NTT DATA
Trusted Global Innovator

グローバルセキュリティ動向四半期レポート
（2018 年度 第 3 四半期）

株式会社 NTT データ
セキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT 担当

目次

1. エグゼクティブサマリー 2
2. 2018 年度 第 3 四半期のトピック 3
2.1. 情報漏えい、個人情報、プライバシー 3
2.2. フィッシング詐欺 5
2.2.1. 国内で増加するフィッシング 5
2.2.2. 国外で進むフィッシング手口の巧妙化 7
2.3. 暗号通貨を狙った攻撃 8
2.3.1. 暗号通貨サービス提供者を狙った攻撃 8
2.3.2. 暗号通貨サービス利用者を狙った攻撃 8
2.3.3. コンピュータの計算リソースを狙った攻撃 10
2.4. 米中対立 10
2.4.1. Super Micro 製マイクロチップ関連の出来事 10
2.4.2. Huawei 関連の出来事 11
2.5. 脆弱性とそれを悪用するサイバー攻撃 12
2.5.1. ゼロデイ攻撃 12
2.5.2. ボットネット 15
2.5.3. その他の攻撃 16
2.6. マルウェア 18
2.6.1. ランサムウェア 18
2.6.2. 重要インフラを標的とするマルウェア 18
2.6.3. 金融機関、金融サービスを標的とするマルウェア 19
2.6.4. その他マルウェア 20
2.6.5. マルウェア対策 22
2.7. IoT 23
2.8. 政府、公共機関、事業者のセキュリティ施策 24
3. 2018 年度 第 4 四半期以降の予測 25
4. 2018 年度 第 3 四半期のタイムライン 26
5. 参照文献 31

1. エグゼクティブサマリー

情報漏洩が複数件発生して話題となりました。特に話題となった例として、9 月末に発生した Facebook からのユーザ 2,900 万人分の情報漏えいや、11 月にマリオットが発表した 5 億人の顧客の情報漏えいが挙げられます。プラットフォーマーと呼ばれる大手 Web サービス事業者では、利用者が数億人単位の場合もあり、情報セキュリティ事故が発生した場合の被害が大きくなる傾向があります。サービス利用者は、適切なサービス事業者を選定する、不用意に情報や資産を預けるのではなく、サービスに登録する情報を選別する、自身が登録している情報を把握する、といったリテラシーが求められます。

前四半期から継続して、Web サービスやクラウドサービスに関係する詐欺やフィッシングが流行しています。攻撃者は、詐欺やフィッシングを使って金銭を盗んだり、パスワードを盗んだりします。攻撃が成功すると、大きな利益を得られる攻撃です。詐欺の手段は、依然としてメールが中心ですが、SMS やソーシャルメディアといった、別のメディアを用いる手口も増えています。例として、IPA は、9 月は 24 件であった、佐川急便を騙った偽 SMS に関する相談件数が、10 月は 169 件、11 月は 182 件であったと報告しています。災害やキャリアのトラブルに便乗した巧妙な文面も見られました。

暗号通貨関連の攻撃では、サーバ、ルータ、IoT 機器など、長期間、自動で稼動している機器を悪用したマイニングが増加しています。これら機器はマイニングにより CPU 資源が消費されても気付きにくく、不正マイニングの検出が遅れがちです。修正プログラムを適用して脆弱性を対策する、強固なパスワードを設定し不正アクセスを防ぐ、といった基本的な対策が有効です。

サービス利用者を狙う攻撃の傾向として、オープンソースソフトウェアを悪用したサプライチェーン攻撃が発生しています。悪意のあるコードが埋め込まれたオープンソースな開発環境(SDK: Software Development Kit)が配布され、それらを使って開発されたソフトウェアやサービスにはバックドアやマイニングプログラムが含まれており、これを使用するとマイニングや乗っ取りの被害が発生するケースがありました。このようなサプライチェーン攻撃は、オープンソースな開発環境を使用してソフトウェアを開発する個人や企業が注意する必要があります。

今後、暗号通貨の市場価格が下落して、不正マイニングによって利益を得にくい状況が続いた場合、攻撃者は、暗号通貨を狙った攻撃に割いていたリソースを別の異なる攻撃に振り替えられるおそれがあります。

2. 2018 年度 第 3 四半期のトピック

2.1. 情報漏えい、個人情報、プライバシー

Facebook 社について、「View As」機能の脆弱性悪用による 2,900 万件のトークン窃取 [1]、Web ブラウザ拡張機能悪用による 8 万 1,000 件の個人データ窃取と情報売買 [2]、写真が外部のアプリ開発者に流出しかねない状況にあったソフトウェア不具合 [3] など、複数の情報漏えいに関する報道がありました。またケンブリッジアナリティカ事案も含んだ個人情報漏えいについて日本の個人情報保護委員会から行政指導 [4]があったことや、英 ICO が重大なデータ保護違反であるとして 50 万ポンドの罰金を科したこと [5] など、各国の行政、制度の観点からも、Facebook 社へ注目が集まりました。

表 1: Facebook 情報漏えい関連の出来事

日付	概要	被害件数
9/28	Facebook がサイバー攻撃を受け、アカウントへログイン可能な「トークン」が最大 5,000 万人分を盗まれ、合計 9,000 万人分のトークンをリセットしたと発表しました。攻撃者は、プロフィール確認の「View As」機能の脆弱性を悪用してトークン情報を盗みました [6]。	5,000 万件
10/12	Facebook が、最大 5,000 万人分の「トークン」が盗まれた件について、2,900 万人が実際に被害を受けたと発表しました。攻撃者が、2,900 万人のうちの 1400 万分の個人の重要情報を盗み見たと報告しています [1]。	2,900 万件（訂正）
10/22	日本政府の個人情報保護委員会が Facebook に対して行政指導を行ったと発表しました。行政指導の対象は、情報が自動で送信されるソーシャルプラグイン、ケンブリッジアナリティカ事案、「View As」機能悪用による情報漏えいの 3 件です [4]。	なし
10/24	イギリスの個人情報保護当局である情報コミッショナー事務局（ICO）が、ユーザデータの収集の問題に関して、Facebook へ 50 万ポンドの罰金を科す計画を実行に移しました。イギリスの 100 万人以上のデータが不当に処理されたとしています [5]。	なし
11/2	BCC は、8 万 1,000 件の Facebook アカウントの個人データが盗まれ、販売されたと報道しました。英語圏のネットフォーラムにて「FBSaler」と名乗るユーザが、アカウント情報を販売すると発表し、サンプルとして 8 万 1,000 件以上のプロフィールデータをネットフォーラムへ投稿しました。Facebook は、Web ブラウザの拡張機能を使用して収集した違法性のない情報であり、情報漏えいは Facebook の欠陥ではないとしています [2]。	8 万 1,000 件
12/14	Facebook は、ソフトウェアの不具合によりスマートフォン内の画像が外部アプリケーション開発者に流出しかねない状況にあったと発表しました。最大 680 万人が影響を受ける状況にありました。[3]	680 万件

その他には、Google 社が API の不具合により最大 50 万件の Google＋アカウントの個人情報を漏えいした件や、世界最大ホテルチェーン「マリオット」グループの不正アクセスによる大規模情報漏えいが話題になりました。マリオットは情報漏えいについて、「スターウッド・ホテルズ&リゾーツ・ワールドワイド」で予約した 5 億人の顧客に影響があると公表しています。2018 年 9 月 8 日に、内部セキュリティツールが不正なデータベースアクセスの試みがあると警告を発し、同社が調査したところ、2014 年からの不正アクセスが判明しました。同社は、影響するユーザに対して個人情報漏えいの有無を監視できる外部サービス「WebWatcher」の 1 年間サブスクリプションを無償提供しています。

表 2: 情報漏えい関連の出来事

日付	概要	被害件数
10/8	Google 社は、API の不具合により、最大 50 万件の Google+アカウントの個人情報が漏えいしたと報告しました。Google は Google+のサービス終了を予定しています [7]。	50 万件
10/9	攻撃グループ「Magecart」は、Shopper Approved 社のプラグイン「review widget」を攻撃しました。「review widget」は、顧客がネット通販サイトで製品をレーティングするために使用するプラグインです [8]。	記載なし
10/13	Associated Press は、米国防総省が第三者請負業者に起因するセキュリティ侵害に遭い、軍人および文民職員役 3 万人が影響を受けたと報じました [9]。	3 万件
10/24	キャセイパシフィック航空が攻撃を受け、最大 940 万人の乗客データに影響がおよぶおそれがあると発表しました。流出した情報は、パスポート番号、身分証明書番号、電子メールアドレス、クレジットカード情報などです [10]。	940 万件
11/6	イタリアの「Anonymous」が新たな情報をリークしました。開示された資料には、国立研究評議会、Equitalia データベース、経済開発省の各研究機関の従業員と関係者の個人情報が記載されていました [11]。	記載なし
11/8	クレジット会社の American Express India は、セキュリティで保護されていない MongoDB サーバをオンラインに公開しました。約 70 万人の顧客情報が含まれていました [12]。	70 万件
11/14	ラジオ番組司会者のアレックス・ジョーンズの Web サイト Infowars のオンラインストアが、攻撃グループ「Magecart」によるクレジットカードスキミング攻撃を受けました [13]。	記載なし
11/22	過去 1 年間にわたり、米国郵政公社のアカウント情報 6,000 万人分が、閲覧可能な状態だったと報じられました [14]。	6,000 万件
11/30	ホテル大手のマリオット社は、2014 年以降、傘下のスターウッド社の予約データベースへの不正アクセスがあったと発表しました。最大 5 億人の個人情報が侵害されるおそれがあります [15]。	5 億件

様々な事業者が利用者の個人情報を収集しています。一方で、利用者が十分に意識していない状態で、個人情報の収集や売買のなされる事例もありました。

表 3 個人情報の収集や売買の事例

日付	概要
10/9	B9 Systems 社が、ヘルスケア関連 Web サイトの個人情報の扱い方を調査した結果を公表しました。調査対象の Web サイトは、平均 57 の外部サイトに個人情報を共有しており、共有先には広告サイト、マーケティングサイト、ソーシャルメディアなどがありました [16]。
10/18	総務省は GAFA[1]等の巨大 IT 企業への規制の在り方などを議論する研究会の初会合を開きました。これらプラットフォーマーは、海外事業者のため、電気通信事業法の適用外で、個人情報の扱いに懸念が生じていました [17]。
10/18	Oxford 大学の研究者が、Google Play ストアのアプリ約 96 万個をダウンロードし、サードパーティによる追跡機能の有無を調査しました。1 アプリあたりのトラッカー数の中央値は 10 で、90%のアプリは 1 つ以上のトラッカーを含んでいました [18]。
12/10	無料 Android アプリで収集された利用者の位置情報が、広告企業に販売されていたことがわかりました。このアプリは、GasBuddy というガソリンスタンドへの経路案内機能などを有するアプリで、販売先は広告企業の Reveal Mobile でした。販売価格は 1000 ユーザあたり 9.5 ドルでした [19]。

2.2. フィッシング詐欺

2.2.1. 国内で増加するフィッシング

国内におけるフィッシング手口の巧妙化が進んでいます。IPA は、11 月に宅配業者を騙る偽ショートメッセージに関する新たな手口について注意喚起を行いました [20]。IPA の情報によると、2018 年 7 月に宅配業者を騙るフィッシングについて相談件数が急増し、10 月、11 月は再度急増しているとのことです（図 1 参照）。Android 端末向けの不審なアプリをインストールさせようとする手口のみでなく、iOS 端末を狙ったフィッシングサイトも増加しています。手口としては、SMS を利用し、URL から本物と見分けのつきにくい偽サイトへ誘導するなどの変化が見られます（図 2、図 3 参照）。佐川急便を騙るフィッシングやヤマト運送を騙るフィッシングなど、バリエーションも増加しています。

また、2018 年 12 月には詐欺メールが急増し、多種多様な詐欺メール例が報告されています。日本サイバー犯罪対策センターの情報によると、Amazon や楽天を騙った詐欺メール、請求書や納品書などを装うビジネス詐欺メール、「パスワードを侵害した」等の脅迫メールなどが報告されています [21]。

[1] Google, Apple, Facebook, Amazon の頭文字をとったもの。

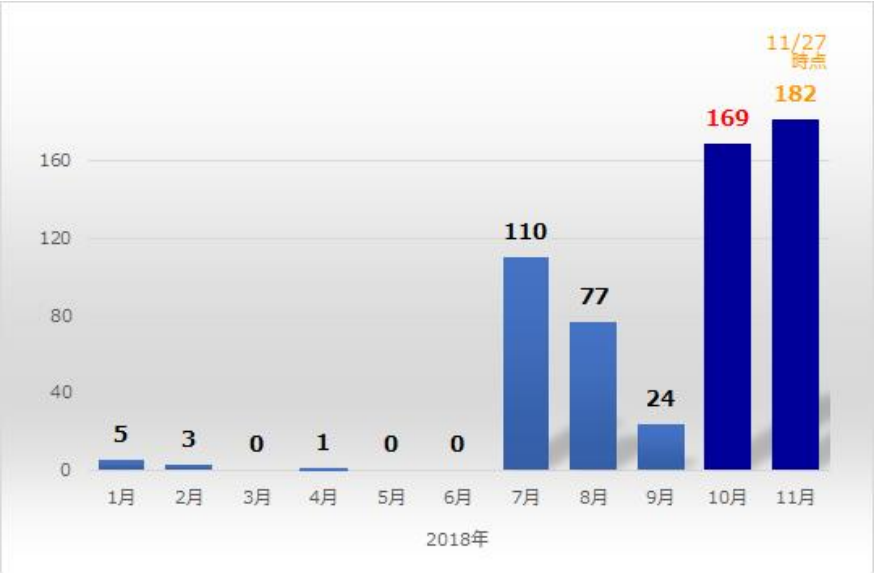

図 1:2018 年の IPA に寄せられた「佐川急便をかたる偽 SMS」に関する相談件数の推移 [20]

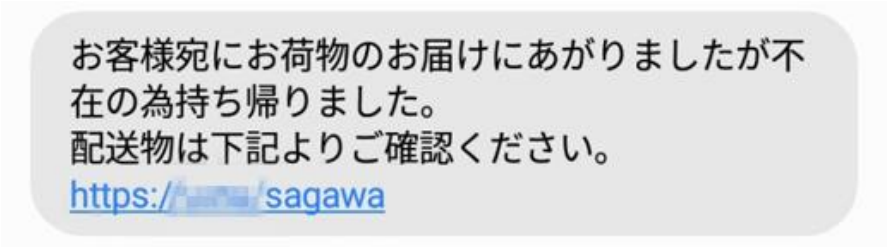

図 2:SMS を利用した不在通知を装うフィッシングの例 [22]

図 3:判別困難な偽サイトの例 (左:偽サイト、右:公式サイト) [23]

2.2.2.　国外で進むフィッシング手口の巧妙化

フィッシングに関して新たな手法が報告されています。10 月 3 日の Netskope Threat Protection の報告によれば、攻撃者は、まず Google ドライブ上のある PDF ファイルを開かせます。Google ドライブ上のある PDF ファイルを開くと、リンクされている Azure BLOB ストレージに置かれた Office 365 のフィッシングページが表示されました。Azure BLOB ストレージは、Microsoft が発行したドメインと SSL 証明書を持つため、ブラウザは SSL で接続されます（図 4 参照）。ユーザは、一見、SSL で正規 Web サイトへ接続されたと勘違いしてしまいます [24]。

