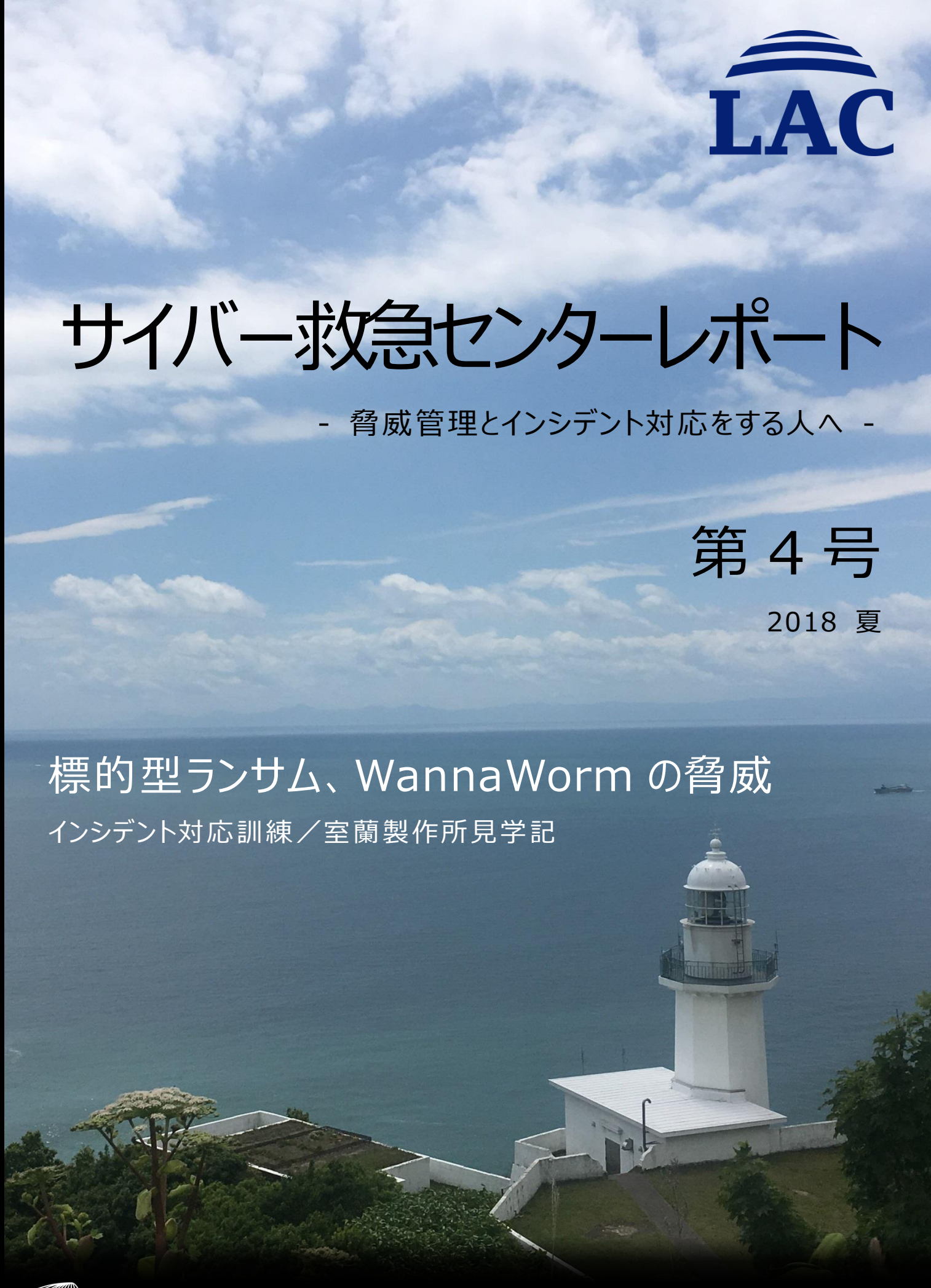

サイバー救急センターレポート

- 脅威管理とインシデント対応をする人へ -

第４号

2018 夏

標的型ランサム、WannaWorm の脅威

インシデント対応訓練／室蘭製作所見学記

CYBER EMERGENCY CENTER

2018 年 8 月 15 日

サイバー救急センター

サイバー救急センターレポート

第 4 号 / 2018 夏

目　　次

03 はじめに

04 サイバー救急センターの出動傾向

07 攻撃者の残した痕跡に学ぶ - 標的型ランサムの出現

10 脅威分析報告 - WannaWorm の脅威

14 コラム：セキュリティ百景
#7 インシデント対応訓練 ～ 雪の中の熱い一日 ～
#8 室蘭製作所 見学記

16 編集後記

サイバー救急センターレポート（以下、本文書）は、情報提供を目的としており、記述を利用した結果生じるいかなる損失についても、株式会社ラックは責任を負いかねます。
本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。
LAC、ラック、サイバー救急センターは、株式会社ラックの商標または登録商標です。
この他、本文書に記載した会社名・製品名は各社の商標または登録商標です。
表紙、裏表紙の写真は、内田法道の著作物です。
本文書を引用する際は出典元を必ず明記してください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© 2018 LAC Co., Ltd. All Rights Reserved.

はじめに

内田 法道

株式会社ラック
サイバー救急センター長

