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1四半期）

2017年7月13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4月～6月）は、ランサムウエアWannaCry、Petya亜種(別名PetrWrap、NotPetya、GoldenEyeなど)の大規模感染が大きく報道されました。これまでのランサムウエア感染は、メール添付ファイルの開封やWebサイトの閲覧など、ユーザー操作が必要でしたが、WannaCryやPetya亜種は、「何もしなくても感染する」「勝手に広がる」といった点が注目を集めました。このような自ら感染拡大するランサムウエアに感染しないためには、端末にセキュリティ更新プログラムを適用し、最新の状態に保つといったことが必要です。また、今後、WannaCryやPetya亜種で見られた感染拡大の自動化手法が、標的型攻撃のネットワーク内での侵害拡大に使用されることを懸念しています。

6月には、中国・韓国の銀行や証券会社に対するサイバー脅迫も行われました。発生事象をタイムラインにまとめ、サイバー脅迫された時の対応や、DDoS攻撃を使った脅迫が行われやすくなっている背景についても取り上げています。

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。WannaCry、Petya亜種に関するものや、IoTマルウエアに関するものなど、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。

I. 2017年度 第1四半期の概要 (1/2)

グローバル

この四半期は、WannaCry、Petya亜種といった、自ら感染拡大するランサムウエアの活動が観測されました(タイムライン[A])。WannaCryはインターネット経由で脆弱性を突いて感染を拡大し、150か国、30万台(*1-1)以上の端末が被害を受けています。Petya亜種もウクライナを中心に、65か国(*1-2)で被害が発生しています。どちらのランサムウエアも身代金のやり取りで稚拙な点があり、目的は金銭ではなく、社会の混乱やインフラの破壊が目的ではないか(*1-3)と考えられています。今回のトピックで詳しく解説します。

国際政治でも、サイバー攻撃が政治や外交に影響を及ぼしました(タイムライン[G])。北朝鮮は世界各国の金融機関へサイバー攻撃を行っていると報告(*1-4)され、国策としてサイバー攻撃を行っていると推測されており、US-CERTが注意喚起を行っています(*1-5)。仏大統領選では、マクロン候補の陣営にサイバー攻撃が行われました(*1-6)。また、昨年の米大統領選でも投票システムへの侵入が試みられていたというNSAの機密文書がリークされました(*1-7)。中東では、カタールの国営放送がハッキングされ、偽ニュースを流された(*1-8)ことが、カタール断交の一因とされています。

サイバー脅迫も複数報道されています(タイムライン[C])。要求に応じなければ不正に入手したデータを公開すると脅すドキシングに関しては、5月に米Netflixやディズニーが映像データを窃取され、金銭を要求されたと報道されました(*1-9,1-10)。 要求に応じなければDDoS攻撃をすると脅すRansom DDoS(RDoS)に関しては、6月にArmada Collectiveを名乗るものが、中国・韓国の銀行や証券会社を脅迫しています(*1-11)。この件については、今回のトピックで詳しく解説します。

また、ビジネスメール詐欺(BEC:Business Email Compromise)による高額の詐欺被害が報告(タイムライン[D])されており、取引先の支払い情報が変更される場合は必ず社内の承認プロセスを経るなど、警戒が必要です。

ばらまき型メールでは、MS Officeの脆弱性「CVE-2017-0199」を狙った攻撃や、 MS OfficeファイルをPDFへ埋め込んだ形式でマルウエアをばらまくやり方が、観測されています(タイムライン[H])。前者は、攻撃者にとって、被害者がマクロを有効にするというステップを省略できる点や、悪意のあるコードの検知を困難にできる点が有用です。後者は、拡張子規制によるメールフィルタリング回避を狙っていると考えられます。

I. 2017年度 第1四半期の概要 (2/2)

日本国内

3月に発覚したApache Struts 2の脆弱性を狙った攻撃が引き続き発生しています(タイムライン[I])。6月にも不正アクセスを受けたという報告がありました(*1-12)。世の中に攻撃手法が広まった、影響が大きい脆弱性は、攻撃者から狙われ続けます。脆弱性の影響を受けると判明した場合には、速やかな対処が必要です。また、情報漏えいや改ざんの被害が多く報告されていますが、4月にはランサムウエアに感染させる攻撃も確認されています(*1-13)。

5月には日本国内でもWannaCryの被害が発生しています(タイムライン[A])。警察庁は5/18までに25件の被害を確認しており(*1-14)、個人からが多数を占めますが、日立製作所やJR東日本といった企業も被害を受けています。日本の被害は海外と比較して軽微だと言われていますが、キルスイッチで救済されている端末も多数あり(*1-15)、パッチ適用の徹底が必要です。また、6月には、キルスイッチが無く暗号化機能も持たないWannaCry亜種によってネットワーク輻輳が発生し、一部のサービスが停止する被害が、日本マクドナルドで発生しています(*1-16)。

