

A blue-tinted background image showing a hand holding a globe. The globe displays the continents of Asia, Australia, and parts of Europe and Africa. The hand is positioned at the bottom right, with fingers spread, supporting the globe from below.

JPCERT **CC**®

Japan Security Analyst Conference 2021
(Opening Talk)

JSAC2021
VIRTUAL

Looking back on the incidents in 2020

JPCERT Coordination Center
Incident Response Group

Takayoshi SHIIGI

January 28th, 2021

Two Major Attack Types

Targeted

(Attack aimed to steal
confidential
information)

Widespread

(Attack aimed to
steal money)

Combining an Attack Type with the Tactics of the Other

**Targeted
Attack**

+

**Tactics of
Widespread
Attack**

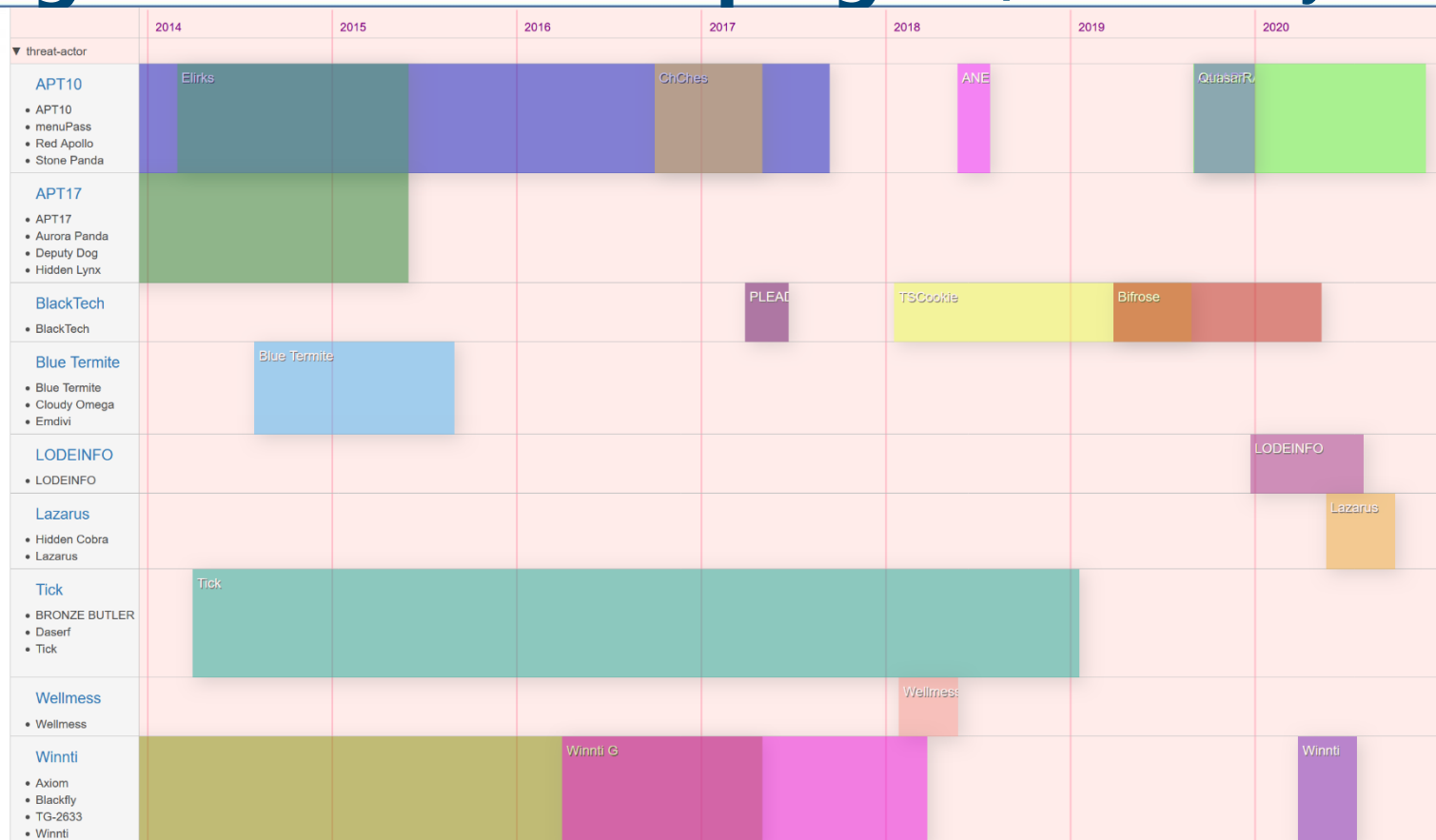
**Widespread
Attack**

+

**Tactics of
Targeted
Attack**

Targeted Attack

Targeted Attack Campaigns (confirmed by JPCERT/CC)



Trends in Recent Targeted Attack

Leverage Cloud Services

- Initial attack vector (SNS services)
- Attack infrastructure (Microsoft Azure, Google Cloud etc.)
- Main attack target (Office365 etc.)
- Part of multi-layer attack (Pasetbin etc.)

