にかけて米国セキュリティ企業のリバースプロキシサーバへの攻撃を観測しています。

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観測では、5月15日から20日にかけてAnonymousによる米国ノースカロライナ州政府Webサイトへの攻撃を検知しています。

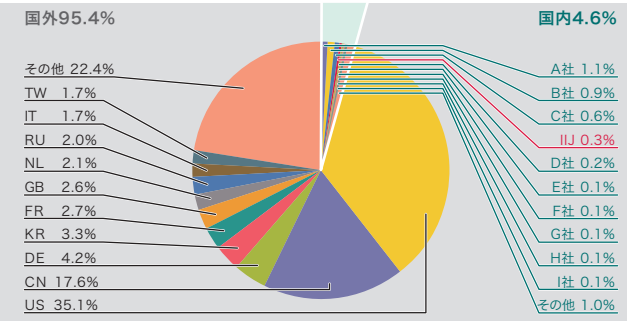


図-5 発信元の分布(国別分類、全期間)

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[*31]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[*32]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4月から6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一番接続回数の多かった53/UDPはその他の通信よりも突出して多かったため、図-6に別途記載し、残りの推移を図-7に示します。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、図-6は国別に、図-7では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。

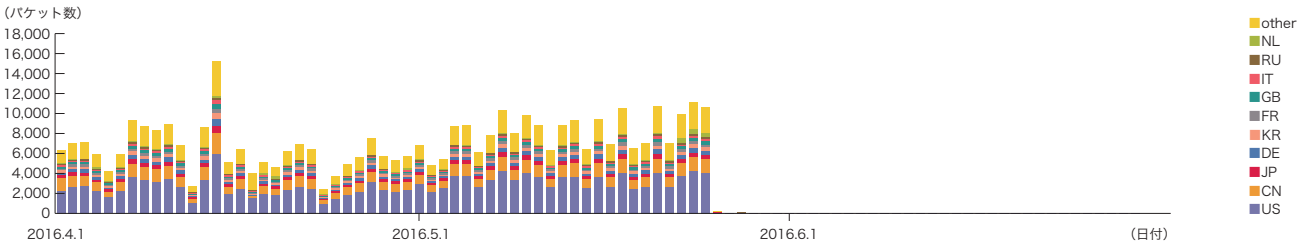


図-6 ハニーポットに到着した通信の推移(日別・53/UDP・1台あたり)

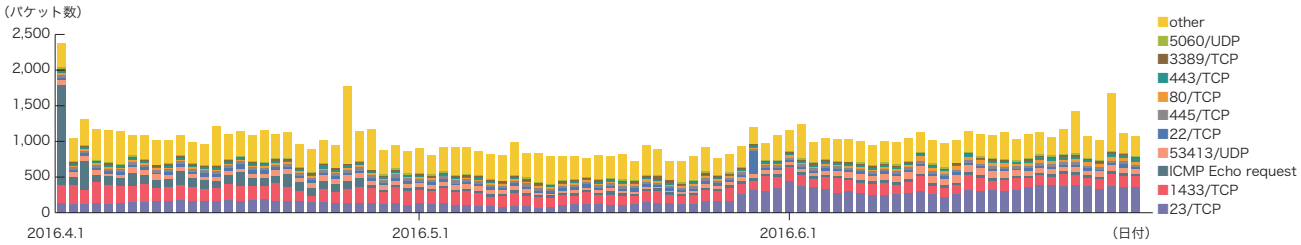


図-7 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*31 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。
*32 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。

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、DNSで使われる53/UDP、telnetで使われる23/TCP、ICMP Echo Request、Microsoft社のOSで利用されている445/TCP、同社のSQL Serverで利用される1433/TCP、Webサーバで使われる80/TCP、443/TCP、sshで使われる22/TCP、RDPで使用される3389/TCP、SIPで使用される5060/UDPなどでした。

前回のレポート期間と同様に、53/UDPの通信が高い値を示しています。この通信について調査したところ、特定のMITFハニーポットのIPアドレスに対し、主に米国、中国などに割り当てられた様々な送信元IPアドレスからのDNS名前解決のリクエストを繰り返し受けています。対象となるドメイン名も複数確認されていますが、多くが中国の通販サイトやゲーム、SF小説などをはじめとする幅広い分野のWebサイトでした。これらの通信のほとんどは「ランダム.存在するドメイン」の名前解決を繰り返し試みたものであったことから、DNS水責め攻撃（DNS Water Torture）であると判断しています[*33]。2016年5月26日以降に観測されなくなっていますが、攻撃者が攻撃の手法を変えたか、あるいは攻撃を停止したために収束したものと考えられます。

1433/TCPについても前回に引き続き通信が増加しています。調査したところ、中国に割り当てられたIPアドレスを中心とした多数のIPアドレスからの通信でした。

本レポート期間中も前回と同様に53413/UDPが増加しています。調査したところ、Netis、Netcore製のルータの脆弱性を狙った攻撃の通信でした。この脆弱性は、2014年8月にトレンドマイクロによって報告されており[*34]、JPCERT/CCが2015年4月から6月にかけて攻撃が増加したことを報告しています[*35]。23/TCPが全体的に増加傾向にあり、特に6月に増加しています。調査したところ、中国とブラジルに割り当てられたIPアドレスを中心に、幅広い国々に割り当てられたIPアドレスからパケットが届いており、ユニークIPアドレスで40万個以上が期間中に出現しています。また4月上旬には日本に割り当てられたいくつかのIPアドレスからICMP Echo Requestが増加しています。

■ 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-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[*36]の総数を総取得検体数、検体の種類をハッシュ値[*37]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。

期間中の1日あたりの平均値は、総取得検体数が74、ユニーク検体数が15でした。未検出の検体をより詳しく調査した結果、台湾、インド、ベトナム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）が観測されています。

未検出の検体の約33%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。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85.1%、ボット

＊33 Secure64 Software Corporation、"Water Torture：A Slow Drip DNS DDoS Attack"（https://blog.secure64.com/?p=377）。日本語での解説としては、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）。MITFハニーポットはDNSの問い合わせパケットを受信しても、権威サーバやキャッシュサーバに問い合わせに行かないため、攻撃には加担していない。
＊34 「UDPポートを開放した状態にするNetis製ルータに存在する不具合を確認」（http://blog.trendmicro.co.jp/archives/9725）。
＊35 「インターネット定点観測レポート（2015年4～6月）」（https://www.jpcert.or.jp/tsubame/report/report201504-06.html）。
＊36 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。
＊37 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。