出動傾向の統計データを毎号載せていますが、仮想通貨発掘ソフト（コインマイナー）関連の相談、およびビジネスメール詐欺（BEC、Business Email Compromise）の相談が増加したことから、今号より分類を追加することにしました。ビジネスメール詐欺については、情報処理推進機構（IPA）が今年の春に公開した「情報セキュリティ10大脅威 2018」においても、前年のランク外から組織部門の第3位にランクインしています。

追加した2つの分類は、いずれも金銭を目的とした攻撃者グループによる脅威と考えられ、あの手この手でサイバー空間から金銭を得ようとする攻撃者による脅威の高まりを示しています。従来から見られた、不正送金マルウェアやランサムウェアに感染させることを目的とした、ばら撒き型メールなどによる脅威も継続しています。また、今号で紹介しているように APT 攻撃の手法を用いた金銭目的の攻撃者グループの存在も確認されています。

これらの多様かつ複雑な脅威で用いられる攻撃手法などへの理解は、インシデント対応、特に初動対応での適切な判断や対処に役立ちます。今号のレポートも、皆様のインシデント対応の一助になれば、幸いです。

サイバー119の出動傾向

2018年4月～6月の出動傾向

当該期間は、「金銭目的の攻撃」により被害を受けた組織からのインシデントの相談が多く見られます。

攻撃の手口としては、不正送金マルウェアに感染させるばらまき型メール、サーバなどへ不正侵入後に仮想通貨発掘ソフト（コインマイナー）の設置は継続しつつ、Office 365、G Suite などのクラウド型メールサービスのアカウント窃取によるビジネスメール詐欺（BEC、Business Email Compromise）が増加傾向にあります。そのため、相談の分類としてコインマイナーおよび BEC の分類を追加しました。