Complex Malware

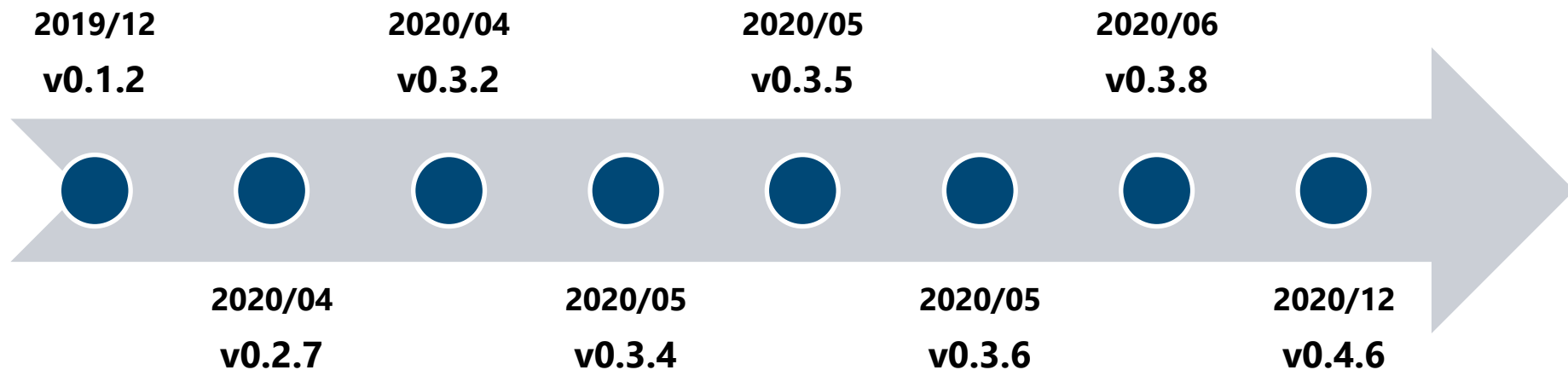
- Fileless
- Modular architecture
- Functions in multiple stages of attacks
- Obfuscation and anti-analysis function

Using Specific/Unique Malware

- New malware
- Targeting servers (Extended for ELF binary)
- Used in combination with generic tools (Open source, legitimate tools, OS commands)