型11.2%、ダウンローダ型3.7%でした。また解析により、7個のボットネットC&Cサーバ[*38]と5個のマルウェア配布サイトの存在を確認しました。

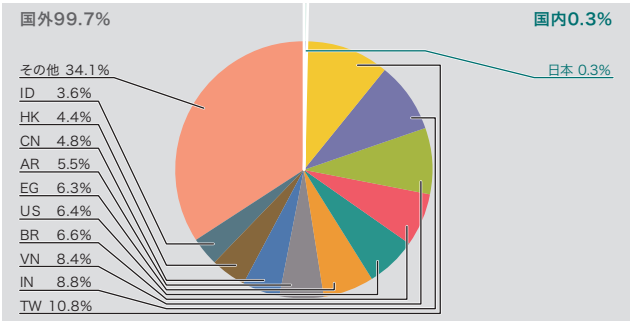


図-8 検体取得元の分布（国別分類、全期間、Conficker を除く）

■ 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8,543、ユニーク検体数は372でした。総取得検体数で99.1%、ユニーク検体数で96.2%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回の対象期間と比較し、約28%減少し、ユニーク検体数は前号から約13%減少しており、全体的に緩やかに減少しています。Conficker Working Group の観測記録[*39]によると、2016年7月現在で、ユニークIPアドレスの総数は55万台とされています。2011年11月の約320万台と比較すると、約17%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。

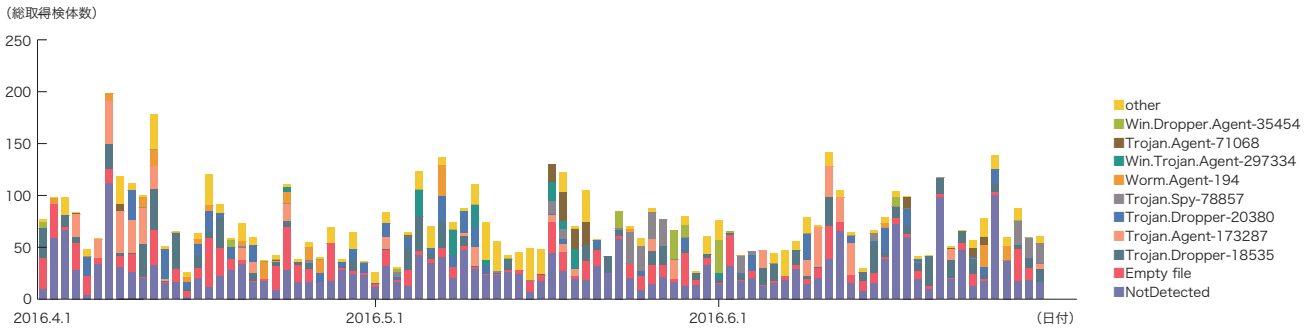


図-9 総取得検体数の推移（Conficker を除く）

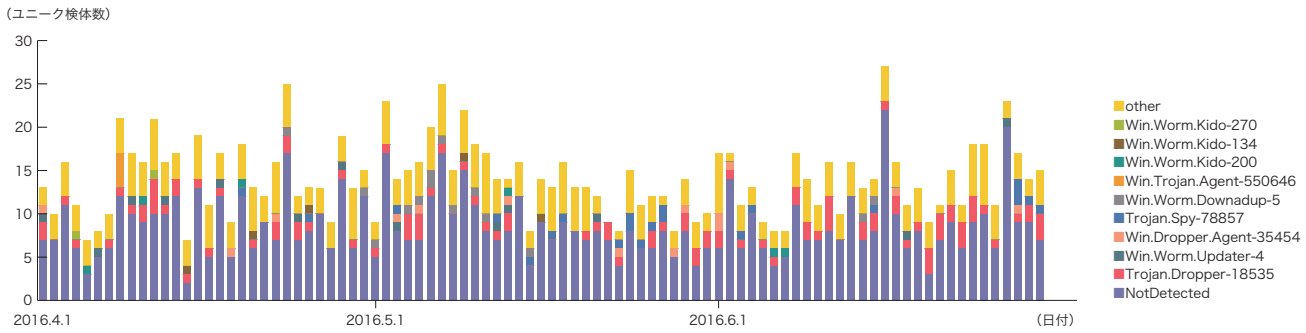


図-10 ユニーク検体数の推移（Conficker を除く）

*38 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。
*39 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1月7日以降表示されていないため、7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。

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[*40]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4月から6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、米国32.3%、中国19.6%、日本17.5%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は前回と比べて減少傾向にあります。

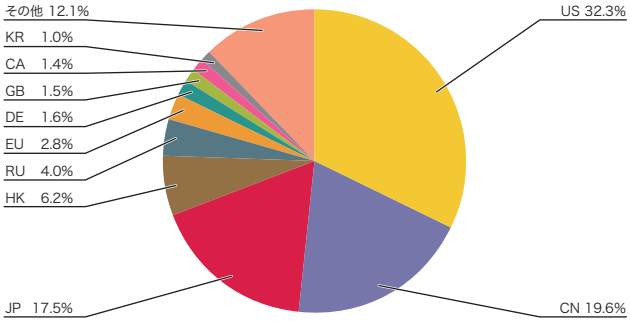


図-11 SQLインジェクション攻撃の発信元の分布

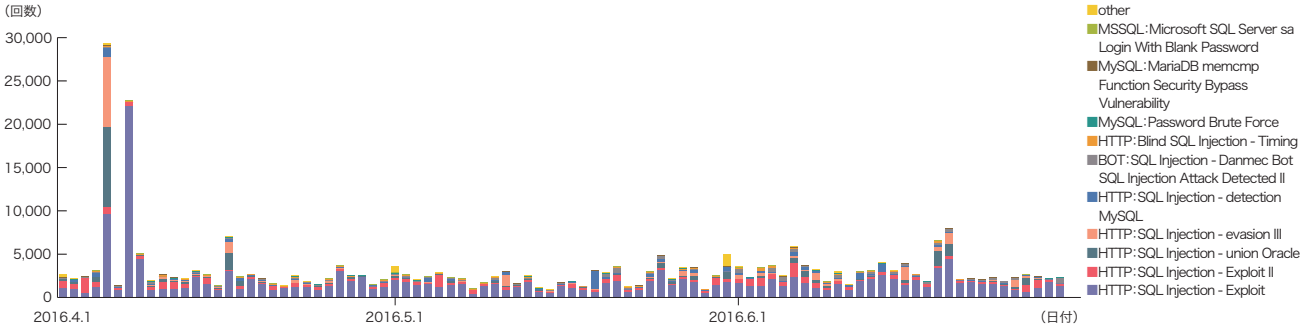


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

この期間中、4月5日には中国の複数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。4月7日には中国、香港、韓国それぞれ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。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[*41]。

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4月から6月までの期間は、検知した受動的攻撃の大部分を、Angler ExploitKitによるドライブバイダウンロード

