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１号

2017 秋

CYBER EMERGENCY CENTER

2017 年 11 月 24 日

サイバー救急センター

CYBER EMERGENCY CENTER

サイバー救急センターレポート

第 1 号 / 2017 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

近年の攻撃者グループの活発な活動を受け、ラックのサイバー救急センターへの相談件数は年々増加傾向にあり、2016 年度 1 年間では約 450 件に上りました。緊急対応サービスの提供を開始した 2006 年から今年までの累計では 2,000 件を超えています。緊急対応をする中で得た様々な知見については、サイバー救急センターを含め、ラックが提供する様々なサービスを通じて提供していますが、この度、サイバー救急センターレポートという形でインシデントやその対応に関連する知見を CSIRT 的な活動をされている皆様へ直接発信していくことにしました。

日本シーサート協議会の会員数は増加の一途で、2017 年 11 月 1 日現在で 261 チームとなっています。私が内閣官房情報セキュリティセンター（現、内閣サイバーセキュリティセンター）と兼務していた 2006 年当時、インシデント対応の必要性を説くために「事故前提」という言葉を利用するとネガティブな反応が多かったものですが、すっかり「事故前提」でのインシデント対応が当たり前の世の中となりました。

本書が、「事故前提」のもとで日々発生する様々なインシデントに対応している最前線の皆様の一助となるよう願っております。

サイバー119の出動傾向

2017年7月～9月の出動傾向

過去の歴史や地政学的な背景から、夏季はセキュリティインシデントの発生が増加すると考えられがちですが、サイバー119への相談からは、このような傾向は、確認されていません。サイバー119への主な相談は、PC等のマルウェア感染および公開サーバへの侵害の2種類になりますが、その割合についても他の時期と大きな変化はありません。

以降は、当該期間での特徴的な傾向と対策について紹介します。

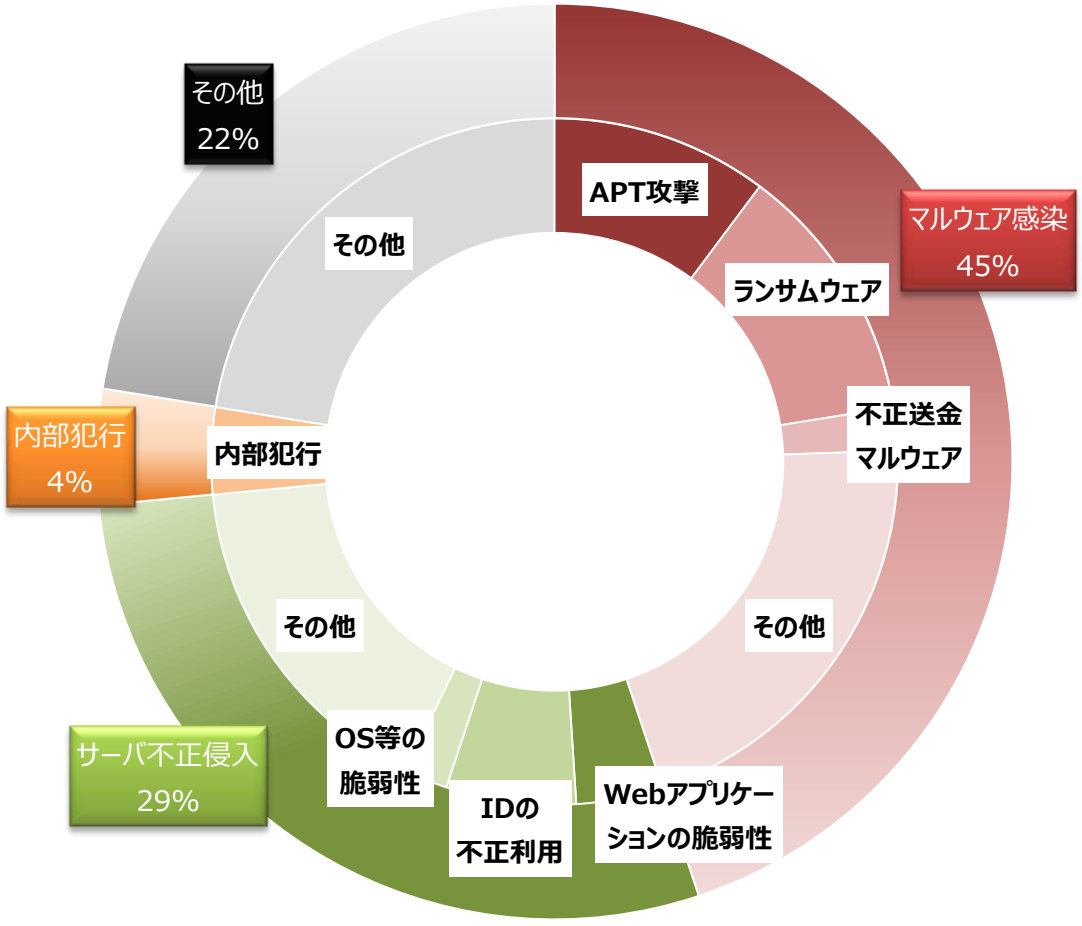

図 1-1 2017年 7月～9月の出動内容

マルウェア関連のインシデント傾向と対策

(1) APT 攻撃（Advanced Persistent Threat 攻撃、標的型攻撃）

サイバー救急センターが受けた APT 攻撃と推測されるインシデントの相談は複数ありますが、被害企業の業種や攻撃手法、利用されているマルウェア等はそれぞれ異なっていました。中には Menupass(APT10)および WINNTI の攻撃グループが関わっている可能性が疑われるインシデントも確認しています。

