JPCERT CC®

Japan Security Analyst Conference 2020
(オープニングトーク)

2019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

2020年1月17日

Hello
I am ...

Malware Analyst

JPCERT CC®

Japan Security Analyst Conference

2大攻撃タイプ

標的型

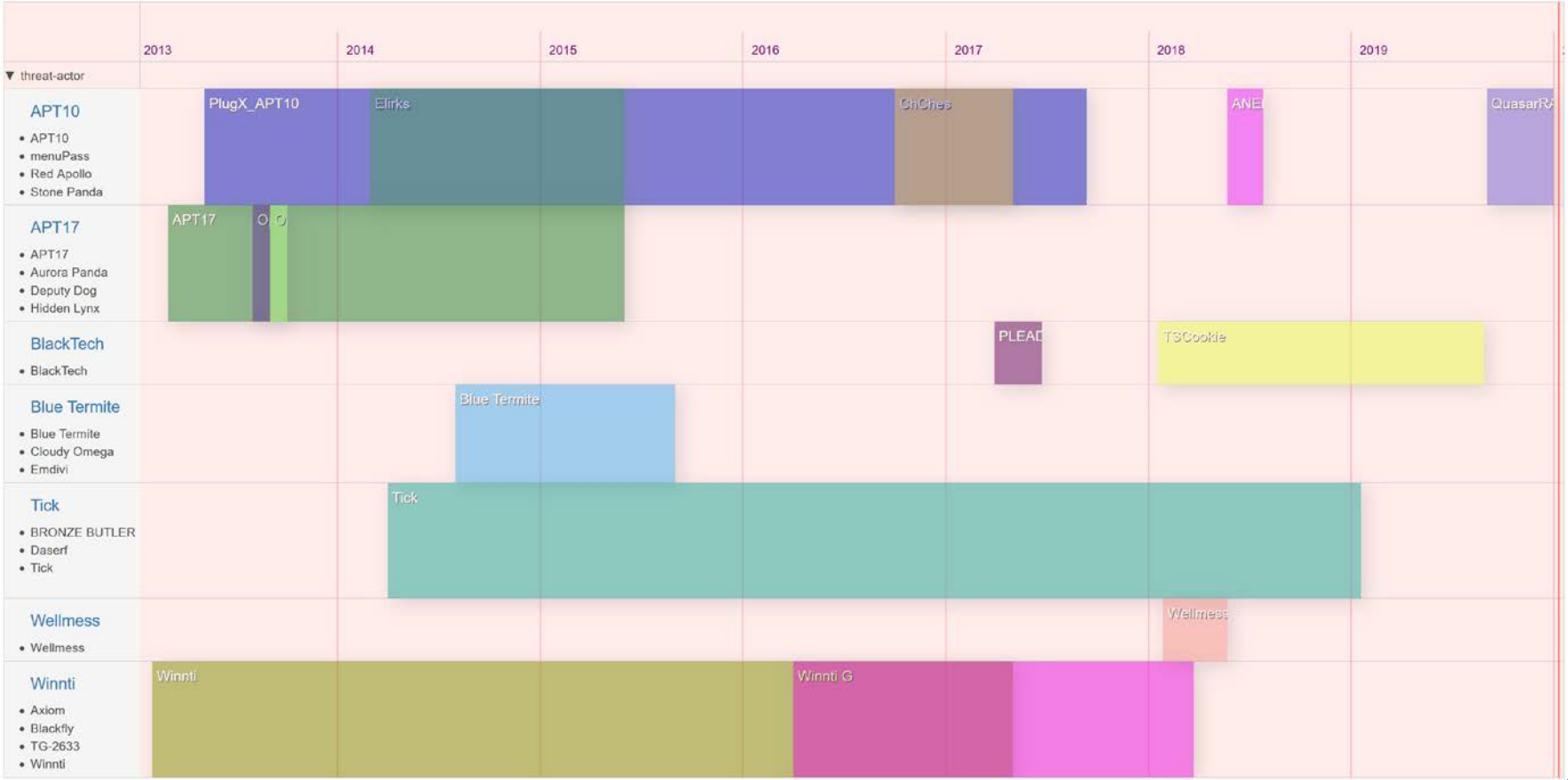
(組織内情報の窃取を
目的とした攻撃)

ばらまき系

(金銭の窃取を
目的とした攻撃)