*40 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。

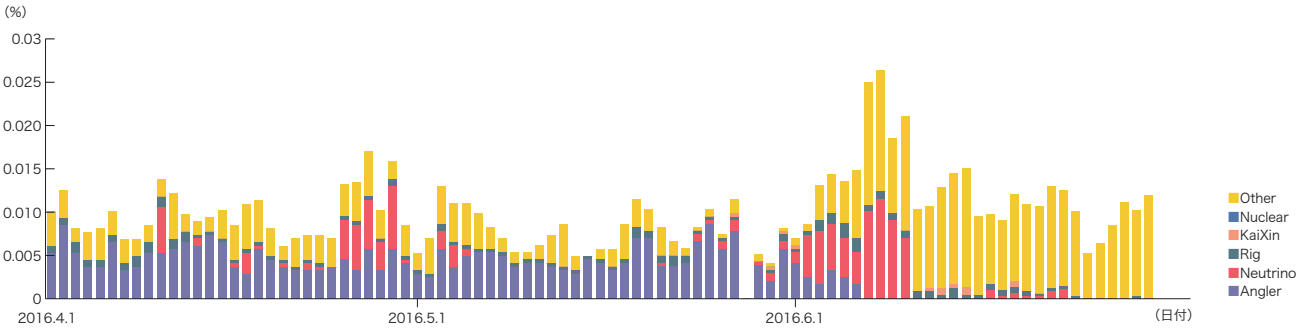
*41 Webクローラによる観測手法については本レポートのVol.22(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf)の「1.4.3 Webクローラによる Webサイト改ざん調査」で仕組みを紹介している。

が占めました(図-13)。Anglerによる攻撃は、2015年7月以来継続して大量に観測されてきました*42が、2016年6月6日を最後に一切検知されなくなりました。このAngler消滅の原因として、直前にロシアでマルウェアを悪用していたとされる犯罪組織が摘発され、50人が逮捕された事件*43が挙げられます*44。その後一時期、Anglerの穴を埋めるかのようにNeutrinoが勢いを増しましたが、6月下旬以降はRigと共に低調に推移しています。

4月中に観測したペイロードの多くはTeslaCryptでしたが、5月にTeslaCryptの開発中止が宣言され*45てからはCryptXXXが取って代わりました。その他にBedepやUrsnifなどのペイロードが確認されました。

6月中旬以降、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して、PUA*46のインストールや偽のサポートセンターへ電話を促す詐欺サイトへの誘導の観測数が急増しています。なお、これらの詐欺サイトの多くでは、Mac OS Xクライアントに対しても類似のダイアログを表示し、Mac OS X環境で実行可能なPUAのインストールを促すことを確認しました。

Anglerの消滅に伴い、ドライブバイダウンロードによる攻撃は収束傾向にあります。一方、詐欺サイトによるPUAインストール誘導が規模を増しています。ブラウザ利用環境では、脆弱性悪用によるマルウェア感染だけでなく、詐欺サイトなどソーシャルエンジニアリングによってPC利用者が意図的にPUAやマルウェアをインストールしてしまうケースへの対策も検討しておくことが重要です*47。Webサイト運営者は、Webコンテンツの改ざん対策及び、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を徹底して継続することが求められます。



※調査対象は日本国内の数十万サイト。近年のExploitKit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。

図-13 Webサイト閲覧時の受動的攻撃発生率(%)(Exploit Kit別)

*42 2015年7月のAngler観測状況や、その機能については本レポートのVol.28(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol28.pdf)の「1.4.2 猛威を振るうAngler Exploit Kit」で詳しく紹介している。
*43 Source - BBC News - © [2016] BBC、「Russian hacker gang arrested over $25m theft」(http://www.bbc.com/news/technology-36434104)。
*44 例えばSophos社も技術向けブログNaked Securityの記事「Is the Angler exploit kit dead?」(https://nakedsecurity.sophos.com/2016/06/16/is-angler-exploit-kit-dead/)で同事件とAngler消滅との関連に触れている。
*45 TeslaCryptの開発終了については本レポートのVol.31(http://www.iij.ad.jp/company/development/report/iir/031.html)の「1.4.1 各種のランサムウェアとその対策」で紹介している。
*46 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。
*47 例えば管理者権限の分限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。

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、Volatility Frameworkプロファイルの生成、マルウェアに感染しないためのWindowsクライアント要塞化(後編)の2つのテーマについて紹介します。

```
Profiles
--------
VistaSP0x64    - A Profile for Windows Vista SP0 x64
VistaSP0x86    - A Profile for Windows Vista SP0 x86
VistaSP1x64    - A Profile for Windows Vista SP1 x64
VistaSP1x86    - A Profile for Windows Vista SP1 x86
VistaSP2x64    - A Profile for Windows Vista SP2 x64
VistaSP2x86    - A Profile for Windows Vista SP2 x86
Win10x64    - A Profile for Windows 10 x64
Win10x86    - A Profile for Windows 10 x86
Win2003SP0x86    - A Profile for Windows 2003 SP0 x86
Win2003SP1x64    - A Profile for Windows 2003 SP1 x64
Win2003SP1x86    - A Profile for Windows 2003 SP1 x86
Win2003SP2x64    - A Profile for Windows 2003 SP2 x64
Win2003SP2x86    - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64    - A Profile for Windows 2008 R2 SP0 x64
Win2008R2SP1x64    - A Profile for Windows 2008 R2 SP1 x64
Win2008SP1x64    - A Profile for Windows 2008 SP1 x64
Win2008SP1x86    - A Profile for Windows 2008 SP1 x86
Win2008SP2x64    - A Profile for Windows 2008 SP2 x64
Win2008SP2x86    - A Profile for Windows 2008 SP2 x86
Win2012R2x64    - A Profile for Windows Server 2012 R2 x64
Win2012x64    - A Profile for Windows Server 2012 x64
Win7SP0x64    - A Profile for Windows 7 SP0 x64
Win7SP0x86    - A Profile for Windows 7 SP0 x86
Win7SP1x64    - A Profile for Windows 7 SP1 x64
Win7SP1x86    - A Profile for Windows 7 SP1 x86
Win81U1x64    - A Profile for Windows 8.1 Update 1 x64
Win81U1x86    - A Profile for Windows 8.1 Update 1 x86
Win8SP0x64    - A Profile for Windows 8 x64
Win8SP0x86    - A Profile for Windows 8 x86
Win8SP1x64    - A Profile for Windows 8.1 x64
Win8SP1x86    - A Profile for Windows 8.1 x86
WinXPSP1x64    - A Profile for Windows XP SP1 x64
WinXPSP2x64    - A Profile for Windows XP SP2 x64
WinXPSP2x86    - A Profile for Windows XP SP2 x86
WinXPSP3x86    - A Profile for Windows XP SP3 x86
```

図-14 Volatilityのデフォルトプロファイル

1.4.1 Volatility Frameworkプロファイルの生成

■ Volatility Frameworkとは

Volatility Framework(以下、Volatility)はコンピュータフォレンジックの際にメモリイメージを解析するために使用されるオープンソースソフトウェアです[*48]。

Volatilityを実行する際にはプロファイルを指定する必要があります。プロファイルは、OSやサービスパック、アーキテクチャごとに用意されており、メモリイメージを取得したシステムと同じものを指定しなければ正しく解析することができません。図-14はVolatilityにデフォルトで同梱されているプロファイルの一覧になります。