APT 攻撃は年々攻撃手法が巧妙化しており、この間に対応した攻撃では以下のような手法が確認されました。

- 巧妙なやり取り型メールによるマルウェア感染
- 以前より難読化されたマルウェアの利用
- 情報窃取後、社内ネットワークへランサムウェアを配布

APT 攻撃を未然に防ぐことは難しいため、予防策に加えてインシデントの早期検知、追跡性確保に向けたセキュリティ対策を検討してください。特に、APT 攻撃事案においては、ドメイン管理者アカウントが窃取される被害が散見されますが、ドメインコントローラの認証ログの保管期間が短く、十分な調査が行えないインシデントが多く発生しています。

インシデント発生時に迅速かつ的確に原因や影響範囲の調査ができるよう、ドメインコントローラの認証ログは可能なら 1 年程度は保管するよう、事前に対策しておくことを強く推奨します。

(2) バラマキ型メール（ランサムウェア、不正送金マルウェア）

バラマキ型メールはここ数年大量に送信されていますが、サイバー119 への相談件数は、昨年度の同時期に比べると減少傾向にあります。これは、セキュリティ対策ソフトの検知率が上昇したことや、ユーザのリテラシーが向上するなどして不審メールに気付くようになり、うっかり添付ファイルを開いたり URL にアクセスしたりすることが減ったためではないかと推察されます。

しかし、攻撃者グループはメールの題名や内容を少しずつ変え続け、メールの受信者の「うっかり」を誘ってきます。たとえば、日本国内の有名企業をかたったメールの題名や文面にしたり、今までと違うファイル形式を利用したり、巧みに攻撃手法を変えてきますので、新たなパターンを確認したら組織内に注意喚起することを推奨します。

なお、最近のバラマキ型メールの特徴については、後述の「脅威分析レポート」をご覧ください。

(3) WannaCry 感染

WannaCry が世界で猛威を振るったのは 2017 年 5 月中旬からですが、7 月下旬以降になってから WannaCry に感染発生したが、組織内ネットワークの感染端末が特定しきれないという相談を、サイバー119 でいくつか受けました。

WannaCry は、攻撃を行う際に TCP の 445 番ポートを利用して通信することから、ネットワーク内部から外部への TCP 445 ポートの通信、または内部ネットワーク間での TCP 445 ポートの通信の有無や通信元を確認することで感染端末の特定が可能です。

- 参考情報： ランサムウェア「WannaCry」対策ガイド rev.1
  https://www.lac.co.jp/lacwatch/report/20170519_001289.html

公開サーバ関連のインシデント傾向と対策

(1)サーバ不正侵入

サーバへの不正侵入事例では、公開サーバの脆弱性を悪用した攻撃者が、仮想通貨を発掘するソフトウェア（CoinMiner）を設置するインシデントが複数ありました。

対策としては、脆弱性の診断とパッチやアップデートの適用が重要ですが、未公開の脆弱性が悪用されるケースも確認していますので、インシデントの早期発見のため、不審なプロセスのチェック、コンテンツの改ざんチェック、CPU の使用率のチェック等のサーバ監視も併せて検討してください。

特に、公開系のサーバやシステムの動作が普段より遅いと感じた場合には、システムの障害やバグだけでなく、CoinMiner が設置されている可能性も考慮することを推奨します。

(2) 問い合わせフォームに対する大量アクセス

公開 Web サーバの問い合わせフォームに対して、大量の問い合わせが行われるという被害も複数起きています。問い合わせフォームに入力された連絡先メールアドレスに対して、受け付け完了メールを自動返信する仕組みの場合、第三者へのなりすましメールの踏み台として悪用される可能性があります。接続元の IP アドレスは、日本国外のものが多く確認されています。

これは、悪用されたのは脆弱性ではなく正常な処理のため、このようなインシデントに対して意識的にセキュリティ対策を行っている組織は少ないと思いますが、今後自組織が攻撃を受けるリスクを考慮し、以下のような対策の検討を推奨します。

- 対策例
  - 問い合わせフォームにアクセスできるIPアドレスの制限（日本国内に限る等）
  - 同一IPアドレスからの連続アクセスの禁止
  - 問い合せフォームへのCAPTHCA等の実装
  - 問い合せを受け付けた後に、自動で返信しない仕様への変更