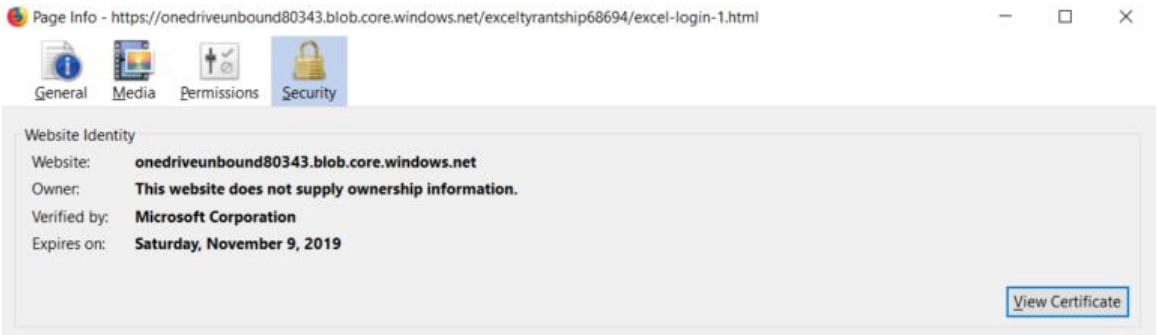

図 4：Microsoft 発行の SSL 証明書で保護されたフィッシングサイトの例

また Bleeping Computer は、このフィッシングについて、攻撃者が CDN サービス企業 CloudFlare 社の P2P ファイルシステム「The InterPlanetary File System(IPFS)」へアクセスするための IPFS ゲートウェイサービスも悪用していると報告しました [25]。CloudFlare 社は 9 月に IPFS ゲートウェイサービスをリリースしました。IPFS ゲートウェイサービスへのすべての接続は CloudFlare 社によって発行された SSL 証明書によって保護されます。したがって、攻撃者は CloudFlare 社が発行した SSL 証明書によって保護された HTTP アクセスを悪用でき、ユーザへ正規の Web サイトの入力フォームへ入力していると思い込ませることができます。

Azure BLOB ストレージ以外にも、Google Cloud Storage サービスを悪用するケースも確認されています。Menlo Labs が銀行や金融サービス会社の従業員を標的とした悪質な電子メールキャンペーンを追跡した結果を報告しています。攻撃者は、電子メールに書かれた悪質なリンクをクリックさせて、Google Cloud Storage サービスのドメイン「srorage.googleapis.com」に置かれたファイルへアクセスさせていました [26]。

PhishLabs が 12 月に公開した報告書によると、フィッシングサイト全体のうち、SSL 証明書を使用したフィッシングサイトは 49.9%でした。PhishLabs は、「フィッシングサイトの SSL 証明書の有無はサイトの正当性を証明するものではないにもかかわらず、ユーザは、Chrome や Internet Explorer に表示された南京錠の印で正規サイトへアクセスしていると誤解する」と述べています [27]。

上記より、SSL 証明書の有無だけでは、Web サイトが、正規のサイトか、フィッシングサイトであるか否かを判断出来ません。ユーザは、Web サイトへアクセスしたにもかかわらず、Azure BLOB や Google Cloud Storage 等のクラウドストレージサービスのドメインへアクセスしている場合は、フィッシングサイトへアクセスしているおそれを疑ってください。Web ブラウザが、SSL 認証が無い Web サイトへアクセスしたときに警告を表示する機能を実装したため、攻撃者は、このように攻撃手段を巧妙化したフィッシングを行っています。

2.3. 暗号通貨を狙った攻撃

表 4 は、暗号通貨を狙った攻撃手法を暗号通貨の取引や標的で分類したものです。本レポートでは、標的別に攻撃を整理しました。

表 4：暗号通貨を狙った攻撃手法の分類

暗号通貨の取引	標的	攻撃の説明、例
暗号通貨取引の当事者	暗号通貨サービス提供者	暗号通貨取引所のウォレットを狙った攻撃など
暗号通貨取引の有無によらない	暗号通貨サービス利用者	暗号通貨取引所へログインする認証情報を窃取する攻撃など
	PC 保有者	暗号通貨マイナーへ感染させる攻撃やドライブバイマイニングなど

2.3.1. 暗号通貨サービス提供者を狙った攻撃

2018 年度 10 月～12 月は、前四半期の 7 月～9 月に比べて、暗号通貨サービス提供者を狙った攻撃が減少しました。また、外部からのハッキングを偽装して内部からコールドウォレットを狙った珍しい攻撃のケースがありました。暗号通貨のウォレットは、ホットウォレットとコールドウォレットの 2 種類に分けられます。ホットウォレットはインターネットに接続した状態で管理し、コールドウォレットはインターネットから切り離した状態で管理します。したがって、コールドウォレットはハッキング等の被害を受けにくいとされています。過去に公開した「サイバーセキュリティに関するグローバル動向四半期レポート」においても「ホットウォレットからコールドウォレットへの移動」をハッキング被害に遭わないための対策例として挙げています。これらの事象から、暗号通貨サービス利用者は利用する取引所の選択にも配慮が必要であるといえます。

表 5：暗号通貨サービス提供者を狙った攻撃の一覧

日付	攻撃の概要	被害額
10/21	スイスの暗号通貨取引所 Trade.io がハッキングを受けたとし、TIO 5,000 万通貨が流出しました。被害総額は 1,100 万ドル程度です。コールドウォレットが狙われた珍しいケースとして話題となりました。コールドウォレットに物理的にアクセスできる人物の犯行とみられています [28]。	1100 万ドル
10/28	カナダの暗号通貨取引所 Maplechange がハッキングを受け、BTC を全失しました。喪失金額は 913BTC 約 600 万ドルです。公式 Web サイトの停止や SNS の消去が行われ、ハッキングは偽造されたもので詐欺ではないかという疑いもあります [29]。	600 万ドル

2.3.2. 暗号通貨サービス利用者を狙った攻撃

Doctor Web のアナリストが、攻撃者「Investimer」が使用している幅広い種類のマルウェアや多岐の攻撃手法について調査報告を行いました。報告内容によると、Investimer は、商用のトロイの木馬型のマルウェアのみでなく、TeamViewer を悪用した Spy-Agent バックドア、VNC プロトコル経由でコンピュータにアクセスする DarkVNC および HVNC バックドア、RMS ベースのバックドアなどのマルウェアも使用しています。さらに管理サーバが jino.ru、marosnet.ru、hostlife.net などの通信会社のサービスやホスティングサービスなどの正規 Web サイトに設置していること、Dogecoin に焦点を当てフィッシングサイトを多数用意していることなどが報告されています [30]。

利用者の多い Web サイトや OSS へ、暗号通貨を盗み取るための悪意のあるコードが埋め込まれる事象が発生しています [31] [32]。OSS は誰でもソースコードを入手してコードが変更可能であるため、悪意のあるコードへ改変されるおそれがあります。Web サイトの改ざんと比べて、OSS の利用者は、OSS 内に埋め込まれた悪意のあるコードを気づくことが困難です。特に開発者や企業は、オープンソースな開発環境(SDK: Software Development Kit)を悪用したサプライチェーン攻撃に注意が必要です。攻撃者が配布した、悪意のあるコードが埋め込まれたオープンソースな開発環境を使ってソフトウェアを開発したところ、バックドアやマイニングプログラムが含まれており、これを使用したユーザがマイニングや乗っ取りの被害を受けたケースがありました。開発者は、OSS を信頼できる Web サイトから取得しましょう。さらに開発者は、オープンソースな開発環境を利用する前に提供元や開発者をよく調査して、変更が無いことを確認しましょう。オープンソースな開発環境の提供元や開発者が変わることは稀なため、もしそれらが変化している場合は、攻撃者が開発者からオープンソースな開発環境を買収して、攻撃手段として悪用しているおそれがあります。攻撃者が提供しているおそれのある不審な開発環境は、使用しないようにしましょう。OSS を使う人は、上記のようなリスクがあることを理解し、自分自身でリスク判断できなければなりません。

国外では、SIM スワッピングと呼ばれる手法を用いて、暗号通貨のウェブウォレットのアカウントを乗っ取る攻撃が発生しました [33]。SIM スワッピングとは電話番号を乗っ取る行為です。手法の一例として、携帯電話の SIM（Subscriber Identity Module：加入者識別モジュール)から電話番号を識別するための暗号化データを取り出して、別の携帯電話の SIM へ書き込む処理があります。

11 月に発生した事例では、攻撃者は、まずカスタマーサービスに連絡してある人物の携帯電話の SIM の変更手続きを行い、攻撃者が用意した新しい携帯電話へある人物の電話番号を紐づけました。つぎに、攻撃者は、暗号通貨のウェブウォレットのアカウントのパスワード変更を要求し、その携帯電話を使って 2 要素認証を突破して、パスワードの変更を成功しました。攻撃者は、変更したパスワードを使って、ある人物の暗号通貨のウェブウォレットへログインして、暗号通貨を不正に取り出しました。ある人物が携帯電話の異変に気づいてプロバイダに連絡するまでの短い時間に 100 万ドル相当の暗号通貨が奪われました。ある人物は「シリコンバレーの大物」とされており、この攻撃は、攻撃者が裕福な特定の人物を狙った標的型攻撃でした。

表 6: 暗号通貨サービス利用者の暗号通貨を狙った攻撃の一覧

日付	攻撃の概要
11/8	ESET は、攻撃者がインターネット上の Web 解析プラットフォーム「StatCounter」に不正侵入して挿入したと思われる悪意のあるコードを発見しました。暗号通貨取引所「Gate.io」の Web インターフェースを通して実行されるあらゆるビットコイン取引を乗っ取るとされています [31]。
11/22	21 歳の攻撃者が、SIM スワッピングと呼ばれる方法を悪用して、約 100 万ドル相当の暗号通貨を盗み取ったとして報じられました。攻撃者は、カスタマーサービスに連絡して SIM 交換を装って、標的のユーザの電話番号を奪ったとされています [34]。
11/27	JavaScript ライブラリ「Event-Stream」に、暗号通貨のウォレットからコインを盗むためのコードが埋め込まれていると報じられました [32]。
11/28	名古屋地検は 18 歳の少年を不正指令電磁的記録作成、同共用の疑いで名古屋家裁に送致しました。暗号通貨「モナコイン」を不正に入手する目的でコンピューターウイルスを作成したとされています [35]。

2.3.3.　コンピュータの計算リソースを狙った攻撃

暗号通貨をマイニングするマルウェア「マイナー」は、依然として広く活動しており、暗号通貨を利用していない場合も注意が必要です。McAfee は 12 月に、前四半期の 2018 年 7 月～9 月にマイニングマルウェアが急激に増加したという内容のレポートを公開しました [36]。コンピュータの計算リソースを狙うことから影響範囲が大きく、今後も警戒が必要であるといえます。

表 7: コンピュータの計算リソースを狙う攻撃の一覧

日付	攻撃の概要
10/11	研究者 Brad Duncan が、Adobe Flash Player のアップデートを装い、マイニングマルウェアをインストールさせる新しい手法を発見しました。ユーザの不信感軽減を狙って、Adobe Flash Player の更新を行う点が今までにない特徴といえます [37]。
10/22	警察庁は、ADB デバッグが有効化された Android デバイスを狙った攻撃について注意喚起を行いました [38]。JVN は当該脆弱性について [39]、警察庁は ADB が使用する 5555/TCP ポートを狙った攻撃について [39]、それぞれ過去に報告や注意喚起を行っています。5555/TCP ポート宛の通信は、マイニングマルウェアをダウンロードしてインストールしようとするものです。
10/25	トレンドマイクロが Docker Engine API を暗号通貨マイニングに悪用する攻撃を発見しました。Docker Engine API の悪用は以前から問題とされていますが、不適切に設定された Docker Engine が未だ存在しており、攻撃は継続しているとのことです [40]。
11/1	聖フランシスコ・ザビエル大学が「cryptcoin mining」と呼ばれる攻撃を受け、ネットワークを遮断しました。対策として、大学のアカウントすべてのパスワードをリセットしました。報道時点で個人情報が侵害された証拠はないものとしています [41]。
11/12	McAfee Labs が被害者のコンピュータを悪用して暗号通貨のマイニングを行う WebCobra という新たなロシア製のマルウェアを発見しました。感染する機器の構成に応じて異なるマイナーを投下する点が特徴的であると指摘しています [42]。
11/19	国際的非営利団体「メイク・ア・ウィッシュ財団」の Web サイト「worldwish.org」が侵害され、暗号通貨 Monero をマイニングするための JavaScript マイニングプログラムである CoinIMP が埋め込まれました。 [43]。

2.4.　米中対立

2.4.1.　Super Micro 製マイクロチップ関連の出来事

米国メディア「Bloomberg Businessweek」が 2018 年 10 月 4 日に特集記事「The Big Hack : How China Used a Tiny Chip to Infiltrate U.S. Companies」 [44]を公開しました。記事の内容は、中国で製造され米国で使用される Super Micro 製のマザーボードに米粒より小さなマイクロチップが埋め込まれており、中国がそのチップを通じて米国の知的財産や機密情報にアクセスしていたというものでした。この記事の内容については、Apple や Amazon、世界各国を巻き込んで大きな話題となりました。

表 8: Super Micro 製マイクロチップ関連の出来事

日付	攻撃の概要
10/4	Bloomberg Businessweek が Super Micro 制のマザーボードにマイクロチップが埋め込まれており、チップを通じて情報にアクセスしていたという内容の特集記事「The Big Hack : How China Used a Tiny Chip to Infiltrate U.S. Companies」を公開しました [44]。
10/4	Amazon、Apple、および Super Micro は、Bloomberg Businessweek の報告の要約に対して、電子メールの声明によって異議を唱えました [45]。
10/4	Amazon は、Bloomberg BusinessWeek の Super Micro 制のマイクロチップに関する記事について、否定の声明を発表しました。ハードウェアに関する問題が見つかったことも、政府との調査もないと主張しました [46]。
10/5	英情報機関・政府通信本部(GCHQ)傘下の国家サイバーセキュリティセンター(NCSC)は、報道を否定した Apple や Amazon を疑う根拠はないとする見解を明らかにしました [47]。
10/8	Apple の情報セキュリティ担当副社長の George Stathakopoulos 氏が、議会宛のメッセージで記事内容を強く否定しました。「Apple は、悪意のあるチップも「ハードウェア改竄」や意図的に仕込まれた脆弱性も、これまでにどのサーバでも見つけたことはない」としています [48]。
11/2	米上院委員会は FBI と国土安全保障省に、Super Micro のサーバーマザーボードに中国の諜報機関が下請け業者を使用して悪意のあるチップを植え付けたという報告書の機密説明を求めました。国土安全保障省は、Bloomberg Businessweek の報告に対する各企業の否定を疑う理由はないと述べました [49]。
12/11	Super Micro Computer が顧客に対する公開書簡にて、調査会社による調査結果を明らかにし、同社のマザーボードに悪質なハードウェアが仕込まれていたと報じられた件について「証拠はまったくなかった」としています [50]。

2.4.2. Huawei 関連の出来事

The Wall Street Journal の報道によれば、米国政府はサイバー安全保障上のリスクになるとして Huawei 製品を使用しないように日本、ドイツ、イタリアなどの同盟諸国に対して要請を行ったとされています [51]。その後、各国政府や大手通信企業が順にそれぞれの声明を発表し大きな話題となりました。