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

- Microsoft Azure
- Google Cloud など

汎用ツールの悪用

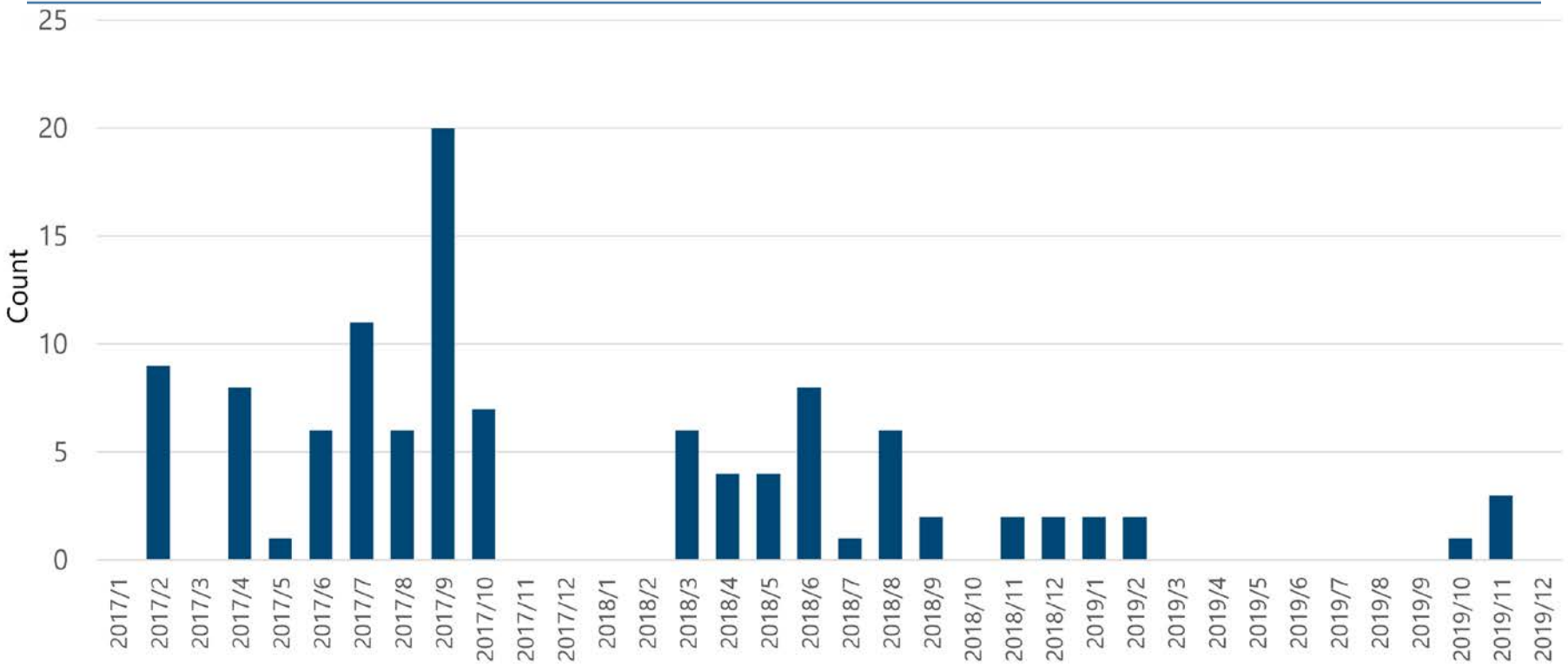
- オープンソースツール
  - PoshC2
  - PowerShell Empire
  - QuasarRAT など
- OSコマンドなど