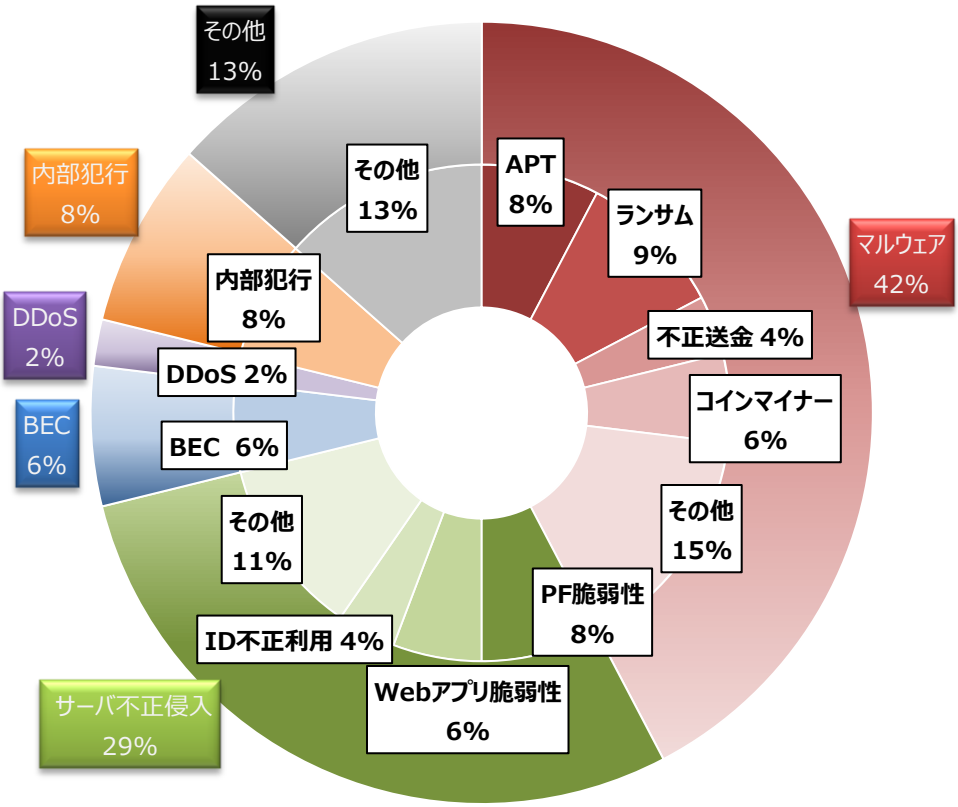

図 1-1 2018年 4月～6月のインシデント傾向

マルウェア関連のインシデント傾向

(1) Advanced Persistent Threat 攻撃（APT 攻撃）

前四半期（2018 年 1 月～3 月）から引き続き、複数の組織から APT 攻撃（執拗に特定の組織を標的とした高度なサイバー攻撃）と推測されるインシデントの相談を受けました。その中には、日本を攻撃対象としている APT2 や APT10 と呼ばれる攻撃者グループが関わっていると推測されるインシデントが確認されており、引き続き日本の企業・団体が狙われております。

攻撃の手口として、関係者を装った標的型メールに加え、認証サーバに対するブルートフォース攻撃による不正侵入も確認しました。当該ブルートフォース攻撃に利用されたアカウントは、Administrator などのデフォルトで作成されているアカウント名だけでなく、各組織で個別に作成されたと思われる特権アカウントも攻撃を受けました。

APT 攻撃は長期間に渡り侵入した組織の環境を探索し機密情報を窃取していきます。また、昨今では、攻撃手法がより巧妙化し未然に防ぐことはますます困難となってきています。そのため、不正侵入されることを前提とし、

- 多層化された対策による早期検知
- ネットワークのアクセス制御の見直し
- 通常業務で利用するネットワークと機密情報を扱うネットワークの分離

など、被害範囲を極小化するセキュリティ対策を検討ください。

(2) WannaCry 感染

2017 年 5 月中旬に話題となった WannaCry ですが、1 年経過した現在でも感染した組織から相談を受けています。感染原因は、セキュリティパッチ「MS17-010」を適用していない PC が外部のネットワークで WannaCry に感染し、当該感染 PC を組織内ネットワークに接続したことにより組織内に感染したと推察されます。また、SIM カード付きの PC がグローバル IP アドレスを保持しており、同時に組織内ネットワークに接続していたため、脆弱性が悪用されてグローバル IP アドレス経由で感染し、更に組織内ネットワークに感染被害が拡大したというケースもありました。

相談を受けた WannaCry の検体は、いずれも自己増殖の機能は有するものの、暗号化機能が無効化されていたため、感染した PC を保有する人は自身の PC が WannaCry に感染していることに気づかず、複数の組織に感染被害を拡大していました。

また、WannaCry に搭載されている自己増殖機能を利用して感染を拡大した後に、ランサムウェア（ファイルの暗号化）ではなく、仮想通貨発掘ソフト（コインマイナー）を実行する亜種も確認しました。

閉鎖されたネットワークにおいてもメンテナンスなどで外部の持出し PC を接続することがある場合は、改めてすべての端末に対して「MS17-010」の適用状況を確認ください。また、把握・管理されていないPC やサーバがネットワークに接続されていないか点検することも推奨します。

BEC のインシデント傾向

ビジネスメール詐欺（BEC、Business Email Compromise）による被害を受けた組織からの相談が増えています。サイバー救急センターで相談を受けた攻撃手口の多くは、正規の取引先のメールアドレスからのメールであり、メールの配送経路を確認しても、送信元メールアドレスの偽装は確認できませんでした。

BEC と同時期に、Office 365 や G Suite といったクラウド型のメールサービスのアカウントを窃取されたという相談件数も増加しています。これは、電子メールの送信元メールアドレスの偽装対策として SPF（Sender Policy Framework）や DKIM（DomainKeys Identified Mail）の導入が進み、送信元メールアドレスを偽装してもメールが届き難くなったという現状があると推察されます。そのため、攻撃者グループが正規なメールアドレスを入手して悪用するために、パスワードのみで悪用可能なクラウド型のメールサービスが狙われていると考えております。

クラウド型のメールサービスは、インターネットに接続できる環境であれば、どこからでもアクセスができるという便利な側面がある一方で、アカウントやパスワードが漏れてしまうとその便利さ故に容易に不正利用ができてしまう問題があります。このような被害を最小限に抑えるためにも、クラウド型のメールサービスを利用する際は、二要素認証や二段階認証などの認証強化、アクセス元の IP アドレスの制限などのセキュリティ対策を、必ず検討、導入ください。