表 9:Huawei 関連の出来事

日付	攻撃の概要
11/23	The Wall Street Journal の報道によれば、米国政府はサイバー安全保障上のリスクになるとして Huawei 製品を使用しないように日本、ドイツ、イタリアなどの同盟諸国に対して要請を行ったとされています [51]。
11/28	ニュージーランドの諜報機関は、国家安全保障への懸念を理由に、国内通信業界初の「Huawei が提供する 5G 機器を使用する」という要求を拒否しました [52]。
12/5	カナダ政府は、米国の要請により Huawei の最高財務責任(CFO)孟晩舟(Wanzhou Meng)氏をバンクーバーで逮捕しました。米国の対イラン貿易制裁に違反した疑いがもたれています。Huawei は容疑に関して把握している情報はなく、孟氏の過失も認識していないとの声明を発表しています [53]。
12/5	イギリス通信大手 BT が、Huawei 製品を既存の 3G、4G の基幹ネットワーク部分から排除し、5G のネットワーク主要部品としても使用しないと表明しました [54]。

12/7	ドイツ政府は、5Gのネットワーク構築に向け、いかなるメーカーやハイテク企業も排除しない方針を示しました。内務省の報道官が明らかにしたものです [55]。
12/10	日本政府は、「中央省庁や自衛隊が使う情報通信機器の調達に関する運用方針」をまとめ、Huawei とZTEの製品を政府調達から排除すると決定しました [56]。
12/14	ドイツテレコムは、これまで複数のベンダーとの取引を戦略に据え、Ericsson、Nokia、Cisco、Huawei を主要企業としてきたことに対して、今は調達戦略を見直していると明らかにしました [57]。
12/14	フランスの通信大手オレンジは、5Gのネットワーク構築で Huawei の製品を使用しない方針を発表しました [57]。

2.5. 脆弱性とそれを悪用するサイバー攻撃

2.5.1. ゼロデイ攻撃

ゼロデイ攻撃とは、ソフトウェアにセキュリティ上の脆弱性が発見されたときに、脆弱性が広く公表される前に、その脆弱性を悪用して行われる攻撃のことです。今四半期では Microsoft 製品、Adobe 製品にゼロデイ攻撃がありました。ゼロデイ攻撃は、脆弱性を悪用された場合の影響が大きく、Microsoft 製品や Adobe 製品は利用者も多いため、製品開発元や公共機関がセキュリティ更新プログラムの早期適用を呼びかけました。

表 10 ゼロデイ攻撃の事例

日付	製品	脆弱性番号	概要
10/9	Windows	CVE-2018-8453	Microsoft 社は Windows に関する脆弱性の修正プログラムを公開しました。この内、CVE-2018-8453 の脆弱性について、同社は「悪用の事実を確認済み」と公表しました [58]。Kaspersky 社によれば、8 月に中東地域に対し、同脆弱性を悪用した標的型攻撃が行われました [59]。
10/23	Windows	-	SandboxEscaper と名乗る Twitter ユーザが、Windows の権限昇格の脆弱性と PoC コードを公開しました(図 5 参照)。 同ユーザは 8 月にも Windows のタスクスケジューラにおける権限昇格の脆弱性を公開しました [60] [61]。
10/31	Cisco ASA	CVE-2018-15454	Cisco は Cisco ASA、Cisco FTD における SIP プロトコルに関する DoS 脆弱性を公開しました。脆弱性をつく不正な SIP 通信を検出したとして、同社は緩和策の適用を呼びかけました。11/6 以降に同社は脆弱性を修正した更新版ソフトウェアを公開しました [62]。
11/8	VirtualBox	-	セキュリティ研究者 Sergey Zelenyuk 氏が VirtualBox の仮想 NIC に関する権限昇格の脆弱性と PoC コードを公開しました。ベンダ(Oracle 社)に関する事前の通知はありませんでした。同氏は脆弱性の修正に半年間待たされる点、バグ報奨金制度への不満などから、問題提起したと述べています [63]。

11/6	WordPress	CVE-2018-19207	WordPress のプラグイン WP GDPR Compliance で権限昇格の脆弱性が発見されました。攻撃者はこの脆弱性を悪用し、複数のサイトにバックドアプログラムを設置していました [64]（図 6 参照）。通報を受け、プラグイン開発者は 11/7 に脆弱性を修正した更新版ソフトウェアを公開しました [65]。
11/13	Windows	CVE-2018-8589	Microsoft 社は Windows に関する脆弱性の修正プログラムを公開しました。この内、CVE-2018-8589 の脆弱性について、同社は「悪用の事実を確認済み」と公表しました [66]。Kaspersky 社によれば、10 月に中東地域に対し、同脆弱性を悪用した標的型攻撃が行われました [67]。
12/5	Adobe Flash Player	CVE-2018-15982	Adobe 社は Flash Player の任意コード実行、権限昇格の脆弱性を修正する更新版ソフトウェアを公開しました [68]。Gigamon 社によれば、11 月にロシアの医療機関を狙い、同脆弱性を悪用した標的型攻撃が行われました [69]（図 7 参照）。
12/11	Windows	CVE-2018-8611	Microsoft 社は Windows に関する脆弱性の修正プログラムを公開しました。この内、CVE-2018-8611 の脆弱性について、同社は「悪用の事実を確認済み」と公表しました [70]。Kaspersky 社によれば、FruityArmor、SandCat など複数のサイバー攻撃集団が同脆弱性を悪用していました [71]。
12/19	Internet Explorer	CVE-2018-8653	Microsoft 社は定例外のセキュリティ修正プログラムを公開しました。このプログラムは Internet Explorer のスクリプトエンジンにおける、遠隔コード実行の脆弱性を修正するものでした。発見者の Google Threat Analysis Group によれば、標的型攻撃で同脆弱性が悪用されていました [72]。
12/21	thinkPHP	-	中国製 PHP フレームワーク ThinkPHP に遠隔コード実行の脆弱性が発見されました。セキュリティ企業 VulnSpy が PoC を公開した直後から Web サーバへの攻撃が開始され、45000 以上の Web サイトが攻撃されました [73]。

図 5: SandboxEscaper が Twitter で Windows の脆弱性と PoC コードを公開した [61]

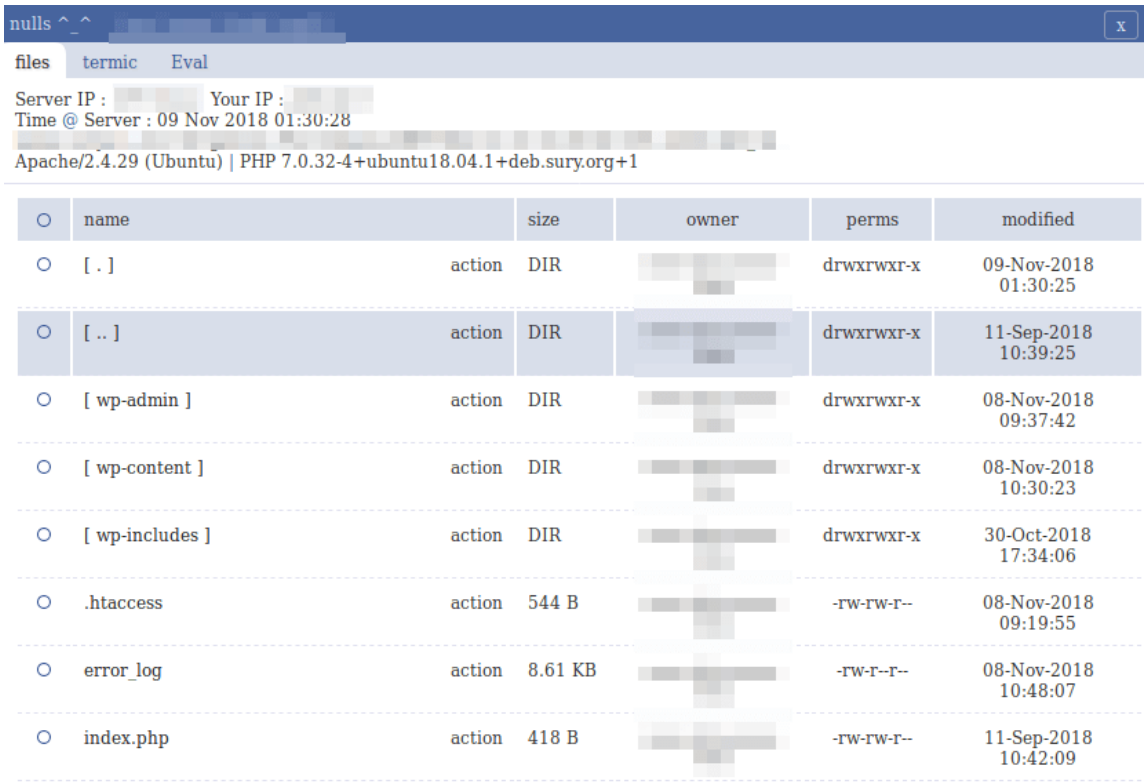

図 6 侵害された WordPress サイトに設置されたバックドアプログラムの表示画面 [64]

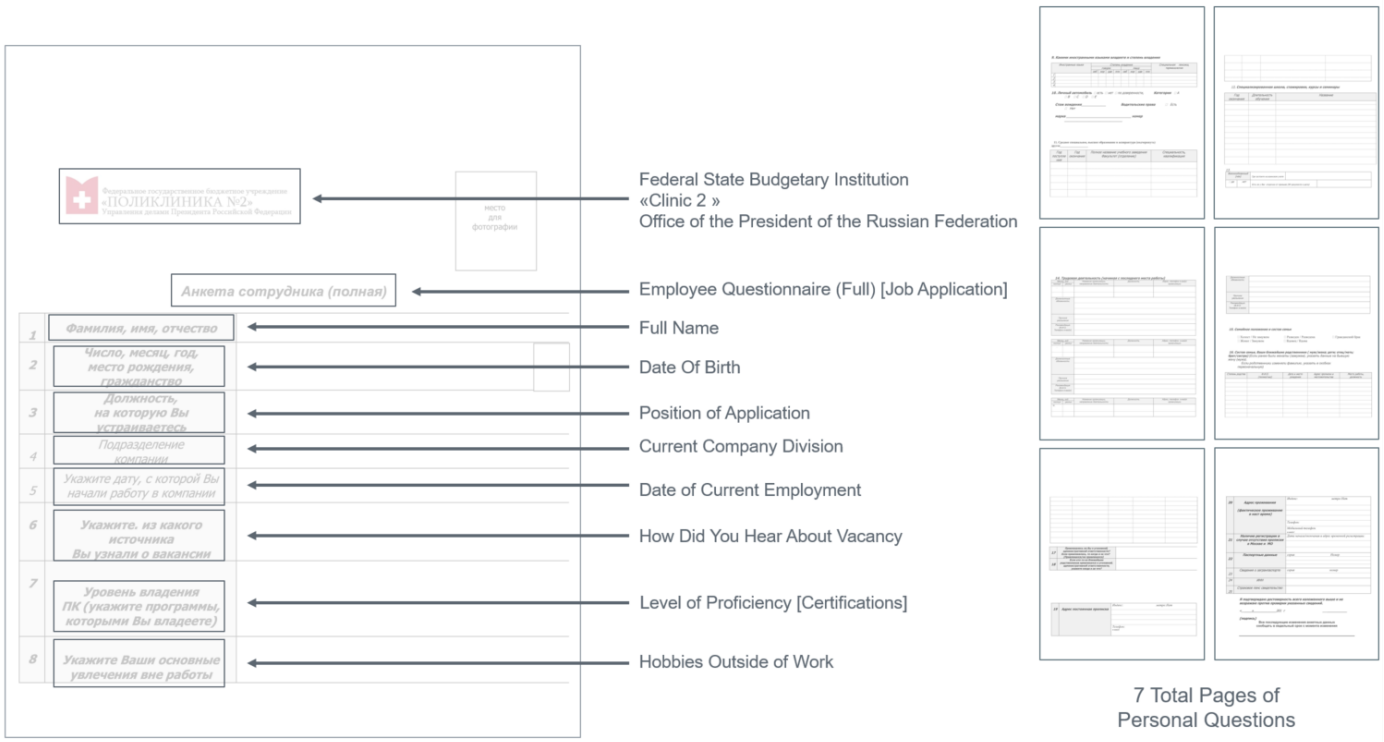

図 7 ロシアの医療機関へ標的型攻撃メールで送付された申込書を装った悪性の文書 [69]

2.5.2. ボットネット

2018 年 3 月、4 月に CMS ソフトウェアの Drupal で、遠隔コード実行の脆弱性 2 件 CVE-2018-7600(Drupalgeddon)、CVE-2018-7602 が続けて発見されました。IBM 社は、10/10 にこの脆弱性を悪用してボットネット Shellbot に感染させる攻撃を報告しました [74]。他にも、以下のような IoT 機器やルータの脆弱性を悪用してボットネットを構成する事例がありました。

表 11 ボットネットの事例

日付	製品	概要
10/25	Hadoop	Radware 社が、2018 年 3 月に公開された Hadoop YARN の遠隔コード実行機能の脆弱性を悪用して感染し、ボットネットを構成する DemonBot を発見したと報告しました。10 月には、同脆弱性を攻撃する通信が 1 日に 100 万回以上発生しました [75](図 8 参照)。
11/1	IoT 機器、Linux サーバなど	TrendMicro 社が、IoT 機器や Linux サーバの脆弱性を攻撃する Perl 言語ベースのボットネットを報告しました。日本の絵画団体の FTP サーバ、バングラデシュ政府の Dovecot メールサーバが、同ボットネットの C&C サーバとして悪用されていました [76]。
11/7	BroadCom 製ルータなど	Qihoo 360 社が、ルータ 10 万台以上(図 9 参照)で構成されたボットネットから、マルウェアへ感染させるためのスパムメールがばらまかれていると報告しました。ボットネットの標的は、BroadCom 製の UPnP 機能を有効にしたルータでした [77]。