イルカ漁などへの反対を主張するサイバー攻撃「OpKillingBay」の被害が4月以降も発生(タイムライン[J])していることは、例年にない特徴です。また、攻撃対象も、一部はイルカ漁に関係のある組織ですが、関係のない水族館、官公庁、交通機関等に対する攻撃も多く確認されています(*1-17)。

II. 2017年度 第1四半期のトピック
A) 自ら感染拡大するランサムウエアの出現

WannaCry、Petya亜種といったランサムウエアは、何もしなくても感染する、勝手に広がるという点が従来と異なります。このようなランサムウエアに対して、どのような点に気を付ける必要があるのでしょうか。

表1：WannaCryとPetya亜種の比較

	WannaCry	Petya亜種
初期感染経路	インターネットからWindowsのSMBv1実装の脆弱性を突いて	会計ソフトMeDocの更新機能を侵害？ 水飲み場攻撃？メール経由？
感染拡大方法	対象：ローカルネットワーク内の端末に加えてグローバルの無作為なIPへ (*2-1) ・SMBv1実装の脆弱性	対象：ローカルネットワークのみ(*2-3) ・Mimikatzを改造したツールで取得した認証情報を用いて、PsExecとWMICを利用して拡散(*2-4) ・SMBv1実装の脆弱性(*2-4)
要求内容	300ドル相当のビットコインの支払い要求	300ドル相当のビットコインの支払い要求
被害地域	150か国以上	主としてウクライナ、その他ロシアや英国等65か国(*1-2)
被害額	約10万ドル(5/22時点)	約1万ドル(7/3時点)
キルスイッチ	特定URLへのアクセスに成功すると処理を終了	特定のファイルが存在すると処理を終了 (*2-3)
対策	Windowsセキュリティパッチの最新化(MS17-010は必須)	・Windowsセキュリティパッチの最新化(MS17-010は必須) ・最小限のユーザーにのみ、Administrator権限を付与する ・NW内の複数の端末で同じパスワードを使い回さない
その他	暗号化時のファイル削除ロジックに不備(*2-2)	暗号化キーを削除するため、マルウエア製作者でも復号困難(*2-4)

利用者の観点からは、WannaCryはメール添付ファイルの開封やWebサイトの閲覧を行わなくても感染し、Petya亜種はさらに、パッチを適用していても感染する場合がある点が、これまでのランサムウエアと大きく異なります。不審メールは開かない、不審サイトにはアクセスしない等の従来の対策だけではWannaCryやPetya亜種の感染拡大を防ぐことができませんが、**定期的にバックアップを取得**し、ランサムウエアがネットワーク経由で到達できない場所に保管するという対策は有効です。詳しくは、NTTデータの緊急調査レポートをご覧ください(*2-5)(*2-6)。

II. 2017年度 第1四半期のトピック
B) 金融機関等へのDDoS攻撃を伴うサイバー脅迫

韓国や中国の金融機関が、DDoS攻撃を回避したければ金銭を支払うよう要求される事件が発生しました。日本でも同時期に金融機関に対するDDoS攻撃が確認されました。JPCERT/CCは注意喚起を出しました。

