Japan Security Analyst Conference 2021
(オープニングトーク)

2020年のインシデントを振り返る

JPCERTコーディネーションセンター
インシデントレスポンスグループ
椎木 孝斉

2021年1月28日

2大攻撃タイプ

標的型

(組織内情報の窃取を
目的とした攻撃)

ばらまき系

(金銭の窃取を
目的とした攻撃)

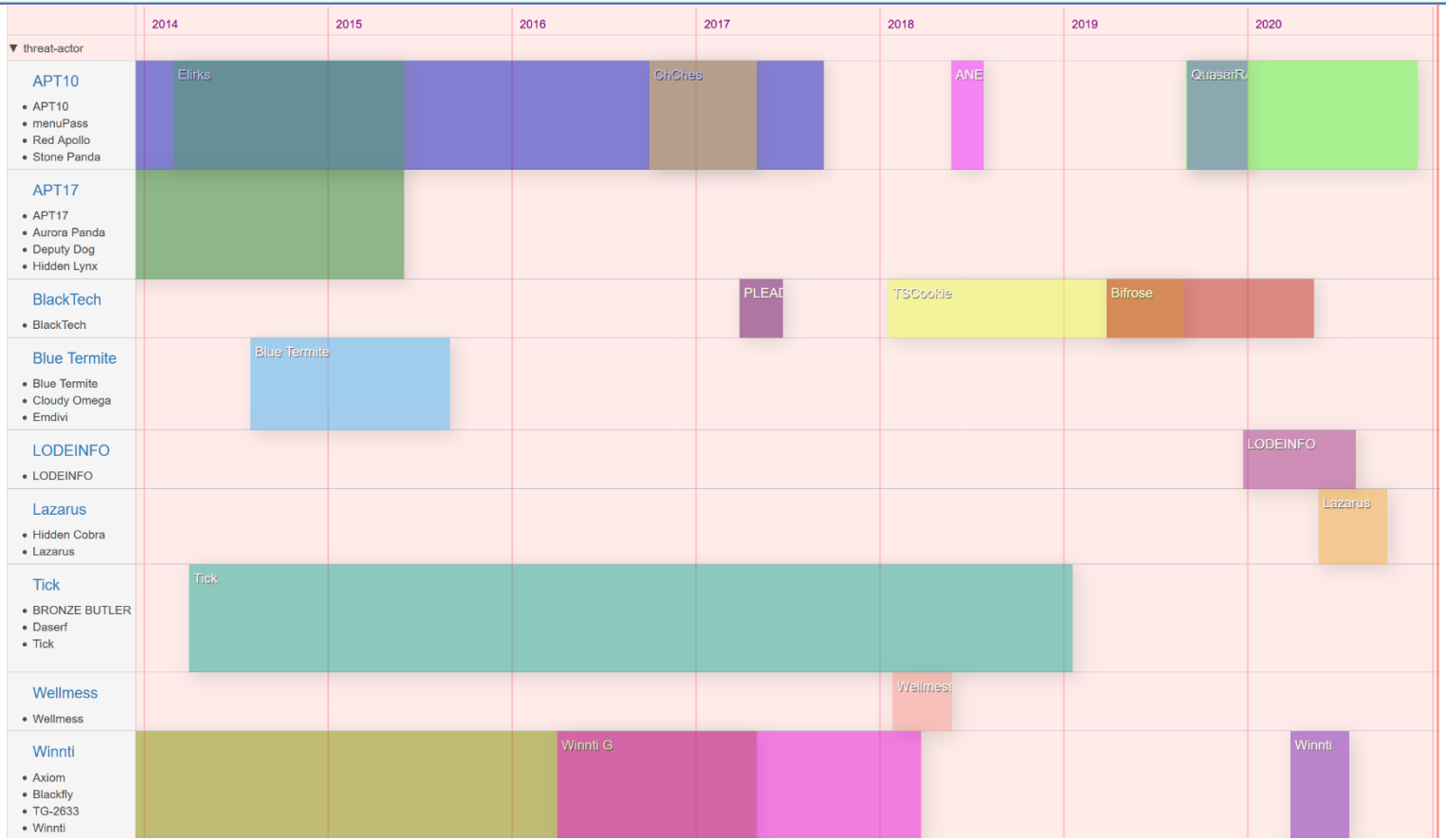
異なる攻撃と手法の組み合わせ

標的型攻撃 ＋ ばらまき系の手法

ばらまき系攻撃 ＋ 標的型の手法

標的型攻撃

JPCERT/CCで確認した標的型攻撃活動



最近の標的型攻撃の特徴

クラウドサービスの悪用

- 攻撃の入り口として (SNSサービス)
- 攻撃インフラとして (Microsoft Azure, Google Cloud など)
- 攻撃ターゲットとして (Office365など)
- 多段攻撃の要素として (Pastebinなど)