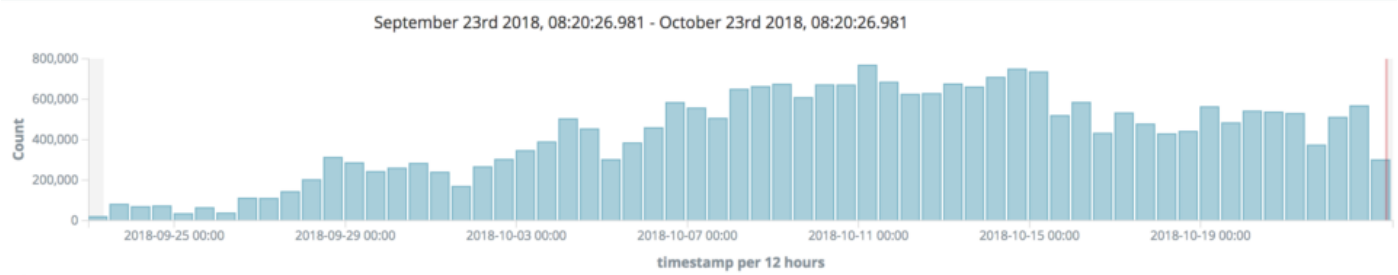

図 8 ボットネット DemonBot の通信回数［75］

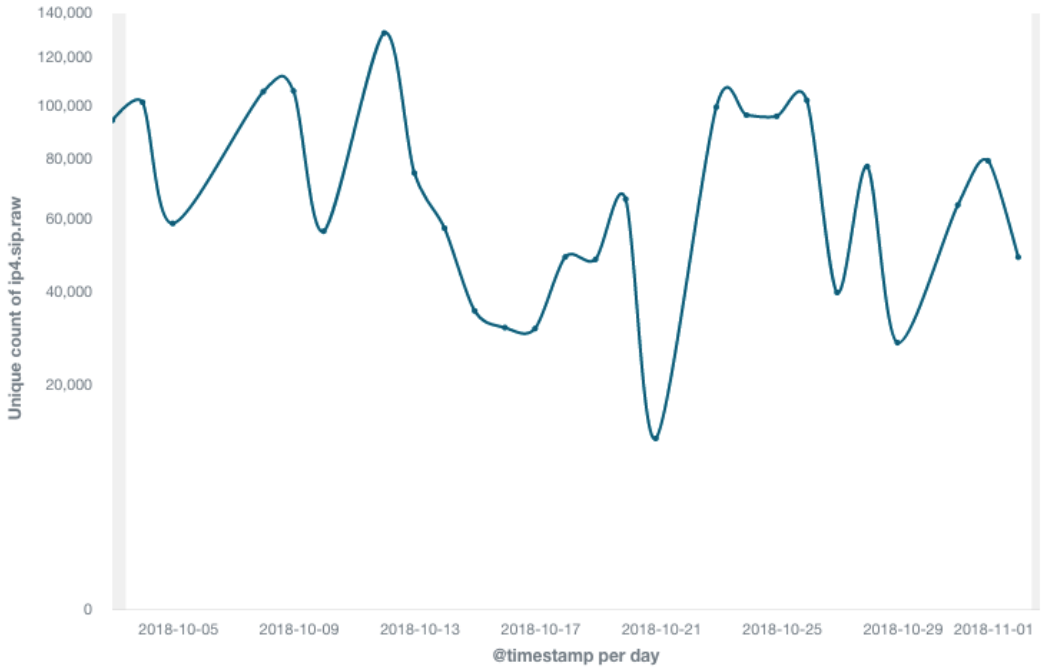

図 9 ボットネットを構成するルータの台数［77］

2.5.3. その他の攻撃

表 12 脆弱性を悪用したその他の攻撃事例

日付	製品	脆弱性番号	概要
11/6	Kibana	CVE-2018-17246	Elasticsearch のフロントエンド Kibana にファイル挿入の脆弱性が発見されました。悪意のある攻撃者が脆弱性を悪用した場合、JavaScript ファイルをアップロードし、任意のコードを実行するおそれがあります。11/21 に発見者の CyberArk 社が脆弱性の詳細や PoC を公開しました［78］。
11/12	Internet Explorer	CVE-2016-0189 CVE-2018-8373 CVE-2018-8174	Qihoo 360 社が IE の VBScript エンジンの脆弱性を悪用する攻撃を検知したと報告しました。同社はサイバー攻撃集団 DarkHotel の手口と分析しました。DarkHotel は北朝鮮との関連を示唆されています［79］。

11/15	nginx	CVE-2018-16843 CVE-2018-16844 CVE-2018-16845	Antuit 社が nginx の脆弱性を悪用する攻撃の前兆を検知したと報告しました。修正プログラムが公開済ですが、未適用の場合には DoS 攻撃や情報搾取などを受けるおそれがあります。ダークウェブやハッカーフォーラムで、同脆弱性に関するやりとりが急増していました [80]。
12/1	-	-	TheHackerGiraffe という Twitter ユーザが、プリンタ 5 万台以上に不正アクセスし、YouTube チャンネル PewDiePie の購読を呼びかけるスパムメッセージ(図 10 参照)を印刷した。このプリンタに不正アクセスしてメッセージを印刷する手法を使うスパム業者も(図 11 参照)登場しました [81]。
12/3	Kubernetes	CVE-2018-1002105	コンテナ管理ソフトウェア Kubernetes に深刻な権限昇格の脆弱性が発見されました。Gravitational 社が、12/5 に PoC コードを公開しました [82]。また、12/9 に研究者が PoC のデモ動画を公開しました [83]。

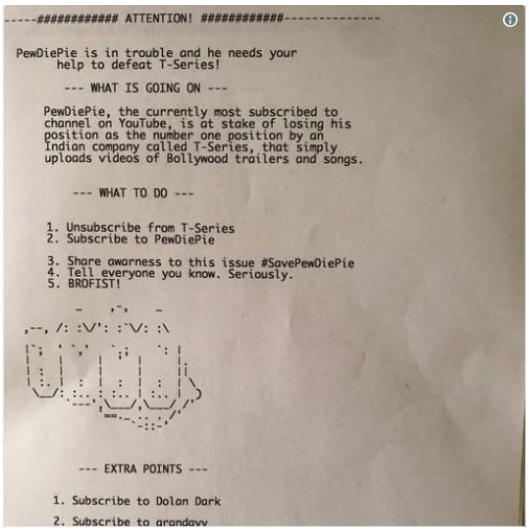

図 10 YouTube チャンネル PewDiePie の購読を呼びかけるスパムメッセージ [81]

図 11 プリンタにメッセージを印刷させるとうたうスパム業者

2.6. マルウェア

2.6.1. ランサムウェア

Sophos 社のレポートによれば、ランサムウェアは、従来の不特定多数を無差別に狙う攻撃から、特定のターゲットを狙う標的型攻撃に移行しつつあるそうです。攻撃者が手動で操作する対話型のランサムウェアも登場しており、1 件あたりの被害額が増大する傾向にあります [84]。

表 13 ランサムウェアの事例

日付	概要
10/25	新種のランサムウェア FilesLocker が RaaS(Ransomware as a Service)として提供されているのを、MalwareHunterTeam が発見しました。支払われた身代金のうち 60%が販売元の取り分になる、アフィリエイト方式で、中国語と英語のバージョンが存在します [85]。
11/25	アメリカ オハイオ州の医療機関がランサムウェアに感染しました [86]。
11/29	モスクワで初のケーブルカーが開業しましたが、開業翌日にランサムウェアに感染し、営業を停止しました。12/1 に営業を再開しました。 [87]。
12/5	中国で PC 10 万台以上がランサムウェアに感染しました。開発用ソフトウェア EasyLanguage に悪性のコードが注入され、同ソフトを用いて作成されたソフトがランサムウェアに感染しました。ランサムウェアはファイルを暗号化し、WeChat 経由で 110 元(1,700 円相当)の身代金支払いを求めるとともに、オンラインサービスの認証情報を盗みとるものでした(図 12 参照)。ランサムウェアは SNS サービスの Douban を用いて C&C サーバと通信していました。12/6 に中国政府はランサムウェア作成の容疑者を逮捕しました [88]。

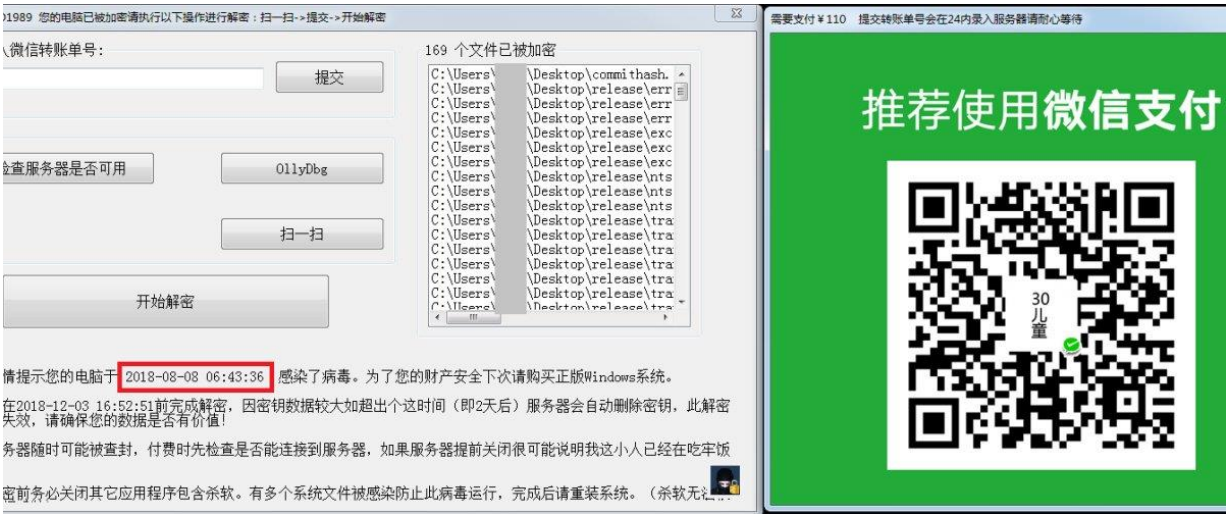

図 12 ランサムウェアが身代金の支払いを要求している画面 [88]

2.6.2. 重要インフラを標的とするマルウェア

電気、ガス、水道などの重要インフラがサイバー攻撃で機能を停止すると、市民生活や企業活動に影響が及び、生命の危機や、経済の損失につながります。

ESET 社は、マルウェア Industroyer と NotPetya のコードが似ている(図 13 参照)ことを発見し、10/11 に報告しました

[89]。サイバー犯罪集団 TeleBots(BlackEnergy)が上記の 2 つのマルウェアの開発に関与していました。 Industroyer は 2016 年にウクライナの電力施設への攻撃に使用され、停電を発生させました。一方、NotPetya は 2017 年に同じくウクライナを中心に流行し、政府や金融機関に被害を及ぼしました。

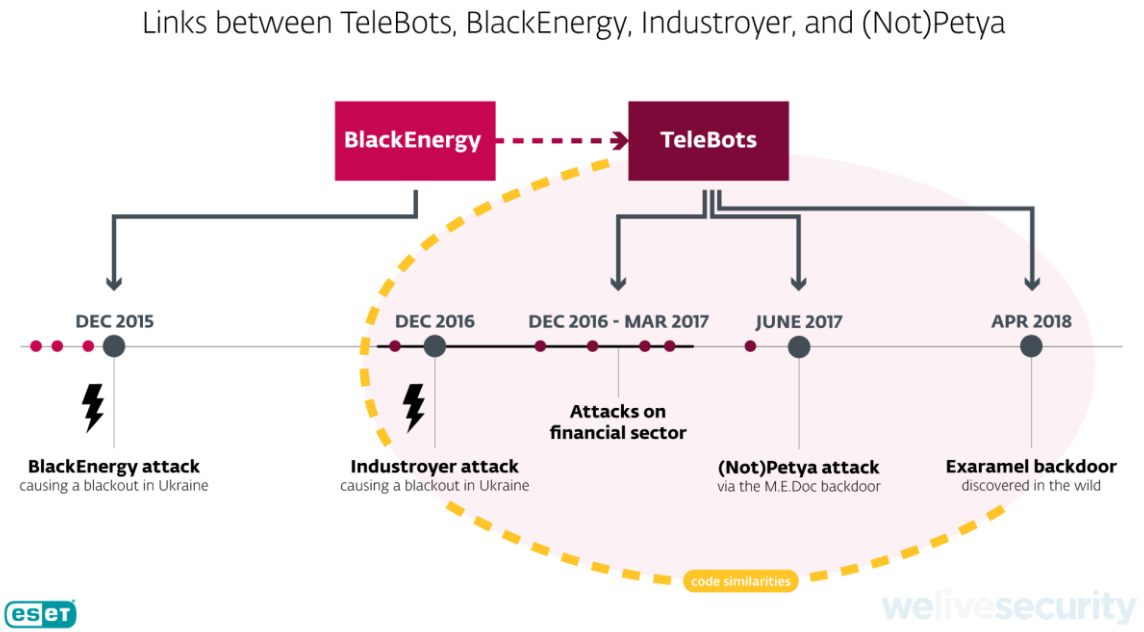

図 13 マルウェア Industroyer と NotPetya の関連性 [89]

表 14 重要インフラの攻撃事例

日付	概要
10/15	アメリカ ノースカロライナ州の水道局 ONWASA がマルウェア Emotet に感染しました。復旧のため同局はデータベースの再作成を強いられました [90]。
10/19	NSA から流出したとされるサイバー攻撃ツール DanderSpritz, FuzzBunch を悪用した攻撃を Kaspersky 社が報告しました。ロシア、イラン、エジプトの Windows 2003/2008 Server 50 台が感染しました。原子力発電、通信、IT、R&D 企業が標的になりました [91]。
10/31	イランのインフラ、戦略ネットワークが Stuxnet に類似したマルウェアの攻撃を受けたと、イスラエルのテレビ局が放送しました。Stuxnet は 2010 年にイランの核燃料施設への攻撃で使用されたマルウェアです [92]。
11/27	レバノン、UAE の政府関連サイトを狙ったマルウェアによる攻撃を Cisco 社が報告しました。DNS クエリを用いて C&C サーバと通信し、DNSリダイレクトでマルウェア配布サイトに誘導する手法でした [93]。

2.6.3. 金融機関、金融サービスを標的とするマルウェア

US-CERT が、サイバー攻撃集団 HIDDEN COBRA による ATM から不正に現金を引き出す活動 FASTCash の分析結果を 10/2 に公開しました。アメリカ政府は、HIDDEN COBRA を北朝鮮政府と関連付けています [94]。また FireEye 社が、10/3 にサイバー攻撃集団 APT38 に関するレポートを公開しました。レポートによれば、同グループは 2014 年以降に 13 ヶ国、16 以上の金融機関から 11 億ドル以上を盗んだとされます。APT38 は北朝鮮政府との関連を示唆されており、北朝鮮政府の外貨獲得が困難になると、サイバー攻撃が活発化するおそれがあります [95]。

表 15 金融機関への攻撃事例

日付	概要
10/2	バンキングマルウェア DanaBot がアメリカの金融機関にも標的を拡大したと CheckPoint 社が報告しました。DanaBot はオンラインバンキングの認証情報を盗むマルウェアで、従来はヨーロッパ、オーストラリアを標的にしていました [96]。
10/9	バンキングトロイ Panda Banker がアメリカ、カナダ、日本を標的に拡散していると Cylance 社が報告しました。クレジットカード、個人情報、暗号通貨のウォレットの情報などを盗み取ろうとしています [97]。
11/7	バンキングトロイの TrickBot が Windows の RAC[2]の情報も収集するようになりました。RAC には、ソフトウェアのインストール履歴や OS で発生したエラーなどが記録されています。作成者の意図は不明ですが、フィッシングメールなどの攻撃に悪用されるおそれがあります [98]。
11/16	サイバー攻撃集団 MoneyTaker と Silence による、ロシアの金融機関を標的にしたフィッシングメール攻撃を Group-IB 社が報告しました。フィッシングメールは、ロシアの中央銀行のメールを装っており、添付ファイルを開くとマルウェアに感染するものでした [99]。
11/20	Trend Micro 社は、サイバー攻撃集団 Lazarus が中南米の金融機関にバックドアをしかけた事実を発見して報告しました [100]。
11/22	Kaspersky 社が、バンキングトロイとランサムウェアの特徴をあわせ持つモバイルマルウェア「Rotexy」を報告しました。このマルウェアは、SMS を盗聴したり、デバイスを使用不能にしたりして、身代金を要求したりします。主にロシアのユーザを標的に、7 万回以上の攻撃が発生しました [101]。
12/6	Kaspersky 社が、東ヨーロッパの銀行へのサイバー攻撃を報告しました。攻撃者は、ネットブック、Raspberry Pi、Bash Bunny[3]を用いて銀行の LAN に侵入し、遠隔操作ツールをインストールしました [102]。
12/11	PayPal アカウントから金銭を盗む Android トロイの木馬を ESET 社が報告しました。Android トロイの木馬は、Android のアクセシビリティ機能を悪用して二要素認証をパスしました [103]。
12/11	サイバー犯罪集団 Cobalt が攻撃ツール ThredKit の新バージョンを利用し、バックドアをインストールする悪性の Office 文書を作成しています。Cobalt は金融機関のネットワークへの侵入を得意としています [104]。
12/19	Menlo Security 社が、アメリカ、イギリスの金融機関を狙ったメールによる攻撃を報告しました。メールの添付ファイルを実行すると、遠隔操作ツールに感染します [105]。