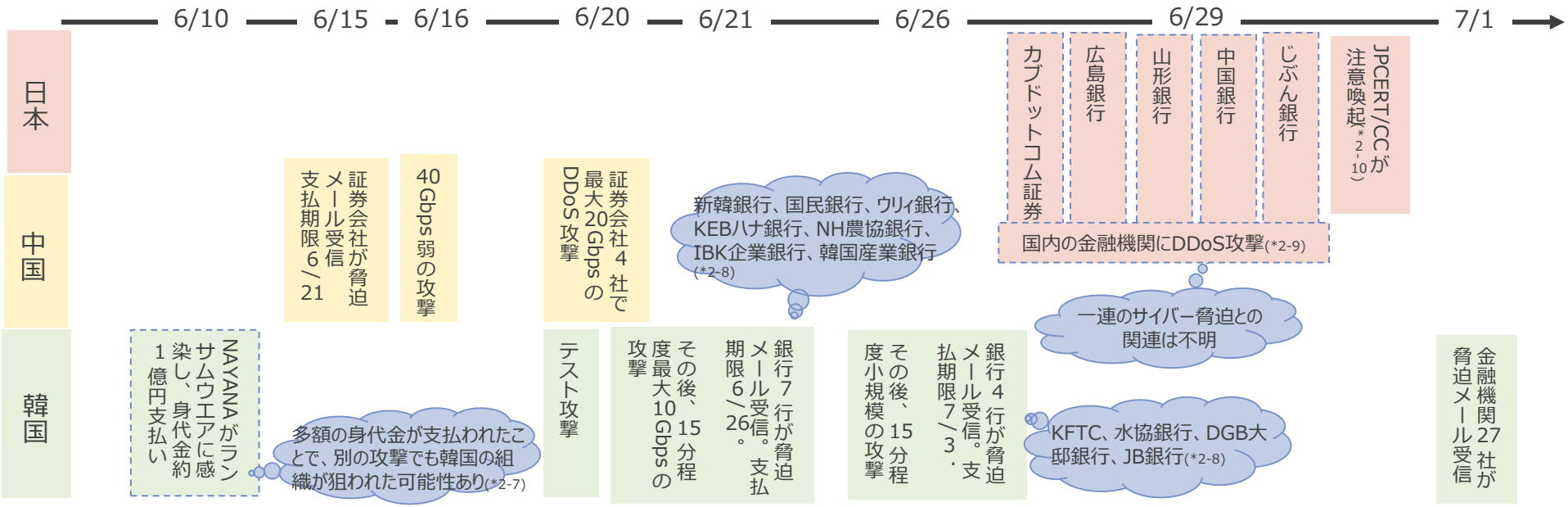

図1: 発生事象のタイムライン

6月、Armada Collectiveを名乗る者から、中国・韓国の銀行や証券会社に対して、DDoS攻撃を受けるか、ビットコインで300～450万円を支払うかを迫るメールが送信されました。脅迫メールの直後に小規模のDDoS攻撃が報告されましたが、金融サービスは通常通り運用可能でした。サービスに支障が出るレベルの大規模な攻撃があったか、脅迫を受けた金融機関が要求に応じたかどうかは確認されていません。

日本では、JPCERT/CCが注意喚起を出しています。同時期に、カブドットコム証券(*2-11)や銀行に対する30～40分程度のDDoS攻撃が複数確認されましたが、日本国内で脅迫メールを受信したかどうかは不明です。

Armada Collectiveは、2015年に最大100Gbps超のDDoS攻撃を伴う脅迫で、 ホスティングサービスProtonMail社から6000ドルの搾取に成功しています(*2-12)。その後、脅迫メールのみを送り付け実際には攻撃しない手口で約10万ドルを得た(*2-13)後、今回の事件まで表立った活動はありません。

II. 2017年度 第1四半期のトピック
B) 金融機関等へのDDoS攻撃を伴うサイバー脅迫

サイバー脅迫では、要求に応じても攻撃を回避できる保証はなく、むしろ別の攻撃の標的となる可能性があります。

6月上旬、韓国のホスティングサービス会社NAYANAがランサムウエアに感染し、復旧のため身代金約1億円を支払ったことが報じられています。セキュリティ企業Radwareは、**NAYANAが多額の要求に応じたことで、広く韓国の組織が別の攻撃の標的とされた可能性**を指摘しています。(*2-7)

脅迫に応じることで被害を回避できる保証はないだけでなく、脅迫に応じた事実が犯罪者に知れ渡りその後別の攻撃の被害を受けるおそれもあります。

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [redacted] will be DDoS-ed starting [redacted]. if you don't pay 10 Bitcoins @ [redacted]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([redacted]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [redacted], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long
time.

This is not a joke.

Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [redacted]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

図2: 脅迫メール文面の例 (*2-10)

攻撃を受けた際に備え、DDoS攻撃対策実施状況の確認や、脅迫を受けた際の対応方針や障害発生時の対応方針の確認等を、予め実施することをお勧めします。下記のように、DDoS攻撃をより容易に実施できるようになってきており、中小企業も攻撃を受けやすい状況になっているとNTTDATA-CERTでは懸念しています。

サイバー脅迫を目的とした大規模なDDoS攻撃がより容易に実現できる環境への懸念があります。

DDoS攻撃を伴うサイバー脅迫は「Ransom DDoS（RDoS）」とも呼ばれ、10年ほど前から断続的に発生しています。国内では、2015年のサイバー攻撃集団「DD4BC」によるセブン銀行等への攻撃が大きく報道されましたが、一般的に被害組織による報道発表は殆どなく、表面化することは多くありません。

しかし、**仮想通貨の流通**により攻撃者が身元を隠して金銭をやり取りしやすくなったこと、**DDoS攻撃のインフラが低価格化**していること、今後の**DDoS攻撃の大規模化予測**(*2-14)などを受けて、**大きな障害につながる攻撃を伴ったRDoS**を実現できる準備が整ってきている懸念があります。脅迫に応じない風潮こそが、RDoSの流行を食い止めることにつながります。

III. 2017年度 第2四半期以降の予測
標的型攻撃で、侵入されたネットワーク内での侵害拡大が自動化される

この四半期での大きなトピックとして、自ら感染拡大するランサムウエアの出現が挙げられます。トピックで記載したように、WannaCryやPetya亜種は、脆弱性を悪用したり、認証情報を窃取することで、自動的に感染拡大します。NTTDATA-CERTは、この**自動的な感染拡大の手法が、標的型攻撃で使用されることを懸念**しています。