マルウエアの複雑化

- ファイルレス
- モジュール化
- 多段構成

Tick

スキャン観測状況



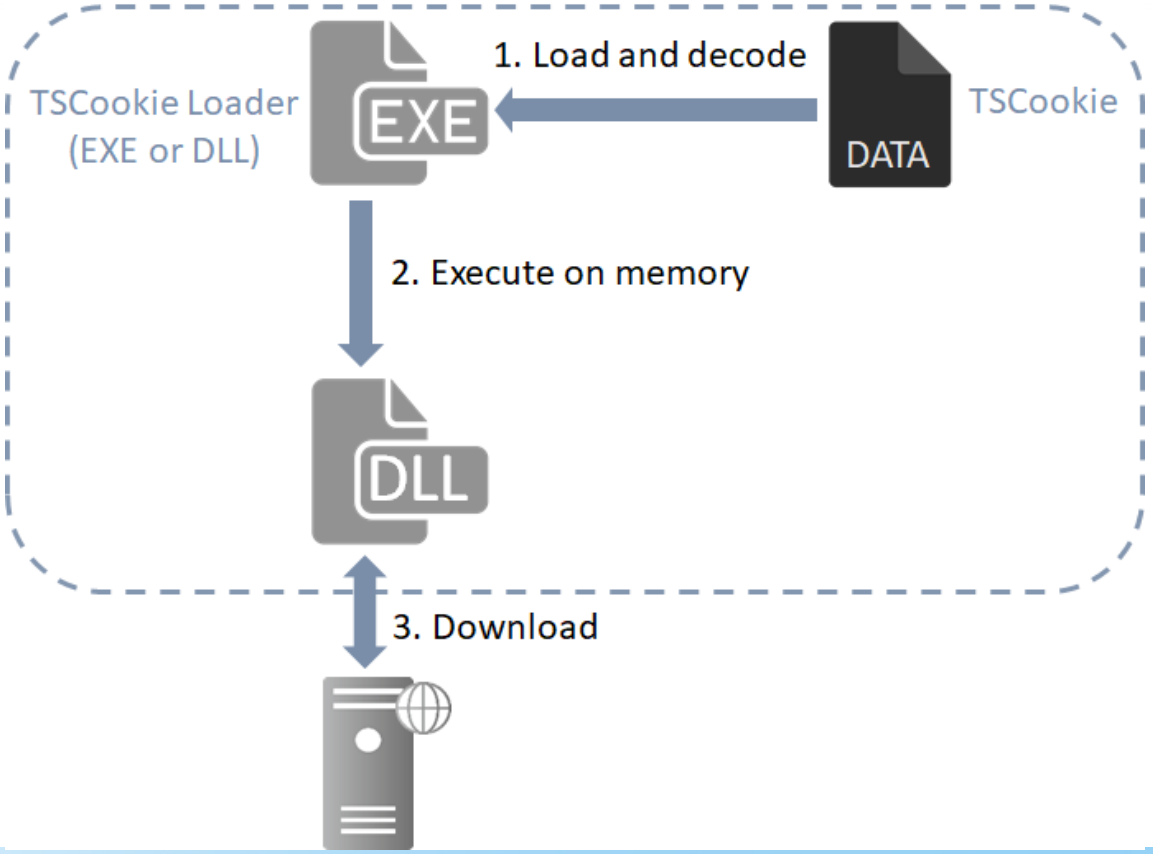
資産管理ソフトウエアの脆弱性を悪用しようとするスキャン観測状況
(TSUBAMEの観測データ: 2017年1月～2019年12月)

マルウエア(NodeRAT)

```
305  case "cmd":
306      ! function({
307          input: e,
308          characterSet: t
309      }) {
310          if (!S) {
311              switch (_) {
312                  case "linux":
313                  case "darwin":
314                      S = p.spawn("bash");
315                      break;
316                  case "win32":
317                      S = p.spawn("cmd")
318              }
319              S.stdout.on("data", e => {
320                  g.notify("connector.userHandler.message", {
321                      type: "cmd",
322                      output: e
323                  })
324              }), S.stderr.on("data", e => {
325                  g.notify("connector.userHandler.message", {
326                      type: "cmd",
327                      output: e
```