2.6.4. その他マルウェア

表 16 その他マルウェアの事例

日付	概要
10/11	Cisco 社は、攻撃者が動的にコードを変更できる新種の Android トロイの木馬を発見したと報告しました。このマルウェアは、“Google Play Market”に偽装して感染し、遠隔でプラグインを挿入する、新しい.NET のソースコードをコンパイルして導入するといった機能を持っています。[106](図 14 参照)。

[2] Reliability Analysis Component
[3] USB メモリを模した機器で、接続先の機器でプログラムを実行できる。

10/11	Microsoft Office の数式エディタの脆弱性 CVE-2017-11882 を悪用する攻撃を発見したと SANS が報告しました。メールに悪性の文書を添付し、トロイの木馬 Razy に感染させる手口でした [107]。
10/24	ブラジルの郵便サービスを装うメールでマルウェアに感染させる攻撃を TrendMicro 社が報告しました。Windows の正規プログラムである、wmic, certutil を用いる点が特徴的でした [108]。
11/19	ドライブシミュレータアプリを装う偽アプリが Google Play で配布されているのを ESET の研究者が発見しました。偽アプリは 13 個あり、合計 56 万回以上ダウンロードされていました [109]。
11/27	悪性の PowerShell スクリプトによる、イタリアを狙ったスパムメール攻撃を Yoroi 社が報告しました。感染したマシンの情報を収集したり、スクリーンショットを採取したりします [110]。
11/27	リムーバブルメディアを介して感染するワームを Trend Micro 社が報告しました。Autoit[4]言語でコンパイルされたファイルレス型のマルウェアで、キーロガーや DDoS ツールとして動作します [111]。
11/28	工業分野を狙った AutoCAD ベースのマルウェアについて Forcepoint 社が報告しました。マルウェア本体はLisp言語で記述されていて、産業スパイ活動を行っていました。中国、インド、トルコ、UAEに感染が拡大していました [112]。
12/11	家庭、SOHO ルータを標的とする新種のエクスプロイトキット Novidade を Trend Micro 社が報告しました。CSRF 脆弱性をついてルータの DNS 設定を書き換え、ルータ配下の利用者を悪性サイトへ誘導します [113]。

図 14 “Google Play Market”に偽装したマルウェア(左側) [106]

[4] Windows 用のプログラミング言語で、主な用途は GUI の自動操作。コンパイル済みのプログラムは、Autoit ランタイムの無いマシンでも動作できる。

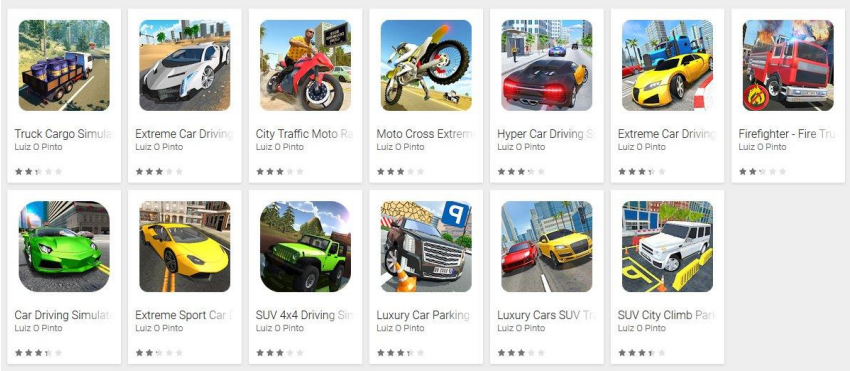

図 15 ドライブシミュレータを装う偽 Android アプリ [109]

2.6.5. マルウェア対策

アメリカ司法省は、3ve(発音は「イブ」)が関係者の逮捕やドメインの差し押さえにより、広告詐欺ボットネットを停止したと発表しました [114]。3ve は不正な広告収入やマルウェア感染、BGP ハイジャックなどに利用されていました。広告詐欺による被害は、2,900 万ドルと推定されています [115](図 16 参照)。

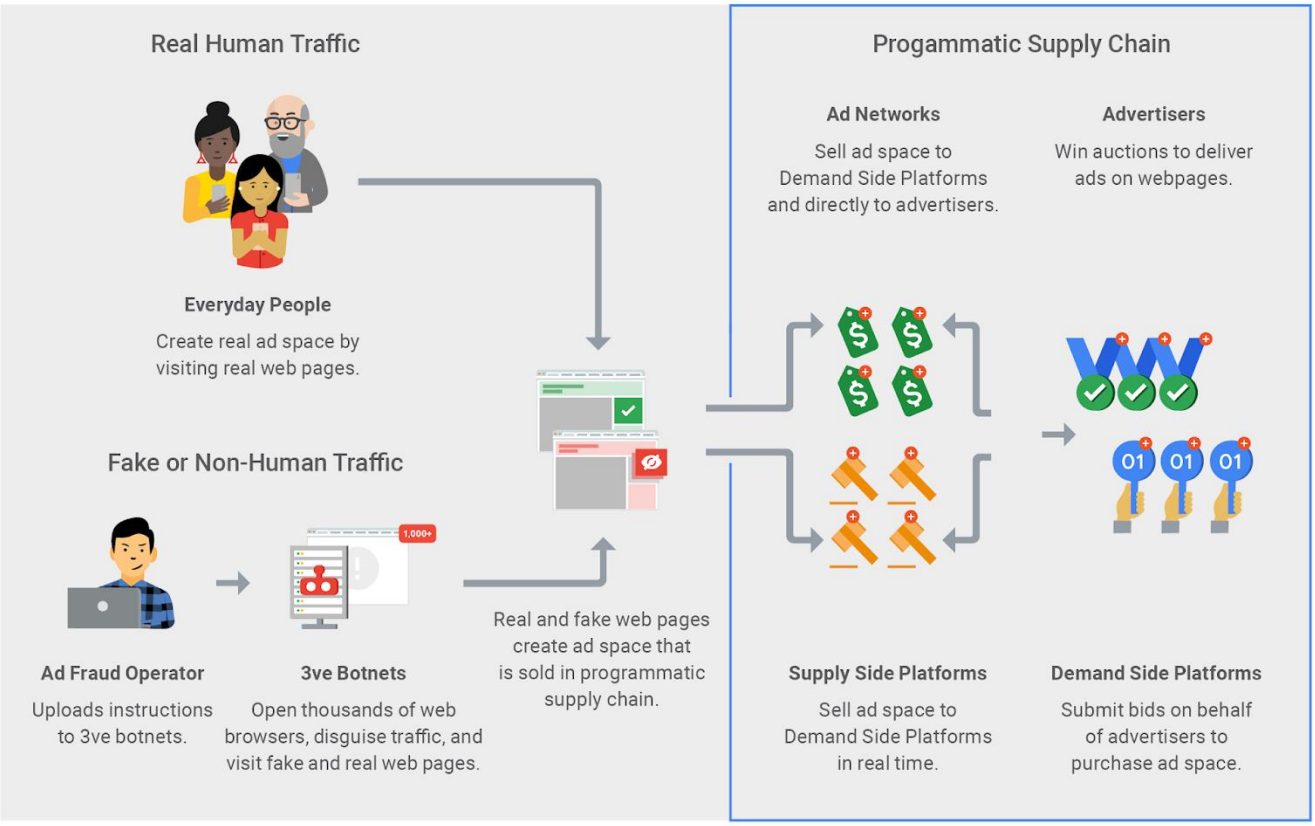

図 16 ボットネット 3ve の挙動 [115]

表 17 マルウェア対策の事例

日付	概要
10/16	ヒズボラ[5]がマルウェア配布に利用していたサーバを閉鎖したと、チェコの情報機関が発表しました。ヒズボラはマルウェアを用いて、標的のモバイルデバイスから情報を盗んでいました［116］。
10/25	シリア内戦の犠牲者向けに、ESET 社がランサムウェア GandCrab の復号ツールを公開しました。GandCrab の作者がダークフォーラムで復号鍵を開示したことを受け、作成されたツールです。
11/8	アメリカ サイバー軍(USCYBERCOM)が、マルウェア解析サイトの VirusTotal にマルウェアのサンプルを提供しました。最初に提供されたものは LoJack というマルウェア種で、Fancy Bear[6]がしばしば用いるものです。
12/5	Blackhat Europe で新しいマルウェア分析サービス SNDBOX が発表されました。無料で利用できるサービスで、機械学習を利用した静的解析、動的解析を行えます［117］。

2.7. IoT

スマートスピーカーやカメラなど、インターネットに常時接続している IT 機器が増加しています。それに伴い、IT 機器に関係したインシデントが増加しています。これら機器に以下のようなセキュリティ面の不備があると、不正アクセスのきっかけになります。

- ファームウェアに脆弱性がある。開発元が修正プログラムを提供していないケースと利用者が修正プログラムを適用していないケースがある。
- 機器の管理用画面にアクセスするパスワードに脆弱なものが設定されている。
- 不要なサービスが動作している。

管理しなければならない IT 機器の台数が多くなり、管理対象から漏れたり、修正を忘れやすくなったりしていることも、インシデント増加の背景になっています。

表 18 IoT への攻撃事例

日付	概要
10/9	中国 Hangzhou Xiongmai Technology 製の監視カメラに深刻な脆弱性を発見したと、SEC Consult 社が報告しました。報告内容には、脆弱な管理者パスワード、平文での通信、ファームウェア更新の脆弱性などが含まれています。報告者は世界で同社機器約 900 万台が稼動していると推定しています［118］。
10/30	CyberX 社が、過去 12 ヶ月間、850 企業を対象にした産業制御システム、IoT に関する脅威レポートを公開しました。調査対象のネットワークのうち、69%で平文のパスワードやりとり、40%でインターネットとの直接の通信、57%でウイルス対策ソフトの保護不備といった問題がありました［119］。

[5] レバノンを拠点に活動しているシーア派のテロ組織。
[6] ロシア政府との関連を疑われている集団。別名 APT 28, Sofacy。

2.8. 政府、公共機関、事業者のセキュリティ施策

表 19 セキュリティ施策の事例

日付	概要
10/22	金融庁が中小金融機関のサイバーインシデント対応能力の底上げのため、「金融業界横断的なサイバーセキュリティ演習」を開催しました。最近の業界動向もふまえ、暗号通貨取引事業者や FX 事業者も参加しました [120]。
11/2	NIST が CVSS のスコア算定に IBM 社の Watson を利用する計画があると報道されました。CVSS スコアは攻撃の複雑性や、リスクの大きさに応じて計算されます。機械学習の採用により、スコア算定の時間短縮が期待されます [121]。
12/12	IPA は、Web サイトの脆弱性や運用管理の不備を悪用された情報漏えい、Web ページの改ざんなどの被害が増加しているため、「安全なウェブサイトの運用管理に向けての 20 ヶ条」(図 17 参照)を公開しました。[122]。

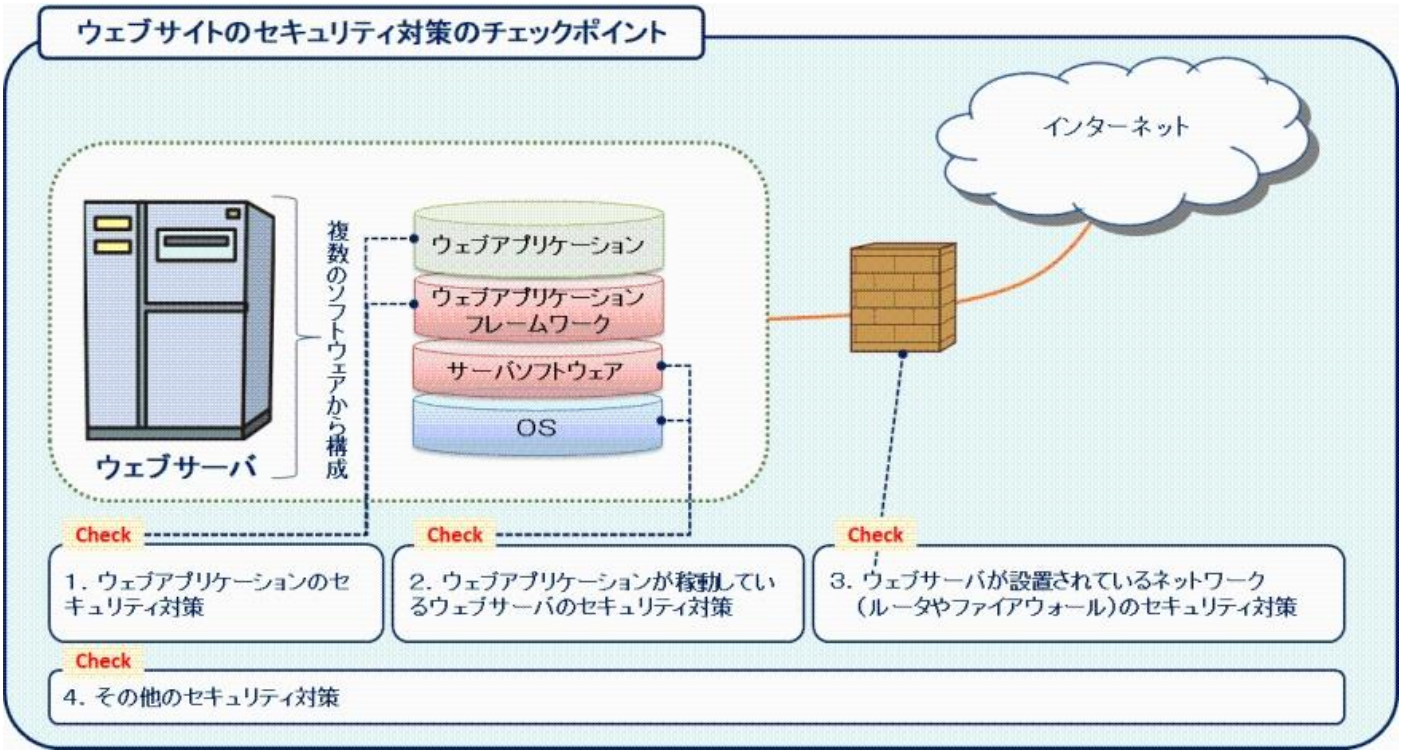

図 17 Web サイトのセキュリティ対策のチェックポイント [122]

3. 2018 年度 第 4 四半期以降の予測

暗号通貨の市場価格の下落により、攻撃者が不正マイニングで利益を得にくい状況が続いています。攻撃者も投資対効果を重視するため、暗号通貨の不正獲得に割いていたリソースを、別の不正な利益獲得手段へ振り替えます。NTTDATA-CERT は、パスワードリスト攻撃[7]などで不正に取得した認証情報を用いた以下のような攻撃が増加すると、予測しています。

- 不正送金を狙ったビジネスメール詐欺
  不正に取得した認証情報を使って、取引先や経理部門になりすましたメールを送信して送金をさせる。特に企業での利用が増加している Office 365 サービスを狙ったビジネスメール詐欺が増加する。
- 脅迫による金銭要求
  不正に取得した認証情報を使って、企業内のユーザの PC やサーバへ不正ログインし、メールの添付ファイルやオンラインストレージの文書を盗む。盗みだした情報を流出させると企業を脅迫して金銭を得る。
- 不正購入
  不正に取得した他人の認証情報を使って、他人になりすましてオンラインショッピングサイトへ不正ログインし、換金性の高い商品やサービスを購入して転売する。企業メールアドレスを使ってオンラインショッピングサイトを利用している従業員は一定数存在するので、注意が必要。