また、自社が適切なセキュリティ対策を実施していたとしても、取引先の会社のアカウントが窃取されている可能性もあります。取引先の正しいメールアドレスから送られたメールであったとしても、振込先の急な変更に関して連絡を受けた場合には、メールで確認するのではなく、電話で先方へ確認する手順とするなど、経理担当者の業務フローの見直しも検討ください。

攻撃者の残した痕跡に学ぶ

標的型ランサム攻撃の出現

(1)APT 攻撃

近年 APT 攻撃と呼ばれる高度な攻撃が注目されています。防衛、航空宇宙産業、金融、政府機関、重要インフラなどを主な標的組織として、フィッシングメールなどを使って侵入後、長期間潜伏して情報を奪っていくことから、APT 攻撃は金銭よりも、情報の窃取を目的とした諜報活動としての意味合いが強いと考えられています。

APT 攻撃で使われるフィッシングメールには、

- 既に侵入済みの他の組織のメールアドレスを送信元とする
- 標的組織とやり取りされているメール文面を転用する
- 違和感のない正しい日本語文面が使われている

など、高度に偽装された相談事案を多く受けています。

フィッシングメールの添付ファイルを標的組織で開いてしまった場合、攻撃者は標的組織内に足掛かりとなるホストを得ることになり、そこを起点にして組織内の複数の他のホストに侵入し、目的となる情報を収集します。それらの操作の多くは、攻撃者が手動で行っているものと考えられます。

(2) ばら撒き型ランサムウェア

一方、近年注目されている別種の攻撃として、ばら撒き型ランサムウェアがあります。2016 年から 2017 年にかけて爆発的に感染報告が増え、サイバー救急センターにも多数の相談がきたこの攻撃は、感染ホスト上のファイル、および感染ホストからアクセス可能なネットワークでファイル共有されているファイルを自動的に暗号化し、復号のための金銭を要求します。

ランサムウェアも感染方法としては APT 攻撃と同様にフィッシングメールが使われますが、

- 送信元アドレスが不審なメールアドレスである
- 多くの対象に同一文面で送信をする
- 文面が英文あるいは違和感のある日本語である

などの違いがあり、偽装が甘く不審さを感じられるメールになっています。

ばら撒き型ランサム攻撃においてフィッシングメールの添付ファイルを開いてしまった場合、ファイルを開いたホスト上のファイル、およびネットワーク経由でアクセス可能な共有フォルダ内のファイルが暗号化されます。さらに、最近では MS17-010 の脆弱性を悪用する EternalBlue と呼ばれる攻撃ツールによって、感染ホストを自動で拡大していく事例も報告されています。

ばら撒き型ランサムウェアは、ファイルが暗号化されて利用できなくなるため感染時の被害や影響は大きいものの、サイバー救急センターの調査では外部に情報を送信する機能を確認していないため、ファイルやデータベースなどの機密情報の漏えいリスクは低いと考えられます。ただし、既に情報漏えいにつながる他のマルウェアに感染していたり、今後情報漏えいの機能を有するランサムウェアが登場する可能性があり、楽観視することはできません。

(3) 標的型ランサム攻撃

2017 年 7 月に、Cylance 社[1]や Cybereason 社[2]により「ONI」と呼ばれるランサムウェアを用いる日本を狙った攻撃についてレポートがありました。この攻撃では、日本ではあまり馴染のない「Ammyy Admin」という遠隔操作ツール[3]が利用されます。また、前述のばら撒き型ランサムウェアとは異なり、攻撃者は APT 攻撃のように遠隔操作ツールを使って手動操作で組織内で侵入を拡大していきますが、最終的に「ONI」と呼ばれるランサムウェアを発動させてファイルを暗号化し、復号を盾に金銭を要求する脅迫文を残すことがレポートされています。

サイバー救急センターでも、ランサムウェア「ONI」を用いる攻撃者グループによるランサムウェア感染の相談は受けておりましたが、最近この攻撃者グループによる犯行と考えられる、ランサムウェアを用いずに金銭の支払いを脅迫する事案の相談を受けました。当該事案では、攻撃者グループは Ammyy Admin を用いて標的組織のネットワークを長期間調査した後、ファイルを暗号化して身代金を要求するのではなく、持ち出した機密情報の公開を示唆して、金銭の支払いを要求してきました。

