NTT DATA
Global IT Innovator

グローバルセキュリティ動向四半期レポート
（2017年度 第3四半期）

2018年3月27日

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

目次

NTT DATA

エグゼクティブサマリー

この四半期(2017年10月～12月)の注目点は、仮想通貨を狙った攻撃の増加と日本国内でのIoTマルウエア感染端末の急増です。

仮想通貨を狙った攻撃は、ドライブバイマイニングの流行など、攻撃手法も多様化しました。多様化する攻撃手法に対して、これまでの通貨を狙った攻撃と比較してどのような特徴があるのか、対比して整理しました。

日本国内でのIoTマルウエア感染端末の急増は、偶発的な条件によって急増した可能性もありますが、意図的な攻撃によって、日本国内で感染端末が急増した可能性も否定できません。

上記のような、仮想通貨を狙った攻撃の増加や、IoTマルウエアの感染端末の増加といった傾向を踏まえ、NTTDATA-CERTでは、IoTボットネットを使った不正な仮想通貨採掘※が流行することを懸念しています。

レポートの最後には、この四半期のセキュリティに関する出来事をタイムラインにまとめています。各出来事はテーマでまとめ、出来事の関連性について考察を行っています。

※仮想通貨「採掘」とは
仮想通貨取引に必要な、取引台帳への取引記録の追記のためにPC等のマシンリソースを提供し、見返りに仮想通貨を得ること。

I. 2017年度 第3四半期のトピック(1/4)
仮想通貨を狙った攻撃の増加(タイムライン[A])

仮想通貨を狙った攻撃は多様化しています。仮想通貨を狙った攻撃にはどのような特徴があるのでしょうか。

■仮想通貨を狙った攻撃手法は多様化している

仮想通貨を狙った攻撃手法は多様化しており、例えば、本四半期には、**Web閲覧中にブラウザで仮想通貨を採掘させる、「ドライブバイマイニング」**の手法が話題になりました。本レポートでは、多様化する攻撃手法を整理しました。表1は、仮想通貨を狙った攻撃手法を、金融機関やネットバンキング利用者を狙った攻撃手法と対比したものです。

■仮想通貨を狙った攻撃の特徴

仮想通貨を狙った攻撃は、標的別に、「マシンリソース保有者」、「サービス利用者」、「サービス提供者」のそれぞれを狙った攻撃に分けることができます。

仮想通貨ならではの攻撃としては、**他者のマシンリソースを使って不正に仮想通貨を採掘する攻撃**(表1の①)、**新規仮想通貨公開(ICO)時における攻撃**(表1の②)が挙げられます。また、最近は、ネットバンキングの不正払戻しや不正送金事犯が減少傾向にある一方で、仮想通貨をターゲットにした不正送金事犯が増加しています(*1-1)。また、攻撃手段をランサムウエアから不正な仮想通貨採掘へ変更した攻撃者グループについても報告される(*1-2)など、**攻撃者の狙いは仮想通貨へシフトしています**。

表1：仮想通貨を狙った攻撃手法と通貨を狙った攻撃手法の対比

標的	仮想通貨	通貨
リソース保有者	・仮想通貨マイナー ・ドライブバイマイニング ①	
サービス利用者	認証情報を窃取し、不正送金(バンキングマルウエア、フィッシング等)	認証情報を窃取し、不正送金(バンキングマルウエア、フィッシング等)
	秘密鍵への攻撃	カード偽造
サービス提供者(金融機関、仮想通貨取引所等)	仮想通貨取引所等のウォレットに不正アクセス	SWIFTを利用した不正送金
	(仮想通貨両替機への攻撃)	ATMマルウエアに感染させ、自由に現金を引き出せるようにする。
	脅迫	脅迫
	新規公開時の仮想通貨に対する攻撃 ②	

I. 2017年度 第3四半期のトピック(2/4)
IoTマルウエアの感染拡大(タイムライン[B])

日本国内でIoTマルウエアの感染端末が急増したのはなぜでしょうか。

■日本国内でIoTマルウエアの感染端末が増加することによる懸念

本四半期には、日本国内でIoTマルウエアの感染端末が急増したことが大きな話題となりました(*1-3)。もし、この感染端末がDDoS攻撃に悪用された際は、国内から攻撃を受けることになり、**DDoS攻撃への暫定対応として、海外IPアドレスからの通信を一律に遮断するという対策が難しくなる**ことが懸念されます。このように、国内の感染端末増加は大きな脅威となるため、今回国内で感染が広がった原因と対策を考察しました。図1は、NICTERで観測された23/TCPと52869/TCPへのスキャン活動です(*1-4)。

■IoTマルウエアの特徴

今回の感染端末の急増では、**機器の脆弱性が狙われていた**ことが分かっています。ZyXEL社のモデムに存在するバックドアアカウントの脆弱性(CVE-2016-10401)(*1-5)、Realtek SDKの脆弱性(CVE-2014-8361)、Huawei社のルーターの脆弱性(CVE-2017-17215)です(*1-4)。