マルウェアの複雑化

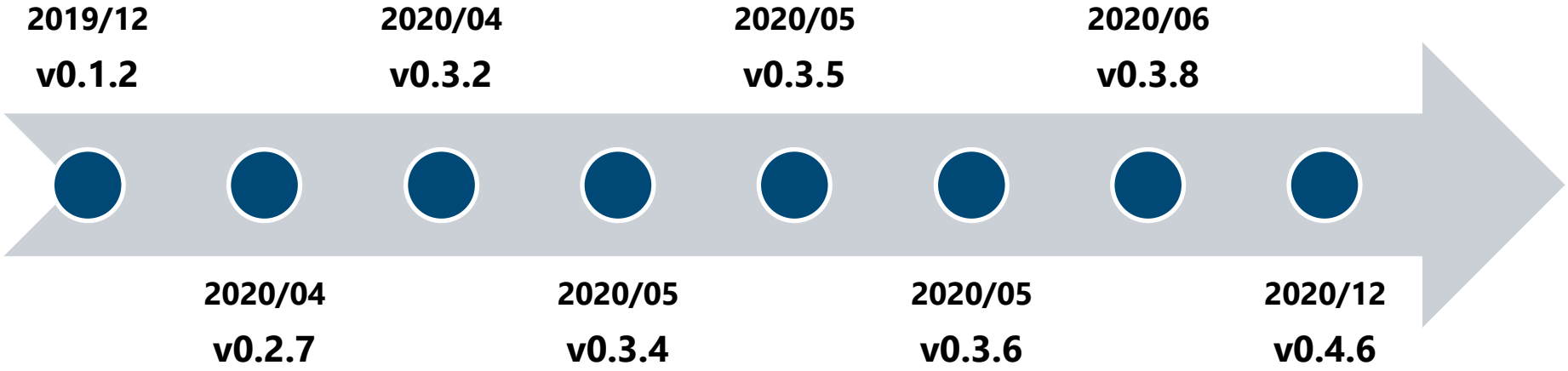
- ファイルレス
- モジュール化
- 多段構成
- 難読化や耐解析機能

特徴的なマルウェアの使用

- 新規マルウェア
- サーバーターゲット (ELF版としての拡張)
- 汎用ツール (オープンソース、正規ツール、OSコマンド)との組み合わせ

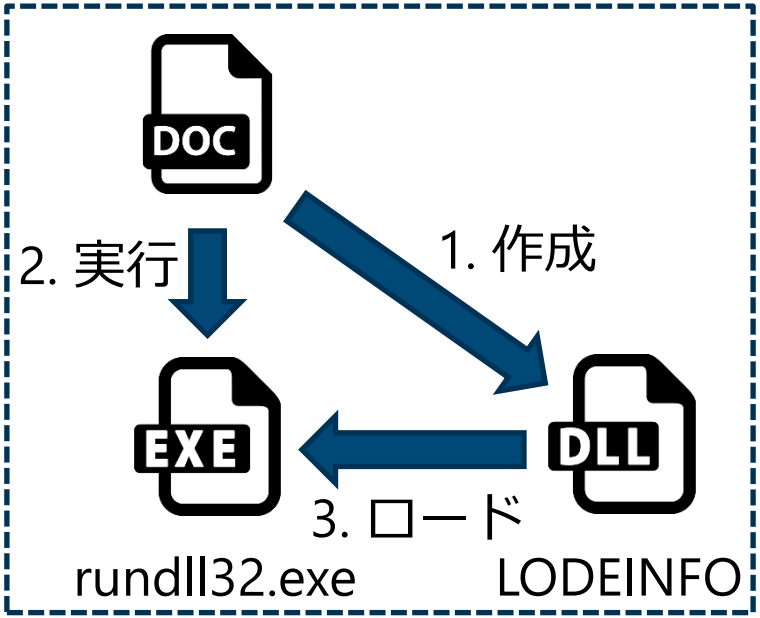
LODEINFO

バージョンの変化

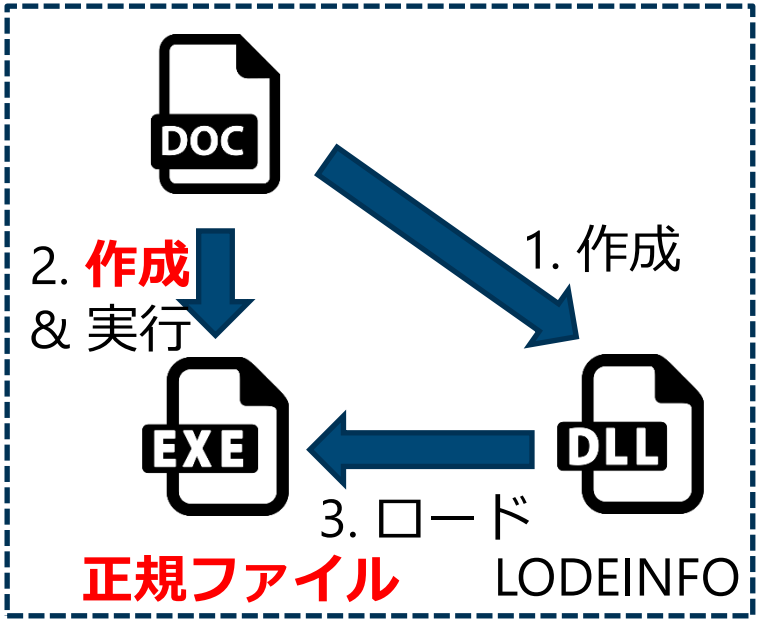


起動方式の変化

Rundll32経由 (～v0.2.7)



DLLサイドローディング (v0.3.2～)



コマンドの変化

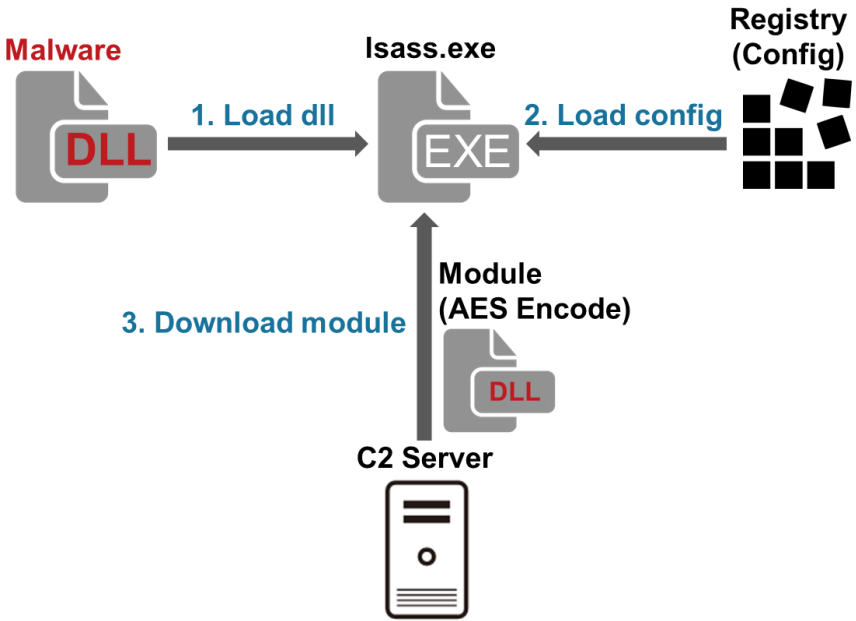
v0.1.2	v0.2.7	v0.3.2	v0.3.4	v0.3.5	v0.3.6	v0.3.8	v0.4.6
•cd •ls •send •recv •cat •memory •kill •ver •command	•cd •ls •send •recv •cat •memory •kill •ver •command	•cd •ls •send •recv •cat •memory •kill •ver •command •print	•cd •ls •send •recv •cat •memory •kill •ver •command •print	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •(keylog)	•cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •keylog •mv •cp •mkdir •ps •pkill

( ): コマンドのみの追加(機能は未実装)