攻撃者の残した痕跡に学ぶ

アプリケーションサーバの侵害原因

2017 年夏、複数のお客様から受けた調査依頼に、JBoss、Tomcat が動作するアプリケーションサーバが侵害され、仮想通貨を発掘するソフトウェア（CoinMiner）が設置されるインシデントがありました。いずれの CoinMiner も設定ファイルは図 2-1 のようになっており、user が一致していることから、サイバー救急センターでは同一の攻撃者グループによる攻撃と判断しています。発掘対象の仮想通貨はアルゴリズムが cryptonight であることから Monero であった模様です。

```
{
    "url" : "stratum+tcp://94.23.206.130:80",
    "user" : "46XG1vfKxfE1yQnPkrwdQoUDdewkqxCz8ZUnjtu4HH6j27uaWdXaC8D43Vax6XVZmGb3MTHaULEBoiBo7DbP3PPJLyffUcF",
    "pass" : "x",
    "algo" : "cryptonight",
    "quiet" : true
}
```

図 2-1 CoinMiner の設定ファイル

調査当初は、近年多発している Struts2 の脆弱性[1]を悪用したインシデントではないかと推測しました（またはみられました）。

JBoss、Tomcat は共に Web アプリケーションとして Java を動作させる際に使用される著名なサーバソフトウェアであり、Java フレームワークである Struts2 と組み合わせて利用されることがあります。Struts2 は遠隔から直接、不正侵入に結び付く危険度の高い脆弱性が数か月毎に見つかっており、加えて国内での採用事例も多く、Struts2 の脆弱性に起因するインシデントが数多く発生しています。また、JBoss、Tomcat と異なる種類のアプリケーションサーバが侵害されていることから、サーバソフトウェア自体ではなく、共通で使われているフレームワークの脆弱性が最も疑わしいと考えられました。

1 https://www.lac.co.jp/lacwatch/alert/20170310_001246.html

しかし、Struts2 の脆弱性が悪用された際に残る特徴的なログは見つからず、侵害原因は Java ライブラリに存在するデシリライゼーションの脆弱性の悪用であることがわかりました。

ところで、このデシリアライゼーションの脆弱性は 2015 年頃から様々なソフトウェアに存在していることが話題になりました。例えば、Apache Myfaces Trinidad や Apache Commons Collections、Spring は公式に脆弱性が公表されています。しかし、利用者が少ないソフトウェア等では公表されていないものがあります。また、ソフトウェアの内部でこれらが使われている場合、開発者や運用者は脆弱性のあるライブラリであることに気付かず運用していることもあります。

攻撃する側としては、Jexboss[2]などを使用すれば、攻撃対象がどんなソフトウェア、バージョンを使っているかにかかわらず、JBoss や Struts2、さらにそこで動く Java ライブラリのデシリアライゼーションの脆弱性悪用まで半自動的に攻撃することが可能です。

使用しているソフトウェアを最新版にすることに加えて、守る側でも自分の管理するサーバに Jexboss 等のツールを使用して、脆弱性の存在を確認することを推奨します。

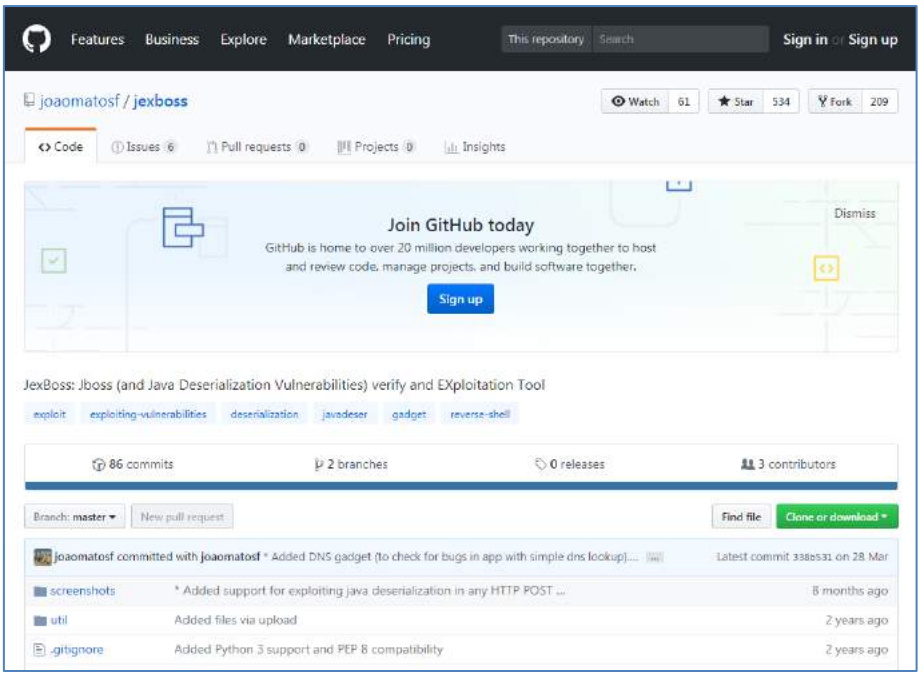

図 2-2 Jexboss の Web ページ

2 https://github.com/joaomatosf/jexboss

脅威分析報告

日本に送られるバラマキ型メールの裏側

電子メールは日々の業務に欠かせないツールですが、スパムメール(迷惑メール)を目にしない日はありません。目にしないという場合、迷惑メールフォルダに振り分けられていて気付いていないだけかもしれません。迷惑メールには、マルウェア等の不正なコンテンツが含まれるメール(以降、マルウェア付きメール)、フィッシングメール、広告や宣伝メール、アダルトメール等、様々なものがあります。