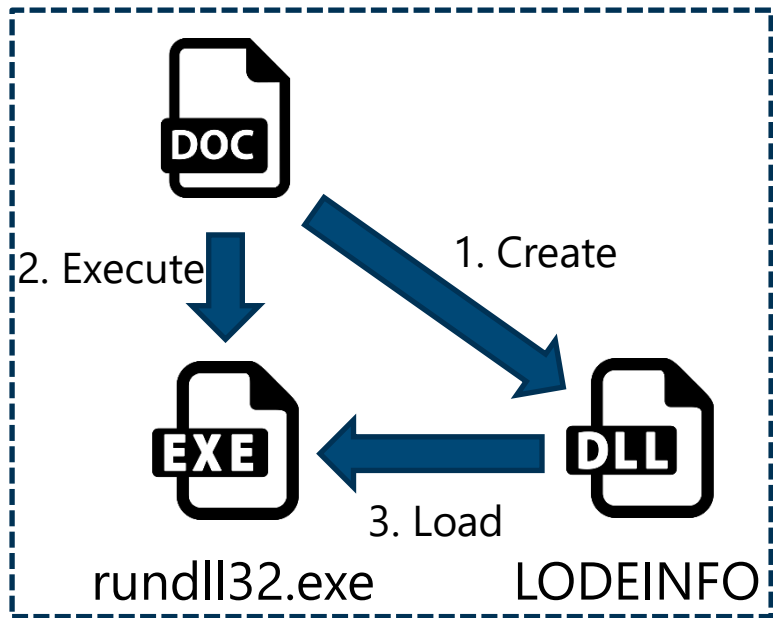
LODEINFO

Version History

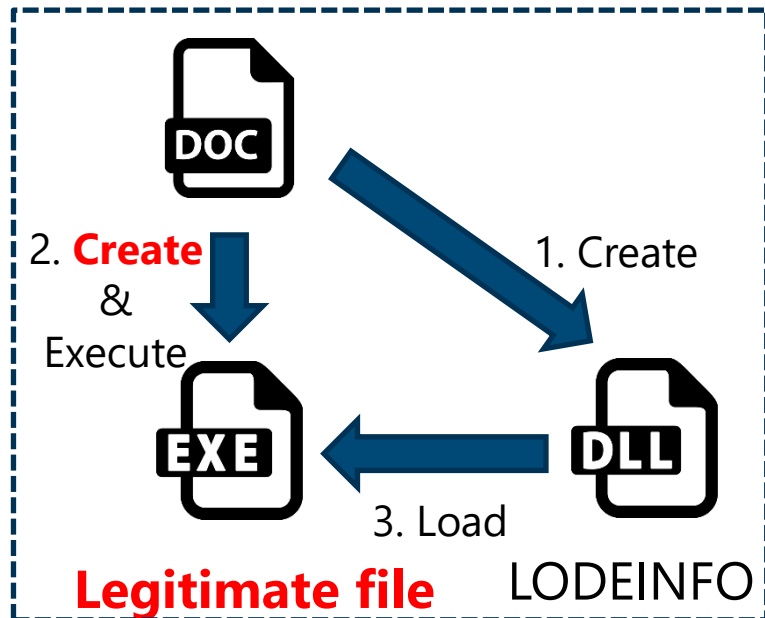


Change in Launch Method

Via Rundll32 (~v0.2.7)



DLL side loading (v0.3.2~)



Changes in commands

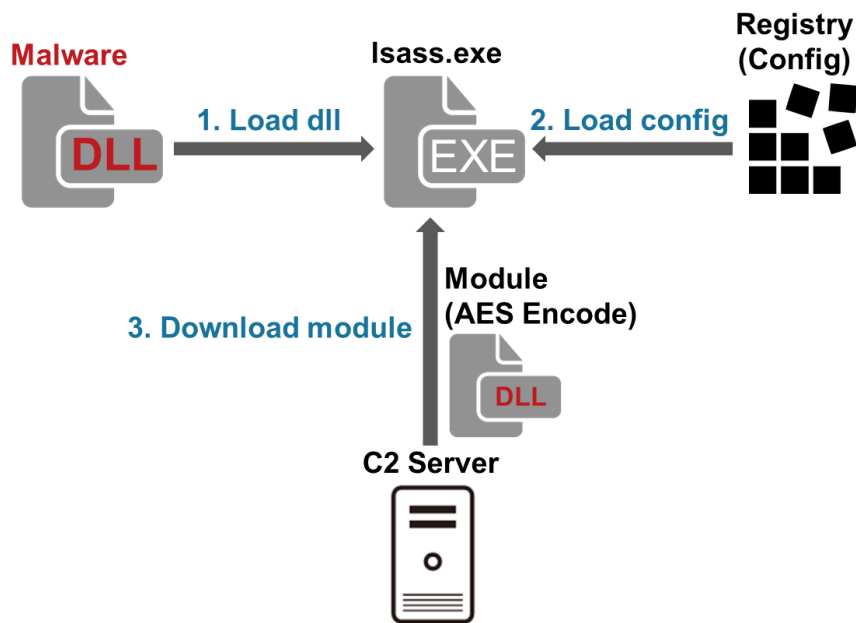
v0.1.2	v0.2.7	v0.3.2	v0.3.4	v0.3.5	v0.3.6	v0.3.8	v0.4.6
<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog) 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •(ransom) •(keylog) 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •(keylog) 	<ul style="list-style-type: none"> •cd •ls •send •recv •cat •memory •kill •ver •command •print •rm •ransom •keylog •mv •cp •mkdir •ps •pkill