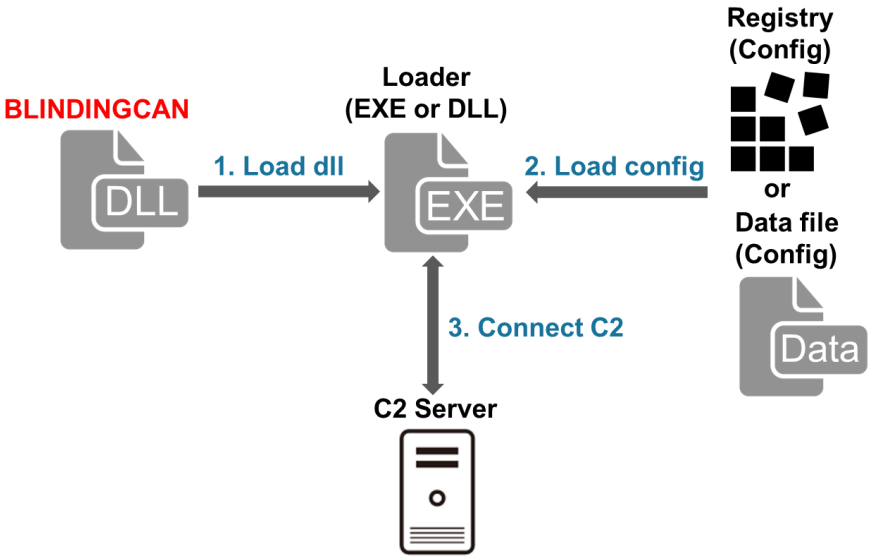
Lazarus

Lazarusが使用するマルウェアの例

■ 侵入後に使用するマルウェア



■ BLINDINGCAN



C2との通信(HTTPS)

侵入後に使用するマルウェア

```
POST /[Path] HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cookie: token=[ランダムな値(4桁)][認証キー(4桁)][通信回数]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77
Safari/537.36
Content-Length: [Size]
Host:[Server]

[param]=[Base64 data]
```

BLINDINGCAN

```
POST /[PATH] HTTP/1.1
Connection: Keep-Alive
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Chrome/28.0.1500.95 Safari/537.36
Host: [Server]
Content-Length: [Length]

id=d3Ztd3lod2t0Tqf42ux9uv3FGH+Y3oAc2w==&bbs=HA==&tbl=hzE4dlKcRq3gokgAGeMQug== &bbs_form=4GQAAA==
```

ばらまき系攻撃

SSL VPN 機器の
脆弱性を悪用した攻撃

情報発信

複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起

最終更新: 2020-01-27

ツイート メール

JPCERT-AT-2020-0003
JPCERT/CC
2020-01-17(新規)
2020-01-27(更新)

I. 概要

JPCERT/CC では、Citrix Application Delivery Controller および Citrix Gatewayの脆弱性 (CVE-2019-19781) について、脆弱性に対する実証コードなどの詳細な情報が公表されていることを確認しています。本脆弱性を悪用された場合、遠隔の第三者が任意のコードを実行する可能性があります。

本脆弱性について、Bad Packets 社より 2020年1月12日 (現地時間) に、脆弱性の悪用を狙ったとみられるスキャンを確認したとの情報が公開されました。

Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を

最終更新: 2020-04-17

ツイート メール

CyberNewsFlash一覧

2020年4月16日 (米国時間)、US-CERT (CISA) は Pulse Connect Secure の脆弱性 (CVE-2019-11510) を悪用した攻撃について、脆弱性の悪用方法や対策方法をまとめた注意喚起 (AA20-107A) を発行しました。注意喚起は、2020年1月に公開された注意喚起 (AA20-010A) の続報で、同脆弱性を悪用してシステムからユーザや管理者アカウントのパスワード情報を窃取する方法などを紹介しています。また、CISA が観測している事案における、侵害後の悪用内容や IoC が公開されており、脆弱な製品の利用者にてアップデートや侵害有無の確認などを行うことが呼びかけられています。

Palo Alto Networks 製品の脆弱性 (CVE-2020-2021) について

最終更新: 2020-06-30

ツイート メール

CyberNewsFlash一覧

2020年6月29日 (米国時間)、Palo Alto Networks から PAN-OS の脆弱性 (CVE-2020-2021) についての情報が公開されています。PAN-OS の SAML (Security Assertion Markup Language) 認証には、署名検証の不備に起因した脆弱性があります。SAML 認証を有効にした状態で、Validate Identity Provider Certificate のオプションを無効にした場合、認証を回避され、結果として遠隔の第三者が SAML 認証によって保護されたリソースにアクセスするおそれがあります。