ここでは、サイバー救急センターの脅威分析チームが 2017 年 7 月から 2017 年 10 月中旬までの約 3 カ月間に受信したバラマキ型のマルウェア付きメールの動向を分析した結果を報告します。

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)、添付ファイル、ダウンロードされるマルウェア情報をマッピングし Maltego で関係性を確認したものです。

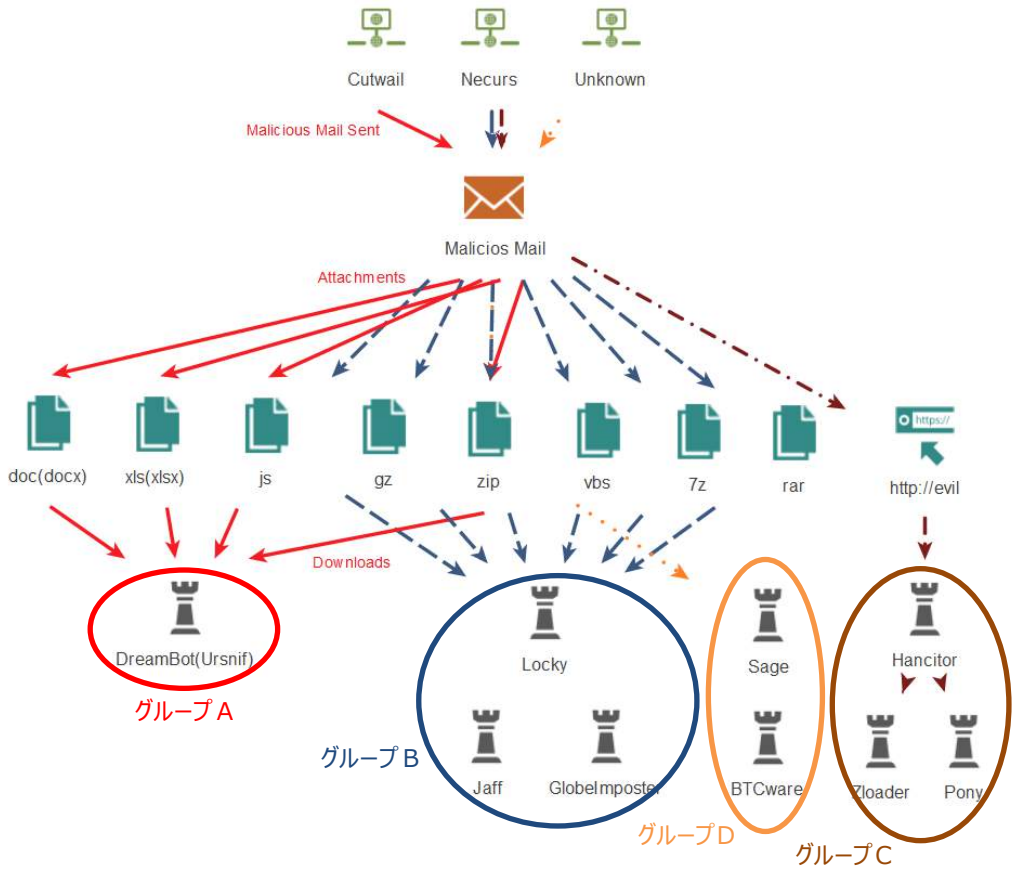

図 3-1 バラマキ型メールで拡散されるマルウェア

図 3-1 の中段のファイルの形をした緑のアイコンは、マルウェア付きメールに添付されているファイル形式を示しています。ファイル形式の種類としては、7z、ZIP、RAR ファイル等の圧縮ファイル[3]、Microsft Word や Excel ファイルの文書ファイル、JavaScript(JS)ファイル、VBScript ファイル等、スクリプトファイルが利用されています。Microsoft Word や Excel ファイルといった文書ファイルは、マクロや脆弱性を悪用するコードを含める方法、あるいはオブジェクトとして LNK（ショートカット）または JS ファイルを埋め込む方法でマルウェアをダウンロードして実行します。

図 3-1 の一番上に 3 つある黄緑のアイコンは Botnet を表し、マルウェア付きメールは、Cutwail、Necurs、Unknown(不明）のいずれかから送信されていることがわかります。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調査すると、A から D の 4 つのグループに分類できます。以降では、この 4 つのグループの特徴を紹介します。

グループ A

グループ A は、Cutwail を利用してマルウェア付きメールを送信し、インターネットバンキングマルウェアとして知られる DreamBot(Ursnif)を拡散させるグループです。メールの特徴として、件名や本文に日本語が使われる点が挙げられます（図 3-2）。2016 年頃から活発に活動し、2017 年 10 月の執筆時点でも、その勢いは継続しているだけでなく、攻撃手口も巧妙化しています。