(): The commands in brackets have not been implemented but just added

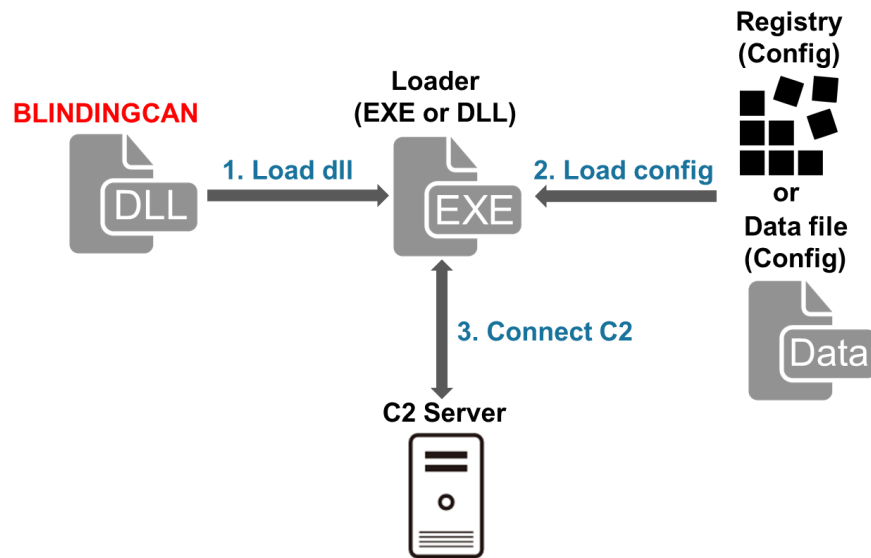
Lazarus

Malware Examples used by Lazarus

■ Malware used after network intrusion



■ BLINDINGCAN



C2 Communication (HTTPS)

■ Malware used after network intrusion

```
POST /[Path] HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cookie: token=[random 4-digit numeric][4-digit authentication key][number of communications]
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=hze4dIKcRq3gokgAGeMQug== &bbs_form=4GQAAA==
```

Widespread Attack

Attack Exploiting Vulnerabilities in SSL VPN Products

Publications

[Updated] Alert Regarding Vulnerability (CVE-2019-19781) in Citrix Products

last update: 2020-01-27

JPCERT-AT-2020-0003
JPCERT/CC
2020-01-17(Initial)
2020-01-27(Update)

[Tweet](#) [Mail](#)

I. Overview

JPCERT/CC confirmed that information including Proof-of-Concept code about a vulnerability (CVE-2019-19781) in Citrix Application Delivery Controller and Citrix Gateway has been made public. A remote attacker leveraging this vulnerability may execute arbitrary code.

On January 12, 2020 (local time), Bad Packets released information about scanning activities that appeared to be leveraging the vulnerability.

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

[Tweet](#) [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

[Twitter](#) [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

[Twitter](#) [メール](#)

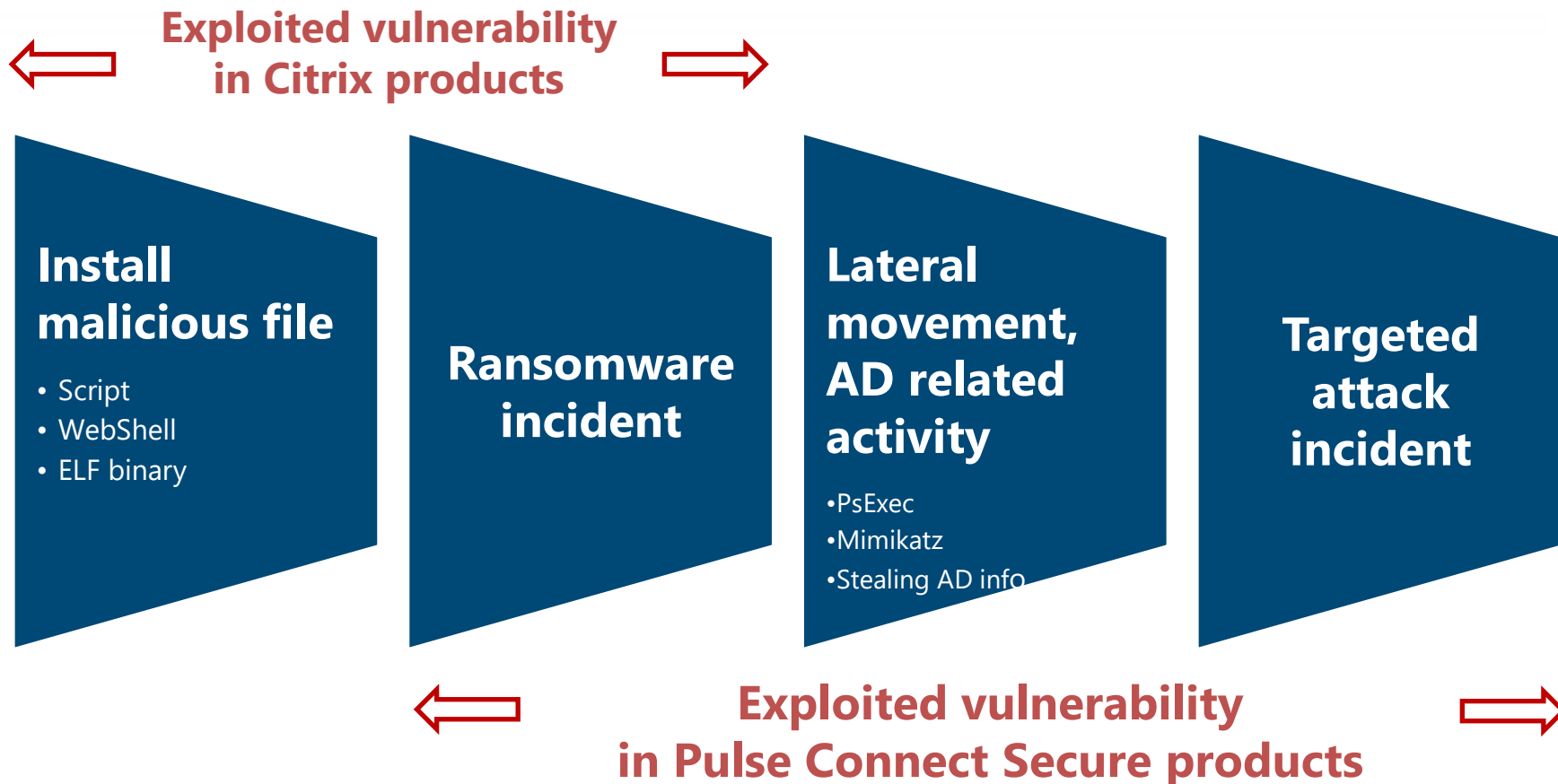
[CyberNewsFlash一覧](#)