一般的に標的型攻撃では、攻撃者は標的ネットワークに侵入後、そのネットワークの情報収集を行い、操作可能な端末を増やそうとします。このネットワーク内部での活動は、攻撃者の遠隔操作により実施されます。今回、WannaCryやPetya亜種の大規模感染から、脆弱性を悪用したり、認証情報を窃取して、自動的に感染拡大する手法が有用であることが確認されました。ネットワークに密かに侵入した攻撃者は、操作可能な端末を増やすために、今後はWannaCryやPetya亜種で見られた自動化手法を使い始めることが想定されます。

それでは、攻撃者にとってはどのような点がメリットでしょうか。攻撃者は遠隔操作する必要が無くなり、遠隔操作のための通信に気付かれて、**侵入が発覚する危険性が低下**します。また、手作業よりも速やかに拡大することができ、**短期間で標的ネットワークを掌握**することができます。

では、攻撃者にとって、どのような点がデメリットでしょうか。**攻撃者が感染拡大を制御できず、侵入が検知されてしまう**という点が大きなデメリットではないかと考えられます。このデメリットに対して、Petya亜種の解析で報告(*3-1)された、ノートンやSymantec製品で使われているプロセスを確認し、プロセスが見つかった場合は脆弱性を悪用した拡散をしないという動作がポイントだと考えています。つまり、**端末のセキュリティ対策状況に応じて感染拡大手法を選択したり、そもそも感染拡大対象としないといった動作を、攻撃者が実装して検知回避**してくることが予測されます。

このような点から、 NTTDATA-CERTは、自動的な感染拡大の手法が標的型攻撃で使用されることを懸念しており、標的型攻撃に対する多層的な防御がさらに重要になると考えています。

IV. 2017年度 第1四半期のタイムライン (1/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

[A] WannaCry等の自ら感染拡大するランサムウエアの出現

対策

- ▲ 3/14 MSがSMB実装の脆弱性を修正するMS17-010を公開
- ▲ 5/12 英国のセキュリティ研究者がWannaCryのキルスイッチを発見。対象のドメインを登録して感染封じ込めに寄与
- ▲ 5/15 MSがWindows XPなどサポート終了OSにSMBの脆弱性の緊急パッチを提供。WannaCry対策として。
- ▲ 6/21 2017年秋リリース予定のWindows10のアップデートからSMBv1サポートが終了予定

脅威

- ▲ 4/14 Shadow Brokersが新たな攻撃ツールを公開。SMBの脆弱性を悪用するEternalBlueやバックドアDoublePulsarなど。SWIFTシステムを標的とした攻撃ツールも
- ▲ 5/9 EternalBlueのコードが公開される（BAE Systemsの指摘）。
- ▲ 5/12 スペインCCN-CERT、US-CERTが注意喚起
- ▲ 5/14 IPAがWannaCryの注意喚起を発出。日曜日に異例の対応
- ▲ 5/16 米高官がWannaCryの被害が150か国30万件に達したと発表
- ▲ 5/17 JPCERT/CCで、持ち出し端末が感染したケースを確認
- ▲ 5/19 Malwarebytes、Wannacryの感染攻撃にEternalBlueやDoublePulsarが使用されたとの見解を表明
- ▲ 5/19 カスペルスキーがWannaCryに感染したPCの98%がWindows 7だったことを公表
- ▲ 5/22 WannaCryの身代金は約10万ドルが支払われたことを確認
- ▲ 6/22 警察庁がWannaCry亜種に対する注意喚起を発出
- ▲ 6/29 JPCERT/CCがグローバルIPアドレスが割り振られているPCやサーバーなどに対する注意喚起を発出

サイバー攻撃

- ▲ 5/12 英国公共医療NHSの48の病院で感染。手術や急患受け入れが中止に
- ▲ 5/12 日産 英国工場
- ▲ 5/15 韓国の大手映画館、広告が表示不可に
- ▲ 5/15 中国で1万8千台以上が感染か（地元メディアの報道）。
- ▲ 5/21 米国の医療機関で医療機器2台に感染
- ▲ 6/22 豪州のスピードカメラや信号機備え付けのビデオカメラが感染し、機能停止
- ▲ 6/19 日本マクドナルドがWannaCry亜種へ感染。ポイントサービスや電子マネーが使用できない状況に
- ◆ 6/21 ホンダが被害に。一時操業停止し、約1千台の生産に影響
- ▲ 5/12 JR東日本
- ▲ 5/12 静岡県富士宮市消防局
- ▲ 5/13 日立総合病院
- ▲ 5/15 日立製作所
- ▲ 5/15 川崎市上下水道局
- ▲ 5/16 トレンドマイクロ、日本国内でWannaCryの攻撃1万6千件以上を確認・ブロックしたと発表。メールでの拡散は確認されず。

Petya亜種

- ▲ 6/27 ウクライナ首都キエフの国際空港、地下鉄、市役所等で不具合が発生。その他欧州やロシア等で感染報告
- ▲ 6/27 ベルギーCERT.be、US-CERTが注意喚起
- ▲ 6/28 IPA、JPCERT/CCが注意喚起