従業員にパスワードの使い回しをさせず、認証の強度を高める多要素認証やリスクベース認証などを導入することで、企業はこのような攻撃を防ぎ、被害を軽減できます。

[7] インターネット上に流出したユーザ名とパスワードの組を用い、Web サービスへの不正ログインを試みること。

4. 2018 年度 第 3 四半期のタイムライン

※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内　▲■◆●:世界共通・国外　△▲:脆弱性　□■:事件、事故　◇◆:脅威　○●:対策

2Q　10月　11月　12月

[A] 暗号通貨

- ◆ 11/12 ロシア製マイニングマルウェア「WebCobra」
- ■ 10/21 Trade.io不正アクセス コールドウォレットから750万ドル相当流出
- ■ 11/19 Webサイト「Make-A-Wish」が不正アクセスを受けマイニングスクリプトが挿入された
- ■ 10/28 MapleChange不正アクセス 600万ドル相当流出
- ■ 11/22 標的の携帯電話をSIMスワッピングによって乗っ取り、約100万USD相当の仮想通貨を窃取
- ■ 11/1 聖フランシスコ・ザビエル大学、クリプトマイニング呼ばれる攻撃を受け、ネットワークを遮断した
- ■ 11/27 event-streamというnpmパッケージにcopayというBitcoinウォレットからクレデンシャルを盗む攻撃コードが混入された
- ■ 11/8 ウェブ解析プラットフォーム「StatCounter」が不正アクセスを受け「Gate.io」のビットコイン取引を乗っ取るコードが挿入された
- ◆ 10/11 Flash Playerのアップデートを騙り、暗号通貨マイニングを行うマルウェア「XMRig」をインストールさせる攻撃キャンペーンを観測
- ◆ 11/16 enSilo社、暗号通貨マイニングやランサムウェアなどを実行するマルウェアキャンペーン「DarkGate」観測
- ◆ 10/25 誤ってREST APIが公開されているDockerコンテナを狙いマイニングマルウェア「XMRig」を感染・拡大を行う攻撃キャンペーンを観測
- ◆ 12/10 バックドア「EmPyre」とマイニングマルウェア「XMRig」を組み合わせた新種のMacマルウェア「DarthMiner」を発見

[B] マルウェア

- ◆ 10/11 新種 GPlayed Banking
- ◆ 10/19 Azorult v3.3
- ◆ 10/25 新種 demonbot
- ■ 10/15 米東海岸の上下水道局「ONWASA」がマルウェア「Emotet」経由でランサムウェア「Ryuk」感染した
- ◆ 10/11 数式エディタの脆弱性を利用しトロイの木馬「Razy」を感染させる攻撃キャンペーンを観測
- ◆ 10/31 Emotetが感染マシンのメール本文を盗み取るように進化した
- ◆ 10/11 広告収入を目的とした採掘できない暗号通貨を採掘すると偽るAndroidアプリを発見
- ◆ 10/15 ウクライナセキュリティサービスは、ウクライナ政府機関の情報通信システムを狙う、攻撃グループ「BlackEnergy」によるバックドア「Industroyer」を感染させる新たな標的型攻撃を発見
- ◆ 10/15 Kaspersky Labは、中央アジアの外交機関を狙い、攻撃グループ「DustSquad」がトロイの木馬「Octopus」を感染させる攻撃キャンペーンを観測
- ◆ 10/16 Cisco TalosはWordの脆弱性を利用しマルウェア「Agent Tesla」「Loki」「Gamarue」を感染させる攻撃キャンペーンを観測
- ◆ 10/17 イタリアの海軍産業狙い、マルウェア「MartyMcFly」を感染させる攻撃キャンペーンを発見
- ◆ 10/24 Windowsの正規機能「WMIC」および「CertUtil」を利用しブラジルのユーザを狙うマルウェアを発見
- ◆ 10/30 攻撃グループ「Cobalt」による金融機関を狙った、新型EK「ThreadKit」に感染させる攻撃キャンペーンを観測
- ● 10/16 チェコのintelligenceチームがヒズボラのハッキングサーバーを閉鎖した
- ● 11/8 アメリカのサイバー軍は発見した未分類のマルウェアサンプルを共有するため、VirusTotalにマルウェアサンプルを提供すると発表した
- ◆ 11/16 新種 tRat
- ◆ 11/27 亜種 Bladabindi
- ◆ 11/29 新種 CARROTBAT
- ◆ 12/11 新種EK「Novidade」
- ◆ 11/27 イタリアのユーザーを狙い、Powershellを利用したマルウェア「SLoad」に感染させる攻撃キャンペーンを観測
- ◆ 11/28 CADソフト「AutoCAD」を利用する企業を狙った攻撃キャンペーンを観測
- ◆ 11/29 中東を狙いマルウェア「DNSpionage」を感染させる攻撃キャンペーンを観測
- ◆ 12/4 イタリアのユーザーを狙い、マルウェア「Ursnif」の亜種に感染させる攻撃キャンペーンを観測
- ◆ 12/10 バックドア「EmPyre」とマイニングマルウェア「XMRig」を組み合わせた新種のMacマルウェア「DarthMiner」を発見
- ◆ 12/14 攻撃グループ「Sofacy」による世界中の政府機関を狙った、バックドア「Zebrocy」と新種のマルウェア「Cannon Trojan」に感染させる攻撃キャンペーンを観測
- ◆ 12/20 イタリアのユーザーを狙い、マルウェア「Danabot」の亜種に感染させる攻撃キャンペーンを観測
- ● 11/27 米国の法執行当局は広告詐欺ボットネット「3ve」をテイクダウンしたと発表した
- ● 12/5 Blackhat EuropeでAIを利用したマルウェア解析サイト「SNDBOX」を立ち上げた

※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内　△▲:脆弱性　◇◆:脅威
▲■◆●:世界共通・国外　□■:事件、事故　○●:対策

2Q　10月　11月　12月

[C]ランサムウェア

- ◆ 10/21 Kraken Cryptor Ransomware v2.0.6
- ◆ 11/22 亜種Zorro Ransomware
- ◆ 10/30 新種CommonRansom
- ■10/16 米東海岸の上下水道局「ONWASA」がマルウェア「Emotet」経由でランサムウェア「Ryuk」感染した
- ■ 11/25 イーストオハイオ州立病院とオハイオバレーメディカルセンターがランサムウェアに感染しER患者の受け入れを中断した
- □ 10/23 宇陀市立病院がランサムウェア「GandCrab」に感染した
- ■ 11/29 モスクワのケーブルカーシステムがランサムウェアに感染した
- ■ 10/23 米Indiana州軍がランサムウェアに感染した
- ■12/5 中国で汚染された開発環境で作られたソフトウェアにより10万台を超えるPCにランサムウェアが感染した
- ■ 11/8 マレーシアのMedia Prima Bhdがランサムウェアに感染した
- ◆ 10/4 「Fallout Exploit Kit」が配布するランサムウェアが「GandCrab」から「Kraken Cryptor Ransomeware」に替わった
- ◆ 11/16 enSilo社、暗号通貨マイニングやランサムウェアなどを実行するマルウェアキャンペーン「DarkGate」観測
- ◆ 12/26 IPMIカードを介して感染するランサムウェア「JungleSec」を発見
- ◆ 10/25 ランサムウェア「FilesLocker」がRansomware as a Serviceとして提供されているのを発見
- ● 10/25 Bitdefender社が、ランサムウェア「GandCrab」の復号ツールの最新版を公開した

[D]IoT機器

- ▲ 11/1 TI製BLEチップの脆弱性「BLEEDINGBIT」CVE-2018-16986、CVE-2018-7080
- ◆ 10/24 Sophos LabsはLinux SSHサーバやLinuxを搭載したIoTデバイスを狙うボットネット「Chalubo」を発見
- ◆ 11/1 トレンドマイクロは脅威グループ「Outlaw」がLinux、Windows、Androidデバイスを標的とするIRCボット「Shellbot」を発見
- ◆ 11/7 Qihoo 360社はルータ10万台以上で構成されるBroadCom製のUPnP機能を有効にしたルータを狙ったボットネットを発見
- ● 9/28 カリフォルニア州で米国初となるIoTセキュリティ法が成立した
- ○ 11/27 IPAは「中小規模向けIoT品質確認チェックリスト」を公開した

[E]重要インフラを標的にした攻撃

- ■10/15 米東海岸の上下水道局「ONWASA」がマルウェア「Emotet」経由でランサムウェア「Ryuk」感染した
- ◆ 10/16 重要インフラを狙う新たな攻撃グループ「GreyEnerg」を発見
- ◆ 12/12 McAfeeは重要インフラを標的とし、マルウェア「Rising Sun」を感染させる攻撃キャンペーン「Operation Sharpshooter」を観測
- ○ 10/3 警察庁は重要インフラの基幹システムに対するサイバー攻撃の訓練を実施した
- ○ 12/5 重要インフラ企業、サイバー対策の関連業者らでつくる協議会の新設を柱とする「改正サイバーセキュリティ基本法」が成立した
- ○ 10/15 IPAは「制御システムのセキュリティリスク分析ガイド 第2版」を公開した
- ○ 12/13 NISCは重要インフラ14分野による分野横断的演習を実施した

※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内　△▲:脆弱性　◇◆:脅威
▲■◆●:世界共通・国外　□■:事件、事故　○●:対策

2Q　10月　11月　12月

[F] フィッシング

- ◆ 10/4 Netskopeは、米法律事務所の顧客基盤を対象にAzureのBlob Storageサービスを利用したフィッシング攻撃を観測
- ◆ 10/12 Booksellerは、出版社を狙う世界的なフィッシング詐欺が急増していると発表した
- ◆ 10/28 Yoroi CERTは、イタリアの海軍及び防衛産業企業に対するフィッシング攻撃を観測
- ◇ 11/14 フィッシング対策協議会は、Appleを装ったフィッシング攻撃に関する注意喚起を行った
- ◆ 11/16 Group-IBは、ロシアの金融機関を狙った攻撃グループ「MoneyTaker」と「Silence」による大規模なフィッシングキャンペーンを観測
- ◆ 11/19 FireEye社は、シンクタンク、法執行機関、メディア、米軍、交通機関、医薬品業界、国家政府等に対するAPT29のフィッシングメールキャンペーンを観測
- ◆ 11/25 AppRiver社は、ストリーミングサービスSpotifyを対象としたフィッシングキャンペーン観測
- ◆ 11/25 AGARI社は、米カリフォルニア州の大規模森林火災に乗じたビジネスメール詐欺を発見
- ◆ 11/29 Palo Alt Networks社は、主に韓国と北朝鮮地域をターゲットにし、カスタムドロッパー「CARROTBAT」を活用した新たなフィッシングキャンペーンを観測
- ◇ 12/10 一部のソフトバンクユーザーにソフトバンクをかたった通信障害の補填に関するメールが届いた
- ◆ 12/16 ISC Handlersは、Office 365からの配信不能通知を装しログイン資格情報を盗もうとするフィッシングキャンペーンを観測
- ◆ 12/19 Menlo Securityは、米国、英国の金融機関を対象にGoogle Cloud Storageサービスを利用したフィッシングキャンペーンを観測
- ◆ 12/20 Amazonの注文確認を装うフィッシングキャンペーンを観測

[G] 金融機関を狙った攻撃

- ◆ 10/2 バンキングマルウェア「DanaBot」を用い米国の銀行を標的とした攻撃キャンペーンを観測
- ◆ 10/2 US-CERTは、FASTCashと呼ばれるATMから現金を奪う活動の背後に北朝鮮の攻撃グループ「HIDDEN COBRA」が確認された
- ◆10/9 バンキングマルウェア「Panda Banker」を用いアメリカ、カナダ、日本のユーザを対象に「銀行、クレジットカード、ウェブウォレット」に関する情報を狙う攻撃キャンペーンを観測
- ○ 10/22 金融庁と金融機関はサイバー攻撃への対応を確認する訓練を実施した
- ◆ 11/16 Group-IBは、ロシアの金融機関を狙った攻撃グループ「MoneyTaker」と「Silence」による大規模なフィッシングキャンペーンを観測
- ◆ 11/20 TrendMicro社は、Lazarusが中南米の金融機関に攻撃を仕掛けバックドアを設置することに成功したと報じた
- ◆ 11/22 モバイルマルウェア「Rotexy」がバンキングトロイとランサムウェアの機能を併せ持つマルウェアに進化した
- ◆ 12/19 Menlo Securityは、米国、英国の金融機関を対象にGoogle Cloud Storageサービスを利用したフィッシングキャンペーンを観測
- ◆12/11 公式のPayPalアプリを標的とし、PayPalの2要素認証を回避するAndroidユーザーを狙ったトロイの木馬を発見

[H] サプライチェーン

- ■10/18 VestaCPの公式配布版が改ざんされDoS攻撃やサプライチェーン攻撃の一端を担わされた。
- ■10/27 Pythonパッケージを管理するためのサービスPyPIに、不正なコードを含む12のライブラリがアップロードされた。
- ■ 11/27 event-streamというnpmパッケージにcopayというBitcoinウォレットからクレデンシャルを盗む攻撃コードが混入された
- ■12/5 中国で汚染された開発環境で作られたソフトウェアにより10万台を超えるPCにランサムウェアが感染した

※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内　▲■◆●:世界共通・国外　△▲:脆弱性　□■:事件、事故　◇◆:脅威　○●:対策

2Q　10月　11月　12月

[I]情報漏えい

不正アクセス

- ■ 10/13 米国防総省、米軍および民間人員の「個人情報及びクレジットカード」3万件漏えいの可能性
- ■ 10/24 キャセイパシフィック航空、「個人情報」940万人分漏えいの可能性
- ■ 11/1 ユーロスター、「顧客アカウント」が漏えいの可能性。顧客のパスワードリセットを実施
- ■ 11/1 Radisson Hotel Group、「個人情報」が漏えい。漏えいしたユーザ数は非公開
- □ 11/22 日本貿易振興機構、「個人情報」が漏えいの可能性
- ■ 11/28 米医療グループAtrium Health、「個人情報」265万件漏えい
- ■ 11/30 Marriott、「個人情報」5億件漏えい
- 12/3 米Oregon州と米Maryland州で1件ずつ訴訟が発生した
- ◆ 12/5 Reutersは中国のハッカーによるサイバー攻撃であると報じた
- ■ 11/16イタリアの国家機関、サイバー犯罪集団「Anonymous」から攻撃を受け「個人情報」が公開された
- ◆ 11/14 InfowarsのWebサイトで、Magecartのクレジットカードスキミング攻撃が検出された
- ● 11/15 Firefox Quantumに以前にデータ侵害があったサイトを訪問したとき警告を表示する機能が実装された
- ■ 12/4 全米共和国議会委員会は、4人の上級補佐官の電子メールアカウントが数ヶ月にわたって監視されていたと報じた
- ■ 12/13 フランスの外務省は、緊急連絡先データベースより「個人情報」54万件漏えいしたと報じた

設定不備

データベース

- ■ 11/8 Amex India、 MongoDB にある「個人情報」70万件が公開されていた
- ■ 11/19 米通信事業者のVoxoxは、データベースの設定ミスにより「個人情報、パスワードリセットリンク、2FAコード」などを含む2600万件のSMSメッセージが漏えい
- ■ 12/6 MongoDBの設計不備により「個人情報」6600万件が公開されているのを発見