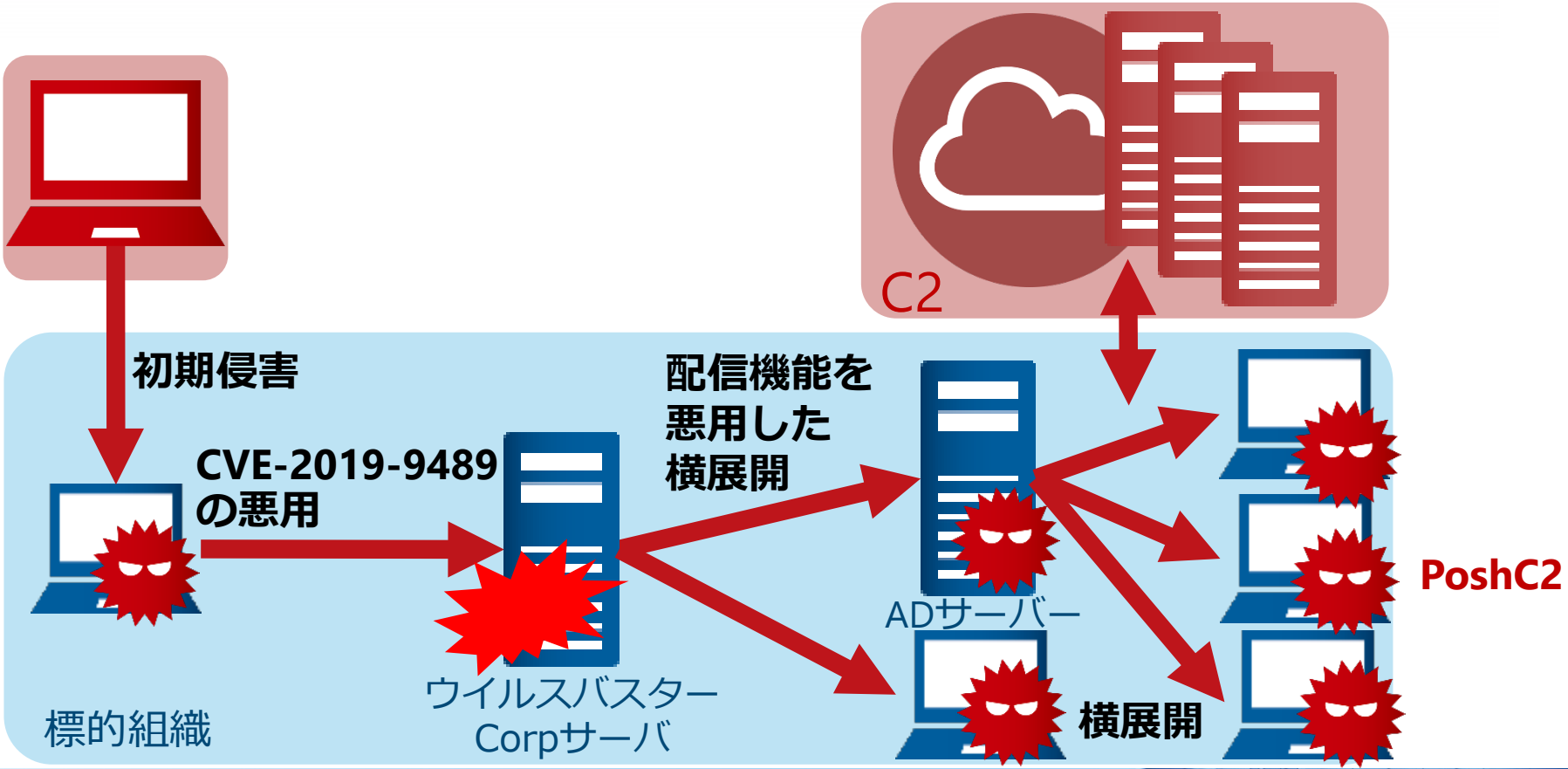
BlackTech

TSCookie Loader & TSCookie



特定製品の脆弱性 (CVE-2019-9489) を悪用する攻撃

攻撃概要



QuasarRAT(APT10)

実行の流れ

設定情報

Config Value	
VERSION	STARTUPKEY
HOSTS	HIDEFILE
RECONNECTDELY	ENABLELOGGER
KEY	ENCRYPTIONKEY
AUTHKEY	TAG
DIRECTORY	LOGDIRECTORY
SUBDIRECTORY	HIDELOGDIRECTORY
INSTALLNAME	HIDELOGSUBDIRECTORY
INSTALL	**DOWNLOAD_URL** NEW
SETUP	**PROXY** NEW
MUTEX	

機能

```
public static Type[] commands()
{
    return new Type[]
    {
        typeof(GetAuthentication),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(GetDesktop),
        typeof(GetProcesses),
        typeof(DoProcessKill),
        typeof(DoProcessStart),
        typeof(GetDrives),
        typeof(GetDirectory),
        typeof(DoDownloadFile),
        typeof(DoMouseEvent),
        typeof(DoKeyboardEvent),
        typeof(GetSystemInfo),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(GetMonitors),
        typeof(object),
        typeof(object),
        typeof(DoShellExecute),
        typeof(DoPathRename),
        typeof(DoPathDelete),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(DoDownloadFileCancel),
        typeof(object),
        typeof(DoUploadFile),
        typeof(object),
        typeof(DoLoadRegistryKey),
        typeof(DoCreateRegistryKey),
        typeof(DoDeleteRegistryKey),
        typeof(DoRenameRegistryKey),
        typeof(DoCreateRegistryValue),
        typeof(DoDeleteRegistryValue),
        typeof(DoRenameRegistryValue),
        typeof(DoChangeRegistryValue),
        typeof(SetAuthenticationSuccess),
        typeof(GetConnections),
        typeof(DoCloseConnection),
        typeof(GetAuthenticationResponse),
        typeof(SetStatus),
        typeof(SetStatusFileManager),
        typeof(object),
        typeof(GetDesktopResponse),
        typeof(GetProcessesResponse),
        typeof(GetDrivesResponse),
        typeof(GetDirectoryResponse),
        typeof(DoDownloadFileResponse),
        typeof(GetSystemInfoResponse),
        typeof(GetMonitorsResponse),
        typeof(object),
        typeof(object),
        typeof(DoShellExecuteResponse),
        typeof(object),
        typeof(object),
        typeof(object),
        typeof(GetRegistryKeysResponse),
        typeof(GetCreateRegistryKeyResponse),
        typeof(GetDeleteRegistryKeyResponse),
        typeof(GetRenameRegistryKeyResponse),
        typeof(GetCreateRegistryValueResponse),
        typeof(GetDeleteRegistryValueResponse),
        typeof(GetRenameRegistryValueResponse),
        typeof(GetChangeRegistryValueResponse),
        typeof(ReverseProxyConnect),
        typeof(ReverseProxyConnectResponse),
        typeof(ReverseProxyData),
        typeof(ReverseProxyDisconnect),

        typeof(DoPluginResponse),
        typeof(DoPlugin)
    };
}
```