(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。

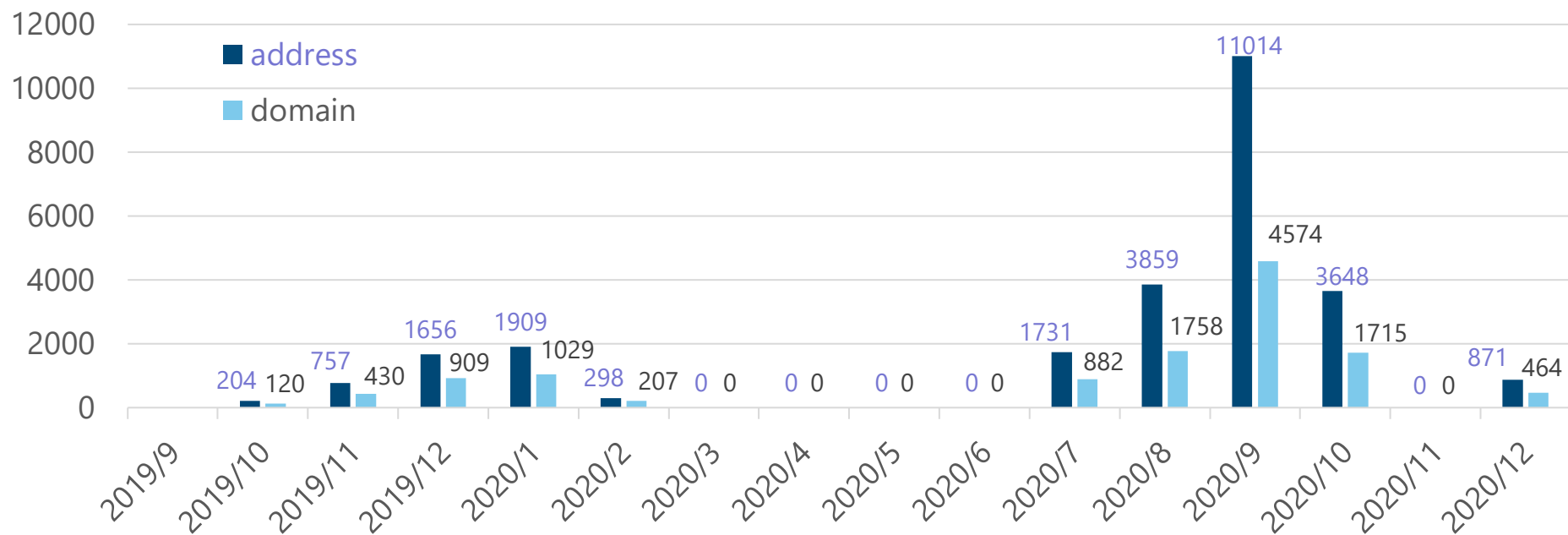
JPCERT/CC は、当該情報に日本の IP アドレスが含まれていることを確認し、連絡可能な対象組織へ、直接または関係組織を通じた情報提供を順次行っています。もし、当該製品を使用しており、脆弱性の影響を受けるバージョンおよび条件で稼働している場合は、公開されてしまった認証情報や脆弱性を悪用した攻撃の被害を受ける可能性があるため、以降に記載の対策や侵害有無確認などを実施することを推奨いたします。

