

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

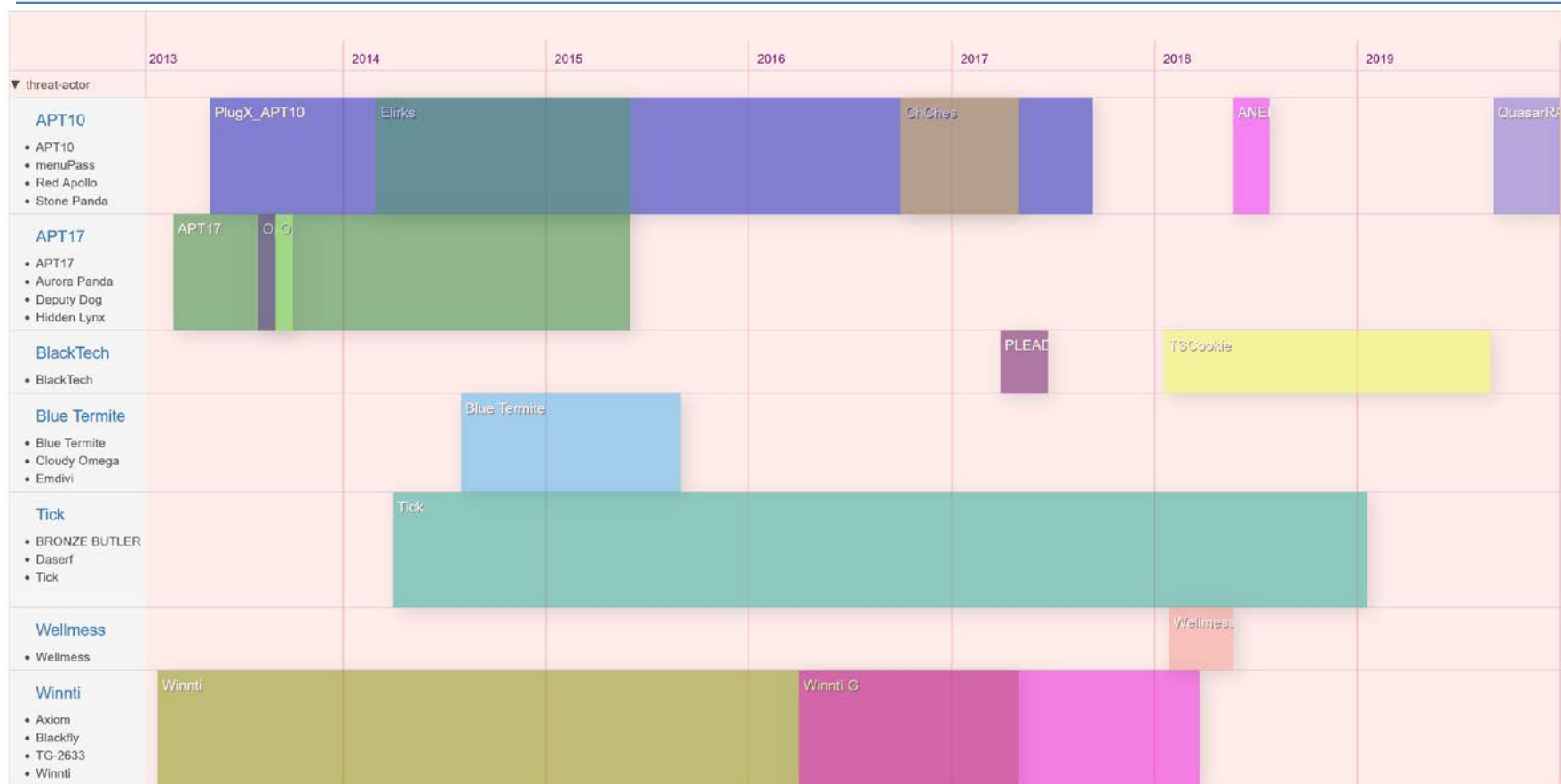
(組織内情報の窃取を
目的とした攻撃)