特に、2017 年 9 月末からは実在する企業の請求書案内をかたったメールが多くなり、メール本文内に含まれたリンク(URL)から ZIP ファイルをダウンロードさせた後、ZIP ファイルを解凍して生成される LNK（ショートカット）または JS ファイル経由で DreamBot をダウンロードさせる手口が利用されていることも確認しています。

2017 年 10 月 13 日時点における DreamBot のバージョンは 216962 で、ターゲットになっているサイトは、金融機関だけでなく、クレジットカード会社、通販会社、仮想通貨取引所等となっています。また、Web インジェクションを行うための不正な JavaScript を配信する C2 サーバ(マニピュレーションサーバ)としては、clicktwicedetect[.]at の存在を確認しています。[4]

3 圧縮ファイルを展開すると、Microsoft Word や Excel ファイルや JavaScript ファイル、VBScript ファイルが含まれる。
4 2017 年 10 月 13 日時点での config 情報であり、変更されている可能性がある。

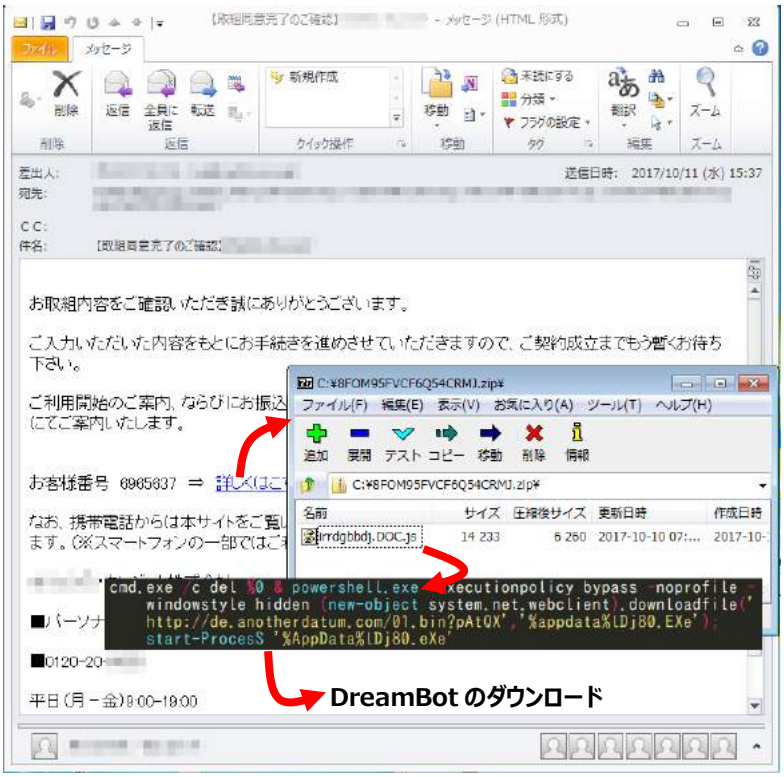

図 3-2 DreamBot を拡散させるスパムメールの一例

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、ランサムウェアを拡散させるグループです。メールの特徴として、件名に"Voice Message"、 "Invoice"、 "Payment"、 "Emailing"、 "Scan Data"等といった英単語が含まれるケースが多く見られます(図 3-3)。拡散されるランサムウェアは時期によって異なり、図 3-4 に示す通り、Jaff(.jaff)は 2017 年 6～8 月頃、Globelimposter (.726)は 2017 年 9 月初旬頃、最近では、Locky(.ykcol/.asasin)が利用されています。

この攻撃者グループが同じランサムウェアを長期間利用せず、短期間で異なる種類のものに変更する意図は、暗号されたファイルを復号するツールの公開の有無[5]に関連しているからではないかと推測されます。また、2017 年 10 月中旬頃から、新たな攻撃手法として、Microsoft Office の Dynamic Data Exchange (DDE)機能[6]を悪用する攻撃を確認しています(図 3-5)。

5 The No More Ransom Project (https://www.nomoreransom.org/en/index.html)
6 About Dynamic Data Exchange
(https://msdn.microsoft.com/ja-jp/library/windows/desktop/ms648774(v=vs.85).aspx)

