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 -

アカウントロックを追え、バラマキ型メールの裏側

フォレンジック女子／フォレンジッカーの悩み

第 5 号

2018 秋

CYBER EMERGENCY CENTER

2018 年 11 月 30 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 5 号 / 2018 秋

目　　次

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

2018年の7月～9月は、Windowsのリモートデスクトップサービスを狙った脅威に関連する相談が、いつにも増して多かったです。リモートデスクトップサービスは、WindowsのPCやサーバをネットワーク経由で遠隔操作する際に利用する便利なサービスです。働き方改革などで推奨されている自宅作業などをする際に、自宅にいても業務環境を利用できる、画面を転送するだけなので情報を持ち出さずにすむ、などの理由から、多くの組織で利用されているものと思います。

セキュリティの教科書的には、安全な認証方法を利用したVPNなどで組織内のLANに接続したのちにリモートデスクトップサービスで対象のWindowsにログオンするというのが安全なプラクティスの1つです。しかしながら、相談をうけた事例では、様々な理由によりインターネットから直接リモートデスクトップサービスに接続できる環境になっていました。この場合、攻撃に対する防御壁はパスワードの強度しかありません（アカウント名はデフォルト想定）。推測が容易なパスワードが設定されていた場合、組織の表門から攻撃者に侵入を許してしまうことになります。サービスを提供するポート番号を変更していた場合でも、侵害されていますので、攻撃者はフルポートでリモートデスクトップサービスを探索している可能性が高いです。

インターネットからアクセス可能なリモートデスクトップサービスが存在していないか、再点検することを推奨いたします。特に、グループ会社、海外拠点、地方拠点など目が行き届かない所にはご注意ください。

サイバー119の出動傾向

2018年7月～9月の出動傾向

当該期間は、2018 年 4 月～6 月の期間に引き続き、Microsoft アカウントの窃取を目的としたフィッシングメールを受信し、Microsoft Office 365 のクラウド型メールサービスを不正利用された組織からの相談がありました。

一般的には、夏休みなどの長期休暇が明けた時期は、大量の未読メールを処理する際にフィッシングメールや標的型メールなどの被害に合いやすいと考えられていますが、Microsoft 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を目的としたフィッシングメールは、時期に関係なく年間を通して確認されています。そのため、社員や職員がフィッシングメールの誘導にひっかかりアカウント情報とパスワードを入力してしまうことを想定した、対策の検討と導入が急務と考えられます。

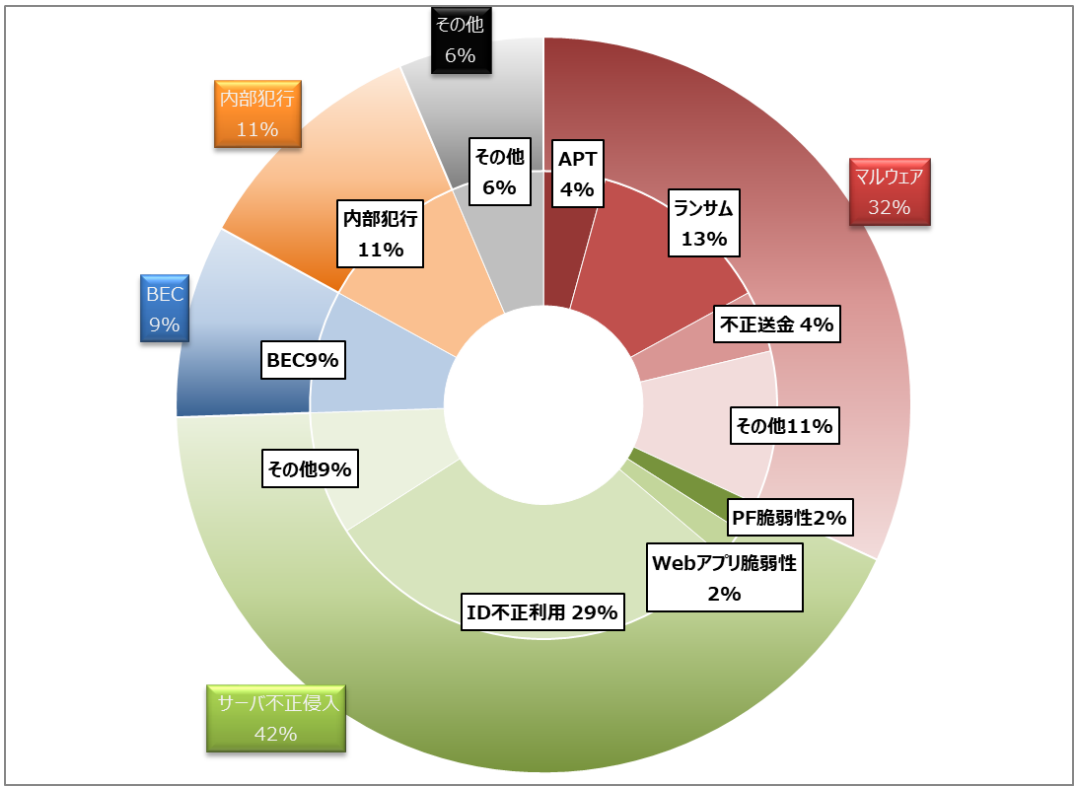

図 1-1 2018 年 7 月～9 月のインシデント傾向

マルウェア関連のインシデント傾向

ランサムウェアによりデータが暗号化されたことを発端として、複数の組織から相談が来ています。相談を受けた組織の中には、WannaCry の感染拡大で悪用されたセキュリティパッチ「MS17-010」をいまだに適用しておらず、WannaCry の亜種に感染した組織も存在していました。他のネットワークと接続していないクローズドなネットワーク空間であっても、メンテナンスなどで外部の PC を接続することがある場合には、改めてネットワーク内のすべての端末およびサーバの「MS17-010」の適用状況を確認ください。また、ウイルス対策ソフトが検知できる場合もあるため、ウイルス対策ソフトの導入、定義ファイルのアップデート、リアルタイムスキャンの有効化も検討ください。

また、WannaCry の亜種以外にもランサムウェアの相談を多く受けました。ランサムウェアの感染経路として想定されるものとしては、バラマキ型メールの添付ファイルや URL により、社員や職員がうっかりファイルを開いて彼らの PC が感染するインシデントが想定されます。しかしながら、本期間に相談を受けたインシデントではそのような経路ではありませんでした。

マルウェア感染被害を及ぼした攻撃者の手口は、意外にもインターネットから Windows の標準機能である RDP（リモートデスクトップ）接続で侵入し、ランサムウェアに感染させるというものでした。本来であれば、インターネットから RDP 接続する場合には、VPN で組織内の LAN に接続して、その後に目的の端末に RDP 接続するべきです。しかしながら、被害を受けた組織では Firewall の設定不備やメンテナンス用途で意図的に許可した設定を悪用されていました。また、パスワードについても容易に推測可能なものが設定されているケースも多くありました。

このようなインシデントの被害にあわないようにするため、Firewall などのネットワーク機器のアクセス制御のルールを改めて再確認する、インターネットから脆弱性診断を実施するなど、これまで不備が無いと判断していた箇所について、改めてチェックすることを推奨します。

フィッシングメールのインシデント傾向

Microsoft Office 365 などのクラウド型メールサービスのアカウント窃取を目的とした攻撃被害にあったと思われる相談が増えてきています。サイバー119 サービスが相談を受けた攻撃手口は、Microsoft 社を装うメール内に URL が記載されており、当該 URL へアクセスするとアカウント情報を入力させるログイン画面が表示されます。この手口は、フィッシングと呼ばれる以前から良く用いられる攻撃手口になります。

攻撃者にアカウントが窃取された後、以下の被害にあうことが想定されます。

- 窃取されたアカウントから取引先などへ、金銭の支払いや入金を指示するビジネスメール詐欺に悪用される
- 本人が送受信するメールを攻撃者が用意したメールアドレスへ自動的に転送される設定に変更され、営業秘密や個人情報などの機密情報が漏えいする
- ばらまき型メールを大量に送信される（仮想通貨の要求、マルウェアの添付、フィッシングメールなど）
- APT 攻撃の対象組織に標的型メールが送信される