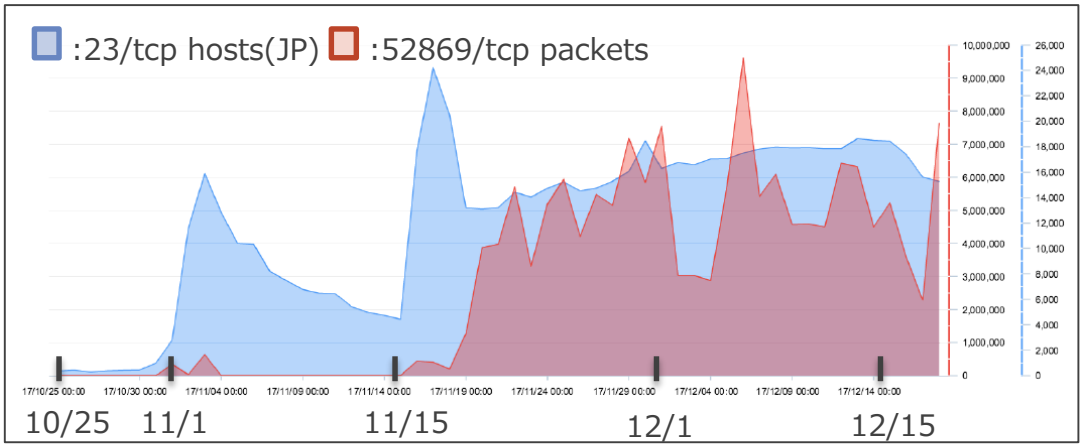

図1：国内で観測された23/TCPと52869/TCPへのスキャン活動(感染拡大活動)
(「NICTER 観測レポート ルータ製品の脆弱性を悪用して感染を広げるMiraiの亜種に関する活動(*1-4)」より引用)

■感染端末急増の原因と対策

急増の原因として、**国内に脆弱性を保有する機器が偶然多かった可能性**が挙げられます。また、52869/TCPのスキャン活動は、11月中は日本でのみ確認されており(*1-6)、**意図的に国内の機器を狙った可能性**もあります。

今回日本国内で感染拡大したIoTマルウエアは脆弱性を狙っており、ID/パスワードを初期設定のままにしないといった対策に加えて、**パッチの適用**が必要です。ルーターやWebカメラ等のIoT機器の利用者は、メーカーのページでパッチを確認してください。また、メーカーは、ID/パスワードをハードコードしないなど、**設計段階からのセキュリティの考慮**が必要です。総務省は、一定のセキュリティ要件を満たすIoT機器に対して認証マークを付与することを検討しており、新たに製造されるIoT機器については、IoTマルウエアの感染拡大が抑制されることが期待されます(*1-7)。

NTT DATA

I. 2017年度 第3四半期のトピック(3/4)
その他トピック

■ 金融機関を狙った標的型攻撃(タイムライン[C])

① 本四半期も銀行が不正アクセスを受け、**SWIFT経由で不正送金される**事象が発生しました。

- ✓ 10月上旬　台湾の銀行 Far Eastern International Bank (*1-8)
- ✓ 10/17　ネパールの銀行 NIC Asia Bank (*1-9)

また、台湾の銀行への攻撃では、攻撃者集団Lazarusの特徴が認められることが報告されました(*1-10)。

② 旧ソ連諸国の金融機関を標的とした攻撃では、偽の個人情報を使って開設した口座でキャッシュカードを作成し、その数か月後にサイバー攻撃でキャッシングの上限額を不正に引き上げ、キャッシュカードを用いてATMで上限額の現金をキャッシングするという手口が報告されました(*1-11)。**物理的な手段とサイバー攻撃を組み合わせた手法**で、正規のキャッシュカードを用いるため、検知しづらい手口です。

③ 攻撃者集団Cobaltは、MS Office数式エディタの脆弱性(CVE-2017-11882)が**公表、修正(*1-12)された約1週間後**に、ロシアとトルコの金融機関を標的とした当該脆弱性を使った攻撃を実施しました(*1-13)。

■ 自ら感染拡大するマルウエアについて

① 自ら感染拡大するマルウエアの脅威は続いています。前四半期のレポートで取り上げた、**自ら感染拡大する情報窃取型トロイの木馬**(QakbotおよびEmotet)に関しては、**企業ユーザーでの検知件数が増加**していることが報告されました(*1-14)。

② 実験段階にあるランサムウエアqkGの、新たな感染拡大方法についても報告されました(*1-15)。qkGの感染拡大方法は完全に自動化されているわけではなく、感染拡大には、ユーザーが暗号化されたファイルを開くことが必要です。**感染するとWordの標準テンプレート「normal.dot」に不正なマクロが追加**され、暗号化されていないWordファイルを開き、閉じる際に、当該ファイルを暗号化します。また、暗号化と同時に、別のユーザーが当該ファイルを開いた際に感染するよう、**自動実行マクロを追加**します。

③ **IoTマルウエア**Mirai亜種にも、スキャン活動の後、自ら感染拡大するワームのような動作をするものが報告されました(*1-16)。

I. 2017年度 第3四半期のトピック(4/4)
その他トピック

■ サイバー脅迫(タイムライン[F])