この図を見れば分かるとおり、デフォルトではWindowsのプロファイルしか同梱されていません。LinuxやMac OS Xのメモリイメージを解析する場合は、VolatilityのGitHubページ[*49]からプロファイルをダウンロードする必要があります。しかし、すべてのOSバージョンに対応したプロファイルが提供されているわけではありません。また、Linuxでは、Kernelのバージョンアップも多く行われますので、同じOSバージョンでもLinux Kernelのバージョンが異なるという状況も考えられます。

このような場合、使用しているシステムに合わせたプロファイルを自身で生成する必要があります。本稿では自身でLinux Kernel用のVolatilityプロファイルを生成する際の手順を解説します。

■ プロファイル生成の準備

■ 解析対象システムのバージョンの確認

Volatilityのプロファイルを生成するには、メモリイメージの解析対象となるシステムと同じバージョンのシステムにVolatilityをインストールする必要があります。主なLinuxディストリビューションでのOSバージョンとLinux Kernelのバージョンを確認する方法は図-15を参照してください。なお、今回は、CentOS Linux 7.2-1511、Linux Kernel 3.10.0-327.22.2.el7.x86_64を例に解説します。

*48 VolatilityのGitHubページ。"GitHub - volatilityfoundation/volatility:An advanced memory forensics framework"(https://github.com/volatilityfoundation/volatility)。

*49 プロファイル配布ページ。"GitHub - volatilityfoundation/profiles:Volatility profiles for Linux and Mac OS X"(https://github.com/volatilityfoundation/profiles)。

■ プロファイル生成マシンの準備

Volatilityプロファイルを生成するためのマシンを用意します(解析対象システムへの変更を最小限にするため、別途マシンを用意してください)。このとき、OSバージョンとLinux Kernelバージョンは上記で確認したものと同じバージョンのものを用意することが望ましいです。なお、プロファイルを生成するマシンはバーチャルマシンでも問題ありません。

■ Volatilityのダウンロード

Volatilityの実行とプロファイルの生成に必要なライブラリをインストールします(図-16)。一部、gitを使用していますが、Linuxディストリビューションによっては、これらのライブラリのパッケージが用意されている場合もあると思いますので、適宜、インストールを行ってください。

```
RedHat
  $ cat /etc/redhat-release

CentOS
  $ cat /etc/centos-release

Debian
  $ cat /etc/lsb-release

Ubuntu
  $ cat /etc/debian_version

Linux Kernel
  $ uname -r
```

図-15 OSバージョンの確認方法

```
diStorm3のインストール
  $ git clone https://github.com/gdabah/distorm.git
  $ cd distorm
  $ sudo python setup.py install

PyCryptoのインストール
  $ sudo yum install python-crypto

DWARFのインストール
  $ sudo yum install libdwarf-tools

elfutilsのインストール
  $ sudo yum install elfutils-libs
```

図-16 関連ライブラリのインストール

次に、Volatilityをダウンロードします(図-17)。Volatilityはシステムにインストールしなくても実行することができるため、今回はこのまま使用します。Volatilityをダウンロードしたディレクトリ内で「$ python ./vol.py --info」と実行して、エラーが発生しないことを確認してください。

■ Linux Kernel開発環境インストール

プロファイル生成の際にカーネルモジュールのコンパイルが必要になるため、Linux Kernelの開発環境をインストールします(図-18)。その他、makeやgccなどのコマンドが必要となりますので、必要に応じて各コマンドをインストールしてください。以上で準備は完了です。

■ プロファイル生成

「volatility/tools/linux」ディレクトリ内で、makeコマンドを実行します。問題がなければ、同じディレクトリに「module.dwarf」というファイルができているはずです。次に、「volatility/volatility/plugins/overlays/linux/」ディレクトリに、module.dwarfとSystem.mapファイルをまとめたZIPファイルを作成します(図-19)。

このZIPファイルがVolatilityのプロファイルとなります。プロファイルに命名規則はありませんが、最低限OSバージョンが分かるようなプロファイル名が望ましいでしょう。より細かく管理するのであれば、Linux Kernelバージョンもプロファイル名に含めてください。

```
Volatilityのダウンロード
  $ git clone https://github.com/volatilityfoundation/volatility.git

Volatilityの実行
  $ cd volatility
  $ python ./vol.py
```

図-17 Volatilityのダウンロードと実行方法

```
$ sudo yum install kernel-devel-3.10.0-327.22.2.el7.x86_64.rpm
$ sudo yum install kernel-headers-3.10.0-327.22.2.el7.x86_64.rpm
```

図-18 Linux Kernel開発環境インストール

```
$ cd volatility/tools/linux
$ make
$ sudo zip volatility/volatility/plugins/overlays/linux/CentOS72.zip ./module.dwarf /boot/System.map-3.10.0-327.22.2.el7.x86_64
```

図-19 プロファイル生成

生成したプロファイルがVolatilityに認識されているかどうかは、図-20のようなコマンドで確認することができます。

■ 異なるバージョンのプロファイルを生成する場合

ここまで説明した手順で、現在動作しているLinux KernelのVolatilityプロファイルは生成できるようになりました。しかし、同じOSバージョンでも異なるバージョンのLinux Kernelやカスタマイズされた Linux Kernelのプロファイルを生成する場合は、作業手順を少し変える必要があります。

■ Linux Kernelのバージョンが異なる場合

「Linux Kernel開発環境インストール」のステップの代わりに、図-21のように適当なディレクトリにプロファイルを生成したいLinux Kernelのパッケージを展開します。

この他の手順は基本的に同じですが「プロファイル生成」に関しては、図-22のようにmakeコマンドの引数として、KDIRとKVERを指定しなければなりません。

注意点として、CentOS 7の場合、/lib/modules/<kernel_ver>/buildのシンボリックリンクがリンク切れとなるため、makeを実行すると「/home/admin/ksrc/lib/modules/<kernel_ver>/buildは存在しない」旨のエラーが発生してしまいます。この場合、図-23のように、buildファイルのシンボリックリンクを張り直すことでエラーを回避することができます。

■ カスタマイズされたLinux Kernelの場合

特定の機器や用途向けにLinux Kernelがカスタマイズされている場合、Linuxディストリビューションが配布しているパッケージをそのまま利用することはできません。このような場合、以下のいずれかの対応を行い、Linux Kernelのソースコードを用意します。

1. カスタマイズされたLinux Kernelのソースコードやパッチが手に入る場合、それを利用する。
2. ソースコードやパッチが手に入らない場合、解析対象システムが利用しているLinux Kernelに可能な限り近いバージョンのLinux Kernelソースコードを用意する。また、解析対象システムのカーネルコンフィグを利用して、可能な限り似通ったコンフィグを行う[*50]。