さらに、Microsoft Office 365の契約プランにより異なりますが、メールサービスだけではなくファイル共有を目的としたSharePointやOneDriveを利用していた場合、それらに保存されている機密情報が漏えいする可能性もあります。そのため、フィッシングメールの被害を受けた場合は、メールサービスだけではなくMicrosoft Office 365で利用していた他のクラウドサービスについても影響を調査することを推奨します。

クラウド型のメールサービスを含むグループウェアは、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、アカウントのパスワードが漏れてしまうと、その便利さ故に攻撃者が容易に不正利用できてしまう場合があります。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、「パスワードは漏れてしまうもの」という前提に立ち、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、パスワードに頼らさないセキュリティ対策が必須となります。

また、アカウントを窃取された後の影響範囲を特定する際には、各サービスの監査ログを取得しておくことが有効です。Microsoft Office 365では、アクセス元のIPアドレス、利用アカウントや送受信のメール履歴などの監査ログはデフォルトで有効にされており 90 日間保存されますが、窃取されたアカウントのメールボックスで攻撃者がどのような操作を行ったのかを記録するメールボックスの監査ログは、デフォルトでは取得されません。そのため、被害を受けた際の影響範囲を確認するためには、管理者がこれらの監査ログ取得設定を有効にする必要があります。クラウド型のサービスを利用さている場合には、監査ログ取得の設定がどのようになっているのか確認し、もし有効でない場合には設定変更をご検討ください。

攻撃者の残した痕跡に学ぶ

アカウントロックの原因を追え

これは、ある大きな組織で発生した事案に基づくストーリーです。

(1)繰り返されるアカウントロック

この事案は最初、アカウントロックの発生として認知されたそうです。元々、利用者が何回かパスワードを間違えるとアカウントがロックされる設定になっていたのですが、その時ロックが発生したのは深夜の、通常はオフィスで人間が活動しているはずのない時間帯でした。

アカウントロックはひとまず解除されたのですが、その後も同様のパスワード間違いは続いたそうです。攻撃元や原因が不明な中で繰り返す再発に関係者は困惑し、本格的に調べることになりました。

(2)セキュリティログで攻撃を確認（イベントID 4776）

ドメインコントローラ（以下、「DC」と表記）のセキュリティログ[1]を確認すると、攻撃の一端が見えてきました。ポイントとなったのはイベントID 4776「資格情報の確認」[2]です（図 2-1）。ここで確認したのはDCのログですが、DCが直接攻撃を受けたわけではありません[3]。4776は、ドメインを構成するいずれかのコンピューターにおいてログオンの失敗があった際（図 2-2）にDCに記録されるものです。

コンピューターがアカウントの資格情報の確認を試行しました。	
認証パッケージ:	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
ログオン アカウント:	administrator
ソース ワークステーション:	DESKTOP-1H2CCQ4
エラー コード:	0xC000006A

図 2-1：イベントID 4776「資格情報の確認」の例（弊社検証環境にて）

1 本稿でセキュリティログは、Windowsイベントログ中の「セキュリティ」ログを指します。

2 4776(S, F): The computer attempted to validate the credentials for an account.
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4776

3 もしDCが直接攻撃を受けていたとするなら、DCのログに4625が記録されているはずですが、そうではありませんでした。

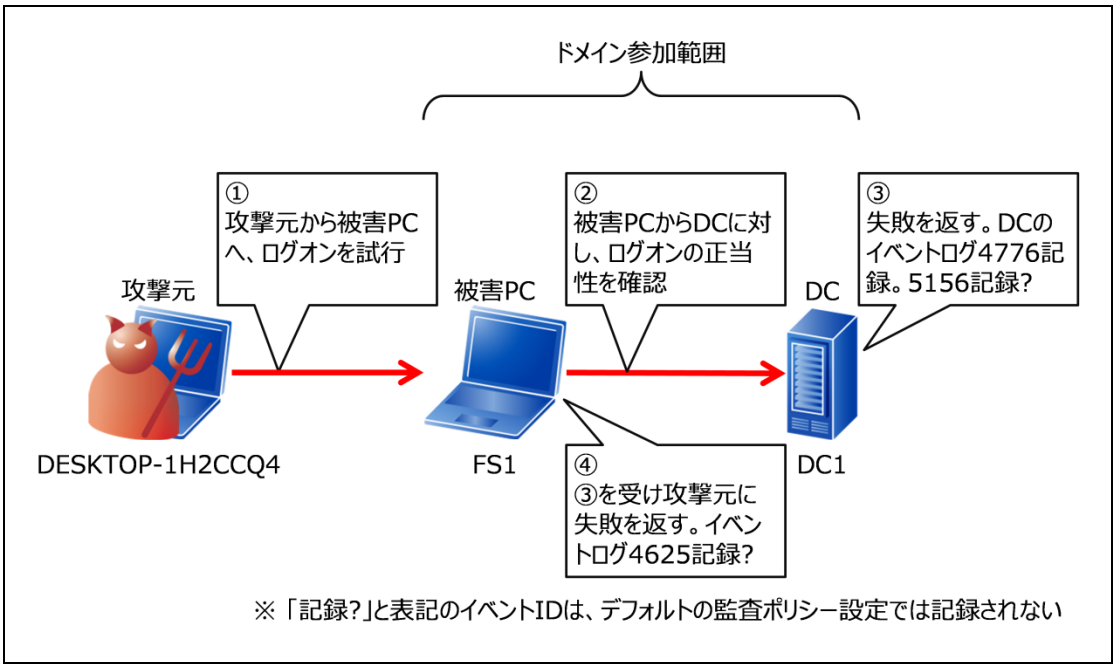

図 2-2：イベント ID 4776「資格情報の確認」が記録される状況（弊社検証環境にて）

この事案では、4776 から、アカウント名とエラーコード[4]を確認できました[5]。そこから、確かに連続してパスワード間違いが生じていることが判り、さらに他の特徴として以下を読み取ることができました。

A) ログオンの試行ごとにアカウント名が異なっており、Reverse brute-force 攻撃に近い
B) アカウント名は存在しないものも多く試されており、辞書に基づいているように見える
C) 攻撃の頻度は低く、数十秒～数分に一回程度。ツールを使えばもっと高頻度の攻撃は可能なはずなので、攻撃者は意図的に頻度を落としている可能性もある
D) 時間帯は、当初は深夜時間帯のみだったが、その後は日中にも攻撃が生じており、一定しない

しかし、被害 PC や攻撃元を示す情報は含まれておらず、このままでは次の調査ポイントを絞れません。

(3)複数手段で攻撃元を追う

攻撃元を追うため、複数の方法を同時並行で試すことにしました。

1) 通信機器のログ確認。プロキシサーバーやファイアウォールなどのログから不審な通信を見つけ、そこからマルウェア感染端末を特定します。
2) 簡易フォレンジック調査。攻撃元となった可能性がある数百台のクライアント PC を簡易調査し、マルウェア感染やアカウント不正利用の痕跡を探します。

---

4 失敗の理由を示すコード。ここから、パスワードや誤りか、それともアカウント名の誤りかなどを識別できます。
5 ソースワークステーションも記録されることがありますが、この事案では記録されませんでした。もし記録されていれば、攻撃元のコンピューター名が判明しますので、話は簡単だったのですが…

3) 監査ポリシーの構成。セキュリティログに記録する項目を増やすことで網を張ります。攻撃が再発した際に、攻撃元の手がかりを探します。
4) パケットキャプチャ。DC の周辺で通信パケットをキャプチャするように設定して網を張ります。攻撃が再発した際に、通信パケットの内容から攻撃元の手がかりを探します。

これらを準備する中で攻撃の再発があり、3) と 4) の布石が攻撃元の手がかりに有効でした。

(4)監査ポリシーを構成して被害 PC に迫る（イベント ID 5156） ［(3) の 3) に対応］

セキュリティログに記録される項目は、監査ポリシーの構成によって変化します。デフォルトでは記録されない項目も多くあり、事案調査には十分でないことがあります。とは言え、やみくもに情報量を増やせばセキュリティログが短期間しか記録されなくなります[6]し、記録期間との両立にははストレージをはじめとしたリソースも必要になります。このため、調査に有用な項目だけを記録できるよう、監査ポリシーを適切に構成[7]していきます。