Incident Cases confirmed by JPCERT/CC



Emotet

Infected E-mail addresses in Japan



Number of ".jp" E-mail addresses used to send Emotet



佐條 研(Ken Sajo)

2019/12/02

マルウェア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: マルウェア Emotet の感染に関する注意喚起

<https://www.jpcert.or.jp/at/2019/at190044.html>

JPCERT/CC: CyberNewsFlash マルウェア Emotet の感染活動について

<https://www.jpcert.or.jp/newsflash/2019112701.html>

JPCERT/CC: CyberNewsFlash マルウェア 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)

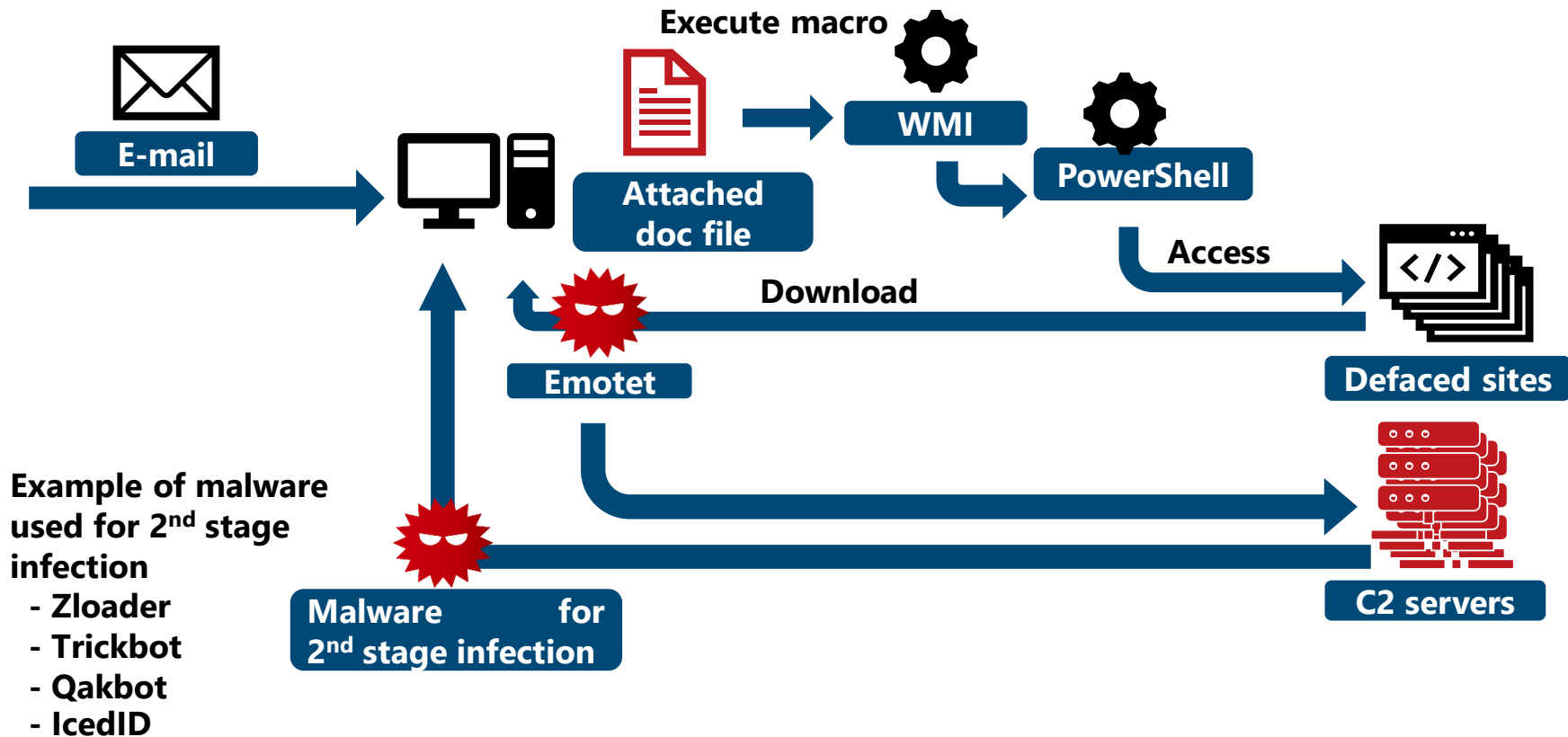
<https://www.jpcert.or.jp/newsflash/2020072001.html>