10月に米教育省が、サイバー脅迫に対して警告を発しました(*1-17)。データセキュリティの弱い学区を狙って学生の個人情報を窃取し、**身代金の要求に応じなければ学生の個人情報を公開する、学生に危害を加えると脅迫する手口**で、少なくとも3つの州が脅迫を受けました。学校に対するサイバー脅迫は、今後日本でも増加する危険性があります。文科省は、「教育情報セキュリティポリシーに関するガイドライン」を公表しています(*1-18)。

■ メール攻撃の動向(タイムライン[H],[I],[J])

マクロを有効にしなくてもマルウエア感染させることができるような新たな攻撃として、**DDE(Dynamic Data Exchange)**が標的型攻撃(*1-19)でもばらまき型メール攻撃(*1-20)でも悪用されました。DDEはWindows OS上で、アプリケーション間でデータを交換したり、コマンドを発行したりするためのメカニズムで、ユーザーがファイルを開く際のポップアップに「はい」と回答させることで、悪意のあるコードを実行させることができます。DDEに対してマイクロソフト社は、アドバイザリーを公開しました(*1-21)。また、MS WordとExcelでDDEを無効化するパッチも提供されています(*1-22)。

また、**実在する組織を騙って、メール本文中の不正なリンクをクリックさせる攻撃**も多く報告されました(*1-23)。

■ 日本航空がビジネスメール詐欺被害に(タイムライン[K])

日本航空が3億8,400万円のビジネスメール詐欺被害にあっていたことが分かりました(*1-24)。振込先が変更されたというメールが取引先から届き、事前にやりとりしていた正規の請求書の訂正版として、振込先を偽の口座に変更したPDFファイルも送られてきたため、信じて振り込んでしまいました。送信元のメールアドレスは、後からよく確認すると1字違っていたようです(*1-25)。事前にやりとりしていた請求書の内容を攻撃者は把握しており、担当者間のやりとりは盗み見されていたと考えられます。

特に金銭を取り扱う業務部署では、**広くばらまかれた攻撃だけではなく、このように狙いすました攻撃を受ける可能性がある**ことを意識しておく必要があります。また、振込先の変更時の承認プロセス等についても適切に規定されているか確認が必要です。

II. 2017年度 第4四半期以降の予測
IoTボットネットによる不正な仮想通貨採掘が流行する

■不正な仮想通貨採掘の流行

不正に仮想通貨を採掘させる手口には、大きく2つあります。1つは、**「仮想通貨マイナー」に感染させ、採掘させる**手口で、検出数の増加が報告されています(*2-1)。もう1つは**「ドライブバイマイニング」**という手口で、Web閲覧時にJavaScriptをダウンロードさせ、閲覧しているブラウザ上で仮想通貨を採掘させます。9月にCoinhiveサービスが開始され、当該サービスを用いたドライブバイマイニングが流行しました(*2-2)。トピックでも取り上げているように、ネットバンキングの不正送金が減る一方で仮想通貨をターゲットにした不正送金が増加していたり(*1-1)、ランサムウエアから仮想通貨マイナーへのシフトといった傾向が報告されています(*1-2)。また、仮想通貨を採掘させる標的は、サーバーやPCだけでなく、スマートフォンも狙われています(*2-3)。

■IoTボットネットによる仮想通貨採掘が流行する

NTTDATA-CERTでは、現在は主にDDoS攻撃に使用されているIoTボットネットが、今後は不正な仮想通貨採掘に使用される傾向が強まるのではないかと考えています。不正な仮想通貨採掘は、「多く」の「高性能な機器」で「気づかれずに長時間」採掘することができれば、多くの利益を得ることができます。一方でサーバーやPC等の高性能な機器は、ウイルス対策ソフト等のセキュリティ対策を導入されていることが多く、気付かれずに長期間採掘させることは難しくなってきています。このような状況においては、ある程度の性能であっても、**気付かれずに長時間採掘させることが可能な機器が狙われる**ことが想定されます。また、IoT機器は性能が低いと考えられがちですが、動画処理をするデジタルビデオレコーダーのように、性能を求められる機器もあります。攻撃者は、「台数が多い」、「ある程度の性能を持つ」、「気づかれにくくネットワークへ長時間接続している」という条件を満たすIoT機器を狙ってボット化し、不正に仮想通貨を採掘させるようになるのではないでしょうか。実際に、家庭用デバイスを対象にした、仮想通貨採掘の通信の検知に関するレポートでは、仮想通貨採掘の通信を行っていた機器のうち、IoT機器が約6%を占めていたことが報告されており(*2-4)、すでに兆候が確認されています(*2-5)。この傾向は今後強まっていくだろうとNTTDATA-CERTでは懸念しています。

III. 2017年度 第3四半期のタイムライン (1/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 | 10月 | 11月 | 12月

[A] 仮想通貨を狙った攻撃

仮想通貨取引所やICO中の仮想通貨を狙った攻撃

- ▲ 10/2 ICO中のEtherpartyのWebサイトが乗っ取られ、出資金をだまし取られる。
- ▲ 12/7 マイニングプールNiceHashから76億円相当のビットコインが盗まれる。
- ▲ 12/12 仮想通貨取引所BitfinexのWebサイトがDDoS攻撃で停止
- ▲ 12/19 韓国の仮想通貨取引所YouBitがハッキング攻撃受け破産申請へ