このように解析対象システムで動作しているLinux Kernelに近い状態のソースコードが必要になりますが、これ以外の作業はこれまで解説した手順と変わりません。

```
$ python ./vol.py --info | grep Linux
Volatility Foundation Volatility Framework 2.5
LinuxCentOS72x64 - A Profile for Linux CentOS72 x64        ←生成したプロファイル
linux_banner             - Prints the Linux banner information
linux_yarascan           - A shell in the Linux memory image
```

図-20 プロファイル確認

```
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-3.10.0-327.3.1.el7.x86_64.rpm
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-devel-3.10.0-327.3.1.el7.x86_64.rpm
$ wget http://ftp.iij.ad.jp/pub/linux/centos/7.2.1511/updates/x86_64/Packages/kernel-headers-3.10.0-327.3.1.el7.x86_64.rpm
$ mkdir ksrc && cd ksrc
$ rpm2cpio ../kernel-devel-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
$ rpm2cpio ../kernel-headers-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
$ rpm2cpio ../kernel-3.10.0-327.3.1.el7.x86_64.rpm | cpio -id
```

図-21 異なるバージョンのLinux Kernelを展開

```
$ make KDIR=/home/admin/ksrc/ KVER=3.10.0-327.3.1.el7.x86_64
```

図-22 異なるバージョンのLinux Kernelプロファイル生成

```
$ cd /home/admin/ksrc/lib/modules/3.10.0-327.3.1.el7.x86_64/
$ rm build
$ ln -s /home/admin/ksrc/usr/src/kernels/3.10.0-327.3.1.el7.x86_64/ build
```

図-23 シンボリックリンクの張り直し

*50 ただし、この場合、作成したプロファイルと解析対象システムの間で、Kernel内部のデータ構造に異なる部分があると、その部分は正常に解析できない場合があるため、それを認識した上で解析を行う必要がある。

なお、Mac OS X用のプロファイルは本稿の冒頭で書いたように、VolatilityのGitHubページからダウンロードすることができますが、新バージョンのリリース直後など、タイミングによっては最新版用のプロファイルをダウンロードすることができない場合があります。生成手順はLinux Kernelとおおよそ同じ[*51]ですので、自分でOS X用プロファイルを生成することを検討してみてはいかがでしょうか。

1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化(後編)

前号のIIRではパッチ適用や一般ユーザ権限のみを付与するなどの基本的な対策に加え、アプリケーションホワイトリスティングと呼ばれる要塞化設定について紹介しました。本稿では残りの対策について紹介します。まだ前号を読んでいない方は、IIR Vol.31「マルウェアに感染しないためのWindowsクライアント要塞化(前編)」[*52]も合わせてご覧ください。

■ EMET

EMET(Enhanced Mitigation Experience Toolkit)は脆弱性の悪用を緩和するためのツールで、マイクロソフトが配布しています[*53]。Windowsのセキュリティ機能を最大限有効化すると共に、既知の攻撃手法への緩和策が実装されています。EMETはドメイン配下のクライアントに一斉インストールし、ポリシーを強制することも可能です[*54]。本稿執筆時点での最新版は5.5であり、それを元にEMETを単一ホストで利用する場合の説明します。インストール後、スタートメニューからEMET GUIを起動すると、EMETの管理ツールが起動します。

1. Quick Profile NameをMaximum security settingsに変更します。この際、再起動が必要である旨のポップアップが出現するため、OKをクリックします(図-24)。
2. Importをクリックし、C:\Program Files (x86)\EMET 5.5\Deployment\Protection Profilesに存在するプロファイルを一通り適用します。
3. 設定を有効にするためにホストを再起動します。

これで基本的な設定は終了です。以降は管理画面からAppsをクリックし、環境に応じて個別のアプリケーションを追加したり、テスト中や利用中に不具合が出たアプリケーションについて、干渉している機能を個別に外すなどの対処を行いながら、運用をしていきます。

■ UACの厳格化

UAC(ユーザアカウント制御)はVista以降導入された機能で、管理者権限アカウントであっても通常は特権を無効化しておきます。OSにとって重要な変更が実行中のプログラムによって行われようとした場合に、ユーザに対してその変更は自身が行ったものであるか確認を求めることで、悪意のある変更を検出する機能です。

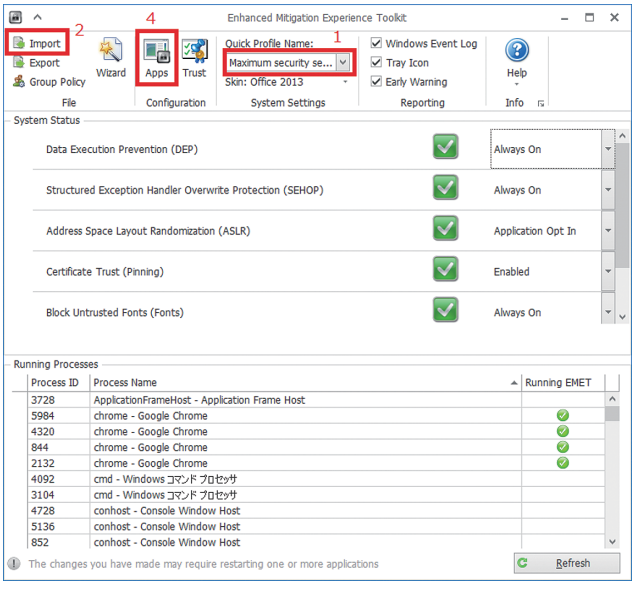


図-24 EMETの設定画面

*51 Mac OS X用プロファイル生成手順詳細(https://github.com/volatilityfoundation/volatility/wiki/Mac)。
*52 「Internet Infrastructure Review(IIR) Vol.31」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol31.pdf)。
*53 EMETに関する情報やダウンロード先は次のURLからたどることが可能。「Enhanced Mitigation Experience Toolkit」(https://technet.microsoft.com/ja-jp/security/jj653751)。
*54 EMETは3.0以降、Active Directory経由でのパッケージの自動インストールや、ポリシーの配信をサポートしている。次のURLでは画像や動画でこれらに関する説明を詳しく行っている。「Active Directoryを利用したEMETの制御」(http://n.pentest.ninja/?p=31157)。"ITSCFORUM Deploy and Manage EMET using a GPO"(https://www.youtube.com/watch?v=4MgODgeDr18&app=desktop)。

UACには大きく分けて4段階の設定値が存在し、Vistaではデフォルトで最高値である「常に通知する」が設定されていました。しかし、XPを単体で利用していたユーザはそのほとんどが常時管理者権限を使用しており、Vistaに乗り換えた際、頻繁にUACのポップアップが出現したため、多くのユーザがこの機能を批判しました。そのため、Windows7以降のデフォルトはそれよりも一段低い「アプリがコンピュータに変更を加えようとする場合のみ通知する」に変更になっています。しかし、これにはいくつか欠陥があり、UACを回避してユーザの同意なしに管理者権限に自動昇格してしまう攻撃が実際の事案でも確認されています[*55]。このような脆弱性を避けるため、UACを常に通知する、に変更して運用した方がよいでしょう[*56]。