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

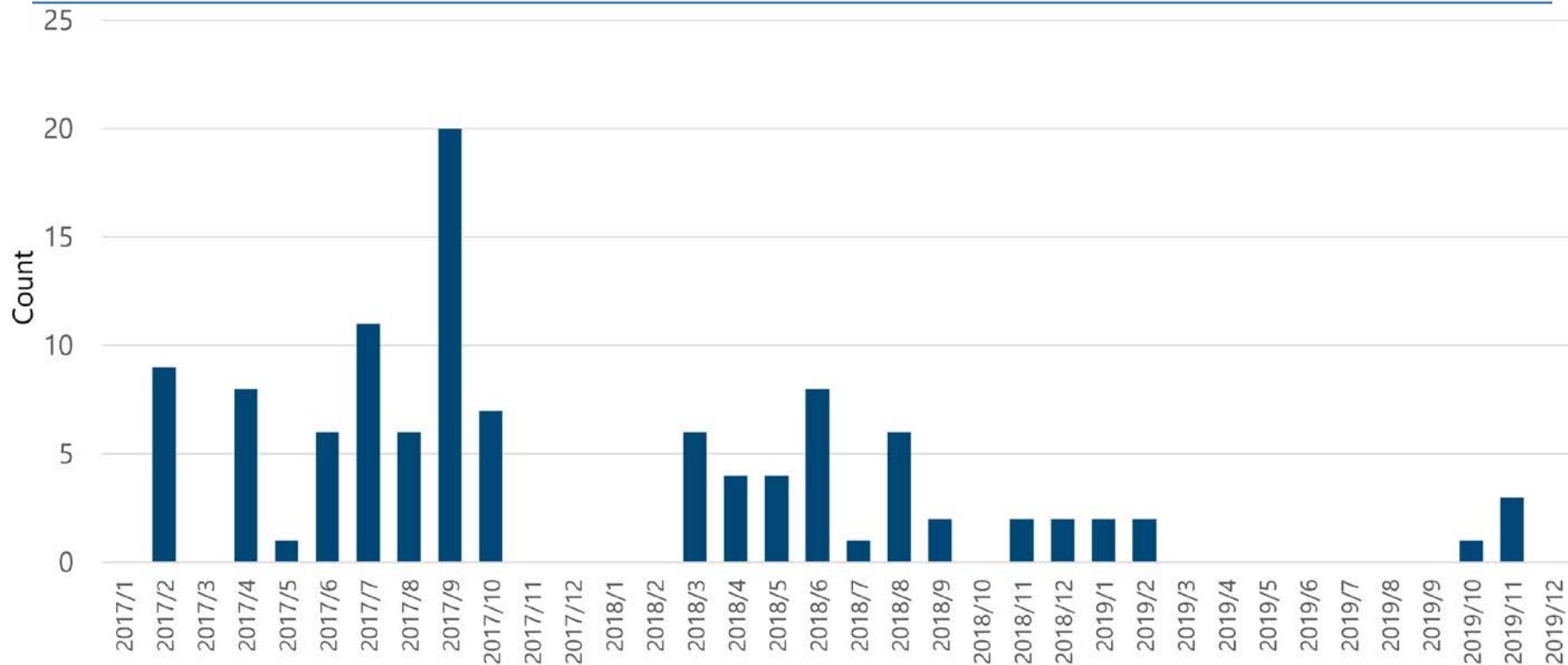
- オープンソースツール
 - PoshC2
 - PowerShell Empire
 - QuasarRAT など
- OSコマンドなど