仮想通貨を不正に採掘させる攻撃

- ▲ 10/1 Roboto Condensedフォントのインストールを装って仮想通貨マイナーCoinMinerに感染させる手法
- ▲ 10/11 torrentファイル検索サイトThe Pirate BayがCoinhiveの稼働を再開
- ▲ 10/12 Alexaランキング上位10万サイトに対する調査で、220サイトでCoinhiveが稼働し、43,000ドル相当の仮想通貨を採掘したことが判明。
- ▲ 10/19 Malwarebytes社の製品でCoinhiveをブロックすることに
- ▲ 10/23 CoinhiveのJavaScriptファイルのダウンロード先が攻撃者によって変更され、変更された期間の仮想通貨を盗まれる。
- ▲ 11/7 電子商取引の2,496サイトで、Coinhiveが検出される。
- ▲ 11/23 ライブチャットのサポートウィジェットLiveHelpNowのJavaScriptファイルにCoinhiveが見つかる。
- ▲ 11/29 ブラウザを閉じてもCoinhiveに採掘を継続させる手法が報告される。
- ▲ 12/2 アルゼンチンの店内WiFiへ接続したところ、Coinhiveを実行される。
- ▲ 12/15 Apache Struts2が動作する端末を標的とし、仮想通貨マイナーmuleを感染させる攻撃キャンペーンZealot
- ▲ 12/15 露石油パイプライン会社Transneftが仮想通貨マイナーに感染

モバイルを標的に

- ▲ 10/30 トレンドマイクロ社が、モバイルデバイスに仮想通貨を採掘させる悪意のあるアプリをGoogle Playで発見
- ▲ 11/6 豪州で、携帯電話でBitcoinを採掘するマルウェアに感染させる、悪意のあるメッセージが送信される。

仮想通貨のウォレットから盗もうとする攻撃

- ▲ 11/18 仮想通貨のウォレットのスキャンが増大。その直前には仮想通貨の価格が高騰
- ▲ 12/5 ダウンローダーQuantに仮想通貨のウォレットを狙う機能が追加される。
- ▲ 12/6 仮想通貨取引所の運営会社10社と警視庁が情報共有を進める協定
- ▲ 12/7 ビットコインのトレーディングボットを餌にOrcus RATへ感染させるフィッシングキャンペーン

NTT DATA

III. 2017年度 第3四半期のタイムライン (2/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[B] IoTボットネットの拡大

- ▲ 10/5 Brother社の約700台のプリンターの管理画面が公開状態に。パスワード無しでの出荷が原因の一つ。
- ▲ 10/19 新たなIoTボットネットIoTroop(IoT_reaper)。9月末ごろから確認され、無線カメラの脆弱性を狙って拡大
- ▲ 10/3 総務省が「IoTセキュリティ総合対策」を公表。ウイルス対策等の安全性の高い機器に認証マークを与える等
- ▲ 11/8 IoTボットネットIoTroopで使用されたIPスキャナが、バックドアが仕掛けられた状態で公開される。
- ▲ 11/22 Mirai亜種による、アルゼンチンを発信元としたアクセス試行が多数確認される。
- ▲ 11/29 Mirai亜種による、コロンビア、エジプト、チュニジアを発信元としたアクセス試行が多数確認される。
- ▲ 12/14 自宅無線LANの暗号化設定は初期設定のままが4割。IPA調査
- ▲ 12/18 11月の日本を発信元とする攻撃ホスト数が、10月の約100倍に。
- ▲ 12/18 Shodanで確認されたLexmark社製のプリンター1,475アドレスのうち、約76%がパスワード未設定の状態
- ▲ 12/19 ロジテック社、Huawei社製BBルータの脆弱性を狙ってMirai亜種が感染拡大

- ▲ 11/16 経済産業省はサイバーセキュリティ経営ガイドラインを改訂。攻撃検知と復旧への備えを追加

[C] 金融機関を狙った標的型攻撃

- ▲ 10/7 台湾の銀行Far Eastern International Bankがハッキングされ、SWIFT経由で不正送金される。
- ▲ 10/10 旧ソ連諸国の金融機関を標的とし、不正開設口座のキャッシング上限をサイバー攻撃で引き上げ、キャッシングする手口
- ▲ 10/17 ネパールの銀行NIC Asia Bankがハッキングされ、SWIFT経由で不正送金される。
- ▲ 11/1 ロシア、マレーシア、アルメニアの銀行を狙った攻撃Silence。フィッシングメールで侵入し、大金を盗むのに十分な情報を得た場合にのみ攻撃を仕掛ける。
- ▲ 11/21 攻撃者グループCobaltが、ロシアとトルコの金融機関を狙ったフィッシングメール攻撃。MS Officeの脆弱性(CVE-2017-11882)を悪用

- ▲ 10/10 MS Office 2007サポート終了
- ▲ 10/16 WPA2のプロトコル標準に情報漏洩の脆弱性KRACKs
- ▲ 11/15 MS Office数式エディタの脆弱性(CVE-2017-11882)が公表、修正される。
- ▲ 11/15 MS社は10月にサポート終了したMS Office 2007に対しても、数式エディタの脆弱性(CVE-2017-11882)のパッチを提供
- ▲ 11/20 Intel Management Engine（ME）などに複数の重要な脆弱性
- ▲ 12/18 マルウエアTelegramRATが数式エディタの脆弱性(CVE-2017-11882)を利用して拡散
- ▲ 12/20 情報窃取型マルウエアLokiの海賊版が数式エディタの脆弱性(CVE-2017-11882)を利用して拡散