この事案では、Windows ファイアウォール監査（図 2-3）による記録が、調査に有用[8]でした。これは、Windows ファイアウォールが通信を許可したことを、イベント ID 5156「フィルターリング プラットフォームの接続」（図 2-4）で記録します。この記録から、いつどんな通信が起きたかを、おおよそ把握できます。

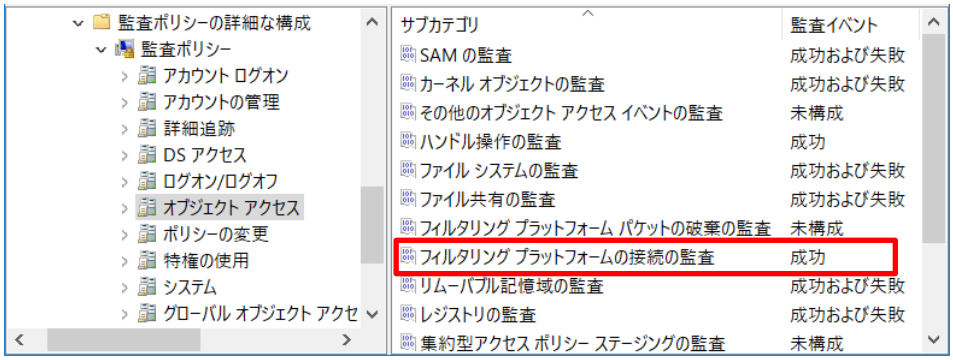

図 2-3：監査ポリシーの設定（Windows ファイアウォール監査の項目）

---

6 Windows のイベントログは、デフォルトでは記録できる容量が固定されています。このため、記録する項目が少なければ、より長い期間の記録を残せますが、記録する項目が多いと短期間の記録しか残せません。

7 Audit Policy Recommendations | Microsoft Docs
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
攻撃者の行動を追跡せよ - 行動パターンに基づく横断的侵害の把握- | JPCERT/CC
https://www.jpcert.or.jp/present/2018/20171109codeblue2017_ja.pdf

8 ただし、この記録は膨大な容量となりがちですので、常に監査するよう構成するのは現実的ではありません。非常時のみに限って監査するなど、柔軟に構成を変更する準備も必要です。

Windows フィルターリング プラットフォームで、接続が許可されました。	
ネットワーク情報:	
方向:	着信
送信元アドレス:	192.168.162.210
ソース ポート:	49759
宛先アドレス:	192.168.162.200
宛先ポート:	135
プロトコル:	6

図 2-4：イベント ID 5156「フィルターリング プラットフォームの接続」の例（弊社検証環境にて）

図 2-1 の③で記録される 4776 には、攻撃元や攻撃先に関する情報は含まれていませんでした。しかし、あわせて記録される 5156 には、被害 PC から DC への通信（図 2-1 の②）の情報が残ります。

この事案では、DC は普段から多くの通信を受けているため、4776 と 5156 は必ずしも一対一対応するわけではありませんでした。しかし、再発した攻撃は複数回だったことから統計的な処理が可能となり、結果的に被害 PC に繋がる IP アドレスを得られました。

(5)通信パケットから被害 PC に迫る［(3) の 4) に対応］

DC の周辺でパケットキャプチャを準備したところ、図 2-1 の②に関する通信を捉えることができました。通信の多くは暗号化されており、そのままでは読めませんが、一部に被害 PC のホスト名が含まれていました（図 2-5）。

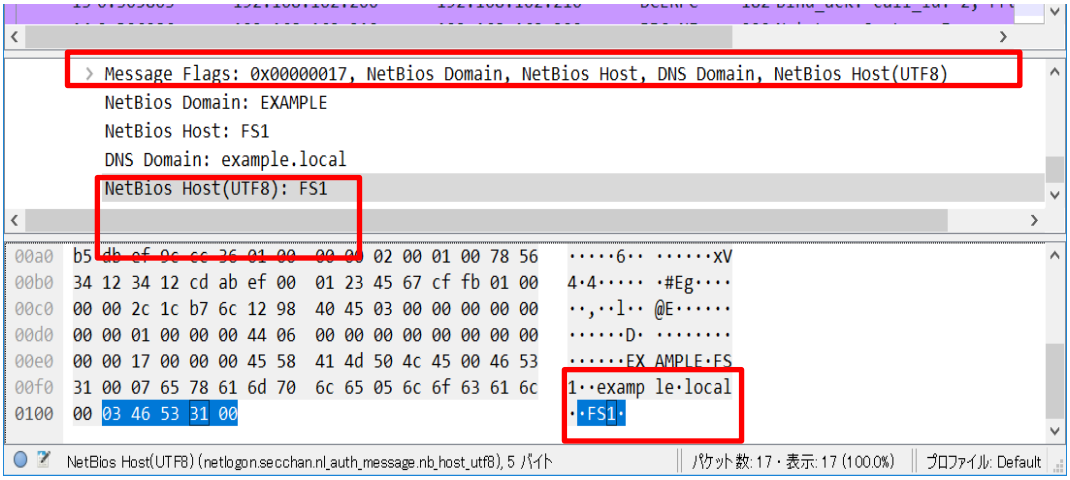

図 2-5：被害 PC のホスト名が含まれるパケット（弊社検証環境）

この事案では、(4) で得られた IP アドレスは被害 PC を直接示すものではなかったため、ホスト名の情報が被害 PC の特定に役立ちました。

(6)被害 PC のセキュリティログから攻撃元に迫る（イベント ID 4625）

この先を追いかけるには、被害 PC のセキュリティログが頼りです。攻撃を受けた時、被害 PC にはイベント ID 4625「ログオン［失敗の監査］」（図 2-6）が記録されます。4625 中には、ログオン元のホスト名や IP アドレスが含まれますので、これで攻撃元を特定できるはずです。

アカウントがログオンに失敗しました。	
ログオン タイプ:	3
ログオンを失敗したアカウント:	
セキュリティ ID:	NULL SID
アカウント名:	administrator
アカウント ドメイン:	example
ネットワーク情報:	
ワークステーション名:	DESKTOP-1H2CCQ4
ソース ネットワーク アドレス:	192.168.162.9
ソース ポート:	60925

図 2-6：イベント ID 4625「ログオン［失敗の監査］」の例（弊社検証環境にて）

ただし 4625 は、デフォルトの監査ポリシー設定では記録されないため、再度の監査ポリシー設定が必要です。また、監査ポリシーを各クライアント PC に配布する必要があったので、Active Direcoty の機能であるグループポリシーオブジェクトが使用されました。

この事案では、図 2-6 の例に反してログオン元のホスト名や IP アドレスが記録されない現象が見られたため、(4) と同様に 5156 も取得するよう監査ポリシーを設定し、次の攻撃を待つことになりました。

(7)事案の終わりと振り返り

しかし、次の攻撃はありませんでした。ちょうど、調査とは別に進められていたネットワークの改修があり、その切り替えと共に攻撃が確認されなくなりました。改修の内容から攻撃元を十分に絞り込めたため、(6) の結果を待つことなく、この事案はクローズとなりました。

近年は、インシデントの追跡にイベントログを活用する話が JPCERT/CC などから出ています[9]が、サイバー救急センターの調査でもイベントログはよく使います。イベントログの有効性を高めるには、平時から監査ポリシーや保存期間をよく検討してログを取得した上で、ログを見ておくことが重要です。平時の状態をよく把握していないと、異常な状態を見つけることは困難です。また、イベントログにはネットワーク関連情報（IP アドレスなど）も多く記録されますが、それを活かすにはネットワーク側のログも欠かせません。DHCP ログや VPN ログなど、IP アドレスとホストの関係が判るログを、ぜひ残しておきましょう。これらのログが揃っていれば、調査もより短期間・低コストで結果を出せるようになります。