攻撃者の最終的な目的は、ばら撒き型ランサムウェアと同じく金銭ではあるものの、フィッシングメールの高度な偽装、遠隔操作ツールを用いて手動で侵入活動を長期間継続するなど、APT 攻撃で見られる手法が多く使われており、金銭目的の攻撃グループが APT 攻撃の手法を取り入れたことがうかがえます。

この標的型ランサム攻撃で見られた特徴は下記の通りです（３種の攻撃の特徴は下表の通り）。

- 日本企業のメールアドレスを送信元（標的組織とは無関係）とする日本語文面のフィッシングメールを用いる

1 https://www.cylance.com/ja_jp/blog/jp-oni-ransomware-globeimposter.html
2 https://www.cybereason.co.jp/blog/ransomware/1830/
3 Ammyy Admin は「Team Viewer」に似た正規のソフトウェアですが、攻撃者による悪用が多いことで知られています。

- フィッシングメールには暗号化ZIPで不正なマクロを含むWord文書が添付されており、メール文面に復号パスワードが記載されている
- Base64エンコードされたバイナリ（ダウンローダ）をレジストリに登録し、タスクスケジューラでこれをデコードし実行する
- Ammyy Adminを起動するよう設定を加えてからイベントビューワを起動することでWindowsのセキュリティ機構であるUAC（ユーザーアカウント制御）を回避する
- 正規のAmmyy Adminを利用するため、rl.ammyy.comへの通信が常時発生する
- PC出荷時にメーカーが作成したフォルダ（Cドライブ直下のIntelやDellなど）にファイルを置く

金銭目的の攻撃者グループが、APT攻撃の手法を用いて、身代金を支払う価値のある情報を窃取し身代金を要求するという脅威の存在が明らかになりました。攻撃者グループの変化に対応して、自組織のセキュリティ対策について定期的に見直すことが重要です。

表2-1 攻撃の特徴まとめ

	APT攻撃	ばら撒き型 ランサムウェア	標的型ランサム
フィッシングメール偽装度	高度	多くの場合不審点有	高度
情報漏えいリスク	高	低	高
潜伏期間	長期	短期	長期
他ホストへの侵入	有（手動）	有（自動）	有（手動）
攻撃者の目的	情報	金銭	金銭・情報

脅威分析報告

WannaWormの脅威

2017年5月にWannaCryと呼ばれるワームが発生し、日本でも複数の企業が被害を受けました。初期の WannaCry は早々に収束しましたが、多数の亜種もしくは類似のワームによる感染事例は、海外を中心に継続して発生しています[4]。日本では、特に複数拠点をWANで接続している環境において、複数の大規模感染事例が確認されています。

WannaCryはEternalBlueと呼ばれる攻撃ツールとDoublePulsarと呼ばれるバックドアを用いることで、感染させたホスト上でファイルの暗号化を行うランサムウェアと、自ら感染を広めるワームの機能を備えていました。サイバー救急センターでは 2017 年 5 月から現在まで複数の相談を受けておりますが、その多くの事案においてランサムウェア（つまりファイルの暗号化）の機能を有していない検体を確認しております（ランサムウェアの機能を有していないWannaCryを、本稿では便宜上WannaWormと呼ぶことにします）。WannaWormは、概ね以下の流れで感染を広めます。

1. ネットワークをスキャンしてTCP/445がオープンしているホストをスキャンする
2. EternalBlueを実行して攻撃に成功すると、DoublePulsarをアップロードして感染させる
3. DoublePulsarを使って、別のマルウェアをアップロードして感染させる
4. アップロードされたマルウェアが1.を実行して感染を広める。

EternalBlue が悪用する脆弱性を修正するパッチ（MS17-010）を適用していれば、WannaWormに感染することはありません。Microsoft社はすでにサポートが終了しているWindows XPなどの一部OSにも当該パッチを提供しているので、万が一古いOSを利用している場合には必ずパッチを適用してください。

---

4 参考URL：
https://www.mbsd.jp/blog/20170607.html
http://www.freebuf.com/articles/system/162874.html
http://www.freebuf.com/articles/network/164869.html
http://blog.netlab.360.com/msraminer-qian-fu-yi-jiu-de-wa-kuang-jiang-shi-wang-luo/

WannaWormの感染力

サイバー救急センターへの相談では、複数拠点をWANで接続している環境において、WannaWormの大規模感染被害の相談を複数受けました。EternalBlueによる攻撃は被害を受けたホストには攻撃を受けたログが残らないため、通信ログなどから感染源や被害状況を調査することになります。残念ながら通信ログなどが残されていない組織が多く、感染源となったホストの特定が困難な事案が多い傾向にあります。