ばらまき系攻撃

SSL VPN 機器の
脆弱性を悪用した攻撃

Alert & Advisory

複数の SSL VPN 製品の脆弱性に関する注意喚起

最終更新: 2019-09-06

ツイート　メール

JPCERT-AT-2019-0033
JPCERT/CC
2019-09-02(新規)
2019-09-06(更新)

I. 概要

JPCERT/CC では、複数の SSL VPN 製品の脆弱性について、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。

- Palo Alto Networks (CVE-2019-1579)
- Fortinet (CVE-2018-13379)
- Pulse Secure (CVE-2019-11510)

これらの脆弱性を悪用された場合に、攻撃者がリモートから任意のコードを実行できる可能性 (CVE-2019-1579) や、任意のファイルを読み取り、認証情報などの機微な情報を取得する可能性 (CVE-2018-13379, CVE-2019-11510) があります。なお、脆弱性の報告者からは、それぞれの製品について、上記以外の脆弱性情報も公開されています。実証コードなどの詳細情報が公開されていることからも、脆弱性を悪用される可能性が考えられるため、対象となるシステムを使用している場合、早急に対策を実施することを推奨します。

公開日：2019/10/17　最終更新日：2019/10/17

JVNVU#93621261
Pulse Secure VPN における複数の脆弱性

概要
Pulse Secure SSL VPN には複数の脆弱性が存在します。
遠隔の第三者によって、VPN サーバやそこに接続してくる VPN クライアントが攻撃される可能性があります。

影響を受けるシステム

- Pulse Secure SSL VPN

詳細情報
Pulse Secure SSL VPN には、次の複数の脆弱性が存在します。

CVE-2019-11510
HTTPS 経由で送信された、細工された URI を処理することにより、任意のファイルが読み出される可能性があります。

CVE-2019-11509
管理用ウェブインターフェースにログインしたユーザによって、Pulse Secure アプライアンス上で任意のコードを実行される可能性があります。

CVE-2019-11508
Pulse Connect Secure の Network File Share (NFS) の実装には脆弱性があり、認証されたユーザが悪意あるファイルをアップロードすることによって、ローカルシステム上に任意のファイルが書き込まれる可能性があります。

CVE-2019-11507
Pulse Secure Application Launcher ページにはクロスサイトスクリプティングの脆弱性が存在します。
対象となる製品は Pulse Connect Secure (PCS) の、8.3R7.1 より前の 8.3.x 系 および 9.0R3 より前の 9.0.x 系です。

CVE-2019-11543
管理用ウェブインターフェースにはクロスサイトスクリプティングの脆弱性が存在します。
対象となる製品は Pulse Secure Pulse Connect Secure (PCS) の、9.0R3.4 より前の 9.0RX 系、8.3R7.1 より前の 8.3RX 系、8.1R15.1 より前の 8.1RX 系、および Pulse Policy Secure 9.0R3.2 より前の 9.0RX 系、5.4R7.1 より前の 5.4RX 系、5.2R12.1 より前の 5.2RX 系です。

CVE-2019-11542
管理用ウェブインターフェースにログインしたユーザから受け取った、細工されたメッセージを処理することによって、スタックバッファオーバーフローが発生する可能性があります。