ラックでは、イベントログについては深く学ぶトレーニングコース[10]も用意しています。本稿を読んで興味を持たれた方がいましたら、一緒にイベントログの世界を探検してみませんか？

---

9 イベントログを可視化して不正使用されたアカウントを調査 ~LogonTracer~（2017-11-28）
https://www.jpcert.or.jp/magazine/acreport-logontracer.html
Sysmon ログを可視化して端末の不審な挙動を調査~SysmonSearch~(2018-09-06)
https://www.jpcert.or.jp/magazine/acreport-SysmonSearch.html

10 実践！デジタル・フォレンジックコース(2) 侵害調査編～Windows 環境の侵害状況調査手法～
https://www.lac.co.jp/service/education/digitalforensic_simplicity.html

脅威分析報告

日本に送られるバラマキ型メールの裏側

～ 2017.10 - 2018.10 ～

今回は、サイバー救急センターレポート 1 号で紹介した”日本に送られるバラマキ型メールの裏側”から 1 年ほど経過したので、その後のバラマキ型メールの観測状況を報告します。今回の分析対象データは、2017 年 10 月中旬から 2018 年 10 月中旬までの約 1 年間に受信したマルウェア付きメール[11]です。

前回からの大きな変化としては、Cutwail を利用した日本語のマルウェア付きメールが、2018 年 8 月初旬から観測されなくなったことが一つあげられます[12]。また、Necurs を利用したものでは、ダウンローダとして動作するマルウェアである Emotet や、リモートアクセスツールである FlawedAmmyy[13]を配布する新たなキャンペーンが確認できた反面、ランサムウェアを配布していたメールが 2018 年 1 月下旬から観測されなくなったことがあげられます。

図 3-1 はマルウェア付きメールを元に、メール送信のインフラ（Botnet）とダウンロードされるマルウェア情報をマッピングして Maltego で関係性を確認したものです。図 3-1 の上段が 1 年前紹介したもので、図 3-1 の下段が今回のものです。確認できた Botnet の種類は 3 種類（Cutwail、Necurs、Unknown）で変化はありませんが、各グループで利用されるマルウェアに変化が見れられることや、新たなグループに分類できることが確認できます。そのため、3 つのボットネットから送信されているメールに注目し、これらのメールに含まれるメールヘッダやメール本文、添付ファイルの特徴を分析した結果、今回（図 3-1 下段）は、7 つのグループ（グループ A（Aa および Ab）、グループ B、グループ C、グループ D、グループ E、グループ F）に分類することができました。本稿では、この 7 つのグループの特徴について考察します。

---

11 マルウェアをダウンロードさせる URL がメール本文に含まれるものも含めています。なお、フィッシングメールや詐欺メールは分析対象外としています。

12 調査期間外ですが、2018 年 10 月 24 日に再び Cutwail を利用した日本語のマルウェア付きメールを確認しました。その後もメールは継続してばら撒かれています。ダウンロードされるマルウェアは Ursnif であり、11 月 1 日時点でのバージョンは 300017 です。

13 FlawedAmmyy は、漏洩した Ammyy Admin バージョン 3 のソースコードを利用して作成されたリモートアクセスツールです。

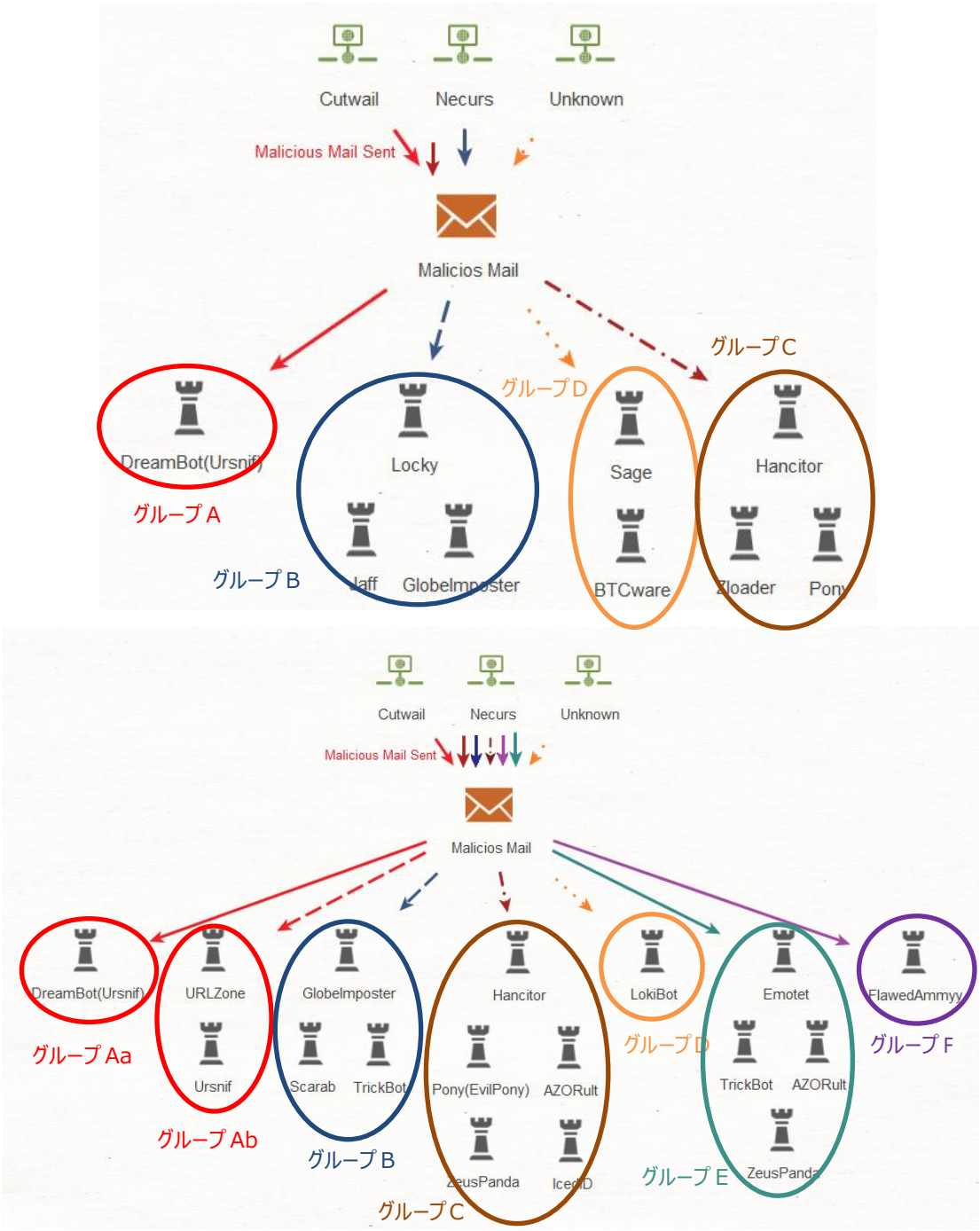

図 3-1 バラマキ型メールで拡散されるマルウェア（上：前回／下：今回）

グループ Aa

グループ Aa は、Cutwail を利用してマルウェア付きメールを送信し、DreamBot（Ursnif）を拡散させるグループであり、前回のグループ A に該当するグループです。メールを確認できた時期は、2017 年 10 月中旬から 2018 年 7 月下旬までです。当該メールの特徴としては、件名や本文に日本語が使われており、その多くは実在する企業を騙ります。メール本文には、リンク（URL）が含まれており、リンクから JS ファイルを内包した ZIP ファイルをダウンロードさせます。その後、ダウンロードされた JS ファイル経由で DreamBot を拡散します（図 3-2）。なお、2018 年 7 月 25 日時点における DreamBot のバージョンは、217016 でありますが、このバージョンでは、マルウェアの自動起動の設定が前バージョン（216996）のものとは異なる設計になっています。前バージョンまでは、DreamBot が実行された際に、ユーザの”AppData”ディレクトリに DreamBot がコピーされ、コピーされた DreamBot が起動時に実行する設定になっていましたが、バージョン 217016 の DreamBot より Powershell を利用してレジストリに格納されたスクリプトを復号することで、DreamBot が自動実行するよう変更されています。