Elasticsearch

- ■ 11/29 米国市民の「個人情報」1億1400万件のデータベースが公開されているのを発見
- ■ 11/29 SKY Brasil、「個人情報」3200万件のデータベースが公開されているのを発見
- ■ 11/22 米国郵政公社、 Webサービスで「個人情報」6000万件が公開されていた
- ■ 11/22 米国や英国のAmazonで手違いにより「ユーザの名前やメールアドレス」が公開された
- ● 11/15 Amazon Web Servicesは、Amazon S3のバケット設定の誤りによる偶発的なデータ漏えいを防ぐ機能をリリースした

- ○ 10/18 総務省はグーグルなど米国の巨大ＩＴ企業「プラットフォーマー」への規制の在り方などを議論する研究会の初会合を開いた
- ● 11/1 カナダで個人情報保護と電子文書法「PIPEDA」の施行開始した
- ○ 12/12 IPAが「安全なウェブサイトの運用管理に向けての20ヶ条」を公開した

※タイムラインに記載している日付は、事象発生日ではなく、記事掲載日の場合があります。

△□◇○:国内　△▲:脆弱性　◇◆:脅威
▲■◆●:世界共通・国外　□■:事件、事故　○●:対策

2Q　10月　11月　12月

[I]情報漏えい

facebook

- ■ 9/28「View As」機能の脆弱性により、「アクセストークン」5000万件漏えい。予防措置として他の4000万アカウントもリセットした
- 9/29 漏えいの数時間後に2名のFacebookユーザにより訴訟を起こされた
- ■ 10/12 実際に被害をうけたユーザは2900万人であった。うち1500万人は「ユーザ名と連絡先」、1400万人は「ユーザ名、性別、国籍/言語、宗教、生年月日」などが漏えいした
- ◇ 10/15 facebook社から日本政府の個人情報保護委員会に日本人の情報も流出した可能性があるという報告があった
- □ 10/16 日本の利用者に、実際にfacebookで使用していたパスワードが記された脅迫メールが送りつけられた
- ○ 10/22 日本政府の個人情報保護委員会が、Facebookに対して行政指導を行った
- ● 10/24 イギリスの情報コミッショナー事務局が、ユーザーデータの収集をめぐってFacebookに50万ポンドの罰金を科した
- ■ 11/2 BCCが、ダークウェブで8万1000件のFacebookアカウントの「個人情報」が漏えいしていると報じた
- ◆ 12/14 Facebookは、ソフトウェアの不具合により、最大680万人のスマートフォン内の画像が外部アプリケーション開発者に流出しかねない状況にあったと発表した

google

- ■ 10/8「Google+」のAPIの脆弱性により、「個人情報」50万件漏えい。2019/08末迄にGoogle+のサービスを終了を決定した
- 10/11 米上院の共和党議員が、Google社に対しSNS「Google+」における問題の公表が遅れた理由などについて、説明を求める書簡を送付した
- ◆ 12/15「Google+」のAPIの脆弱性により、「個人情報」5250万件が漏えいする恐れがあったと発表した。2019/04末にサービス終了を早めることを決定した

5. 参照文献

[1] 日本経済新聞社,“1400 万人の重要情報盗み見される フェイスブック,” 13 10 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO36460990T11C18A0MM0000/.

[2] BBC Russian Service,“Private messages from 81,000 hacked Facebook accounts for sale,” 2 11 2018. [オンライン]. Available: https://www.bbc.com/news/technology-46065796.

[3] 日本経済新聞,“FB、スマホ内の写真が流出の恐れ 最大 680 万人影響も,” 15 12 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO38989240V11C18A2000000/.

[4] 個人情報保護委員会,“個人情報の保護に関する法律に基づく指導について,” 22 10 2018. [オンライン]. Available: https://www.ppc.go.jp/news/press/2018/20181022/.

[5] CNET,“Facebook hit with $645,000 fine in UK over Cambridge Analytica scandal,” [オンライン]. Available: https://www.cnet.com/news/uk-information-commissioners-office-hits-facebook-with-645000-fine/.

[6] Facebook,“Security Update,” 28 9 2018. [オンライン]. Available: https://newsroom.fb.com/news/2018/09/security-update/.

[7] BLEEPING COMPUTER,“Google+ Shutting Down After Bug Leaks Info of 500k Accounts,” 8 10 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/google-shutting-down-after-bug-leaks-info-of-500k-accounts/.

[8] ZDNet,“New Magecart hack detected at Shopper Approved,” 9 10 2018. [オンライン]. Available: https://www.zdnet.com/article/new-magecart-hack-detected-at-shopper-approved/.

[9] AP NEWS,“Pentagon reveals cyber breach of travel records,” 13 10 2018. [オンライン]. Available: https://www.apnews.com/7f6f4db35b0041bdbc5467848225e67d.

[10] CATHAY PACIFIC,“Data security event,” 24 10 2018. [オンライン]. Available: https://infosecurity.cathaypacific.com/en_HK.html.

[11] Security Affairs,“New attack by Anonymous Italy: personal data from ministries and police have been released online,” 6 11 2018. [オンライン]. Available: https://securityaffairs.co/wordpress/77717/hacktivism/anonymous-italy-attacks.html.

[12] Security Affairs,“689,272 plaintext records of Amex India customers exposed online,” 8 11 2018. [オンライン]. Available: https://securityaffairs.co/wordpress/77815/data-breach/amex-india-data-leak.html.

[13] BLEEPING COMPUTER,“Infowars Store Affected by Magecart Credit Card Stealing Hack,” 14 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/infowars-store-affected-by-magecart-credit-card-stealing-hack/.

[14] BLEEPING COMPUTER,“US Postal Service Exposes Data of 60 Million Users for Over a Year,” 22 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/us-postal-service-exposes-data-of-60-million-users-for-over-a-year/.

[15] BLEEPING COMPUTER, “Marriott Data Breach Affects 500 Million Starwood Guests,” 30 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/marriott-data-breach-affects-500-million-starwood-guests/.

[16] Help Net Security, “Health websites routinely share your activity with 57 third-parties,” 9 10 2018. [オンライン]. Available: https://www.helpnetsecurity.com/2018/10/09/health-websites-privacy/.

[17] 産経新聞, “グーグルなどへの規制強化も 総務省研究会が初会合,” 18 10 2018. [オンライン]. Available: https://www.sankei.com/economy/news/181018/ecn1810180016-n1.html.

[18] ZDNet, “Android news and kids apps contain the most third-party trackers,” 18 10 2018. [オンライン]. Available: https://www.zdnet.com/article/android-news-and-kids-apps-contain-the-most-third-party-trackers/.

[19] CNET, “Location data from a gas station app sold for $9.50 per 1,000 people,” 10 12 2018. [オンライン]. Available: https://www.cnet.com/news/location-data-from-a-gas-station-app-sold-for-9-50-per-1000-people/.

[20] IPA 独立行政法人 情報処理推進機構, “宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhone も標的に～ 不審アプリのインストールに加えて、フィッシングにも注意！ ～,” [オンライン]. Available: https://www.ipa.go.jp/security/anshin/mgdayori20181129.html.

[21] 日本サイバー犯罪対策センター事務局, “不正送金等の犯罪被害につながるメールに注意,” 7 11 2016. [オンライン]. Available: https://www.jc3.or.jp/topics/virusmail.html.

[22] 佐川急便株式会社, “佐川急便を装った迷惑メールにご注意ください,” 10 10 2018. [オンライン]. Available: http://www2.sagawa-exp.co.jp/whatsnew/detail/721/.

[23] 時事通信社, “佐川急便かたるメールに注意,” [オンライン]. Available: https://www.jiji.com/jc/p?id=20180817082809-0027960591.

[24] Netskope, “Phishing in the public cloud: You’ve been served,” 3 10 2018. [オンライン]. Available: https://www.netskope.com/blog/phishing-in-the-public-cloud.

[25] Bleeping Computer, “Phishing Attacks Distributed Through CloudFlare’s IPFS Gateway,” 4 10 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/phishing-attacks-distributed-through-cloudflares-ipfs-gateway/.

[26] Menlo Security, “A ″JAR″ Full of Problems for Financial Services Companies,” 19 12 2018. [オンライン]. Available: https://www.menlosecurity.com/blog/a-jar-full-of-problems-for-financial-services-companies.

[27] PhishLabs, “49 Percent of Phishing Sites Now Use HTTPS,” 6 12 2018. [オンライン]. Available: https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https.

[28] ZDNet, “Trade.io loses $7.5Mil worth of cryptocurrency in mysterious cold wallet hack,” 22 10 2018. [オンライン]. Available: https://www.zdnet.com/article/trade-io-loses-7-5mil-worth-of-cryptocurrency-in-mysterious-cold-wallet-hack/.

[29] “MapleChange Crypto Exchange Hacked For Bitcoin (BTC),” 30 10 2018. [オンライン]. Available: https://ethereumworldnews.com/maplechange-crypto-exchange-hacked-for-913-bitcoin-btc-exit-scam-likely/.

[30] 株式会社 Doctor Web Pacific, “Doctor Web による報告:オンラインスキャマーにより 24,000 ドルを超える被害、被害者数は 10,000 人超え,” 19 10 2018. [オンライン]. Available: https://news.drweb.co.jp/show/?lng=ja&i=12886&c=5.

[31] ZDNet, “Hackers breach StatCounter to hijack Bitcoin transactions on Gate.io exchange,” 6 11 2018. [オンライン]. Available: https://www.zdnet.com/article/hackers-breach-statcounter-to-hijack-bitcoin-transactions-on-gate-io-exchange/.

[32] Ars Technica, “Widely used open source software contained bitcoin-stealing backdoor,” 27 11 2018. [オンライン]. Available: https://arstechnica.com/information-technology/2018/11/hacker-backdoors-widely-used-open-source-software-to-steal-bitcoin/.

[33] NEW YORK POST, “Man hacked into Silicon Valley execs’ phones to steal cryptocurrency: cops,” 20 11 2018. [オンライン]. Available: https://nypost.com/2018/11/20/man-hacked-into-silicon-valley-execs-phones-to-steal-cryptocurrency-cops/.

[34] ZDNet, “SIM-swapping 21-year-old scores $1 million by hijacking a phone,” 22 11 2018. [オンライン]. Available: https://www.zdnet.com/article/sim-swapping-21-year-old-scores-1-million-by-hijacking-a-phone/.

[35] 日経新聞社, “仮想通貨狙いウイルス作成疑い、家裁送致 名古屋地検,” 28 11 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO38288260Y8A121C1CN8000/.

[36] McAfee Labs, “McAfee Labs Threats Report December 2018,” 18 12 2018. [オンライン]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.

[37] Bleeping Computer, “CoinMiners Use New Tricks to Impersonate Adobe Flash Installers,” 11 10 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/coinminers-use-new-tricks-to-impersonate-adobe-flash-installers/.

[38] NICTER, “継続する 5555/TCP ポート宛攻撃通信と ADB が有効化された脆弱な Android エミュレータについて,” 22 10 2018. [オンライン]. Available: https://blog.nicter.jp/2018/10/android-5555/.

[39] JVN, “JVN#60702986,” 24 10 2018. [オンライン]. Available: https://jvn.jp/jp/JVN60702986/.

[40] TREND MICRO, “Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware,” 25 10 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/misconfigured-container-abused-to-deliver-cryptocurrency-mining-malware/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Anti-MalwareBlog+%28Trendlabs+Security+Intelligence+Blog%29.

[41] ST. FRANCIS XAVIER UNIVERSITY, “STFX SYSTEMS UPDATE,” 4 11 2018. [オンライン]. Available: https://www.stfx.ca/about/news/stfx-systems-update-0.

[42] McAfee, “WebCobra Malware Uses Victims’ Computers to Mine Cryptocurrency,” 12 11 2018. [オンライン]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/.

[43] Trustwave, “Hacker’s Wish Come True After Infecting Visitors of Make-A-Wish Website With Cryptojacking,” 19 11 2018. [オンライン]. Available: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hackers-wish-come-true-after-infecting-visitors-of-make-a-wish-website-with-cryptojacking/.

[44] Bloomberg Businessweek, “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies,” 4 10 2018. [オンライン]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2.

[45] Bloomberg Businessweek, “The Big Hack: Statements From Amazon, Apple, Supermicro, and the Chinese Government,” 4 10 2018. [オンライン]. Available: https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond.

[46] Amazon, “Setting the Record Straight on Bloomberg BusinessWeek’s Erroneous Article,” 4 10 2018. [オンライン]. Available: https://aws.amazon.com/jp/blogs/security/setting-the-record-straight-on-bloomberg-businessweeks-erroneous-article/.

[47] REUTERS, “中国による悪意のチップ埋め込み疑う根拠なし＝英政府機関,” 8 10 2018. [オンライン]. Available: https://jp.reuters.com/article/china-cyber-britain-idJPKCN1MI0B7.

[48] SCRIBD, “Letter October 8th Version,” 8 10 2018. [オンライン]. Available: https://ja.scribd.com/document/390401381/Letter-October-8th-Version.

[49] Bloomberg, “Senate Panel Seeks FBI Briefing on Super Micro Hacking Report,” 2 11 2018. [オンライン]. Available: https://www.bloomberg.com/news/articles/2018-11-01/senate-panel-seeks-fbi-briefing-on-super-micro-hacking-report.

[50] Super Micro, “Supermicro Refutes Claims in Bloomberg Article,” 11 12 2018. [オンライン]. Available: https://www.supermicro.com/newsroom/pressreleases/2018/press181004_Bloomberg.cfm.

[51] THE WALL STREET JOURNAL, “Washington Asks Allies to Drop Huawei,” 23 11 2018. [オンライン]. Available: https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105?tesla=y.

[52] REUTERS, “New Zealand rejects Huawei’s first 5G bid citing national security risk,” 28 11 2018. [オンライン]. Available: https://www.reuters.com/article/us-spark-nz-huawei-tech/new-zealand-government-agency-rejects-sparks-plan-to-use-huawei-5g-equipment-idUSKCN1NX08U?feedType=RSS&feedName=technologyNews.

[53] engadget, “ファーウェイ CFO がカナダで逮捕。米国からの要請、対イラン制裁に違反した疑い,” 6 12 2018. [オンライン]. Available: https://japanese.engadget.com/2018/12/05/cfo/.

[54] REUTERS, “英BT、5Gで華為製品使用せず　3G・4Gからも排除,” 6 12 2018. [オンライン]. Available: https://jp.reuters.com/article/bt-group-huawei-tech-idJPKBN1O42V1.

[55] RUTERS, “ドイツ、ファーウェイを政府調達から排除せず　5G整備巡り,” 8 12 2018. [オンライン]. Available: https://jp.reuters.com/article/germany-telecoms-idJPKBN1O628P.

[56] 日本経済新聞, “機密漏洩防止へ調達指針　政府、ファーウェイ念頭,” 10 12 2018. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO38728050Q8A211C1MM0000/.

[57] CNN.co.jp, “ファーウェイ製品の採用、仏独通信大手が方針見直し,” 15 12 2018. [オンライン]. Available: https://www.cnn.co.jp/tech/35130180.html.

[58] Microsoft, “CVE-2018-8453 | Win32k の特権の昇格の脆弱性,” 9 10 2018. [オンライン]. Available: https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2018-8453.

[59] Kaspersky, “Zero-day exploit (CVE-2018-8453) used in targeted attacks,” 10 10 2018. [オンライン]. Available: https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/.

[60] Bleeping Computer, “New Windows Zero-Day Bug Helps Delete Any File, Exploit Available,” 23 10 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/new-windows-zero-day-bug-helps-delete-any-file-exploit-available/.

[61] ZDNet, “Microsoft Windows zero-day disclosed on Twitter, again,” 23 10 2018. [オンライン]. Available: https://www.zdnet.com/article/microsoft-windows-zero-day-disclosed-on-twitter-again/.