WannaWormの感染力は強く、WAN内に感染端末が発生すると、WANで接続されている複数拠点に短期間で感染被害が広まります。WannaWormは、まず感染ホストが接続するネットワークセグメント内のIPアドレスにスキャンを行い、TCP/445がオープンしているホストを探します。加えて、ランダムなIPアドレスに対してもスキャンを行います。その過程でTCP/445がオープンしているホストの存在を確認すると（TCP/445の応答があるWindowsや、Sambaが動作しているLinuxもおそらく対象となります）、当該ホストのIPアドレスが含まれるネットワークセグメント内のIPアドレス（サブネットマスクが/24の範囲）に対して同様のスキャンを行います。この探索手法によって、複数拠点で別々のネットワークアドレスを使用していても、時間が経過すればするほど、多数の拠点に感染が広まることになります。

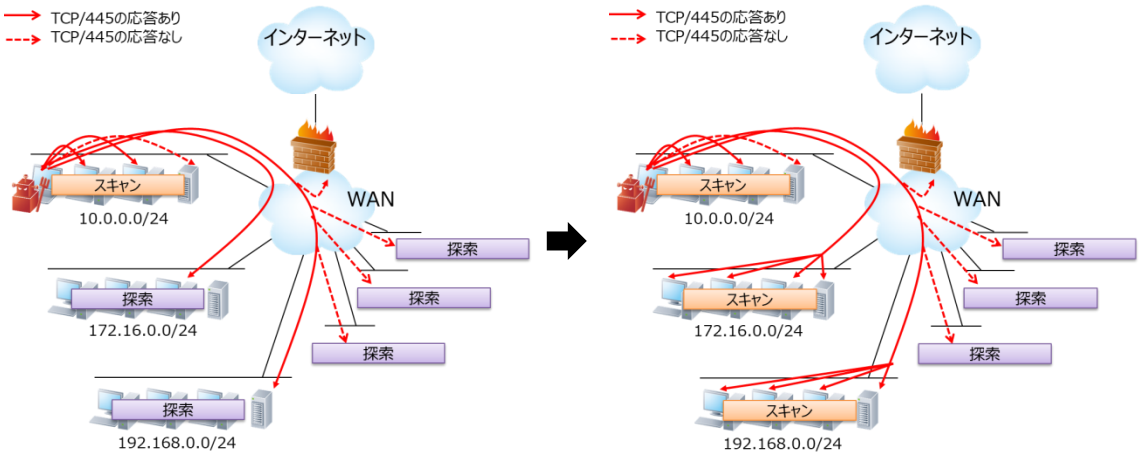

図 3-1 WannaWormの探索手法

先に述べたとおりパッチが適用されていれば影響は受けませんが、多数の拠点がある場合には、下記の理由でパッチが適用されていないホストが残っている場合があり、WAN内で複数台のホストに感染が広まることになります。

- インターネットに接続していないため、パッチを適用していない
- パッチ適用の検証にコストがかかるため、パッチを適用していない
- 管理者のセキュリティ対策意識が低く、パッチを適用していない（海外拠点に多い）
- 管理者が把握しておらず、パッチ適用もされていないホスト（野良ホスト）がネットワークに無断で接続されている

WannaWorm 感染ホストの特定方法

WAN 環境で大規模な WannaWorm の感染被害が発生した場合の対処としては、感染しているホストを特定して、ネットワークから隔離したうえで、マルウェアの完全なクリーンアップが必要となります。ただし、全ての感染ホストが特定できていることが必要になります。

感染しているホストを特定するためには、各拠点の全てのトラフィックが通過するコアスイッチなどで、通信パケットを取得、解析し、感染ホストを特定します。大量の通信パケットを解析するのは非常に手間と時間がかかりますが、Splunk などの分析ツールを利用してトラフィックを可視化することで、WannaWorm に関連する異常なトラフィックを特定しやすくなります。

WannaWorm は先に述べたとおり、まず感染ホストが接続するネットワークセグメント内の IP アドレスをスキャンしつつ、ランダムスキャンで発見したホストが含まれるネットワークセグメントのスキャンをするため、多数の IP アドレスの TCP/445 ポートに対して接続を試みます。さらに、接続先の IP アドレスから応答が無くても継続して接続を試みます。これは通常のアプリケーションには見られない動作ですが、Windows サーバを使用している場合には、複数の IP アドレスに恒常的にアクセスが発生する場合もあります。