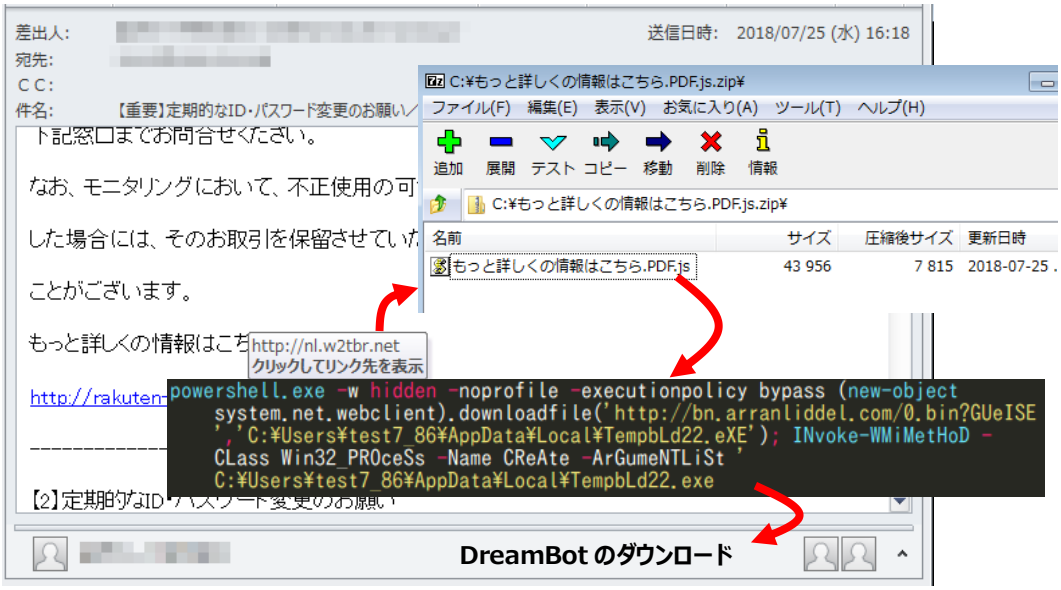

図 3-2 DreamBot を拡散させるスパムメールの一例

グループ Ab[14]

グループ Ab も、Cutwail を利用してマルウェア付きメールを送信するグループであり、Ursnif（バージョン 3）を拡散させます。メールが確認できた時期は、2017 年 10 月中旬から 2018 年 8 月初旬までです。メールの特徴としては、グループ Aa と同じように、件名や本文に日本語が使われていますが、多くの場合マクロ付の Word や Excel ファイルがメールに添付されています。もう 1 つの特徴として、2018 年 8 月 6 日に確認した事例では、Word や Excel ファイルではなく、Office クエリファイル".iqy"が添付され、当該ファイルがダウンローダとして動作するマルウェア URLZone（Bebloh）をダウンロードします。その後、URLZone 経由で Ursnif を拡散します（図 3-3）。なお、2018 年 8 月 6 日時点における、Ursnif のバージョンは 300016 です。

図 3-3 Ursnif を拡散させるスパムメールの一例

グループ B

グループ B は、Necurs を利用してマルウェア付きメールを送信し、主にランサムウェアを拡散させるグループです。メールが確認できた時期は、2017 年 10 月中旬から 2018 年 1 月下旬頃までです。メールの特徴としては、件名に、"Copy", "Scanned", "Invoice", "Payment", "Document"などといった英単語が含まれるケースが多く見られ、添付ファイルは、JS ファイルを内包した 7z ファイルが多く利用さ

14 グループ Ab は、グループ Aa と同じ種類のインターネットバンキングマルウェア（Dreambot/Ursnif）を利用しているため、新しいグループを定義せず、グループ A という中でサブグループを定義しています。

れています。また、メール本文に何も文字が含まれていないケースが多く確認されています（図 3-4）。調査期間中における、拡散されたランサムウェアの多くは、GlobeImposter であり、2017 年 11 月下旬に Scarab を数件確認しています。また、2017 年 12 月中旬にインターネットバンキングマルウェア TrickBot が数件拡散されたことも確認しています（図 3-5）。なお、この際に確認した、TrickBot のバージョンは、1000102 です。

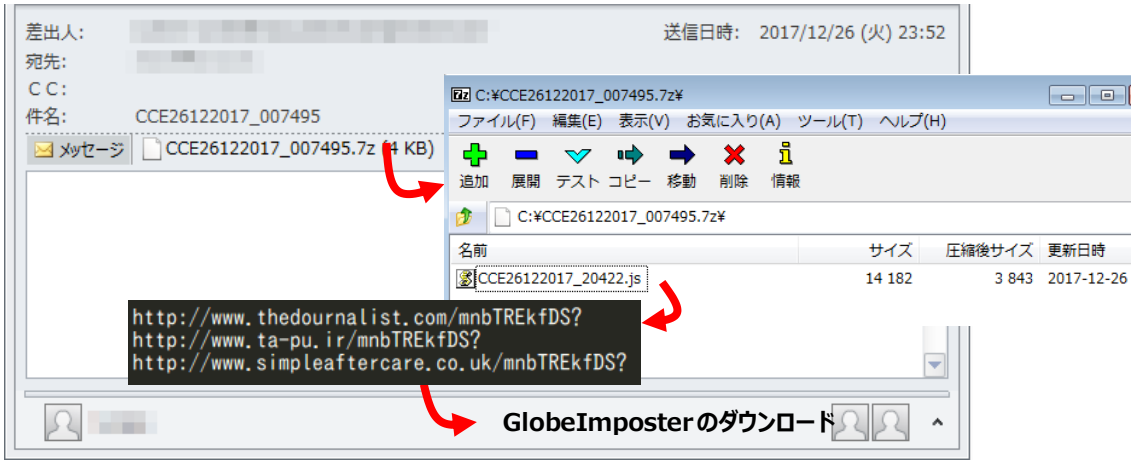

図 3-4 GlobeImposter を拡散させるスパムメールの一例

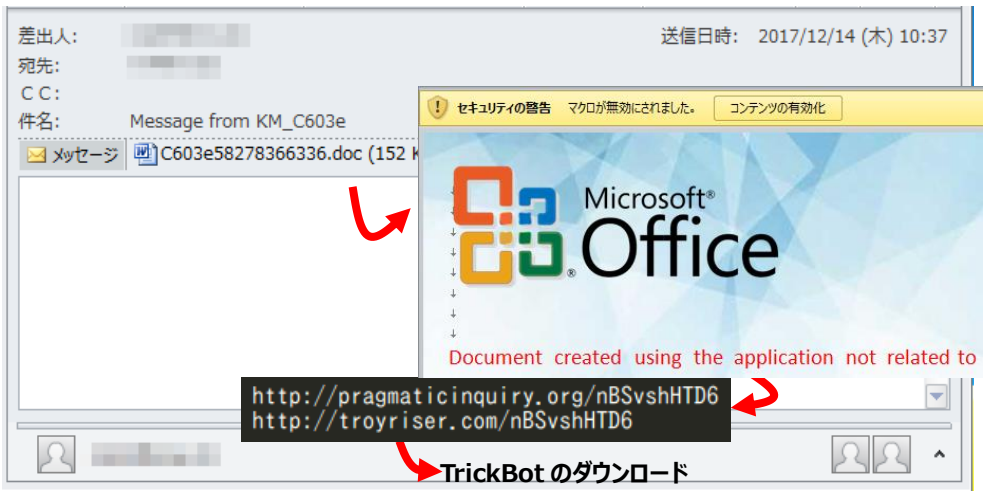

図 3-5 TrickBot を拡散させるスパムメールの一例

グループ C

グループ B と同じく Necurs を利用してマルウェア付きメールを送信し、ダウンローダとして動作するマルウェア Hancitor を拡散させます。メールが確認できた時期は、2017 年 10 月中旬から 2018 年 10