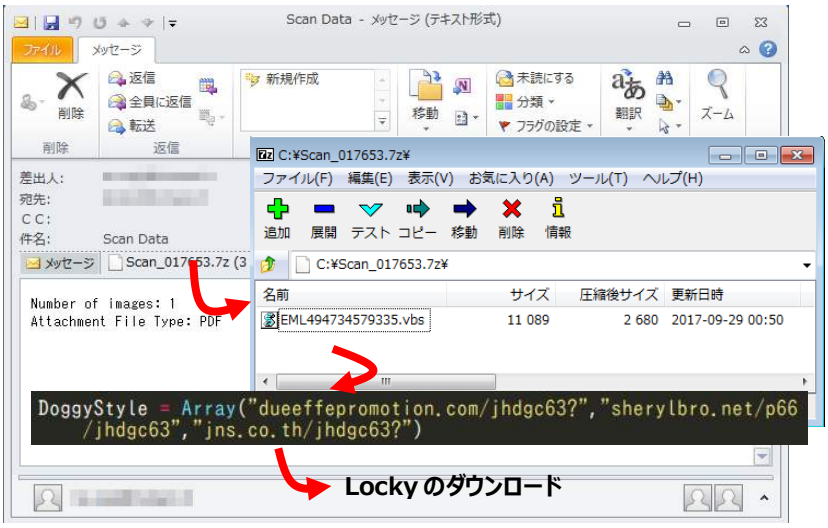

図 3-3 Locky を拡散させるスパムメールの一例

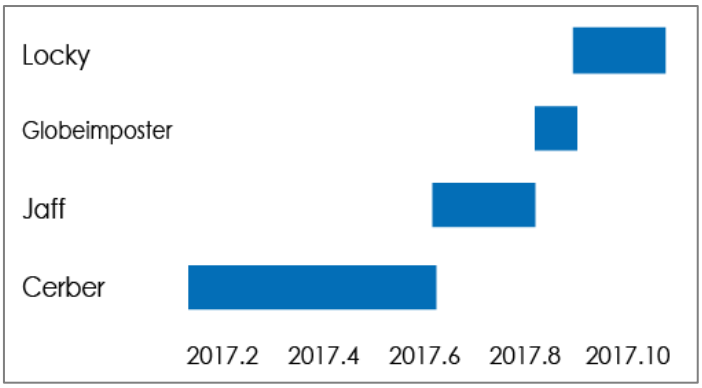

図 3-4 攻撃者が利用するランサムウェアの変遷

図 3-5 DDE 機能を悪用して Locky をダウンロードするコード例

グループ C

グループ C は、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て、ダウンローダとして動作するマルウェア（Hancitor）を拡散させるグループです。

メールの特徴は、図 3-6 に示すような HTML 形式メールを利用し、実在する企業からの領収書やドキュメントを共有する案内等をかたる点です。

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、正規プロセスである explorer.exe または svchost.exe にインジェクションして実行されます。その後、Hancitor は、調査を実施した期間では、パスワードやアカウント窃取機能を有する Pony や Zeus およびその亜種をダウンロードする Zloader 等の複数のマルウェアをダウンロードします。Zloader については、感染後、インターネットバンキングマルウェア Zeus の亜種[7]をダウンロードすることを確認しています。

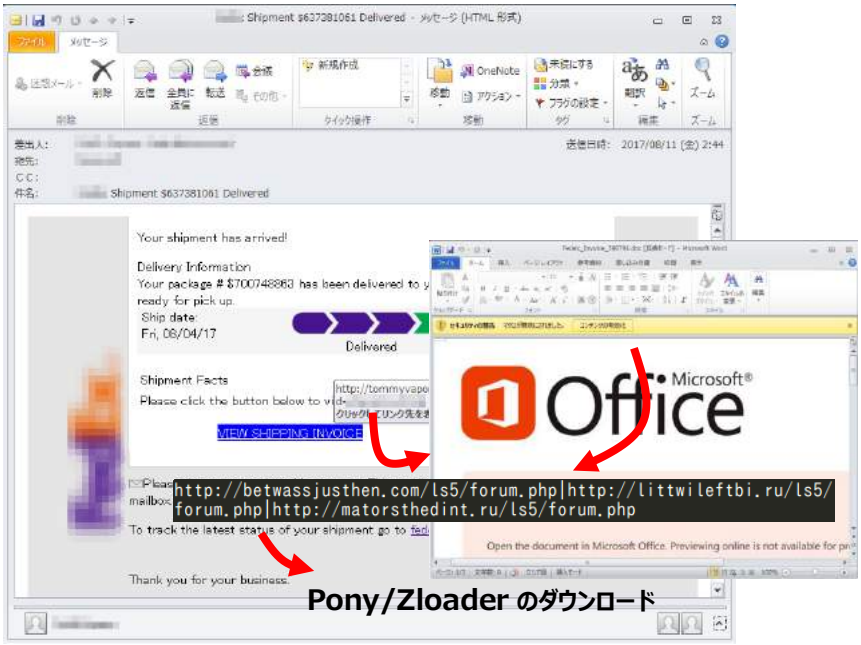

図 3-6 Hancitor を拡散させるスパムメールの一例

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、ランサムウェアを拡散させるグループです。メールの特徴として、件名や本文に何も文字が含まれていないケースが多数確認されています(図 3-7)。

7 32/64bit バージョンそれぞれの Tor 機能を有する検体と有さない検体

拡散されるランサムウェアは時期によって異なり、2017 年 6～8 月頃は BTCWare(.btcware)、2017 年 9 月頃から以降は Sage(.sage)を確認しています。2017 年 9 月末に Sage を拡散させる日本語のメールが報告[8]されていますが、このスパムメールは入手できていないため、グループ D との関連は不明です。