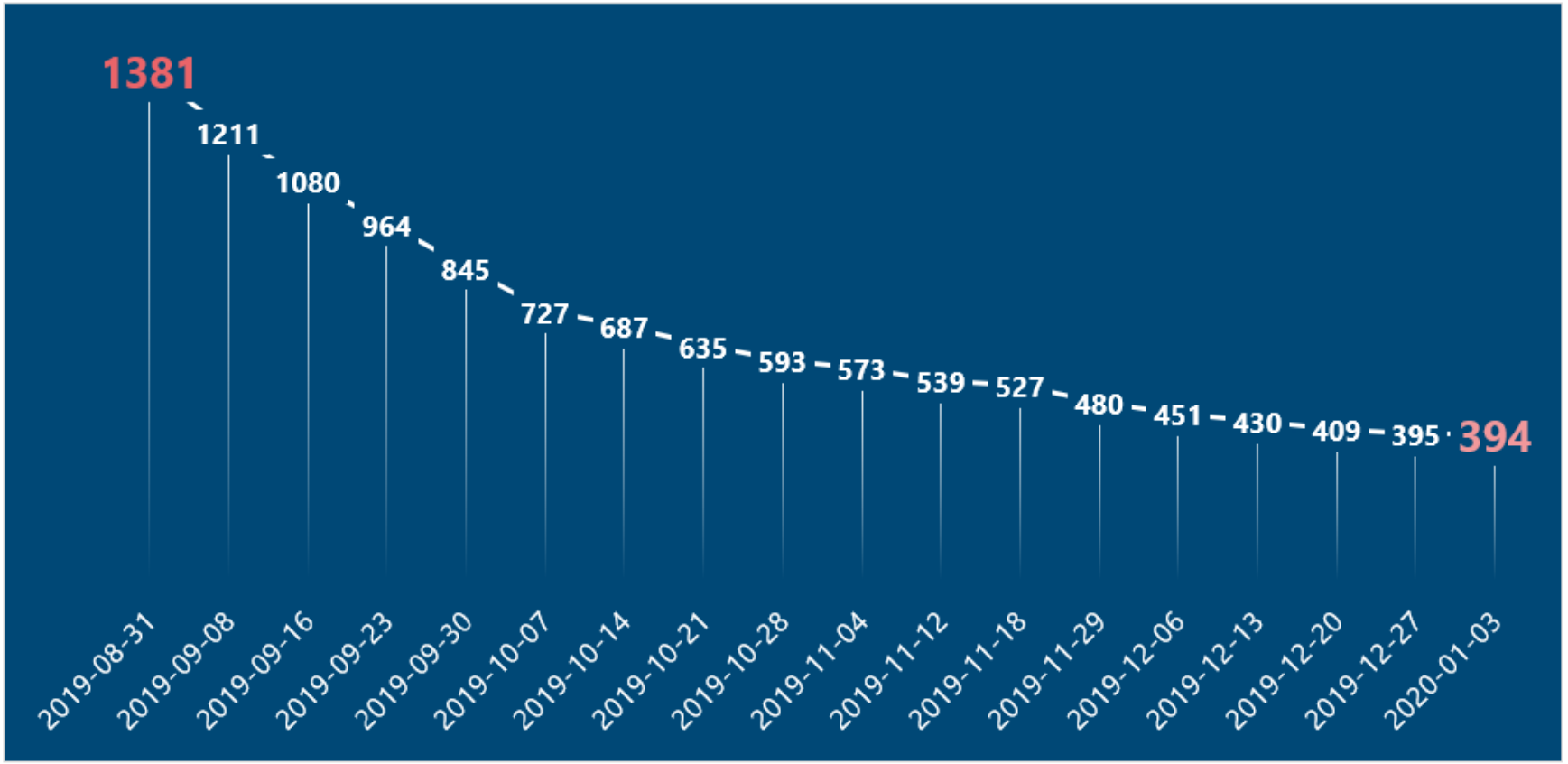
CVE-2019-11541
Reuse Existing NC (Pulse) Session オプションで SAML 認証を使用しているユーザの認証情報が漏えいする可能性があります。

CVE-2019-11540
Pulse Secure には脆弱性があり、遠隔の攻撃者によって VPN サーバに接続するエンドユーザを対象としたセッションハイジャック攻撃が行われる可能性があります。

CVE-2019-11539
管理用ウェブインターフェースにログインしたユーザによって、任意のコマンドが実行される可能性があります。

CVE-2019-11538
Pulse Connect Secure の Network File Share (NFS) の実装には脆弱性があり、認証されたユーザによってローカルファイルシステム上の任意のファイルにアクセスされる可能性があります。

日本における CVE-2019-11510 脆弱性のある Pulse Secure VPN ホストの数



Emotet

情報発信

マルウエア Emotet の感染に関する注意喚起

マルウエア Emotet の感染活動について

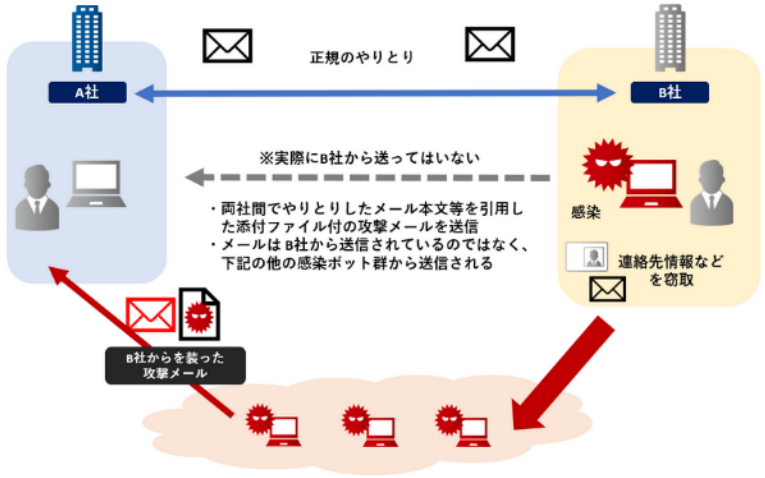
最終更新: 2019-12-02

ツイート　メール

CyberNewsFlash一覧

JPCERT/CC では、2019年10月後半より、マルウエア Emotet の感染に関する相談を多数受けています。
Emotet に感染した端末から情報が窃取され、窃取された情報が悪用されて取引先などに不審メールが送られている状況を確認しています。