NTT DATA

IV. 2017年度 第1四半期のタイムライン (2/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

脆弱性

- ▲ 4/14 Bosch社の自動車向け走行履歴記録機器に遠隔からエンジンを停止できる脆弱性が見つかる。
- ▲4/25 Twitterに第三者が勝手にツイートできる脆弱性があったことが発覚
- ◆5/9 MSのマルウエア対策エンジンに重大な脆弱性
- ▲5/11 HPのPCでキーロギング機能を持ったドライバが見つかる。
- ▲5/25 MSのマルウエア対策エンジンに再び脆弱性
- ▲5/23 動画プレイヤーで、字幕ファイルを用いたシステム乗っ取りの脆弱性
- ★5/24 Sambaの脆弱性(CVE-2017-7494)を公表
- ▲6/23 MSのマルウエア対策エンジンに再び脆弱性
- ▲ 6/15 WordPress用プラグイン「WP Job Manager」に画像をアップロードされる脆弱性が見つかる。

脅威

- ▲ 4/4 WordPressにブルートフォース攻撃で不正ログインし、.jsファイルに悪意あるコードを挿入する攻撃
- ▲ 4/4 iOS向けスパイウエア「Pegasus」のAndoroid版が発見される。
- ▲ 4/6 ATMをリモート操作するファイルレスマルウエア "ATMitch"
- ▲ 4/25 カスペルスキーがファイルレスマルウエアが増加傾向にあると報告
- ▲4/26 MSのサポートを装った詐欺について注意喚起
- ▲5/30 Sambaの脆弱性を狙った仮想通貨マイニングマルウエアが発見される。
- ▲5/23 ワーム機能を持ったマルウエアQakbot/Pinkslipbotの活動が観測される。
- ▲6/20 トレンドマイクロが、不正広告キャンペーンAdGholasに関する報告
- ▲6/20 トレンドマイクロが、2月前後からバンキングマルウエアRAMNITが日本のクレジットカード会社を情報詐取対象としていると報告
- ◆ 6/12 US-CERTが重要インフラを狙ったマルウエアCrashOverrideへ注意喚起
- ▲ 6/9 Morphisec Labが米国のレストランを標的としたFIN7によるファイルレスマルウエア攻撃について報告

感染させる

[B] IoTマルウエアの脅威増大

- ▲ 4/8 IoTマルウエアBrickerbotが感染拡大。感染すると機器が使用不能に。Miraiと同様にtelnetをブルートフォース攻撃
- ◆ 4/17 IoTマルウエアHajimeがMiraiと感染拡大を争う。
- ▲ 4/27 4つの異なるプロトコルを利用するIoTマルウエアLinux/Shishigaが発見される。
- ▲ 5/11 ネットワークカメラをボット化するIoTマルウエアPersiraiが出現
- ▲5/23 AkamaiがボットIoTデバイスを利用したログイン試行について報告
- ▲ 5/25 ペースメーカーが多数の脆弱性を持つことに注意喚起
- ▲ 6/21 カスペルスキーの調査で、ハニーポットでのIoTマルウエアの観測数が、すでに昨年の2倍を超える。

サイバー攻撃

- ▲ 4/3 「GitHubを使うプログラマー」を狙ったマルウエア攻撃が発生
- ▲ 4/10 米テキサス州ダラスで警報システムのサイレンが鳴り続ける。何者かが無線で偽の制御信号を送信したか。
- ▲ 6/14 英ロンドン大学とアルスター大学がランサムウエアMole被害に
- ▲ 6/25 英議会を狙ったサイバー攻撃

NTT DATA

IV. 2017年度 第1四半期のタイムライン (3/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定

◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

サイバー攻撃

▲ 6/10 韓国のWebホスティングサービスNAYANAがランサムウエアErebusに感染。身代金を支払う。

[C] サイバー脅迫

ドキシング

▲ 5/1 thedarkoverlordというハッカーがNetflixオリジナル作品の次期シーズンを公開。同社が金銭要求に応じなかったため。

▲ 5/19 MacやiOSのアプリベンダPanicからソースコードが盗まれ、金銭を要求される。

▲ 5/16 米ディズニーへサイバー攻撃。新作映画が盗まれ、金銭を要求される。

▲ 5/17 印Zomatoへサイバー攻撃。顧客情報が流出するが、攻撃者の要求に応じることで、流出データ削除に合意

関連？

RDoS

▲ 6/21 韓国の銀行が、ハッカー集団Armada CollectiveからDDoS攻撃のサイバー脅迫

関連？

▲ 6/29 カブドットコム証券に対するDDoS攻撃

[D] ビジネスメール詐欺(BEC)