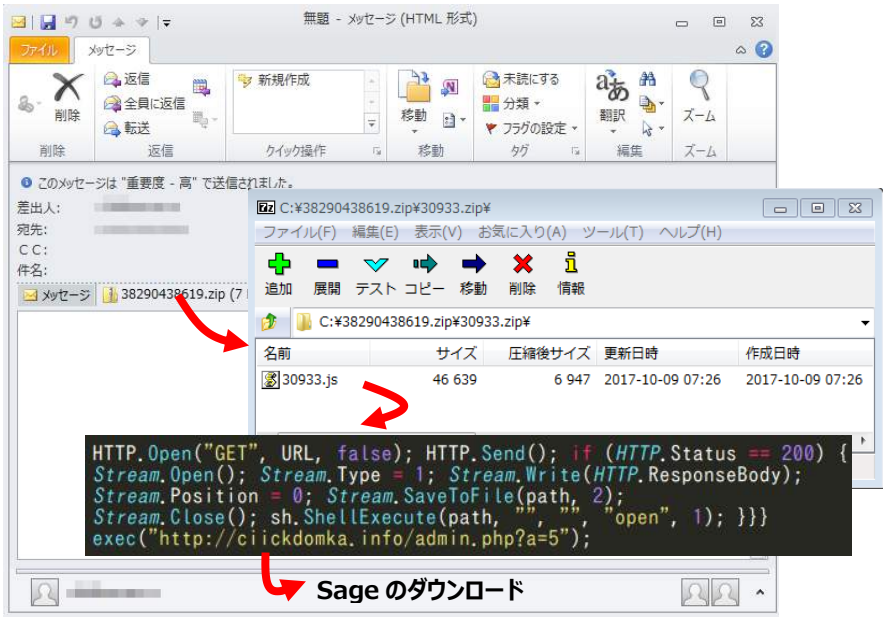

図 3-7 Sage を拡散させるスパムメールの一例

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、サイバー救急センター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、その裏側にはいくつかの攻撃者グループの存在がうかがわれます。今回の調査では、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等もあることから、今後も引き続き分析を行う予定です。

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】

379ea84966cdf4bb8663f72cf21dd98a

fe91c2b095380bd38da256bbe5a3d101

f8b8600ebd23b7edd6bb930fcc22508c

da797bd3ae93abee84c9f365785203c6

8【重要】So-net を装った不審な迷惑メールにご注意ください
(https://www.so-net.ne.jp/info/2014/op20140715_0062.html)

コラム：セキュリティ百景 #1

CodeBALI 2017

皆さんは「CodeBALI」というイベントをご存じでしょうか？ 観光地として有名なインドネシアのバリ島で 2015 年から開催されているセキュリティカンファレンスです。今年は 2017 年 9 月 26 日~29 日に開催されました。

ラックからは私を含め 2 名がスピーカーとして登壇、私は 26 日のデジタル・フォレンジックに関連したワークショップを担当しました。

写真 4-1 ワークショップ風景

ワークショップのタイトルは「Sherlocking Malware」で、名探偵シャーロック・ホームズをリスペクトして付けました。セキュリティ技術者に、目視でマルウェアやファイルを探していただく内容です。

このワークショップ向けに新規に作成した演習として「紙ベースのカービング」があります。カービングとは、通常はディスク上から削除されたファイルを復元する際に利用される手法ですが、その概念を理解してもらうことを目的として、紙ベースで実施可能な演習を考案しました。

やり方は簡単で、次ページに掲載したような 2 つの表を用意します。

1 つ目の表「HardDisk Table」は、ハードディスクの内部構造を HEX で表したものです。この表の中から各ファイルタイプの特徴的なシグネチャを見つけ出し、シグネチャに隣接する数値を参照します。その数値を元に、2 つ目の表「MFT Sheet」を参照すると、発見したファイルの名称・ファイルパスが判明するという仕組みです。

単純にシグネチャを見つけ出すだけではなく、受講生には『なぜ、そのファイル名・ファイルパスになるのか？』、という点にも着目してもらいました。

例えば、シグネチャは「RAR（圧縮ファイル）」を示しているのに、「MFT Sheet」で参照したファイルの拡張子が「PDF」になっている場合は、拡張子偽装を疑ってみたり、「○○.jpg:XX.zip」のように、異なるファイルタイプがコロンで結ばれたファイル名が導き出された場合は、ADS（Alternate Data Stream）に隠されたファイルであることを推測してみたり、というようにです。

この演習は、カービングの概念だけではなく、攻撃者がよく利用するファイル隠蔽手法を学ぶことも目的としています。

読者の皆さんも時間があれば、次ページの「紙カービング」の演習に挑戦してみてください。

サイバー救急センター：郷 晴奈

紙カービングの演習例

■やり方

1. HardDisk Table から EXE ファイルのシグネチャ「4D 5A 90 00」を発見する（答え：G 行）
2. シグネチャ「4D 5A 90 00」に隣接する数値を確認する（答え：「03」）
3. MFT Sheet から「03」のマス目を参照しファイル名を発見する（答え：「$RD46GO9.exe」）