図-25 ユーザーアカウントの設定画面

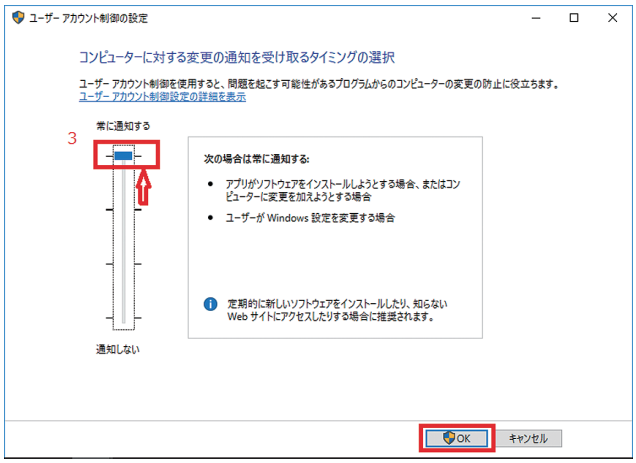


図-26 ユーザーアカウント制御設定の変更

1. コントロールパネルから、ユーザーアカウント、ユーザアカウントとたどります。
2. ユーザアカウント制御設定の変更をクリックすると、図-25が表示されます。
3. Windows 7以降は上から2番目が設定されているので、スライドを一番上に引き上げ、OKを押します(図-26)。

これで自動昇格が起こらず、常にポップアップが出現し、管理者ユーザが異常に気づきやすくなります。

■ WSHの無効化

WSH(Windows Script Host)はホスト上でVBScriptやJScriptを実行するための機能です。前号のIIR Vol.31「1.4.1 各種のランサムウェアとその対策」でも記載したとおり、TeslaCryptやLockyではJScript(.js)がメールに添付された事例が確認されています。また、過去にはショートカットファイル(.lnk)内にVBScript(.vbs)を埋め込んだものをメールで送信する手口も確認されています。このような攻撃を防ぐために、レジストリエディターを使用して以下のキーに値を追加し、この機能を無効化します。

- キー
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings
- 値の名前
  Enabled
- 値のデータ(DWORD値)
  0

無効化すると、jsやvbsをダブルクリックしたり、cscript.exeを実行した場合、警告が出ることが確認できます(図-27)。

*55 IIR Vol.21「1.4.1 標的型攻撃で利用されるRAT「PlugX」」(http://www.iij.ad.jp/company/development/report/iir/021.html)では、PlugXにおけるUACの迂回による管理者権限への自動昇格について触れている。また、過去にはDridexなどがPlugXとは異なるsdbを使用したUAC回避を用いていた。次のURLでは、その手法について解説している「Dridexが用いる新たなUAC回避手法(2015-02-09)」(https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html)。ある研究者はWindows7以降のデフォルト値で運用した場合のUAC回避手法を一覧にまとめ、それを検証ツールとして公開している。"UACMe"(https://github.com/hfiref0x/UACME)。

*56 ドメイン環境では、グループポリシー管理エディターで行う。コンピュータの構成、ポリシー、Windowsの設定、セキュリティの設定、ローカルポリシー、セキュリティオプション、とたどり、ユーザーアカウント制御の項を組み合わせることで同様のことが可能。

■ rundll32.exe、regsvr32.exeの通信の禁止

rundll32.exe、regsvr32.exeはVBScript(.vbs)やJScript(.js)ファイルをリモートのホストからhttpなどを経由して取得し、実行する機能があります。これは攻撃者に使われうる機能であるため、禁止すべきです。ただし、rundll32.exeやregsvr32.exeは通常のWindowsの処理中にも使われているため、実行そのものを禁止することはできません。そこで、セキュリティが強化されたWindowsファイアウォールの送信の規則など、パーソナルファイアウォールの機能を用いて、これらの実行ファイルが外部と通信するのをブロックします。64bit環境の場合、SysWOW64側にも実行ファイルが存在するため、同様にブロックします。

```
C:\Windows\System32\rundll32.exe
C:\Windows\System32\regsvr32.exe
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\SysWOW64\regsvr32.exe
```

また、C:\Windows\WinSxS以下のフォルダ内にもこれらの実行ファイルが存在する可能性があるため、それも禁止する必要があります。

■ PowerShellの禁止

PowerShellはWindowsの管理やWindows APIを呼び出したりできるなど、非常に強力なWindowsのスクリプティング言語です。デフォルトではファイル化されたスクリプトが実行できないようになっていますが、この制限は簡単に回避できてしまいます。また、ショートカットや外部に存在するスクリプトをHTTP経由で直接実行することができるなど、実際の攻撃に利用されていることが確認されているため、一般ユーザが実行できないようにAppLockerやソフトウェアの制限のポリシーなどで、次のパス以下を全体的に制限すると良いでしょう。

```
C:\Windows\System32\WindowsPowerShell
C:\Windows\SysWOW64\WindowsPowerShell
```

また、C:\Windows\WinSxS以下のフォルダ内にもpowershell.exeやpowershell_ise.exeが存在する可能性があるため、それも禁止する必要があります。

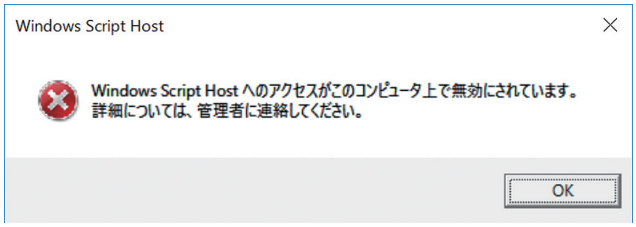


図-27 WSHが無効化されたことの確認

■ HTAの禁止

HTA(.hta)はHTMLで記述されたアプリケーションであり、HTML、VBScriptやJScriptを用いてコードを記述することが可能です。例えば最近ではLockyを使う攻撃者が.htaファイルを添付したメールを送信し、それをユーザに開かせることで感染を試みた事例が存在します。それ以外にも、少なくとも2007年からマルウェアが悪意のあるHTAを利用した事例が存在します[*57]。これに対処するために、mshta.exeをAppLockerやソフトウェアの制限のポリシーなどで制限すると良いでしょう。C:\Windows\WinSxS以下のフォルダ内にも存在する可能性があるため、それも禁止する必要があります。グループポリシーエディターで.htaの関連付けを外す手法も限定的な解決策の1つですが、厳密に言えば、mshta.exeをショートカット経由で呼び出された場合に回避されてしまうため、完全な解決策ではありません。

■ Webブラウザのプラグインを自動実行させない(Click to Play)

Google ChromeやFirefoxにはClick to Playと呼ばれる、ユーザが明示的に許可した場合のみWebブラウザプラグインの実行を許可する設定を行うことができます[*58]。これにより、Flashなどが自動的に実行されなくなり、これらの脆弱性を悪