▲ 5/3 GoogleとFacebook、合計100億円以上の被害にあっていたことが発覚

▲ 5/30 英国の法律事務所が10万ポンド以上の被害に

▲ 6/12 米Southern Oregon Universityが約190万ドルの被害に

▲ 6/21 ニューヨーク最高裁判事が約100万ドルの被害に

▲ 4/5 ブラジルの銀行、ハッカーにDNSを5時間乗っ取られ、ユーザーの認証情報の窃取やマルウエア配布が発生

▲ 4/26 米防衛企業Northrop Grummanの従業員向けサイトがハッキング。個人情報が流出

▲ 5/18 教育プラットフォームEdmodoから個人情報約7,700万件が流出

▲ 6/30 音楽ストリーミング配信サービス8tracks、1,800万人分の顧客情報が流出

NTT DATA

IV. 2017年度 第1四半期のタイムライン (4/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

サイバー攻撃

[E] イベントを狙った攻撃

- ▲ 4/10 「マイナンバー制度の更新が必要」とだますメールが流通。新年度のタイミング狙った攻撃か。
- ▲ 4/17 米国の確定申告者を狙った攻撃メールが流通。添付ファイルにJavaベースのトロイの木馬

[F] PoS経由で決済カード情報を窃取する攻撃

- ▲ 4/14 Inter Continental HotelでPoSマルウエア感染が発生。今年2回目
- ▲ 4/14 米レストラン・チェーン「Shoney's」でPoSシステムがマルウエアに感染
- ▲ 4/19 PoSマルウエア「RawPoS」、米国の運転免許証の情報を狙う。
- ▲ 5/30 米レストランチエーンChipotleで、PoSマルウエア感染によるカード情報漏えい

[G] 国際政治に関連した攻撃

- ◆ 4/3 カスペルスキーが攻撃者グループLazarusと北朝鮮とのつながりを指摘
- ▲ 4/6 中国に関連した攻撃グループが米国の経済団体のwebサイトに情報窃取マルウエアのリンクを仕掛けたと報道。米中首脳会談の直前
- ◆ 4月下旬から5月上旬にかけ、北朝鮮による世界各国の金融機関へのサイバー攻撃に関する言及が相次ぐ。
- ▲ 4/23 中国のハッカーが韓国軍にサイバー攻撃、ミサイル迎撃システム配備に関連か。
- ◆ 4/25 仏大統領選でマクロン候補の関係者へサイバー攻撃
- ▲ 4/25 独政党のシンクタンクへサイバー攻撃
- ▲ 5/11 米CIA、対北朝鮮の専門組織を設立
- ▲ 5/13 朝鮮総連HPにサイバー攻撃。不正なプログラムを仕込まれる。
- ▲ 5/20 北朝鮮の制裁決議違反を調査している国連安全保障理事会制裁委員会へサイバー攻撃
- ▲ 5/29 カタールの国営放送がハッキングされる。
- ▲ 6/3 UAEの米国大使のメールが漏えい
- ▲ 6/6 2016年の米大統領選挙で、ロシアの情報機関が選挙システムへ侵入を試みていたとするNSAの機密文書がリークされる。
- ▲ 6/8 カタールに拠点を置く報道機関アルジャジーラへサイバー攻撃
- ▲ 6/14 US-CERTが北朝鮮のサイバー攻撃に対して注意喚起
- ▲ 6/21 米政府高官が、ロシアのハッカーが米国の21州で選挙システムを攻撃していたことを証言

NTT DATA

IV. 2017年度 第1四半期のタイムライン (5/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

サイバー攻撃

[H] ばらまき型メール攻撃

MS Officeの脆弱性「CVE-2017-0199」

- ◆ 4/10 MS Officeにゼロデイ脆弱性(4/11にパッチ公開)。Dridexばらまきに悪用、日本での被害はなし
- ▲ 6/7 CVE-2017-0199の脆弱性を突いたUrsnifの日本語ばらまきメール

MS OfficeファイルをPDFへ埋め込む

- ▲ 4/21 VBAマクロを含むWordファイルがPDFに埋め込まれた形式でランサムウエアLockyがばらまかれる。
- ▲ 5/11 NecursボットネットがランサムウエアJaffをばらまく。MS OfficeドキュメントがPDFに埋め込まれた形式
- ▲ 5/23 ランサムウエアJaffがばらまかれる。MS OfficeドキュメントがPDFに埋め込まれた形式
- ▲ 6/14 エクセルマクロをPDFに埋め込む形式でバンキングマルウエアTrickBotがばらまかれる。

- ▲ 6/2 パワーポイントファイルのハイパーリンクにマウスオーバーするとZusyトロイに感染するメールがばらまかれる。
- ▲ 6/7 ランサムウエアJaffがばらまかれる。
- ▲ 6/7 NecursボットネットがバンキングマルウエアTrickBotをばらまく。
- ▲ 6/8 UrsnifにBootkit機能が追加されたことが報告される。