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

最終更新: 2020-11-27

ツイート メール

CyberNewsFlash一覧

(1) 概要

JPCERT/CC は、2020年11月19日以降、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストに関する情報が、フォーラムなどで公開されている状況を確認しています。当該情報は、FortiOS の既知の脆弱性 (CVE-2018-13379) の影響を受けるとみられるホストの一覧です。この一覧は、攻撃者が脆弱性を悪用可能であることを確認した上で作成したものとみられ、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザーアカウント名や平文のパスワードなどの情報が含まれているとのことです。

JPCERT/CC は、当該情報に日本の IP アドレスが含まれていることを確認し、連絡可能な対象組織へ、直接または関係組織を通じた情報提供を順次行っています。もし、当該製品を使用しており、脆弱性の影響を受けるバージョンおよび条件で稼働している場合は、公開されてしまった認証情報や脆弱性を悪用した攻撃の被害を受ける可能性があるため、以降に記載の対策や侵害有無確認などを実施することを推奨いたします。

JPCERT/CCが確認した侵害事案の例

Citrix製品の脆弱性の悪用事例

不正ファイルの設置
- スクリプト
- WebShell
- ELFバイナリ

ランサムウェアによる侵害

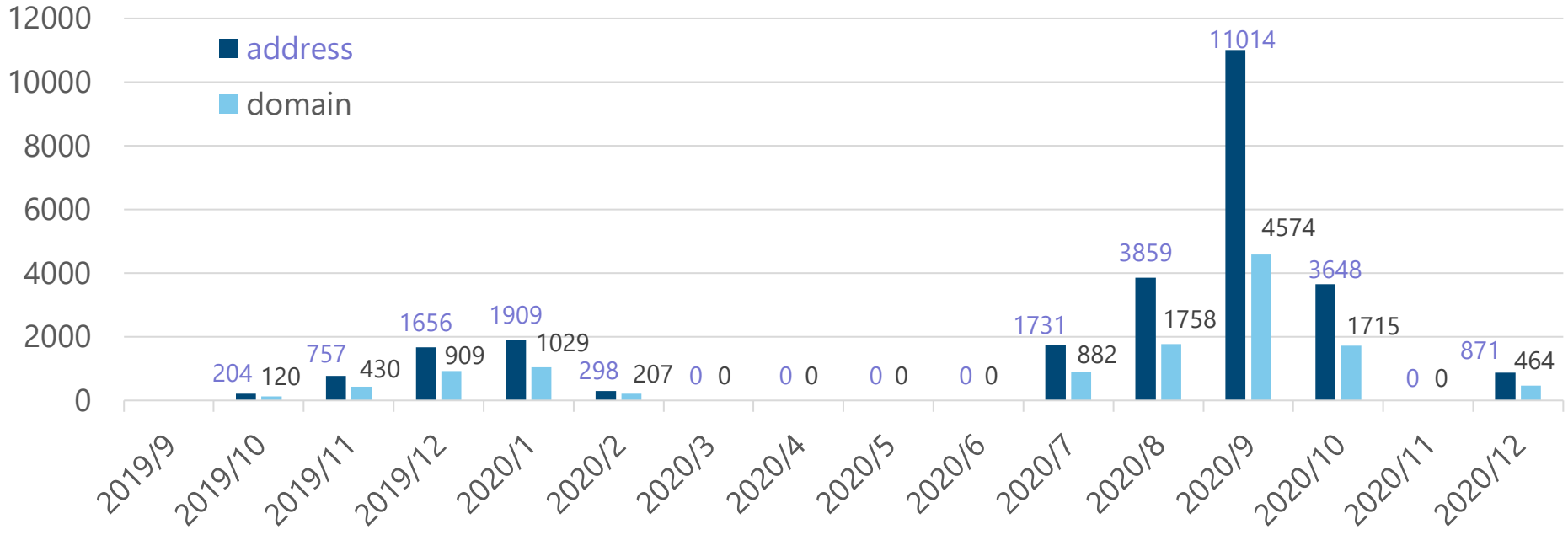
内部探索、AD侵害の試み
- PsExec
- Mimikatz
- AD情報窃取