[62] Cisco, “Cisco Adaptive Security Appliance Software and Cisco Firepower Threat Defense Software Denial of Service Vulnerability, ” 31 10 2018. [オンライン]. Available: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181031-asaftd-sip-dos.

[63] S. Zelenyuk, “VirtualBox E1000 Guest-to-Host Escape,” 7 11 2018. [オンライン]. Available: https://github.com/MorteNoir1/virtualbox_e1000_0day.

[64] Wordfence, “Trends Emerging Following Vulnerability In WP GDPR Compliance Plugin,” 9 11 2018. [オンライン]. Available: https://www.wordfence.com/blog/2018/11/trends-following-vulnerability-in-wp-gdpr-compliance-plugin/.

[65] WP GDPR Compliance Plugin, “WP GDPR Compliance 1.4.3 Security Release,” 7 11 2018. [オンライン]. Available: https://www.wpgdprc.com/wp-gdpr-compliance-1-4-3-security-release/.

[66] Microsoft, “CVE-2018-8589 | Windows Win32k の特権の昇格の脆弱性,” 13 11 2018. [オンライン]. Available: https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2018-8589.

[67] Kaspersky, “A new exploit for zero-day vulnerability CVE-2018-8589,” 14 11 2018. [オンライン]. Available: https://securelist.com/a-new-exploit-for-zero-day-vulnerability-cve-2018-8589/88845/.

[68] Adobe, “Security updates available for Flash Player | APSB18-42,” 5 12 2018. [オンライン]. Available: https://helpx.adobe.com/security/products/flash-player/apsb18-42.html.

[69] Gigamon, “Adobe Flash Zero-Day Exploited In the Wild,” 5 12 2018. [オンライン]. Available: https://atr-blog.gigamon.com/2018/12/05/adobe-flash-zero-day-exploited-in-the-wild/.

[70] Microsoft, “CVE-2018-8611 | Windows カーネルの特権の昇格の脆弱性,” 11 12 2018. [オンライン]. Available: https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2018-8611.

[71] Kaspersky, “Zero-day in Windows Kernel Transaction Manager (CVE-2018-8611),” 12 12 2018. [オンライン]. Available: https://securelist.com/zero-day-in-windows-kernel-transaction-manager-cve-2018-8611/89253/.

[72] Bleeping Computer, “Microsoft Releases Out-of-Band Security Update for Internet Explorer RCE Zero-Day,” 19 12 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/microsoft-releases-out-of-band-security-update-for-internet-explorer-rce-zero-day/.

[73] ZDNet, “Chinese websites have been under attack for a week via a new PHP framework bug,” 21 12 2018. [オンライン]. Available: https://www.zdnet.com/article/chinese-websites-have-been-under-attack-for-a-week-via-a-new-php-framework-bug/.

[74] IBM, “Threat Actors Prey on Drupalgeddon Vulnerability to Mass-Compromise Websites and Underlying Servers,” 10 10 2018. [オンライン]. Available: https://securityintelligence.com/threat-actors-prey-on-drupalgeddon-vulnerability-to-mass-compromise-websites-and-underlying-servers/.

[75] Radware, “New DemonBot Discovered,” 25 10 2018. [オンライン]. Available: https://blog.radware.com/security/2018/10/new-demonbot-discovered/.

[76] TrendMicro, “Perl-Based Shellbot Looks to Target Organizations via C&C,” 1 11 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/perl-based-shellbot-looks-to-target-organizations-via-cc/.

[77] Qihoo 360, “BCMPUPnP_Hunter: A 100k Botnet Turns Home Routers to Email Spammers,” 7 11 2018. [オンライン]. Available: https://blog.netlab.360.com/bcmpupnp_hunter-a-100k-botnet-turns-home-routers-to-email-spammers-en/.

[78] CyberArk, “A Local File Inclusion in Kibana allows attackers to run local JavaScript file,” 21 11 2018. [オンライン]. Available: https://www.cyberark.com/threat-research-blog/execute-this-i-know-you-have-it/.

[79] Qihoo 360, “A Missed 0day ? - Reveal another Cyber Arsenal of APT-C-06,” 12 11 2018. [オンライン]. Available: http://blogs.360.cn/post/VBScript_vul_EN.html.

[80] 時事通信, “Nginx の脆弱性を悪用する攻撃準備中か、ダークウェブの観察で判明,” 15 11 2018. [オンライン]. Available: https://this.kiji.is/435938239837946977?c=220450040231249399.

[81] Forbes, “A Hacker Forced 50,000 Printers To Spread PewDiePie Propaganda -- And The Problem Is Much Bigger Than You Know,” 3 12 2018. [オンライン]. Available: https://www.forbes.com/sites/thomasbrewster/2018/12/03/a-hacker-forced-50000-printers-to-spread-pewdiepie-propagandaand-the-problem-is-much-bigger-than-you-know/.

[82] Gravitational, “gravitational/cve-2018-1002105,” 5 12 2018. [オンライン]. Available: https://github.com/gravitational/cve-2018-1002105.

[83] Twistlock, “Demystifying Kubernetes CVE-2018-1002105 (and a dead simple exploit),” 9 12 2018. [オンライン]. Available: https://www.twistlock.com/labs-blog/demystifying-kubernetes-cve-2018-1002105-dead-simple-exploit/.

[84] Sophos, “ソフォスの「2019 年版脅威レポート」:被害者から数百万ドルを搾取する、特定ユーザーを狙った標的型攻撃の台頭が明らかに,” 22 11 2018. [オンライン]. Available: https://www.sophos.com/ja-jp/press-office/press-releases/2018/11/sophoslabs-2019-threat-report.aspx.

[85] Bleeping Computer, “New FilesLocker Ransomware Offered as a Ransomware as a Service,” 25 10 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/new-fileslocker-ransomware-offered-as-a-ransomware-as-a-service/.

[86] The Times Leader, “Hospitals: Patient information safe in EORH, OVMC computer attack,” 25 11 2018. [オンライン]. Available: http://www.timesleaderonline.com/news/local-news/2018/11/hospitals-patient-information-safe-in-eorh-ovmc-computer-attack/.

[87] Bleeping Computer, “Moscow’s New Cable Car System Infected with Ransomware the Day After it Opens,” 30 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/moscows-new-cable-car-system-infected-with-ransomware-the-day-after-it-opens/.

[88] Bleeping Computer, “Ransomware Infects 100K PCs in China, Demands WeChat Payment,” 5 12 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/ransomware-infects-100k-pcs-in-china-demands-wechat-payment/.

[89] ESET, “New TeleBots backdoor: First evidence linking Industroyer to NotPetya,” 11 10 2018. [オンライン]. Available: https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/.

[90] ONWASA, “Cyber-criminals target critical utility in hurricane-ravaged area,” 15 10 2018. [オンライン]. Available: https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A.

[91] Kaspersky, “DarkPulsar,” 19 10 2018. [オンライン]. Available: https://securelist.com/darkpulsar/88199/.

[92] The Times of Israel, “TV report: Israel silent as Iran hit by computer virus more violent than Stuxnet,” 31 10 2018. [オンライン]. Available: https://www.timesofisrael.com/tv-report-israel-silent-as-iran-hit-by-computer-virus-more-violent-than-stuxnet/.

[93] Cisco, “DNSpionage Campaign Targets Middle East,” 27 11 2018. [オンライン]. Available: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html.

[94] US-CERT, “HIDDEN COBRA - FASTCash Campaign,” 2 10 2018. [オンライン]. Available: https://www.us-cert.gov/ncas/alerts/TA18-275A.

[95] FireEye, “北朝鮮国家の支援を受ける 新たな脅威グループ「APT38」の詳細を発表,” 3 10 2018. [オンライン]. Available: https://www.fireeye.com/blog/jp-threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html.

[96] Proofpoint, “DanaBot Gains Popularity and Targets US Organizations in Large Campaigns,” 2 10 2018. [オンライン]. Available: https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns.

[97] Cylance, “Threat Spotlight: Panda Banker Trojan Targets the US, Canada and Japan,” 9 10 2018. [オンライン]. Available: https://threatvector.cylance.com/en_us/home/threat-spotlight-panda-banker-trojan-targets-the-us-canada-and-japan.html.

[98] Bleeping Computer, “TrickBot Banking Trojan Starts Stealing Windows Problem History,” 17 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-starts-stealing-windows-problem-history/.

[99] Group-IB, “Two hacker groups attacked Russian banks purporting to be the Central Bank of Russia,” 16 11 2018. [オンライン]. Available: https://www.group-ib.com/media/cbrf-double-attack/.

[100] Trend Micro, “Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America,” 20 11 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-continues-heists-mounts-attacks-on-financial-organizations-in-latin-america/.

[101] Kaspersky, “The Rotexy mobile Trojan - banker and ransomware,” 22 11 2018. [オンライン]. Available: https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/.

[102] Kaspersky, “DarkVishnya: Banks attacked through direct connection to local network,” 6 12 2018. [オンライン]. Available: https://securelist.com/darkvishnya/89169/.

[103] ESET, “Android Trojan steals money from PayPal accounts even with 2FA on,” 11 12 2018. [オンライン]. Available: https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/.

[104] Bleeping Computer, “Cobalt Bank Robbers Use New ThreadKit Malicious Doc Builder,” 11 12 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/cobalt-bank-robbers-use-new-threadkit-malicious-doc-builder/.

[105] Menlo Security, “A ″JAR″ Full of Problems for Financial Services Companies,” 19 12 2018. [オンライン]. Available: https://www.menlosecurity.com/blog/a-jar-full-of-problems-for-financial-services-companies.

[106] Cisco, “GPlayed Trojan – .Net playing with Google Market,” 11 10 2018. [オンライン]. Available: https://blog.talosintelligence.com/2018/10/gplayedtrojan.html.

[107] SANS, “New Campaign Using Old Equation Editor Vulnerability,” 11 10 2018. [オンライン]. Available: https://isc.sans.edu/forums/diary/New+Campaign+Using+Old+Equation+Editor+Vulnerability/24196/.

[108] TrendMicro, “Malware Targeting Brazil Uses Legitimate Windows Components WMI and CertUtil as Part of its Routine,” , 24 10 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/malware-targeting-brazil-uses-legitimate-windows-components-wmi-and-certutil-as-part-of-its-routine/.

[109] Bleeping Computer, “Fake Apps in Google Play Get over Half a Million Installs,” 19 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/fake-apps-in-google-play-get-over-half-a-million-installs/.

[110] Yoroi, “The SLoad Powershell Threat is Expanding to Italy,” 27 11 2018. [オンライン]. Available: https://blog.yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/.

[111] Trend Micro, “AutoIt-Compiled Worm Affecting Removable Media Delivers Fileless Version of BLADABINDI/njRAT Backdoor,” 27 11 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/autoit-compiled-worm-affecting-removable-media-delivers-fileless-version-of-bladabindi-njrat-backdoor/.

[112] Forcepoint, “AutoCAD Malware – Computer Aided Theft,” 28 11 2018. [オンライン]. Available: https://www.forcepoint.com/blog/security-labs/autocad-malware-computer-aided-theft.

[113] Trend Micro, “New Exploit Kit “Novidade” Found Targeting Home and SOHO Routers,” 11 12 2018. [オンライン]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/.

[114] Department of Justice, “Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud,” 27 11 2018. [オンライン]. Available: https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing.

[115] Bleeping Computer, “3ve Ad Fraud Botnet with Billions of Daily Ad Requests Shut Down,” 27 11 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/3ve-ad-fraud-botnet-with-billions-of-daily-ad-requests-shut-down/.

[116] ZDNet, “Czech intelligence service shuts down Hezbollah hacking operation,” 16 10 2018. [オンライン]. Available: https://www.zdnet.com/article/czech-intelligence-service-shuts-down-hezbollah-hacking-operation/.

[117] Bleeping Computer, “SNDBOX - an AI Powered Malware Analysis Site is Launched,” 5 12 2018. [オンライン]. Available: https://www.bleepingcomputer.com/news/security/sndbox-an-ai-powered-malware-analysis-site-is-launched/.

[118] SEC Consult, “REMOTE CODE EXECUTION VIA XMEYE P2P CLOUD IN XIONGMAI IP CAMERAS, NVRS AND DVRS,” 9 10 2018. [オンライン]. Available: https://sec-consult.com/en/blog/advisories/vulnerabilities-xiongmai-ip-cameras-nvrs-dvrs-cve-2018-17915-cve-2018-17917-cve-2018-17919/.

[119] CyberX, “2019 GLOBAL ICS & IIOT RISK REPORT,” 30 10 2018. [オンライン]. Available: https://cyberx-labs.com/resources/risk-report-2019.

[120] 金融庁, “「金融業界横断的なサイバーセキュリティ演習,” 19 10 2018. [オンライン]. Available: https://www.fsa.go.jp/news/30/sonota/20181019/20181019-cyber.html.

[121] Nextgov, “NIST Teams Up with IBM’s Watson to Rate How Dangerous Computer Bugs Are,” 2 11 2018. [オンライン]. Available: https://www.nextgov.com/cybersecurity/2018/11/nist-teams-ibms-watson-rate-how-dangerous-computer-bugs-are/152545/.

[122] IPA, “安全なウェブサイトの運用管理に向けての 20 ヶ条 ～セキュリティ対策のチェックポイント～,” 12 12 2018. [オンライン]. Available: https://www.ipa.go.jp/security/vuln/websitecheck.html.

[123] Yoroi, “Cyber-Espionage Campaign Targeting the Naval Industry (“MartyMcFly”),” 17 10 2018. [オンライン]. Available: https://blog.yoroi.company/research/cyber-espionage-campaign-targeting-the-naval-industry-martymcfly/.

[124] Kryptos Logic, “Emotet Awakens With New Campaign of Mass Email Exfiltration,” 31 10 2018. [オンライン]. Available: https://blog.kryptoslogic.com/malware/2018/10/31/emotet-email-theft.html.

[125] Yoroi, “Dissecting the latest Ursnif DHL-Themed Campaign,” 4 12 2018. [オンライン]. Available: https://blog.yoroi.company/research/dissecting-the-latest-ursnif-dhl-themed-campaign/.

[126] ABC30 News, “Girl Scouts’ personal information affected by recent data breach,” 26 10 2018. [オンライン]. Available: https://abc30.com/4561129/.

[127] MSE News, “Eurostar customers told to reset passwords after attempted hack,” 31 10 2018. [オンライン]. Available: https://www.moneysavingexpert.com/news/2018/10/eurostar-customers-told-to-reset-passwords-after-attempted-hack/.

[128] ZDNet, “Radisson Hotel Group suffers data breach, customer info leaked,” 2018, 1 11. [オンライン]. Available: https://www.zdnet.com/article/radisson-hotel-group-chain-suffers-data-breach/.

[129] The New York Times, “FIFA, Hacked Again, Braces for New Revelations,” 30 10 2018. [オンライン]. Available: https://www.nytimes.com/2018/10/30/sports/soccer/fifa-uefa-hack.html.

[130] BBC, “HSBC bank confirms US data breach,” [オンライン]. Available: https://www.bbc.com/news/technology-46117963.

[131] ITmedia, “Amazon ユーザーの氏名やメールアドレス、手違いで公開,” 22 11 2018. [オンライン]. Available: http://www.itmedia.co.jp/news/articles/1811/22/news060.html.

[132] 警察庁, “仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について,” 12 3 2018. [オンライン]. Available: https://www.npa.go.jp/cyberpolice/important/2018/201803121.html.

2019 年 2 月 13 日発行

株式会社 NTT データ
セキュリティ技術部 情報セキュリティ推進室 NTTDATA-CERT 担当
nttdata-cert@kits.nttdata.co.jp