NTT DATA

III. 2017年度 第3四半期のタイムライン (3/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[D] 政府組織や重要インフラを狙った標的型攻撃

- ▲ 9/22 米電力会社を標的としたスピアフィッシングメール攻撃
- ▲ 10/5 FTPサーバーをC2に使用するバックドアSYSCONが、赤十字やWHO関係者を狙うフィッシング攻撃で拡散
- ▲ 10/5 米韓の防衛、航空、製造請負業者に対して情報窃取マルウエアFormBookを拡散させる攻撃キャンペーン
- ▲ 10/6 米大統領主席補佐官John Kelly氏の個人用スマートフォンがハッキングされていた可能性
- ▲ 10/10 攻撃者グループOilRigがトロイの木馬ISMInjectorを使ってUAEの政府機関を攻撃
- ▲ 10/10 オーストラリアの諜報機関ASDから、戦闘機、軍用機および海軍の船舶の詳細等、軍事能力に関するデータが窃取
- ▲ 10/12 攻撃者グループBRONZE BUTLER(別名Tick)が、日本の組織から知的財産等の機密情報を窃取
- ▲ 10/10 中東の攻撃者グループBlackOasisが、Adobe Flashの脆弱性(CVE-2017-11292)を悪用
- ▲ 10/16 Adobe Flashの脆弱性(CVE-2017-11292)が公表、修正される。
- ▲ 10/18 APT28による、Adobe Flashの脆弱性(CVE-2017-11292)を用いた、政府組織や航空宇宙産業等を狙った攻撃
- ▲ 10/22 APT28が、セキュリティ会議Cyber Conflict U.S.を装ったWordドキュメントでDDEを用いてマルウエアSeduploaderに感染させる攻撃キャンペーン
- ▲ 10/20 米政府機関や重要インフラを狙った攻撃が発生しているとしてUS-CERTが注意喚起
- ▲ 11/15 北朝鮮の攻撃者グループが用いるトロイの木馬Volgmerに対する警戒情報をUS-CERTが公開
- ▲ 12/21 北朝鮮の攻撃者グループが用いるトロイの木馬BANKSHOTに対する警戒情報をUS-CERTが公開

NTT DATA

III. 2017年度 第3四半期のタイムライン (4/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[E] ランサムウエア攻撃

ランサムウエア被害

- ▲ 9月上旬 東芝メモリでランサムウエア被害
- ▲ 10/3 米コロラド州エングルウッドの役所にランサムウエア攻撃
- ▲ 10/11 2015年8月に倒産した保険会社へランサムウエア攻撃。データベースが暗号化
- ▲ 10/17 米医療機関グループFirstHealth of the CarolinasがWannaCry亜種に感染。社内ネットワークが停止
- ▲ 10/24 ロシア、ウクライナ等でランサムウエアBadRabbitの被害
- ▲ 10/25 アイカ工業がWebサイトを一時閉鎖。BadRabbit拡散に利用される。
- ▲ 11/2 ランサムウエアBadRabbitによる攻撃と同時に、ウクライナでフィッシング攻撃
- ▲ 11/16 米テネシー州スプリングヒル市へランサムウエア攻撃。
- ▲ 12/8 米ウィスコンシン州ナショタ村で自治体のPCがランサムウエア感染。暗号解除のために身代金を支払う。

新種/亜種

- ▲ 10/9 RDP経由でランサムウエアBTCWareの新しい亜種を手動で感染させる攻撃
- ▲ 10/13 Androidのユーザー補助サービスを悪用したランサムウエアDoubleLocker。データ暗号化とPIN変更機能を持つ。
- ▲ 10/16 ランサムウエアTyrantがイラン国内で流行
- ▲ 10/24 削除しようとするとランサムウエアに変わってロックする、Androidバンキングマルウエア LokiBot
- ▲ 10/29 サンドボックス回避と権限昇格機能を備えたランサムウエアSage2.2亜種
- ▲ 11/7 ランサムウエアGIBON
- ▲ 11/9 サーバーを標的としたランサムウエアLockCrypt。RDPのブルートフォース攻撃で拡散。
- ▲ 11/22 MS Wordのテンプレートに感染し、拡散するランサムウエアqkG。PoC段階のものがVirusTotal上で見つかる。
- ▲ 12/6 RDP経由でランサムウエアHC7へ感染させる攻撃。同一ネットワーク内での感染拡大にPsExecを使用。
- ▲ 12/10 主にボスニア・ヘルツェゴビナ等の地域を狙ったランサムウエアSpider
- ▲ 12/13 ランサムウエアCryptoMixの亜種「.WORK」