標的型攻撃による悪用

Pulse Connect Secure の脆弱性の悪用事例

Emotet

国内の感染アドレス数推移



Emotetのメール送信に使われるメールアドレスのうち.jpのアドレス数推移

情報発信

佐條 研(Ken Sajo)

2019/12/02

マルウエアEmotetへの対応FAQ

メール

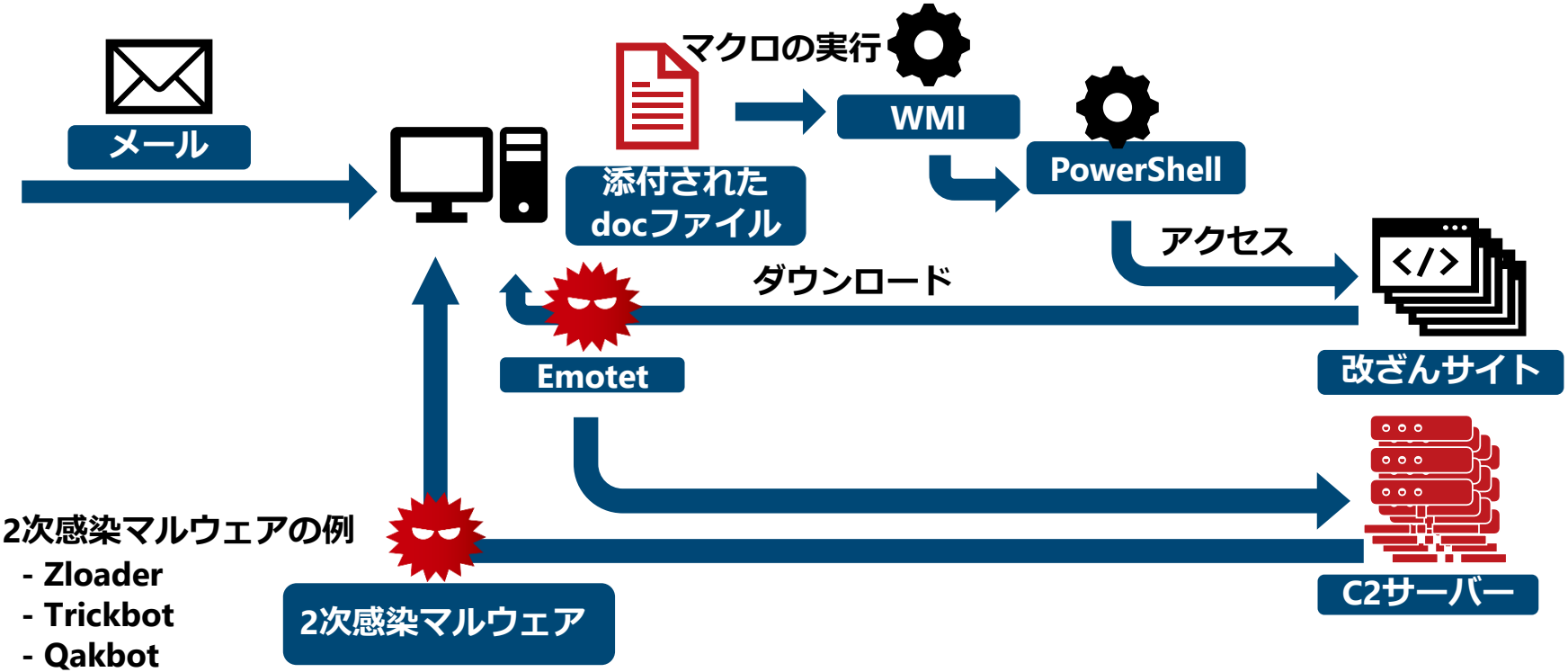
最終更新日:2020.12.23

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

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

本ブログでは、2019年12月時点のEmotetに感染した疑いがある場合の確認方法や、感染が確認された場合の対処方法など、Emotetに関するFAQを掲載しています。なお、ここに記載されている調査方法がわからない場合は、専門のセキュリティベンダへの相談を検討してください。