■問題：下表の HardDisk Table には、上記 EXE ファイルの他にも①拡張子偽装された PDF ファイルのシグネチャ：「52 61 72 21」、②ADS を利用して隠蔽された ZIP ファイルのシグネチャ「50 4B 03 04」の 2 つが隠れています。ファイル名を発見できますか？

◇ HardDisk Table

➢Partition 1

OFF SET	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	52	61	72	21	1A	07	00	CF	90	73	00	00	D0	00	00	00
B	00	00	00	00	00	00	F5	F7	74	20	90	2A	00	D6	04	00
C	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60
D	28	A2	8A	00	28	A2	8A	00	0F	FF	FD	90	00	00	00	00
E	50	4B	03	04	0A	00	00	00	08	00	D1	5A	1C	4B	41	19
F	65	F1	75	20	D3	01	50	4B	05	06	00	00	00	00	01	00
G	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00

◇ MFT Sheet

	0	1	2	3	4	5	6	7	8	9
0	Pictures	4.jpg	Internet Explorer	$RD46GO9.exe	Sample Music	config	Vss	LocalLow	SysWOW64	Public
A	:Sig.zip	2.pdf	$RECYCLE.BIN	Intel	Cookies	2.lnk	4.gif	WebCache	AppData	5.dll
B	Program Files (x86)	inf	Start Menu	Microsoft	Common Files	Temp	Automatic Destinations	PerfLogs	Accessories	Recent
C	Program Files	System	Users	Desktop	Prefetch	Libraries	Fonts	System32	3.xlsx	All Users
D	Unknown	Music	Help	1.doc	History	Local	Drivers	5.mp3	Downloads	Sample Videos
E	Photo	ProgramData	Tasks	Chrome	Documents	Windows	Temporary Internet Files	winevt	Adobe	Contacts
F	1.txt	microsoft shared	3.pf	Videos	Explorer	Custom Destinations	Code8All.png	Mozilla	Favorites	System Volume Information

セキュリティ百景 #2

情報セキュリティワークショップ in 越後湯沢

♨ デジタルフォレン塾 ♨

2017 年 10 月 6 日(金)～7 日(土)に、米どころ新潟で「情報セキュリティワークショップ in 越後湯沢」が開催されました。前日 5 日(木)にはデジタルフォレンジックに関するハンズオンセミナーの「デジタルフォレン塾」が開催され、ラックからは私を含めた 3 名が講師として参加しました。

今回のテーマは、「Windows 環境における認証とイベントログ」です。Active Directory 環境では認証の仕組みとして Kerberos 認証が主に利用されますが、攻撃者が悪用する手口として、Golden チケットと Silver チケットと呼ばれる手法があります。

今回は Kerberos 認証で通常発生するイベントや、チケットが侵入者により偽造された際に発生するイベントログ等を、ハンズオン形式で実際に確認することで、正常時と侵害時の違いを受講者に学習していただきました。

話をわかりやすくするため、おとぎ話「三匹の子豚」をモチーフに概念を説明し、次に専門用語を使って解説する二段構えとしました。

おとぎ話で理解が進んだ方もいたようで、後の懇親会では「斬新な説明だった」との感想もいただきました。

図 5-1 Golden チケットの説明

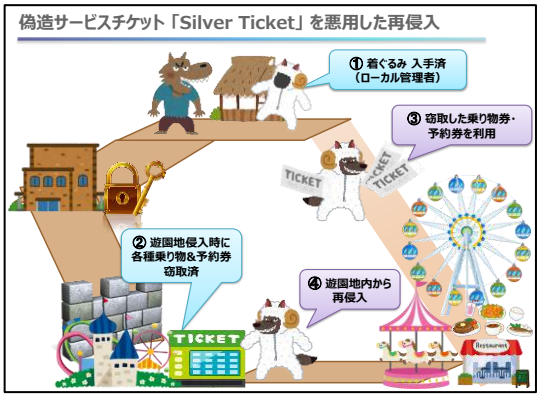

図 5-2 Silver チケットの説明

皆さんの組織内ネットワークに、着ぐるみをまとって侵入している狼（侵入者）はいませんか？

サイバー救急センター：永安 佑希允

編集後記

今後は四半期毎に発行する予定ですので、次号もぜひ読んでいただけますと幸いです。このように発表することができた本文書が、様々な組織でインシデント対応を担う皆様のお役に立てることを願っています。

今後の企画の 1 つとして、様々な組織の CSIRT として活躍されている読者の皆様の訪問記や対談等も載せていきたいと考えています。「訪問、対談 OK です！」という方がいらっしゃいましたら、ぜひご連絡ください。（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、読者アンケートを実施いたします。以下の URL または QR コードから、忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/BXZ7QQR

編集長　内田 法道

編集者・執筆者　伊原 秀明、田原 祐介、関 宏介、高松 啓、石川 芳浩、永安 佑希允、郷 晴奈

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

TEL: 03-6757-0113 （営業）

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。