マルウェアの複雑化

- 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



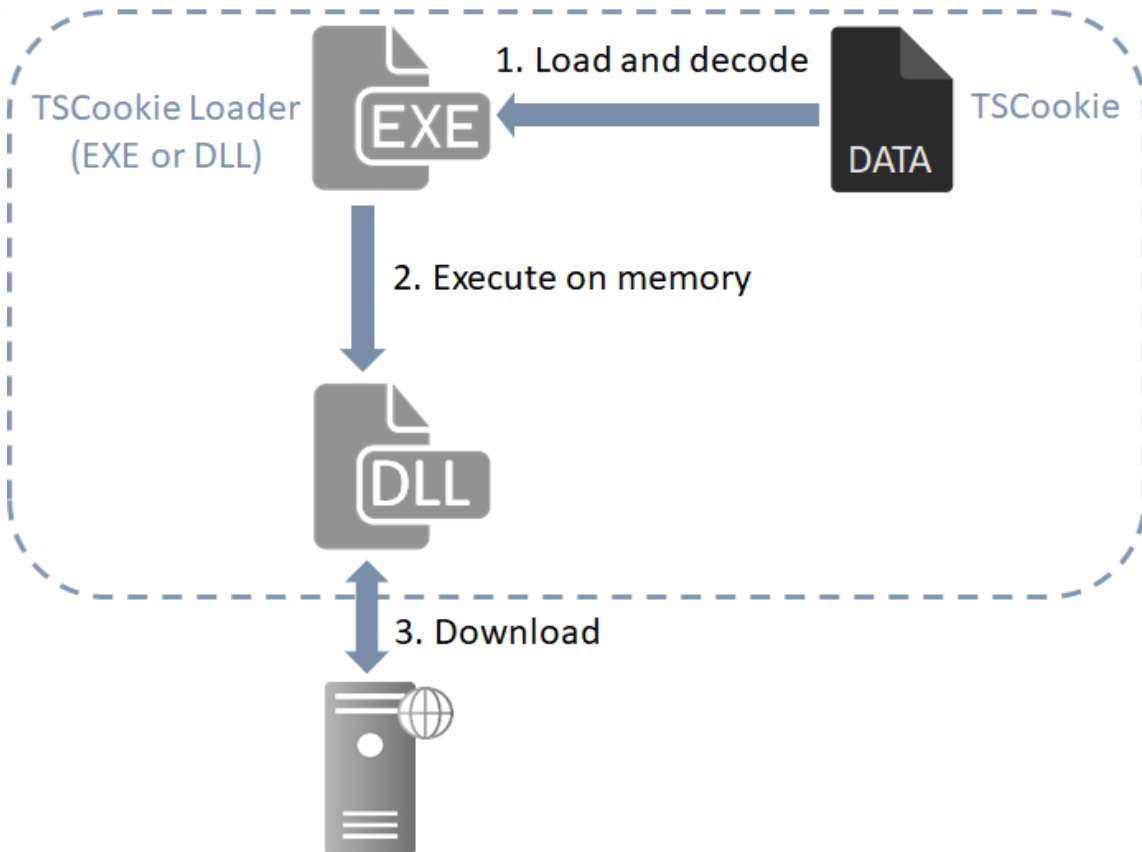
資産管理ソフトウェアの脆弱性を悪用しようとするスキャン観測状況
(TSUBAMEの観測データ: 2017年1月～2019年12月)