これらを踏まえて、接続先の IP アドレス件数に閾値を設定して、当該閾値を超えた接続元 IP アドレスを Splunk で可視化したものが以下の図になります。

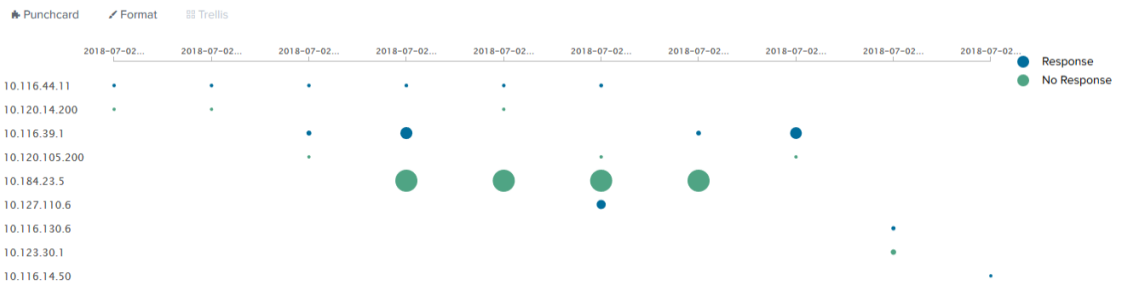

図 3-2 Splunk で可視化した WannaWorm の感染活動

図 3-2 は、縦軸に送信元 IP アドレス、横軸に時間をとり、送信元 IP アドレスからの TCP/445 通信を 1 時間単位で集計した図になります。丸の大きさは、接続先 IP アドレスのユニークな件数を表しています。また、TCP/445 の応答の有無を色分け（応答があれば青、応答が無ければ緑）しています。

例えば、10.184.23.5（縦軸の上から 5 番目）は、255 件のユニークな接続先 IP アドレスに接続を試みているため、WannaWorm に感染していることが一目でわかります。このように、Splunk などの分析ツールを利用すると、判断に必要な情報のみを適切に可視化することで、一目で異常を判断することができます。

おわりに

本稿では、WannaWorm の脅威、感染手法および特定方法について説明しました。しかしながら、そもそも、このようなインシデントを発生させないようにするためには、どうすればよいのでしょうか。

以下にサイバー救急センターで相談を受けた複数の事例に共通するポイントを纏めて一般的なシナリオにしてみました。これらのポイントが、自組織にあてはまらないかを確認していただき、WannaWorm を含めたワーム感染対策を考える際の参考にしていただければ幸いです。

1. 保守などの業務で使用するホストを、パッチ未適用かつウイルス対策ソフトの定義ファイルのアップデートが行われていない状態でインターネットに直接接続し、WannaWorm に感染する
2. 感染した WannaWorm は暗号化を行わないタイプであるため、ホストの利用者は WannaWorm の感染に気づかない
3. 上記の WannaWorm に感染したホストを、ある拠点でネットワークに接続する
4. 拠点間は WAN で接続されており、特にアクセス制限がされていないため、WannaWorm が無差別に感染を試みる
5. パッチが適用されておらず、ウイルス対策ソフトの定義ファイルのアップデートも行われていないホストが感染する
6. 感染したホストから、WAN 内の他のホストに WannaWorm の感染が広がる
7. ネットワークトラフィック監視での大量の TCP/445 通信の検知、脆弱性はあるがウイルス対策ソフトが最新化されていたホストでの WannaWorm の検知などで、WannaWorm の大規模感染が発覚する

コラム：セキュリティ百景 #7

インシデント対応訓練
～ 雪の中の熱い一日 ～

日々のインシデント対応で、サイバー救急センターには新鮮な知見が集まり続けています。このため、時にはインシデント以外でもお客様をアシストする機会があります。2018 年も明け、お正月ムードも一段落したある日。東京にも雪が舞う寒い日でしたが、燃え盛るように熱いインシデント対応の訓練を拝見する機会がありました。

今回ご縁があったのは、都内のとある会社さんです。最近は、インシデント対応を訓練する組織も増えてきましたが、この会社さんは一歩進んで、第三者からの評価を受けることで、より高い訓練効果を狙っていました。今回は、サイバー救急センターから 2 名がお伺いし、1 日かけて訓練の様子を拝見しました。

大規模なシステムを運用されている会社さんですので、その訓練も本格的なものです。司令室、コンピュータ室、会議室など複数の部屋を行き来しながらのインシデント対応の中で、運用会社さんも複数登場します。その中で、状況の把握や判断を統括するマネジメント系と、感染端末の切断や復旧を実機確認するテクニカル系の双方が連携しながら、訓練は進んでいきました。