月中旬までです。メールの特徴としては、図 3-6 に示すような HTML 形式を利用し、実在する企業からの領収書やメッセージ、請求書などを騙ります。このグループは、添付ファイルではなく、メール本文に含まれたリンク（URL）から悪性ファイルをダウンロードさせる手口を利用する点も特徴的です。メール内の URL からダウンロードする Word ファイルには、Hancitor を内包したマクロが含まれており、マクロを実行することで、ユーザの”%TEMP%”ディレクトリに”6c.pif”ファイル[15]として保存され、実行されます。この動作は、前回の“explorer.exe”または”svchost.exe”にインジェクションして実行されるものと異なります。その後、Hancitor は、調査を実施した期間においては、パスワードやアカウント、仮想通貨などを窃取する機能を有する Pony（EvilPony）や AZORult、インターネットバンキングマルウェア ZeusPanda（PandaBanker）などの複数のマルウェアをダウンロードします。また、Proofpoint[16]によれば、2018 年 9 月末頃から Hancitor が、DanaBot と呼ばれるインターネットバンキングマルウェアをダウンロードすることを確認していると報告しています。

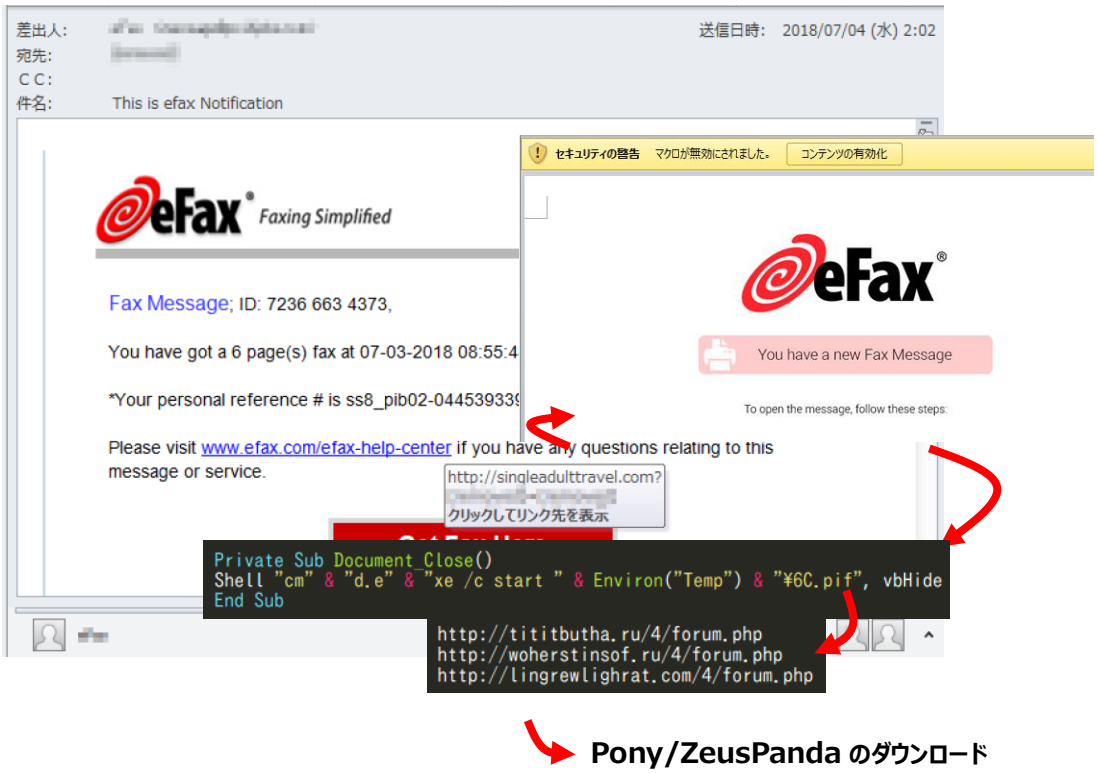

図 3-6 Hancitor を拡散させるスパムメールの一例

15 亜種によっては、ファイル名が異なるまたは実行形式のファイルが保存される場合もあります。

16 https://www.proofpoint.com/us/threat-insight/post/danabot-gains-popularity-and-targets-us-organizations-large-campaigns

グループ D

グループ D は、未確認の Botnet からスパムメールを送信し、パスワードやアカウント、仮想通貨などを窃取する機能を有する LokiBot を拡散させるグループです。メールが確認できた時期は、2018 年 2 月中旬であり、数件のみの確認です。メールの特徴としては、図 3-7 に示すような HTML 形式を利用し、実在する企業からの領収書や請求書などを騙り、添付ファイルにリンクを参照させる PDF ファイルが含まれています。前回は、攻撃者はこの Botnet を利用してランサムウェアを配布していましたが、今回は、LokiBot を拡散させていたことを確認しています。

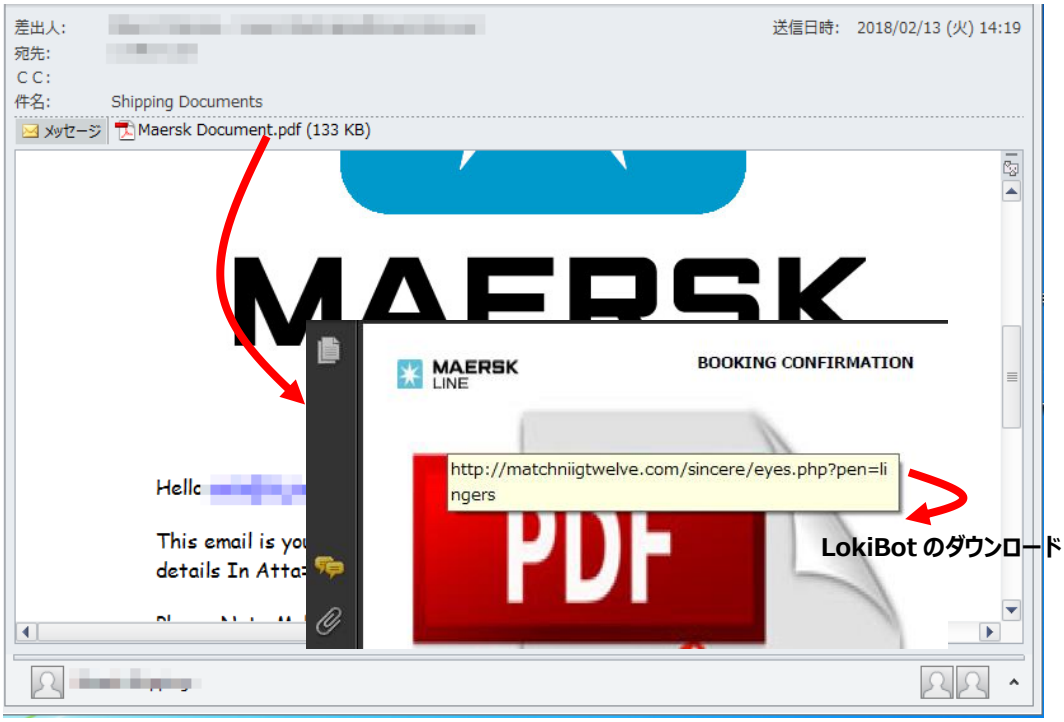

図 3-7 LokiBot を拡散させるスパムメールの一例

グループ E

グループ B、C と同じく Necurs を利用してマルウェア付きメールを送信し、Emotet を拡散させます。メールが確認できた時期は、2017 年 10 月中旬から 2018 年 10 月中旬までです。メールの特徴としては、件名に、"Wire", "Invoice", "Payment", "Account"などといった英単語が含まれるケースが多く見られ、メール本文では、請求書や領収書、アカウント情報の確認などを騙ります。（図 3-8 および図 3-9）また、このグループは、図 3-10 に示すような 3 種類の攻撃手口を使い分けて Emotet 拡散させていることを確認しています。その後、Emotet は、調査を実施した期間においては、インターネットバンキ