- ▲ 10/11 2016年から2017年の間に、ダークウェブ上でランサムウエアの販売数が2,502%上昇
- ▲ 10月中旬 Windows10で、フォルダ制御アクセス機能がリリース
- ▲ 10/17 Petya亜種(NotPetya)で暗号化されたシステムの復号方法。対象システムの状況に合わせた手動操作が必要
- ▲ 11/10 Petya亜種(NotPetya)の経済損失額は10億米ドルを超えている。
- ▲ 12/11 ランサムウエアの標的の26%は企業ユーザー。昨年の23%から上昇。
- ▲ 12/20 ランサムウエアVenusLockerを用いていた攻撃者グループが仮想通貨の採掘へ移行

- ▲ 11/6 ワーム機能を持ったバンキングマルウエアQakbotおよびEmotetの企業ユーザーでの検知件数が増加

NTT DATA

III. 2017年度 第3四半期のタイムライン (5/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[F] サイバー脅迫

- ▲ 9/30 DDoS恐喝グループPhantom Squadが、世界中の企業に対してDDoS攻撃をたてに脅迫
- ▲ 10/1 オンラインゲームRainbow Six Siegeの統計情報提供サービスのDBが消去され、身代金を要求される。
- ▲ 10/1 英National LotteryへDDoS攻撃。
- ▲ 11/4 加フレーザーバレー大学のネットワークから個人情報が窃取され、身代金を要求される。
- ▲ 12/15 MongoDB上で公開されていた米カリフォルニア州の有権者情報が消去され、身代金を要求される。

The Dark Overlordが学校、医療機関、映画会社を狙う

- ▲ 9/18 攻撃者グループThe Dark Overlordが米モンタナ州の学区に対して脅迫
- ▲ 9/29 攻撃者グループThe Dark Overlordが米テキサス州の学区に対して脅迫
- ▲ 10/2 攻撃者グループThe Dark Overlordが米アイオワ州の学区に対して脅迫
- ▲ 10/16 米教育省が、学校に対してサイバー攻撃を行う新たな脅威について注意喚起。
- ▲ 10/18 攻撃者グループThe Dark Overlordが米の医療機関AMTAへ不正アクセスし、患者情報を窃取
- ▲ 10/24 攻撃者グループThe Dark Overlordが、英の美容形成外科のネットワークに侵入し、機密情報や写真を窃取
- ▲ 11/8 攻撃者グループThe Dark Overlordが、米映画会社「Line204」から顧客情報を窃取

[G] 重要インフラや産業システムを狙った攻撃

- ▲ 10/11 スウェーデンの交通システムに対するDDoS攻撃
- ▲ 10/18 文科省が「教育情報セキュリティポリシーに関するガイドライン」を公表
- ▲ 11/18 米カリフォルニア州サクラメント交通局でデータの一部が消去され、身代金を要求される。
- ▲ 12/14 産業制御システムを狙うマルウエアTriton

NTT DATA

III. 2017年度 第3四半期のタイムライン (6/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[H] DDE(Dynamic Data Exchange)を使った攻撃

- ▲ 10/12 DDEを利用して任意のコードを実行する手法が公開される。
- ▲ 11/8 MS社がDDE攻撃に対するアドバイザリーを発行
- ▲ 12/12 MS社がWordでDDEを無効化するアップデート
- ▲ 10月ごろ 中国、ロシアの攻撃者グループがDDEを一斉に悪用し始める。

[I] Necursボットネットによる攻撃

- ▲ 10/20 NecursボットネットがDDE攻撃を用いてランサムウエアLockyに感染させるメールをばらまく。
- ▲ 10/17 Necursボットネットがランサムウエア Lockyやトロイの木馬Trickybotを拡散させる。また、ダウンローダーがデスクトップイメージやエラー情報を収集する。
- ▲ 11/23 Necursボットネットがランサムウエア Scarabを拡散

[J] メール本文に不正なURLを記載したメール攻撃

- ▲ 11/7 JCBカードを騙った攻撃メール
- ▲ 11/29 楽天カード社を騙った攻撃メール
- ▲ 12/28 Apple サポートセンターを騙った攻撃メール

[K] ビジネスメール詐欺

- ▲ 9月 三菱東京UFJ銀行が、ビジネスメール詐欺への注意喚起文書を顧客企業向けに配布
- ▲ 10/5 ニュージーランドのブドウ栽培者のメールアカウントが侵害され、別口座への請求メールが送付される。普段使われる絵文字が無いことに気づき、被害を免れる。
- ▲ 11/8 不動産取引で頭金の割引を餌に購入者をだます手口
- ▲ 12/20 日本航空が8月から9月にかけてビジネスメール詐欺の被害に。合計で約3億8千万円の被害。スカイマークにも同様のメールが届く。

NTT DATA

III. 2017年度 第3四半期のタイムライン (7/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[L] EK(Exploit Kit)を用いたマルバタイジング攻撃

- ▲ 10/4 RIGエクスプロイトキットを用いたマルバタイジングでバンキングマルウエアRamnitに感染させるキャンペーン
- ▲ 10/10 RIGエクスプロイトキットを用いたマルバタイジングで技術サポート詐欺サイトへリダイレクトし、Quant Loader経由で情報窃取マルウエアFormBookに感染させるキャンペーン
- ▲ 10/23 韓国で、Magnitudeエクスプロイトキットを用いたマルバタイジングで、ランサムウエアMAGNIBERに感染させるキャンペーン