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ーへの相談を検討してください。

Infection Flow



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

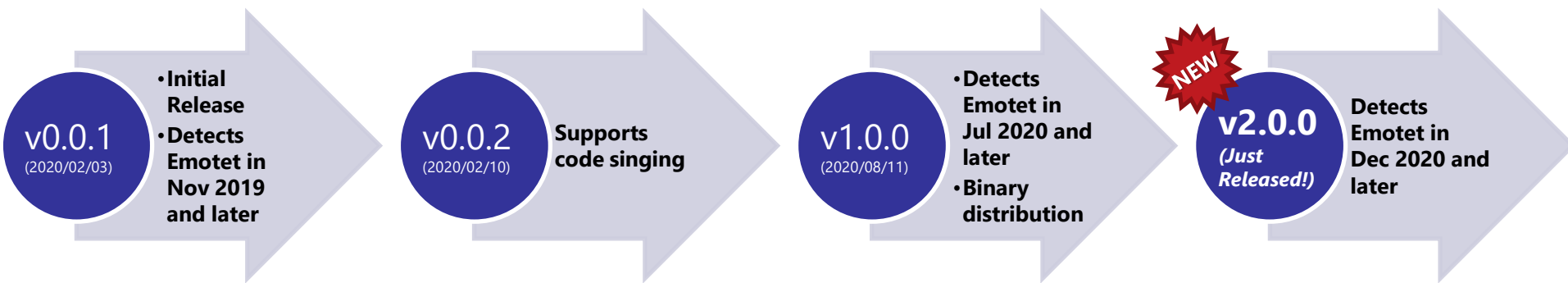


Emotet detection tool by JPCERT/CC.

Version : 1.0.0

Release Date : 2020/07/20

URL : <https://github.com/JPCERTCC/EmoCheck>



Analysis Tool

Published Training Contents

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形式

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

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



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

Updates to Existing Tools



github.com/JPCERTCC/MalConfScan



- ☐ Linux memory scan function
- ☐ Support malware families

- ☒ AsyncRAT

- ☒ WellMess (Windows/Linux)

- ☒ ELF_PLEAD

(Total: 28)