ングマルウェア ZeusPanda（PandaBanker）や TrickBot などの複数のマルウェアをダウンロードしていました。

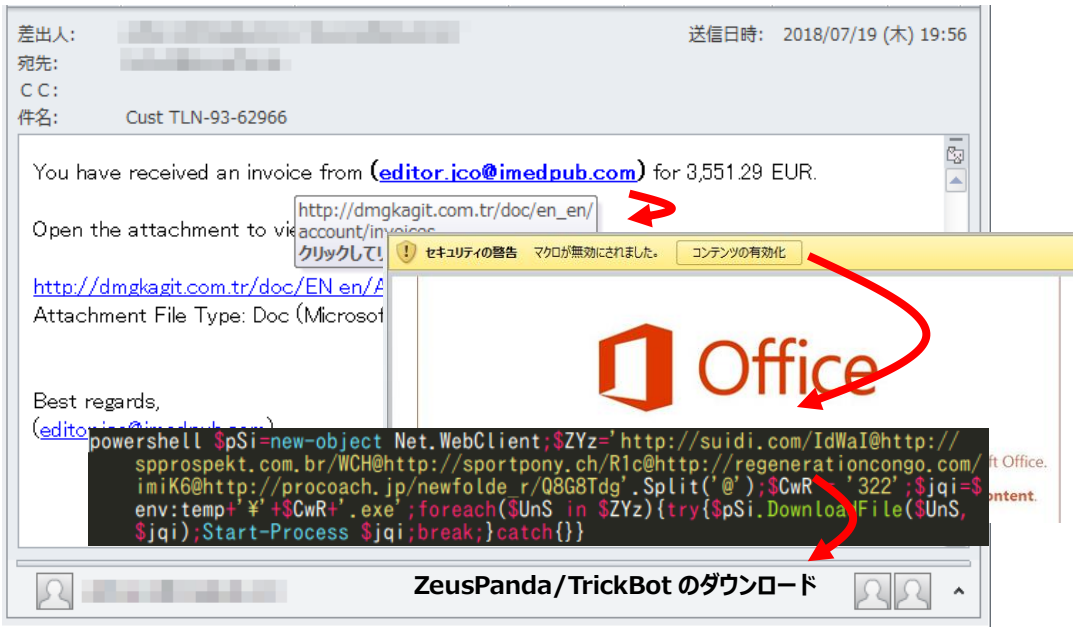

図 3-8 Emotet を拡散させるスパムメールの一例

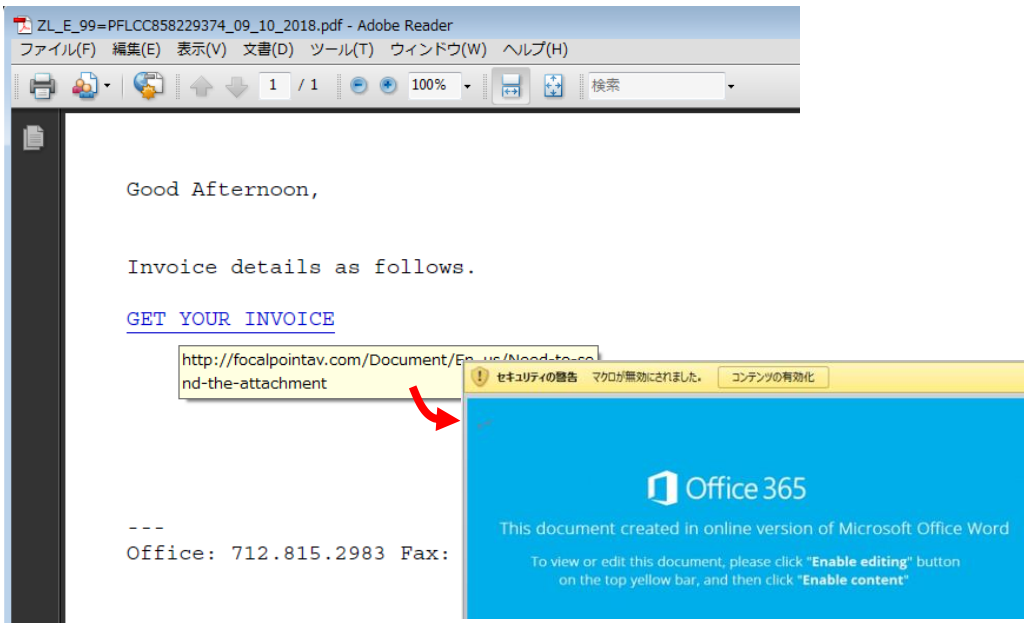

図 3-9 Emotet を拡散させるスパムメールに添付された PDF ファイルの一例

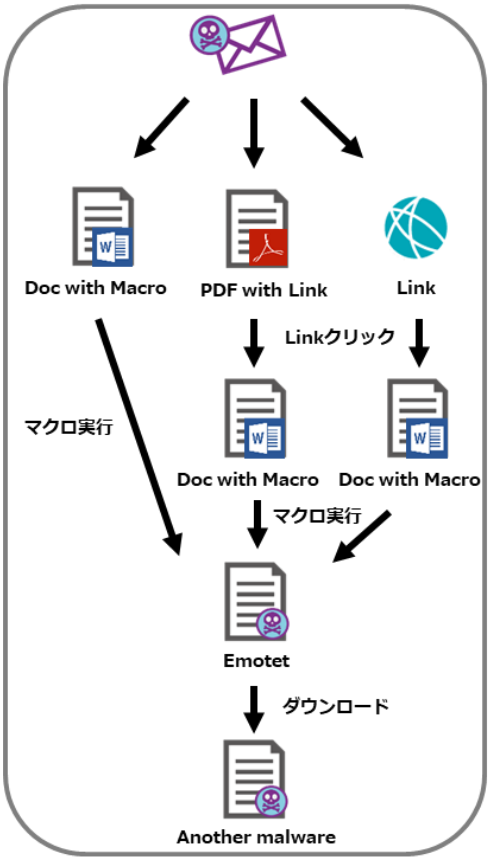

図 3-10 Emotet を利用した攻撃手口例

グループ F

グループ B、C、E と同じく Necurs を利用してマルウェア付きメールを送信し、FlawedAmmyy を拡散させます。メールが確認できた時期は、2018 年 10 月中旬からです。メールの特徴としては、件名に、"Invoice"いった英単語が含まれ請求書の確認などを騙ります。（図 3-11）添付ファイルはマクロ付の Word や Publisher ファイルが利用されています。今回確認した事例では、Word ファイルに内包されるマクロを実行すると、ユーザの”%TEMP%”ディレクトリに偽の Microsoft Windows Installer（MSI）パッケージである”pixie.exe”ファイルをドロップし、実行します。その後、Windows Installer の実行ファイル”msiexec”を利用して不正な MSI パッケージ “tech”がダウンロードおよびインストールされ、最終的には、FlawedAmmyy がダウンロードされます（図 3-12）。