インシデント

- ▲ 6/20 米有権者1億9800万人分の個人情報が、誰でもアクセス可能な状態で保存されていたことが発覚

政府の取組み

- ▲3/31 ドイツがサイバー軍を設立
- ▲ 6/1 中国でサイバーセキュリティ法が施行
- ▲ 6/30 豪州が軍にサイバー部門を新設

対策

- ▲ 4/13 セキュアIoTプラットフォーム協議会は、IoT機器のセキュリティ標準の整備を開始。デバイス製造時に電子証明書の格納など
- ▲5/10 SHA-1証明書、MS EdgeとIE11で無効に
- ▲5/23 YahooがYahoo MailでのImageMagickライブラリの利用を終了
- ▲6/14 ランサムウエアJaffで暗号化されたファイルを復号するツールをカスペルスキーが提供
- ▲6/2 Googleが、機械学習モデルがスパムとフィッシングメールを99.9%の精度で検出できるようになったと発表

NTT DATA

IV. 2017年度 第1四半期のタイムライン (6/6)

▲：世界共通
▲：海外の一部地域限定
▲：日本国内限定
◆：記事数10件以上
★：記事数20件以上

※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。

3月 4月 5月 6月

脅威

▲ 4/26 2016年にIPA情報セキュリティあんしん相談窓口に寄せられた相談の分析で、偽サポート詐欺被害の相談相次ぐ。

▲ 4/27 PW管理が甘いサーバーに対して直接ログインし、暗号化される被害についてIPAが報告

▲ 5/25 Windowsアプリケーションでの DLL読み込みやコマンド実行に関する脆弱性に対する注意喚起

▲5/25 警視庁が、サポートが終了した IIS6.0の脆弱性を狙う攻撃を観測

サイバー攻撃

[I]Apache Struts 2の脆弱性を狙った攻撃

▲ 4/6 SANSが注意喚起：Apache Struts 2の脆弱性CVE-2017-5638を悪用し、Windowsコンピュータにランサムウエアを感染させる攻撃

▲ 4/13 総務省の統計情報サイトが不正アクセスを受け、個人情報2.3万件超が流出した恐れ

★ 4/25 ぴあが運営していたB.LEAGUEのサイトから15万件超の個人情報が流出した恐れ

▲5/1 GMOペイメントゲートウェイ(株)が、再発防止委員会の調査報告を公開

▲5/2 NICTの研究所公開サーバーへの不正アクセスが判明。378件の利用者情報が流出した恐れ

▲6/6 国交省「土地総合情報システム」へ不正アクセス。個人情報の流出は確認されず。

▲ 4/1 アリアファームのwebサイトが不正アクセスを受け、スパムメール送信の踏み台に。WordPressの脆弱性を悪用される。

▲ 4/7 公正取引委員会の「審決等データベース」が不正アクセスを受け、スパムメール送信の踏み台に

▲ 4/11 SKYSEA Client Viewの脆弱性を悪用する攻撃が重要インフラ向けに発生、警視庁が捜査

▲ 4/11 東京都の宅地建物取引業者情報のインターネット情報提供システムが不正アクセスを受け、4/11からサイト閉鎖

▲ 4/25 通販サイト優生活へ不正アクセス。3,989件の、カード情報を含む個人情報が流出した恐れ

▲ 5/22 InterFM897のWebサイトへ不正アクセス。2,728件の個人情報が流出した恐れ

▲ 6/20 SBSグループがランサムウエア被害に

▲ 6/8 医療品情報提供サイトオフィス・トウェンティーワンへ不正アクセス。個人情報流出の恐れ

[J] OpKillingBayによるDDoS攻撃

▲ 4/18,25,26 国立国会図書館

▲ 4/22 裁判所

▲ 4/27 警視庁

▲ 4/30 国立公文書館

▲ 5/30 鳥羽水族館

▲ 5/31 伊丹空港

▲ 6/11 JR西日本

インシデント

▲ 6/22 メルカリ、顧客5万人分の個人情報が一時閲覧可能に

政府の取組み

▲ 4/1 NICT、ナショナルサイバートレーニングセンターを設置

▲ 4/1 IPA、産業サイバーセキュリティセンターを発足

▲ 4/3 警視庁、サイバー攻撃対策センターを発足

◆ 5/30 改正個人情報保護法施行

▲ 6/20 日本政府は地方自治体やインフラ関連企業を対象にサイバー防御演習CYDERを開始

NTT DATA

引用一覧 (1/2)