[M] パスワードリスト攻撃

- ▲ 10/13 東邦ガスの会員サイトへパスワードリスト攻撃。103人分の個人情報が流出した可能性
- ▲ 11/4,5 ディノスセシールオンラインショップへパスワードリスト攻撃

[N] WordPressへの脅威

- ▲ 11/13 WordPressに感染するマルウエアwp-vcdの最新亜種
- ▲ 12/6 5,500近くのサイトが悪質なスクリプトに感染。キーストロークの記録や仮想通貨マイナーのロードを行う。
- ▲ 12/14 WordPressのテーマNewspaperおよびNewsmagの、旧バージョンの脆弱性を悪用するマルウエア
- ▲ 12/19 公式プラグインストアに設置されたWordPressのCaptchaプラグインにバックドアが仕掛けられていた。

NTT DATA

III. 2017年度 第3四半期のタイムライン (8/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 | 10月 | 11月 | 12月

[O] Infineon製RSAライブラリの脆弱性(ROCA)

- ▲ 10/16 インフィニオン社製セキュリティチップで用いられる暗号化ライブラリに脆弱性(CVE-2017-15361)
- ▲ 10/16 エストニア政府が個人IDカードでの対応方針を発表
- ▲ 10/30 エストニアの個人IDカードにセキュリティアップデートが行われ、新たな証明書が発行されることを発表

[P] カスペルスキー社のウイルス対策ソフトへの各国政府の対応

- ▲ 10/10 カスペルスキー社のウイルス対策製品を介してロシア政府がNSAの機密文書を窃取したことをイスラエル政府が検知し、米国に通知していた。
- ▲ 10/11 独政府は、カスペルスキー社のセキュリティソフトが米政府の機密情報を窃取した証拠はないと表明
- ▲ 10/12 カスペルスキー社は、サイバー犯罪の脅威データをインターポールと共有することに同意
- ▲ 10/23 カスペルスキー社は、同社のセキュリティ製品に対し、独立した第三者のソースコード監査を実施すると発表
- ▲ 12/1 英政府機関NCSCは、各省庁に対し、国家安全保障上のリスクから、ロシアに拠点を置くウイルス対策ソフト会社を選ぶべきではないと勧告
- ▲ 12/12 米大統領が、米連邦政府機関でカスペルスキー社製品の利用を禁じる条項を含む2018年度の国防権限法に署名
- ▲ 12/18 カスペルスキー社が、同社製品に対する米政権の禁止措置取り消しを求め、米連邦裁判所に提訴

NTT DATA

III. 2017年度 第3四半期のタイムライン (9/9)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
：脆弱性
：脅威
：サイバー攻撃・インシデント
：対策
：政府の取組

※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。

9月 10月 11月 12月

[Q] Amazon S3の設定ミスによる情報漏えい

▲ 9/6 米国防総省が収集したとみられるニュースに対するコメント等の大量の情報がAmazon S3上で公開状態に。

▲ 9/17 コンサルティング会社アクセンチュアが、Amazon S3上で機密情報を公開状態に。

▲ 9/26 中国ドローンメーカーDJIがAmazon S3上で顧客の個人情報を公開状態に。

▲ 9/27 米陸軍とNSAに属するINSCOMの機密データがAmazon S3上で公開状態に。

▲ 9/29 米ヘルスケア会社Patient Home Monitoringが、Amazon S3上で47GB以上の医療データを公開状態に。

▲ 10/3 米で信用履歴回復サービスを提供するNCFが、Amazon S3上で4万人弱の顧客情報を公開状態に。

▲ 10/6 米データ分析企業Alteryxのものと考えられる米国1億2,300万世帯の個人情報がAmazon S3上で公開状態に。

▲ 11/1 Amazon S3上のデータを不正な物と入れ替えることで、当該データを参照するWebサイトなどで中間者攻撃が可能に。GhostWriterと名付けられる。

▲ 11/6 Amazon S3に5件のセキュリティ機能が追加。外部アクセス可能なバケットは、目立つようインジケータを表示

▲ 10/5 Office 365のシステムアカウントを狙った、ボットネットによるKnockKnock攻撃

▲ 10/19 公式サイトで提供されているElmedia Playerが侵害され、遠隔接続ツールOSX/Protonを拡散させる。

▲ 10/24 Dell社PCのバックアップアプリケーションの接続先ドメインが更新漏れで6月から第三者の管理下に置かれ、不適切なコンテンツやマルウエアを配信

▲ 12/22 2015年11月に開催された国際会議Cyber3 Conference Okinawa 2015のドメインが第三者に取得され、出会い系サイトの宣伝に利用される。

引用一覧 (1/2)