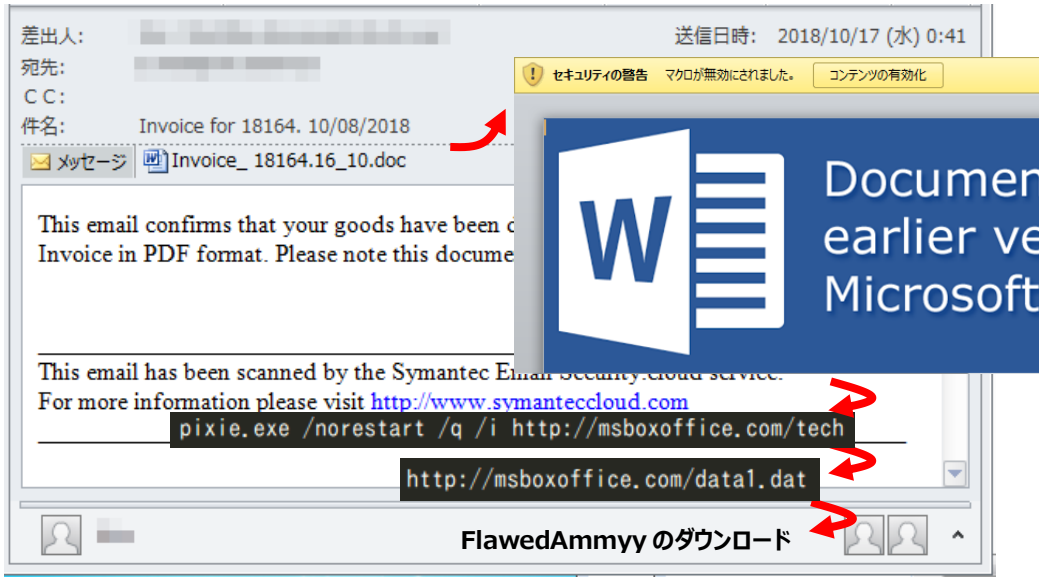

図 3-11 FlawedAmmyy を拡散させるスパムメールの一例

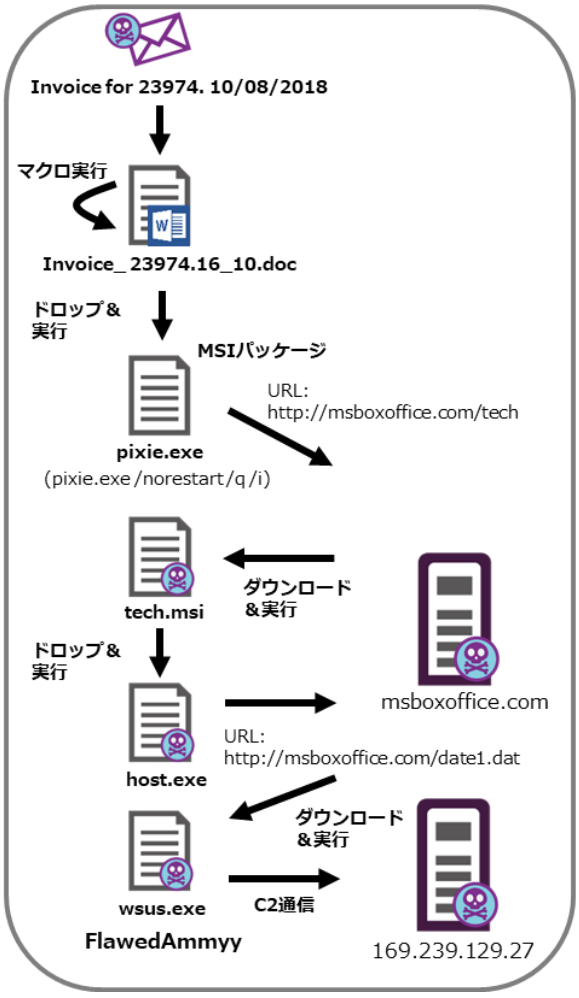

図 3-12 FlawedAmmyy を拡散させる攻撃手口例

おわりに

毎日、多くの似たようなマルウェア付きメールがばら撒かれていますが、弊社の脅威分析チームが受信したメールを対象とした分析でも、その裏側には Botnet を悪用する攻撃者の存在がうかがわれます。前回の調査と比較して受信するマルウェア付きメールの数は減少しているように感じられますが、判別できなかった Botnet や受信できていないマルウェア付きメールなどもあることから、今後も引き続き分析を行い、また 1 年後のサイバー救急センターレポートで報告できればと思います。

最後に、基本的なセキュリティ対策として、「怪しげなメールに含まれる添付ファイルや URL は不用意に開かない」ことに改めて注意するとともに、組織内での周知徹底もお願いします。

【IOC 情報】

6cb2e954864f4b661de5aa07f04b1e80
ef9ea3ab606adf5bbeffc75b0dccdae2
373d87dfaded5d3d3dc9b869f06ab1d9
916f1a229b73d5720aa51e596be52ee5
56649a8141c72d442ef3070dbf743563
7fa8c27d6a55a6d0ae74b8876013b172
31fd99548accf7e4dcdfadf815f898ac
a8eda3039c4cbbb362eb5847ed38e37a

コラム：セキュリティ百景 #9

フォレンジック女子の目線

今年７月、弊社で開催された女子学生限定のサマーインターンシップに、サイバー救急センターで働く女性社員として参加する機会がありました。フォレンジック分野で働いている女性は少ないため、インターンシップでは業務内容や職場の雰囲気について質問されることがありました。そこで、今回は女性の目線でフォレンジッカーの仕事について紹介します。

セキュリティ業界自体が女性比率の低い分野なうえに、フォレンジックに携わっている女性となると必然的に絶対数が少なくなります。そのため、社内やカンファレンスでも目立ちやすく、顔を覚えていただきやすいです。

また、女性のフォレンジッカーは珍しいため、興味を持っていただき、先方から話しかけていただくこともあります。自分から人に話しかけるのは苦手なのですが、会話の機会を得たり人脈を広げることができて助かっています。

違う部署の方や社外の方と接する機会が増えると、自然とフォレンジック分野以外の話を聞く機会も増えます。自分とは違う分野の知識を得られると、フォレンジック調査をする際の着眼点が増えますし、純粋に知的好奇心を満たす楽しみがあります。

また、お客様を訪問しフォレンジックの説明をすると、私をフォレンジッカーだと思っていなかった方から驚かれることがあります。技術者に見えないと話の説得力に欠けるのではないかと思い、最初はその点にコンプレックスを感じていました。

しかし、今では技術者に見えないことも自分の強みになると感じています。ある時、「技術者に見えない女性が質疑応答でフォレンジックの話をすると、意外性があって面白い」と言われたことがありました。意外性で関心を持っていただいたところでお客様に分かりやすい説明ができれば、技術者に見えないこともプラスに作用させることができます。

実際に仕事をしている中で、女性であることでハンデを感じる場面は少ないですし、フォレンジックに性別は関係ありません。男性女性に関わらず、フォレンジック業界の技術者が増えることを楽しみにしています。

コンピューターフォレンジックグループ

コラム：セキュリティ百景 #10

フォレンジッカーの悩み
～ IDF 講習会にて ～

特定非営利活動法人デジタル・フォレンジック研究会（IDF）が開催している「IDF講習会」をご存知でしょうか。本講習会は毎年９月に開催されるフォレンジック関連ツールやトレーニングの体験ができる講習会です。

今年、IDF講習会に初めてラックが講師として参加しました。コース内容を考えるにあたり念頭に置いたのは、事故対応の現場で実際に役立つ事、３時間の枠の中で消化不良にならないようにする事、の２点でした。以前、他社にクラウド上のホストのフォレンジック調査を相談したが、クラウドは対象外と断られてラックに依頼したとお客様からお聞きしたことがあります。確かに世の中のフォレンジック、インシデント対応トレーニングも実機を対象としたものが多く、現場で悩んでいる方も多いかもしれないとの思いから、コース内容は「クラウドの証拠保全(AWS編）」としました。

細かいコマンドを含めた全工程をステップバイステップで解説したため、やや冗長ではあったものの受講者の理解度は高く、概ね満足いただけたように思います。

質問やアンケート結果から、現場の皆さんが以下のような悩みを抱えている事に気づきました。

1. 自組織で使用しているフォレンジックツールやマニュアルが古く更新されていない
2. フォレンジックの実戦経験を積む場がない
3. フォレンジックで技術的に困った時に相談できる人がいない

自組織のCSIRTの一員としてインシデントに対応している場合、大きな組織でなければフォレンジック要員は少ないか、自分一人という場合もあると思います。通常業務と兼務の場合には、自分のスキルを向上させる時間の確保は難しいと思われます。

CECレポートでは、現場で頑張る皆様に役立てて頂けるよう、今後も可能な限り実務的な内容をお届けしたいと考えています。

関 宏介

編集後記

本書でサイバー救急センターレポートは 2 年目に入りました。2 年目に向けて新たな試みをしたいと思いつつも、1 年目と同じスタイルでの提供となってしまいました。様々な組織の CSIRT 的立場で動かれている皆様の訪問記をやりたいという想いは常にあるのですが、なかなか難しいものがあります。3 年目に入る時には、リニューアルをお伝えできるよう頑張ります。2 年目もよろしくお願いいたします。（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/TT8BFMC

編集長　内田 法道

編集者・執筆者　遠藤 裕樹、関 宏介、永安 佑希允、石川 芳浩、コンピューターフォレンジックグループ

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。