(*1-1) 2017/5/16 米高官 サイバー攻撃の被害は約１５０か国で３０万件以上 | NHKニュース
http://www3.nhk.or.jp/news/html/20170516/k10010983131000.html
(*1-2) 2017/6/27 New ransomware, old techniques: Petya adds worm capabilities | The new Microsoft Malware Protection Center blog https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
(*1-3) 2017/6/28 ExPetr/Petya/NotPetya is a Wiper, Not Ransomware | SECURELIST
https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/
(*1-4) 2017/4/3 Lazarus Under The Hood | SECURELIST https://securelist.com/lazarus-under-the-hood/77908/
(*1-5) 2017/6/13 HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure | US-CERT https://www.us-cert.gov/ncas/alerts/TA17-164A
(*1-6) 2017/4/25 仏大統領選でハッカー攻撃、ロシア関与か | THE WALL STREET JOURNAL
http://jp.wsj.com/articles/SB10571167453707423750304583105451548776808
(*1-7) 2017/6/6 TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION | The Intercept https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/
(*1-8) 2017/5/24 カタール、国営通信社がハッキング被害＝首長の偽声明文を掲載 | 時事通信
http://www.jiji.com/jc/article?k=2017052400450
(*1-9) 2017/5/1 Netflix番組の新シーズンをハッカーがリークか | CNET Japan https://japan.cnet.com/article/35100581/
(*1-10) 2017/5/16 ハッカーがディズニーに支払い要求、新作映画盗んだと主張＝米誌 | REUTERS http://jp.reuters.com/article/walt-disney-cyber-idJPKCN18C094
(*1-11) 2017/6/21 Hacker group threatens to launch cyberattack against S. Korean banks | YONHAP NEWS
http://english.yonhapnews.co.kr/search1/2603000000.html?cid=AEN20170621016100320
(*1-12) 2017/6「土地総合情報システム」における不正アクセスおよび情報流出の可能性について | 国土交通省
http://www.mlit.go.jp/report/press/totikensangyo05_hh_000129.html
(*1-13) 20174/6 Java Struts2 Vulnerability Used To Install Cerber Crypto Ransomware | SANS ISC
https://isc.sans.edu/forums/diary/Java+Struts2+Vulnerability+Used+To+Install+Cerber+Crypto+Ransomware/22264/
(*1-14) 2017/5/19 警察庁把握は計２５件に　ランサムウエア被害 | 産経ニュース
http://www.sankei.com/affairs/news/170519/afr1705190033-n1.html
(*1-15) 2017/6/13「WannaCryはまだ終わっていない」――キルスイッチで毎日1000台が救われている | @IT
http://www.atmarkit.co.jp/ait/articles/1706/13/news081.html
(*1-16) 2017/6/28 ［特報］「WannaCry亜種に感染」、マクドナルド障害のマルウエア判明 | ITpro
http://itpro.nikkeibp.co.jp/atcl/news/17/062801786/
(*1-17) 2016/8/22 OpKillingBay 2016および、OpWhales、OpSeaWorld メモ | (n)inja csirt http://csirt.ninja/?p=824

引用一覧 (2/2)

(*2-1) 2017/5/18 ランサムウェア「WannaCry／Wcry」のワーム活動を解析：侵入／拡散手法に迫る | トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/14920
(*2-2) 2017/6/1 WannaCry：暗号化されたファイルに復元の可能性 | Kaspersky Blog https://blog.kaspersky.co.jp/wannacry-mistakes-that-can-help-you-restore-files-after-infection/15898/
(*2-3) 2017/6/30 話題のMBR破壊型ワームランサムウェアの内部構造を紐解く | MBSD Blog http://www.mbsd.jp/blog/20170630.html
(*2-4) 2017/6/28 続報：欧州を中心に甚大な被害、暗号化ランサムウェア「PETYA」の活動を詳細解析 | トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/15353
(*2-5) 2017/5/17 大規模ランサムウエア感染に関する緊急調査レポートを公開 | NTTデータ
http://www.nttdata.com/jp/ja/news/information/2017/2017051701.html
(*2-6) 2017/6/29ランサムウエア「Petya」亜種の大規模感染に関する緊急調査レポートを公開 | NTTデータ
http://www.nttdata.com/jp/ja/news/information/2017/2017062901.html
(*2-7) 2017/6/23 The Bottom Line: RDoS On The Rise | radware https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/bottom-line-rdos-rises/
(*2-8) 2017/6/27 Korean banks on alert over cyber attack | THE KOREA TIMES
http://www.koreatimes.co.kr/www/biz/2017/06/488_232011.html
(*2-9) 2017/7/2 | 辻伸弘氏のツイート https://twitter.com/ntsuji/status/881538946127110144
(*2-10) 2017/6/29 Armada Collective を名乗る攻撃者からの DDoS 攻撃に関する情報 | JPCERT/CC
https://www.jpcert.or.jp/newsflash/2017062901.html
(*2-11) 2017/6/29 6月29日(木)に発生したサイバー攻撃について | カブドットコム証券
http://kabu.com/company/pressrelease/info/2017/0629_001.html
(*2-12) 2015/11/5 ProtonMail Statement about the DDOS Attack | ProtonMail
https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/
(*2-13) 2016/4/25 Empty DDoS Threats: Meet the Armada Collective | CLOUDFLARE https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/
(*2-14) akamai's [state of the internet] / security Q1 2017 report | Akamai
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-security-report.pdf
(*3-1) 2017/6/29 Petya ランサムウェアの猛威: 現時点で知っておくべきこと |シマンテック公式ブログ
https://www.symantec.com/connect/ja/blogs/petya

NTT DATA

Global IT Innovator