(*1-1) 2017/9/7 平成29年上半期におけるサイバー空間をめぐる脅威の情勢等について | 警察庁
http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf
(*1-2) 2017/12/20 Group Behind VenusLocker Switches From Ransomware to Monero Mining | FORTINET
https://blog.fortinet.com/2017/12/20/group-behind-venuslocker-switches-from-ransomware-to-monero-mining
(*1-3) 2017/12/19 Wi-Fi端末92万台感染も　ＩｏＴ狙うサイバー攻撃 |日本経済新聞
https://www.nikkei.com/article/DGXMZO24822170Z11C17A2TJ1000/
(*1-4) 2017/12/19 ルータ製品の脆弱性を悪用して感染を広げるMiraiの亜種に関する活動 | NICTER観測レポート
http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf
(*1-5) 2017/12/7 国内における Mirai 亜種の感染急増 (2017年11月の観測状況) | IIJ-SECT
https://sect.iij.ad.jp/d/2017/12/074702.html
(*1-6) 2018/1/18 インターネット定点観測レポート(2017年 10～12月) | JPCERT/CC
https://www.jpcert.or.jp/tsubame/report/report201710-12.html
(*1-7) 2017/10/3「IoTセキュリティ総合対策」の公表 | 総務省
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html
(*1-8) 2017/10/7 Taiwanese bank tracing lost funds after hacker attacks | XINHUANET
http://www.xinhuanet.com/english/2017-10/07/c_136663819.htm
(*1-9) 2017/11/5 NIC Asia Bank seeks CIB help to track down SWIFT server hacker | The Himalayan TIMES
https://thehimalayantimes.com/business/nic-asia-bank-seeks-cib-help-to-track-down-swift-server-hacker/
(*1-10) 2017/10/16 TAIWAN HEIST: LAZARUS TOOLS AND RANSOMWARE | BAE SYSTEMS THREAT RESEARCH BLOG
http://baesystemsai.blogspot.jp/2017/10/taiwan-heist-lazarus-tools.html
(*1-11) 2017/10/10 Post-Soviet Bank Heists: A Hybrid Cybercrime Study | SpiderLabs Blog
https://www.trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/
(*1-12) 2017/11/14 CVE-2017-11882 Microsoft Office Memory Corruption Vulnerability | Microsoft セキュリティ TechCenter
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/CVE-2017-11882
(*1-13) 2017/11/28 Gaffe Reveals Full List of Targets in Spear Phishing Attack Using Cobalt Strike Against Financial Institutions | RISKIQ https://www.riskiq.com/blog/labs/cobalt-strike/
(*1-14) 2017/11/6 Mitigating and eliminating info-stealing Qakbot and Emotet in corporate networks | Microsoft Secure
https://cloudblogs.microsoft.com/microsoftsecure/2017/11/06/mitigating-and-eliminating-info-stealing-qakbot-and-emotet-in-corporate-networks/
(*1-15) 2017/11/27 Wordファイルの暗号化および自己複製機能を備えた暗号化型ランサムウェア「qkG」を確認 |トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/16463
(*1-16) 2017/12/5 Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869 | 360 netlab
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
(*1-17) 2017/10/16 ALERT! - CyberAdvisory - New Type of Cyber Extortion/Threat | Federal Student Aid
https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html

NTT DATA

引用一覧 (2/2)

(*1-18) 2017/10/18 教育情報セキュリティポリシーに関するガイドライン | 文部科学省
http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/__icsFiles/afieldfile/2017/10/18/1397369.pdf
(*1-19) 2017/11/7 Threat Group APT28 Slips Office Malware into Doc Citing NYC Terror Attack | McAfee
https://securingtomorrow.mcafee.com/mcafee-labs/apt28-threat-group-adopts-dde-technique-nyc-attack-theme-in-latest-campaign/
(*1-20) 2017/10/19 Necurs Botnet malspam pushes Locky using DDE attack | SANS ISC InfoSec Forums
https://isc.sans.edu/forums/diary/Necurs+Botnet+malspam+pushes+Locky+using+DDE+attack/22946/
(*1-21) 2017/12/13 マイクロソフト セキュリティ アドバイザリ 4053440 | Microsoft セキュリティ TechCenter
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx
(*1-22) 2017/12/12 ADV170021 Microsoft Office Defense in Depth Update | Microsoft Security TechCenter
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170021
(*1-23) 注意情報 2017年11月 | JC3 https://www.jc3.or.jp/topics/v_log/201711.html
(*1-24) 2017/12/20 日本航空、偽メールで３億８千万円詐欺被害 | 日本経済新聞
https://www.nikkei.com/article/DGXMZO24866680Q7A221C1CC1000/
(*1-25) 2017/12/22アドレス１字違い見逃す　日航3.8億円メール詐欺被害 | 日本経済新聞
https://www.nikkei.com/article/DGXMZO24979150S7A221C1EA5000/
(*2-1) 2017/9/12 Miners on the Rise | SECURELIST https://securelist.com/miners-on-the-rise/81706/
(*2-2) 2017/11/9 Exploit KitおよびScamサイトの衰退とCoinhiveの台頭 | wizSafe Security Signal
https://wizsafe.iij.ad.jp/2017/11/120/
(*2-3) 2017/10/30 Coin Miner Mobile Malware Returns, Hits Google Play | TrendLabs SECURITY INTELLIGENCE Blog
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/
(*2-4) 2017/11/30 2017年第3四半期セキュリティラウンドアップ サイバー犯罪者の狙いは仮想通貨に拡大 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/sr/sr-2017q3.html
(*2-5) 2018/1/3 NEW PYTHON-BASED CRYPTO-MINER BOTNET FLYING UNDER THE RADAR | F5 Networks
https://f5.com/labs/articles/threat-intelligence/malware/new-python-based-crypto-miner-botnet-flying-under-the-radar

NTT DATA

Global IT Innovator