感染の流れ



2次感染マルウェアの例
- Zloader
- Trickbot
- Qakbot
- IcedID

EmoCheck

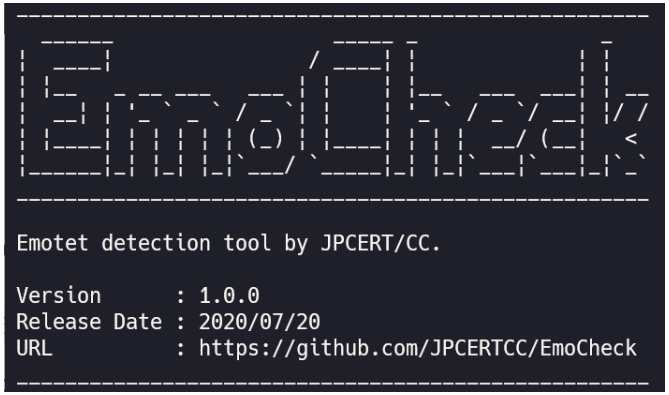
https://github.com/JPCERTCC/EmoCheck

EmoCheck

Emotet detection tool for Windows OS

security　malware-detection　emotet

C++　41　296　3　0　Updated on Aug 11



- **v0.0.1** (2020/02/03)
  - Initial Release
  - 2019/11～のEmotet対応
- **v0.0.2** (2020/02/10)
  - コード署名付与
- **v1.0.0** (2020/08/11)
  - 2020/07～のEmotetに対応
  - バイナリ配布
- NEW **v2.0.0** *(Just Released!)*
  - 2020/12～のEmotetに対応

分析ツール

トレーニングコンテンツの公開

Log Analysis Training

このコンテンツはセキュリティインシデントを調査する際に、Windowsイベントログ (セキュリティログおよびSysmonログ) やプロキシログを活用する方法をトレーニング形式で学ぶことができるコンテンツです。

コンテンツの概要

このコンテンツは、`Material`および`Hands-on`から構成されています。各コンテンツは以下の通りです。

コンテンツ	説明
`Material`	ハンズオン資料 (PDF)
`Hands-on`	ハンズオンに使用するログ一式

目次
- コンテンツ概要
- 得られる知識
- 対象者
- トレーニング詳細
- ダウンロード
- 注意

このトレーニングから得られる知識

このコンテンツは、以下の知識を得ることができます。

- 攻撃者の典型的なネットワーク侵入の手口
- 侵入の痕跡を見つけるために必要なWindowsのログ設定
- Windowsログの調査手順
- ログ調査のポイント
- Active Directoryログから攻撃の痕跡を分析する手法の基礎

https://jpcertcc.github.io/log-analysis-training/

既存ツールアップデート

MalConfScan

github.com/JPCERTCC/MalConfScan

□Linuxメモリスキャン機能
□サポートマルウェアファミリー

- AsyncRAT
- WellMess (Windows/Linux)
- ELF_PLEAD

(合計: 28)