*57 次のURLでは、悪意のあるHTAの事例について紹介している。"The Power of (Misplaced) Trust:HTAs and Security"(https://nakedsecurity.sophos.com/2009/10/16/power-misplaced-trust-htas-insecurity/)。
*58 Internet ExplorerにもClick to Playに類似する機能としてActiveXフィルターという機能が存在する。「Internet Explorer 11とInternet Explorer 10でActiveXコントロールを使う」(https://support.microsoft.com/ja-jp/help/17469/windows-internet-explorer-use-activex-controls)。

用してマルウェアに感染させる攻撃(ドライブバイダウンロード)を緩和することができます。

Google Chrome

1. Google Chromeのメニューから、設定をクリックします(図-28)。
2. ページの一番下にある、詳細設定を開く、をクリックします。
3. プライバシーのコンテンツの設定をクリックします。
4. プラグインのプラグインコンテンツをいつ実行するかを選択する、をクリックします。
5. 完了ボタンをクリックすれば、Click to Playが有効になります(図-29)。

Firefox

1. URLバーにabout:configと入力します。その際に、警告が出ますが、細心の注意を払って使用する、をクリックします(図-30)。
2. plugins.click_to_playの値をtrueにすることで、Click to Playが有効になります(図-31)。

■ マッシュアップコンテンツを制限する

Firefoxのアドオンには、NoScript Security Suite[*59]やRequestPolicy Continued[*60]のような、スクリプトの実行を許可するサイトを限定したり、URLバーに入力したドメインとは異なるドメインへのアクセスを制限するプラグインが存在します。これらを利用することで、普段閲覧しているWebページが改ざんされていても外部サイトにはリダイレクトされないため、悪意のあるWebサイトに誘導されにくくなり、結果としてマルウェア感染を緩和することが可能です。

■ ストアアプリの禁止

Windows 8以降では、ストアアプリが利用できますが、ユーザが自由にアプリをインストールできてしまうため、ストア内にマルウェアなどが混入していた場合に誤ってインストール

図-28 Chromeの設定

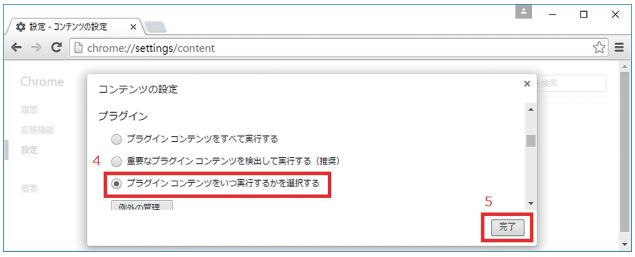


図-29 Chrome - コンテンツの設定

図-30 Firefoxの詳細設定画面

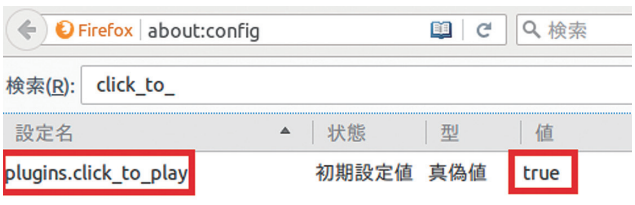


図-31 Firefox - Click to Playの設定

*59 "NoScript Security Suite"(https://addons.mozilla.org/ja/firefox/addon/noscript/)。
*60 "RequestPolicy Continued"(https://addons.mozilla.org/ja/firefox/addon/requestpolicy-continued/)。

してしまう可能性があります。また、デフォルトでもゲームなどが含まれており、ビジネス環境においては好ましくありません。そこで、ストアアプリの利用を一律禁止します。

1. 管理者権限でローカルグループポリシーエディターを起動してください。これはgpedit.mscを実行することで起動することが可能です。
2. メニュー左側のツリーからコンピューターの構成、管理用テンプレート、Windowsコンポーネント、ストア、とたどります（図-32）。
3. 以下の項目を有効に切り替えます（図-32）。
   - ストアアプリケーションをオフにする
   - Windowsストアからすべてのアプリを無効にする（この項目はWindows 10以降のみ）
4. ポリシーを強制したいホストを再起動するか、管理者権限でコマンドプロンプトを開き、gpupdate /forceコマンドを実行すると、ソフトウェアの制限のポリシーが有効になります。

無効にした後にストアにアクセスすると、アプリにアクセスできなくなっているのが分かります（図-33）。また、AppLockerでもアプリを制御することができます。

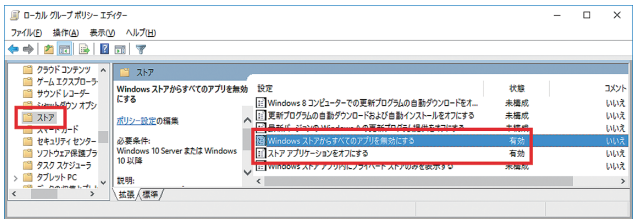


図-32 ストアアプリの設定画面

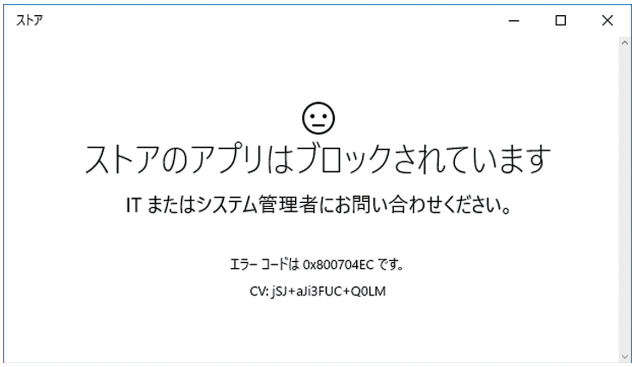


図-33 ストアアプリ – 拒否されたときに表示される画面

■ 各対策と侵入経路の効果

各侵入経路ごとの各対策の有効性を以下の表-1にまとめました。

表-1 各対策とそれぞれの侵入経路の効果

対策	Web	メール	備考
アプリケーションホワイトリスティング	○	○	マルウェアはユーザディレクトリ以下にダウンロード、インストールされることが多いため、感染を防ぐことができる。アイコン偽装がされている実行ファイルや、.js、.vbsファイルをメールで受信し、誤ってダブルクリックしても防御できる。
利用者に管理者権限を与えない	△	△	マルウェアの活動範囲を1アカウントのみに制限できる。意図しないプログラムの混入を防ぐ。
EMET	△	△	悪意のあるWebコンテンツや文書ファイルなどのExploitを緩和することができる。
UACの厳格化	△	△	管理者ユーザで実行してしまった場合でも、被害を最小限にすることができる。
WSHの無効化		○	.js、.vbsファイルをメールで受信した場合やショートカット内にJScriptやVBScriptが含まれていた場合に防ぐことができる。
rundll32.exe、regsvr32.exeの通信の禁止	○	○	ドライブバイダウンロードの途中で使われた場合に最終的な感染を緩和する。悪意のあるショートカットなどを用いてメールで配布された場合に防ぐことができる。
PowerShellの禁止	○	○	ドライブバイダウンロードの途中で使われた場合に最終的な感染を緩和する。悪意のあるショートカットなどを用いてメールで配布された場合に防ぐことができる。
HTAの禁止	○	○	.htaファイルをメールで受信した場合やドライブバイダウンロードの途中で使われた場合に最終的な感染を緩和する。
Webブラウザのプラグインを自動実行させない（Click to Play）	○		ドライブバイダウンロードの発生を緩和する。
マッシュアップコンテンツを制限する	○		ドライブバイダウンロードの発生を緩和する。
ストアアプリの禁止			意図しないプログラムの混入やストアアプリ内にあるマルウェアやPUA（Potentially Unwanted Application）のインストールを防ぐことができる。