訓練の計画は綿密に練られていましたが、それでもトラブルは起きるものです。キーマンの不在でマネジメント側の判断が遅れたり、データの処理に時間がかかってテクニカル側の手順が進まなかったり、様々なことが起きます。さらに、訓練とはいえ通常と違うことをしているのですから、ヒューマンエラーも起きやすくなります。これを、仕組みや体制でどうカバーできるのかが試されてきます。

しかし、これは実際のインシデントでも発生することです。こういった、予想外のことを事前に経験することで、訓練の意味も深まっていきます。

あっという間の一日が終わり、後日、訓練の振り返りを実施しました。話題は、今回の訓練だけに留まらず、次回以降はどんな訓練にすればより高い効果が望めるかなどに及び、さらなる高みを目指すお客様の姿勢が印象に残りました。

永安 佑希允

コラム：セキュリティ百景 #8

室蘭製作所 見学記

最近のサイバー脅威に関して説明する機会があり、2018 年 6 月 21 日(木)～22 日(金)に、株式会社日本製鋼所様の室蘭製作所を訪問しました。さらに日本製鋼所様のご好意で、室蘭製作所の工場見学をさせていただいたので、北海道室蘭の見所と併せてご紹介したいと思います。

日本製鋼所は 1907 年(明治 40 年)に北海道室蘭に設立されました。現在、本社は東京に移転され、室蘭では「日本製鋼所 室蘭製作所」として稼動し続けています。設立時は日本国内初の民間兵器工場として、戦艦の主砲などを製造していましたが、現在は 100 年以上続く製鋼技術を基に、原子力発電機の内部機材(ロータシャフトなど)や風力発電機などを製造しています。

ところで、みなさんは「製鉄」と「製鋼」の違いをご存知でしょうか。「製鉄」とは鉄鉱石から「鉄」を取り出すことです。一方、「製鋼」とは鉄から「鋼」を作ることです。鋼は鉄に比べ強靭で加工性に優れています。

室蘭製作所では「製鋼」を行っています。良質な金属スクラップ(自動車部品のプレス後の残材など)を、製造するものに合わせた添加剤とともに電気炉で溶かし、出来上がった鋼の塊(鋼塊)を巨大なプレス機で加工しています。

実際に室蘭製作所内を見学した際は、スケールの大きさに圧倒されてしまいました。製造工程ごとに建物が分かれており、建物間には巨大な鋼塊を運ぶため専用列車の線路が敷かれています。数百トンの鋼塊を作るための「型」は直径だけでも自分の身長以上の大きさで、その鋼塊を加工する 1 万 4000 トン油圧プレス機が動くさまは圧巻の一言でした。

北海道室蘭には工業地域以外にも様々な岬や白鳥大橋などの見所があります。チキウ岬(地球岬)からは水平線が見られるだけでなく、内陸側に目を向けると室蘭製作所がある工業地域が一望できます。白鳥大橋にも日本製鋼所の技術が使われているのだとか。

北海道を訪れた際は、「鉄のまち」室蘭に立ち寄ってみてはいかがでしょうか。

木本 悠佑

編集後記

コラム：セキュリティ百景でご紹介したインシデント対応訓練に、私も同席しておりました。インシデント発生時の対応＝有事対応を専門とするサイバー救急センターですが、平時において、お客様のセキュリティ対策に寄与することができる新たな一面を発見する、とても良い機会となりました。

もし同様のご要望をお持ちの組織、CSIRT 関係者の方がいらっしゃいましたら、私達の知見を平時にフィードバックできる良い機会であり、また私たちにとっても良い経験となりますので、是非ご相談ください。

最後になりますが、本号でもアンケートへのご協力をお願いいたします。前号では巻頭でアンケート記入についてお願いした効果で、これまでの 3 倍程度の回答をいただきました。厳しいご意見も含め紙面に反映していきますので、ご協力をお願いいたします。（法）

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/LTWXJNQ

編集長　内田 法道

編集者・執筆者　田原 祐介、遠藤 裕樹、関 宏介、永安 佑希允、木本 悠佑

株式会社ラック

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

E-MAIL: sales@lac.co.jp

https://www.lac.co.jp/

緊急対応窓口：サイバー救急センター

24時間365日 緊急対応コール

0120-362-119

CYBER EMERGENCY CENTER

ご相談は予約不要、24時間対応。すぐにご連絡ください。