【Emotet の感染により発生する被害のイメージ図】



Emotet に感染した端末で構成されるメール送信用のボットネット
感染先から窃取した連絡帳やメール認証情報を使って攻撃メールの配信を行う。

佐條 研(Ken Sajo)　2019/12/02

マルウエアEmotetへの対応FAQ

メール

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

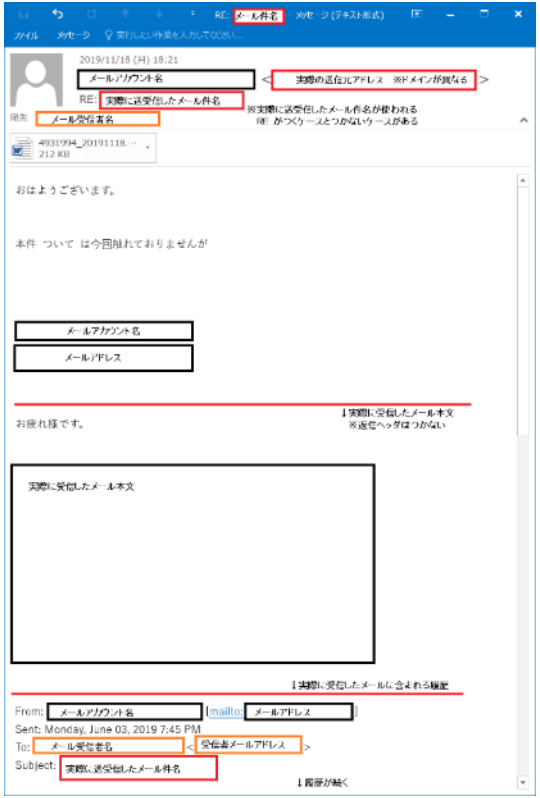
JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html

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。

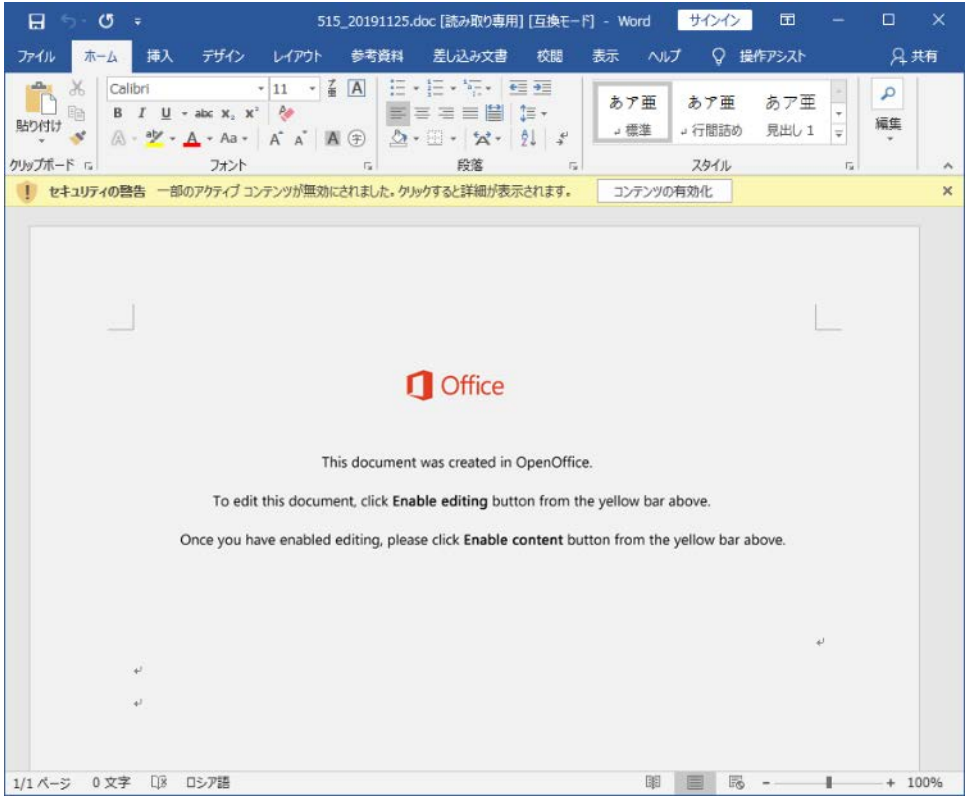
参考：JNSAサイバーインシデント緊急対応企業一覧
https://www.jnsa.org/emergency_response/