※Webはドライブバイダウンロードを想定、メールは添付ファイルを想定、URLはドライブバイダウンロードに含める。

○：効果あり　△：条件付きで効果あり

■ 攻撃成立の可能性

上記対策を行うことで多くのマルウェア感染を止められますが、以下のような条件下では攻撃を防ぐことはできません。

- 任意のコード実行の脆弱性を突くExploitによる攻撃が成立
- 権限昇格の脆弱性を用いてSYSTEM権限など、高い権限でマルウェア実行
  もしくは、マルウェアをメモリ上のみに展開し、実行

ただし、EMETを回避した上で未知の脆弱性(0-day)を成立させるなど、条件としては非常に厳しいものであり、ほとんどの攻撃は成立しないと考えています[*61]。

■ 副作用

AppLockerやソフトウェアの制限のポリシーを利用した場合、通常のGoogle Chromeは動かなくなります。これはChromeが一般ユーザのユーザディレクトリにインストールされるためです。この代替案として、スタンドアローンインストーラを利用することで、Program Files以下にインストールすることができます。ただし、この状態でもGoogle Chromeのアップデート用プログラムはユーザのtempディレクトリ上に実行ファイルを展開して実行しようとするため、正常にアップデートが行われなくなってしまいます。これを回避するために、このアップデータが持つ証明書を許可ルールとして登録しておくと良いでしょう[*62]。

WSHを無効化した場合、ログオンスクリプトなどにVBScriptを用いているとこれらの実行ができなくなります。PCの管理にPowerShellを用いていた場合はPowerShellの実行が禁止されると影響が出ます。

メールで文書をやりとりする場合、ファイルを暗号化する際に自己展開形式にして送信する文化が日本には根強く残っていますが、アプリケーションホワイトリスティングを導入した場合、ユーザが保存できる領域に存在する実行ファイルを例外なく拒否することになるため、受信者は添付ファイルの中身を

---

*61 本レポート期間中、Angler Exploit Kitが最新のEMETを完全に突破し、攻撃を成立させるとの報告があった。"Angler Exploit Kit Evading EMET"(http://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html)。過去に研究者によっていくつかの脆弱性が報告されたことはあったが、実際の攻撃で確認されたのは筆者の知る限りではこの事例が初めてである。ただしこの攻撃が出回った時点でAngler Exploit Kitは未知の脆弱性を利用していなかったため、パッチ適用が適切に行われていれば被害は出なかった。EMETの次回のアップデートではこの手法に対する対策が行われる可能性はあるが、本稿執筆時点で、EMETでこの手法を防ぐことは難しいと考えられる。報告された手法を緩和するためには、FlashやSilverlightを無効化しておくか、Click to Play機能でFlashなどに関連するDLLが自動的にロードされないようにすることである。このように、1つの対策が突破されても、他の手法で防ぐ、いわゆる多層防御が必要である。また、攻撃情報を収集し、それを緩和するための手段を普段から検討しておくことも必要である。EMETはあくまでも脆弱性を緩和するためのツールである。EMETを導入することで、パッチ適用を回避するという誤った判断をしてはならない。

*62 ChromeはWindowsドメイン上のクライアントに一斉インストールし、グループポリシーで一元管理、ユーザにポリシーを強制することが可能なChrome for Workを配布している(https://www.google.com/intl/ja/chrome/business/browser/admin/)。この仕組みであれば、管理者が強制的に全クライアントに対して新バージョンを配信をさせることが可能である。またユーザに勝手な拡張機能やアドオンをインストールされることを防ぐこともできる。FirefoxやThunderbirdについても、Mission Control Desktop(MCD)やAutoConfigと呼ばれる仕組みを用いることで、ユーザに利用環境を自由に変更できないようにし、管理者の設定を強制させることのできる機能が存在する(https://www.mozilla.jp/business/faq/tech/setting-management/)。

チェックすることができなくなります。しかし、例えば一昨年に標的型攻撃で頻繁に使われたEMDIVIも自己展開形式を使用していましたが、攻撃者が送信元の組織と同一のアーカイバや暗号化ツールを入手し、自己展開形式でファイルを作成してメールを送信した場合、無害な添付ファイルと攻撃の区別がつきません。添付ファイルの暗号化を行いたい場合はパスワード付きzipや、より強い暗号化強度が必要であればGPGを使用して暗号化した上で添付する、もしくは信頼できるオンラインストレージサービスを利用してhttpsで通信路を暗号化してファイル共有するか、PGP/MIMEやS/MIMEなどでメール全体を暗号化するなどして代替し、このような悪しき文化を早く根絶していくべきです。

これまで紹介してきた設定で運用していると、この他にもいくつかの不具合に直面することがあります。そのときは、不具合がルールや運用を工夫することで回避できるかを検討していく必要があります。また、今回はマルウェアに感染しないことに特化して記述しましたが、よりセキュアに運用するためには、例えばプロセス生成やファイルの生成、書き込みイベントなどの監査ポリシーを設定したり、サードパーティの監査ソフトウェアなどを用いて監視するなど、他の対策も検討すべきです。Windows 10では、最新の脅威に合わせ、Device Guard[*63]やCredential Guard[*64]など、セキュリティを守るためのより強力で新しい実装があります。これらも導入を検討していくと良いでしょう。また日々新しい脅威が発見されているため、情報収集を行い、それらの脅威に対応するための方法を考え、定期的にポリシーの見直しを行う必要があります。

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、Volatility Frameworkプロファイルの生成、マルウェアに感染しないためのWindowsクライアント要塞化(後編)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)
小林 稔(1.4.1 Volatility Frameworkプロファイルの生成)
鈴木 博志(1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化(後編))
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

*63「Device Guardの概要」(https://technet.microsoft.com/ja-jp/library/dn986865(v=vs.85).aspx)。
*64「Credential Guardによるドメインの派生資格情報の保護」(https://technet.microsoft.com/ja-jp/library/mt483740(v=vs.85).aspx)。