github.com/JPCERTCC/LogonTracer

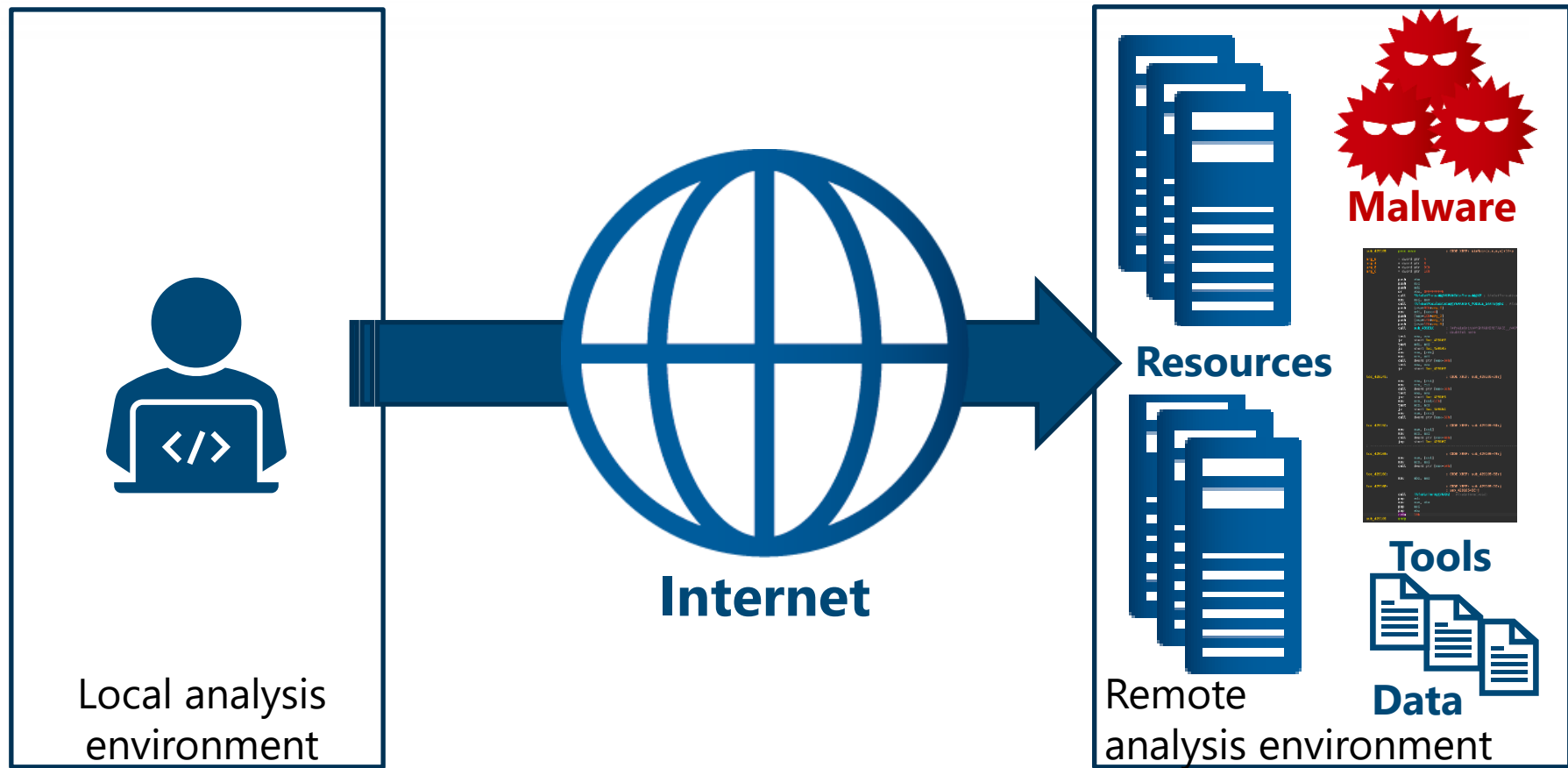


- ☐ Realtime AD log analysis function



Elasticsearch

Remote Analysis Environment



How to Enjoy

The logo for JSAC2021 VIRTUAL. It features the text "JSAC2021" in large, bold, white capital letters on a black background. Below it, the word "VIRTUAL" is written in smaller, white capital letters. The background of the logo is a collage of various text elements, including "Security Analysis", "Hello", and "VIRTUAL".

JSAC2021
VIRTUAL

Presentation

Topic	Title	Topic	Title
A	NanoCoreHunter: Track NanoCore C&C Server and Monitor RAT Operator for 180 Days	C	A Picture of Business Email Compromise Triggered by A Security Breach at Business Partners
A	LuoYu, the eavesdropper sneaking in multiple platforms	D/A	What was Discovered through Emotet Campaign Observation in Japan
A/C	A41APT case ~Analysis of the Stealth APT Campaign Threatening Japan	D	Grasping a Big Picture of Shathak Attack Campaign
A/D	When you gaze into the Bottle,...	D	Threat Hunting of Attack Campaign Targeting Cryptocurrency Service Providers
A/D	Knock, knock, Neo. - Active C2 Discovery Using Protocol Emulation	D	GhostDNSbusters: Tracking and Responding to a Large Scale DNS Hijacking Campaign
B	Accelerating the Analysis of Offensive Security Techniques Using DetectionLab		

[A] Malware

[B] Forensics

[C] Incident

[D] Threat trends, intelligence

Workshop

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] Malware

[C] Incident

Networking



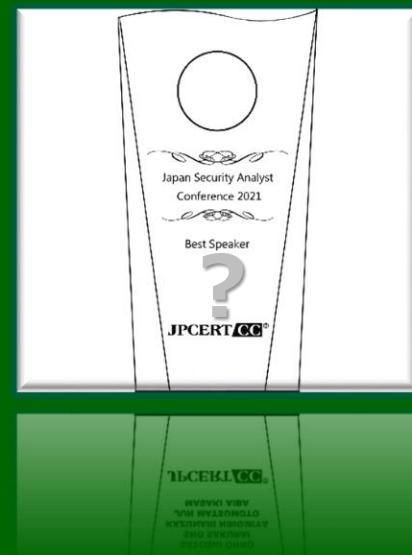
Powered by



slack

Follow-up Event

- Title: After JSAC2021
- Delivery: YouTube live stream(tentative)
- Date & Time: 2/19(Fri.)
16:00 - 17:00
- Contents(tentative):
 1. Best speaker award
 2. Looking back on JSAC 2021
 3. Messages for those interested in applying for JSAC 2022



Thank you!