攻撃メールの例

メール本文



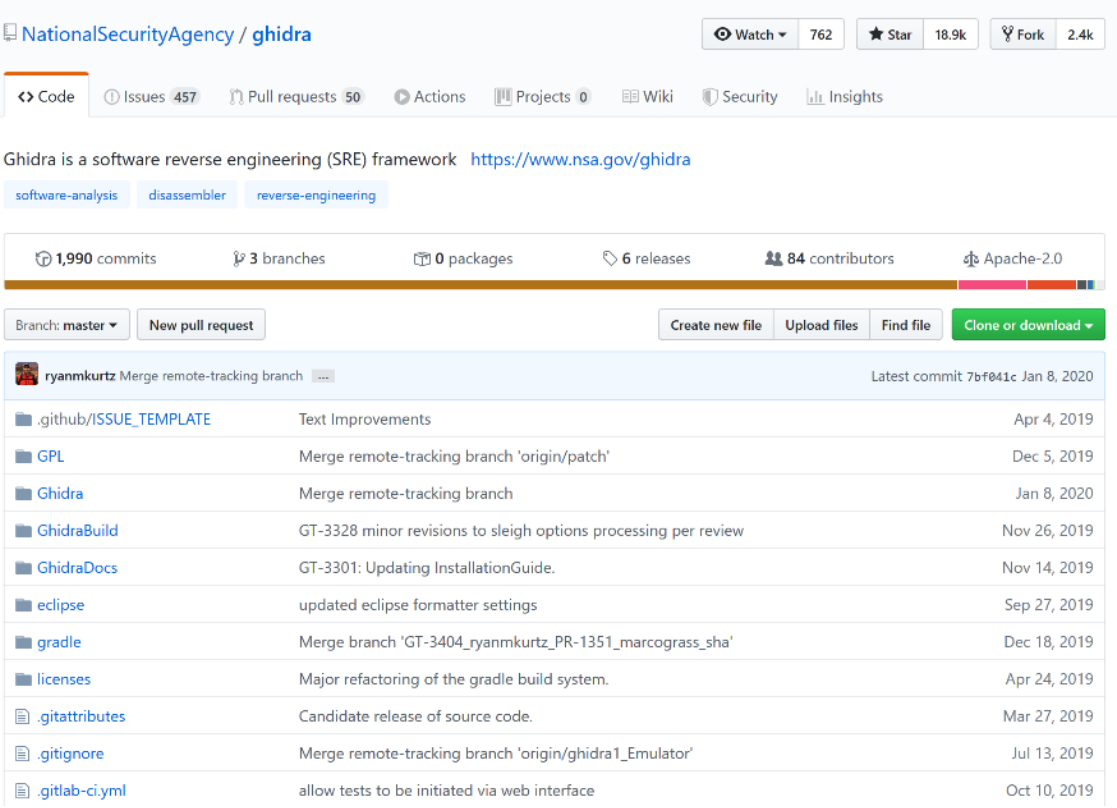
添付ファイル



分析ツール

Ghidra

https://ghidra-sre.org/



https://github.com/NationalSecurityAgency/ghidra

IDA: Undo

MalConfScan

https://github.com/JPCERTCC/MalConfScan

Supported Malware Families		
Ursnif	TSCookie	AZORult
Emotet	TSC_Loader	NanoCore RAT
Smoke Loader	xxmm	AgentTesla
PoisonIvy	Datper	FormBook
CobaltStrike	Ramnit	NodeRAT
NetWire	HawkEye	njRAT
PlugX	Lokibot	TrickBot
RedLeaves	Bebloh	Remcos
QuasarRAT		

JSAC 2020の楽しみ方

インシデントに関する技術共有の場として

分類	タイトル
A	Evil Hidden in Shellcode: The Evolution of Malware DBGPRINT
A/D	攻撃キャンペーン「Operation Bitter Biscuit」を実行した 標的型攻撃グループに関する脅威情報
B/A	macOS用アーティファクト収集ツールと 簡易マルウェア解析サンドボックスの実装と利用方法
B	自作ツールを使用したMac Forensicsの調査効率化
C	ランサムウェアに標的型攻撃手法を求めるのは間違っているだろうか
D	100 more behind cockroaches? or how to hunt IoCs with OSINT
D	日本を狙うばらまきメールキャンペーンの脅威動向分析と対策
D	An Overhead View of the Royal Road

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

交流の場として

15:00 - 15:30 コーヒーブレーク / Coffee break

Thank you!