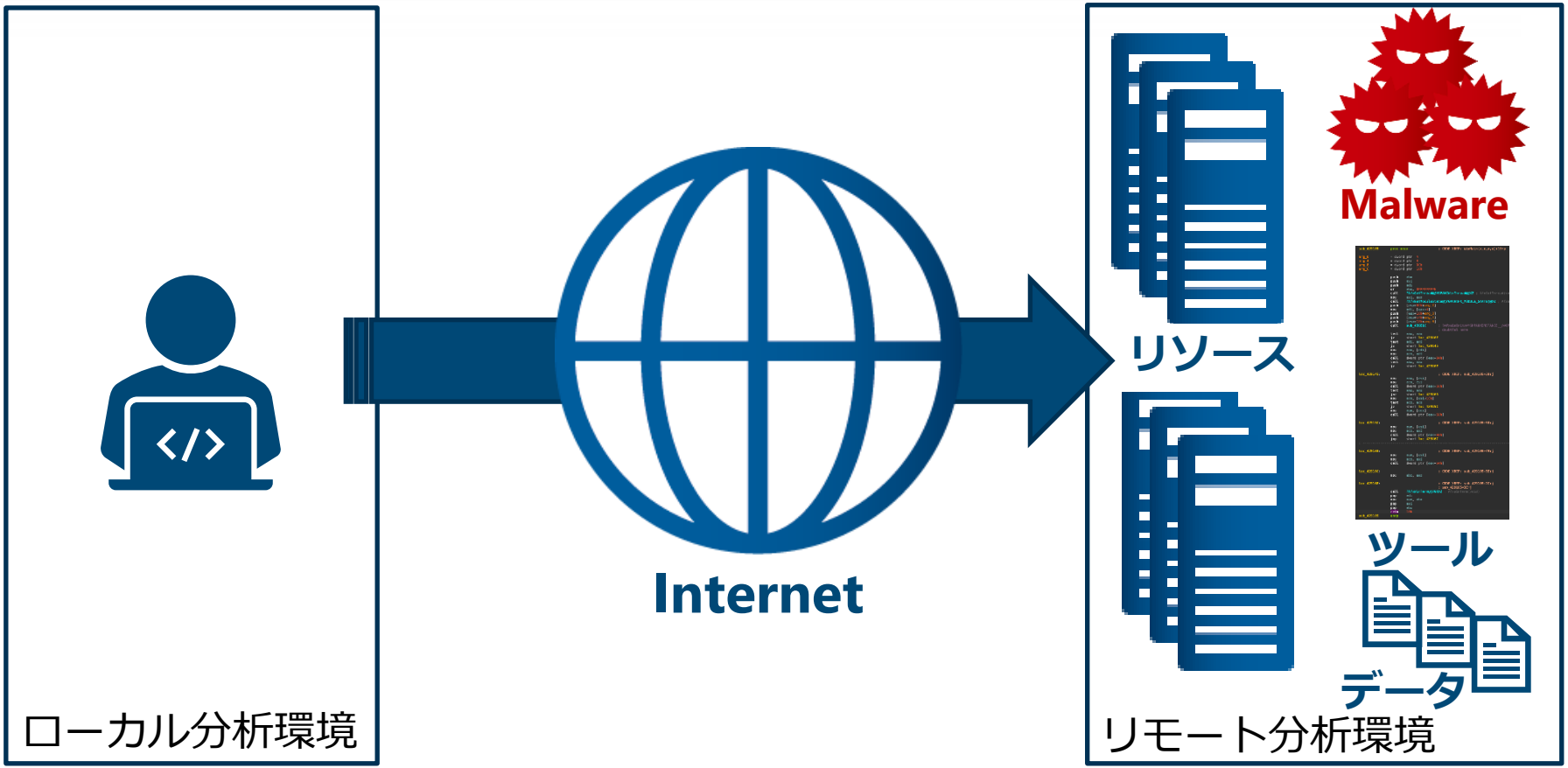
LOGONTRACER

github.com/JPCERTCC/LogonTracer

□リアルタイムADログ分析機能

Elasticsearch

リモート分析環境



の楽しみ方

講演

分類	タイトル
A	NanoCoreHunter: NanoCore C&Cサーバの追跡と180日間のRATオペレータの行動監視
A	LuoYu, the eavesdropper sneaking in multiple platforms
A/C	A41APT case ~Analysis of the Stealth APT Campaign Threatening Japan
A/D	When you gaze into the Bottle,...
A/D	Knock, knock, Neo. - Active C2 Discovery Using Protocol Emulation
B	Accelerating the Analysis of Offensive Security Techniques Using DetectionLab

分類	タイトル
C	取引先のセキュリティ侵害から発生するビジネスメール詐欺の実態
D/A	とあるEmotetの観測結果
D	Shathakに関する攻撃キャンペーンの全体像
D	仮想通貨事業者を標的とした攻撃キャンペーンに関する脅威情報のハンティング
D	GhostDNSbusters: Tracking and Responding to a Large Scale DNS Hijacking Campaign

[A] マルウェア関連
[B] フォレンジック関連
[C] インシデント調査・対応事例・攻撃手法
[D] 脅威動向・インテリジェンス

ワークショップ

分類	タイトル
W[A]	Malware Analysis at Scale ~Defeating EMOTET by Ghidra
W[C]	Shuffle the SOC - automating anything, anytime, anywhere

[A] マルウェア関連
[C] インシデント調査・対応事例・攻撃手法

交流の場

Powered by slack

フォローアップイベント

- イベント名: After JSAC2021
- 開催形式:　オンライン(YouTube配信予定)
- 日時:　2/19(金) 16:00 - 17:00
- 内容(予定):
  1. ベストスピーカー表彰
  2. JSAC2021振り返り
  3. これからCFPに応募する人へ

Thank you!