マルウェア(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
```

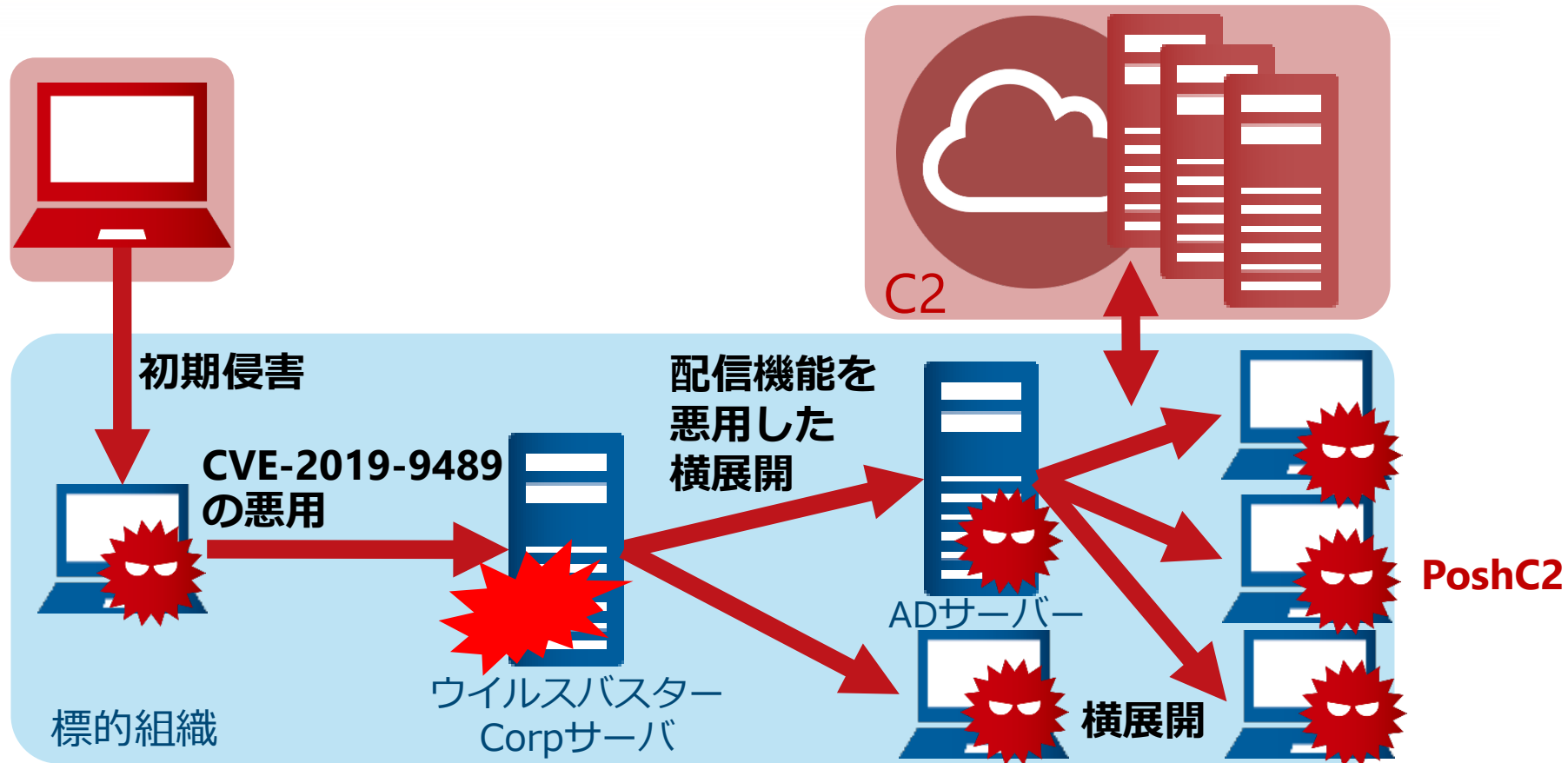
BlackTech

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

Service start



Loader



**エンコードされた
QuasarRAT本体**

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 
SETUP	PROXY 
MUTEX	

```
10 public static Type[] commands()
11 {
12     return new Type[]
13     {
14         typeof(GetAuthentication),
15         typeof(object),
16         typeof(object),
17         typeof(object),
18         typeof(object),
19         typeof(object),
20         typeof(object),
21         typeof(object),
22         typeof(GetDesktop),
23         typeof(GetProcesses),
24         typeof(DoProcessKill),
25         typeof(DoProcessStart),
26         typeof(GetDrives),
27         typeof(GetDirectory),
28         typeof(DoDownloadFile),
29         typeof(DoMouseEvent),
30         typeof(DoKeyboardEvent),
31         typeof(GetSystemInfo),
32         typeof(object),
33         typeof(object),
34         typeof(object),
35         typeof(GetMonitors),
36         typeof(object),
37         typeof(object),
38         typeof(DoShellExecute),
39         typeof(DoPathRename),
40         typeof(DoPathDelete),
41         typeof(object),
42         typeof(object),
43         typeof(object),
44         typeof(object),
45         typeof(DoDownloadFileCancel),
46         typeof(object),
47         typeof(DoUploadFile),
48         typeof(object),
49         typeof(DoLoadRegistryKey),
50         typeof(DoCreateRegistryKey),
51         typeof(DoDeleteRegistryKey),
```

```
52         typeof(DoRenameRegistryKey),
53         typeof(DoCreateRegistryValue),
54         typeof(DoDeleteRegistryValue),
55         typeof(DoRenameRegistryValue),
56         typeof(DoChangeRegistryValue),
57         typeof(SetAuthenticationSuccess),
58         typeof(GetConnections),
59         typeof(DoCloseConnection),
60         typeof(GetAuthenticationResponse),
61         typeof(SetStatus),
62         typeof(SetStatusFileManager),
63         typeof(object),
64         typeof(GetDesktopResponse),
65         typeof(GetProcessesResponse),
66         typeof(GetDrivesResponse),
67         typeof(GetDirectoryResponse),
68         typeof(DoDownloadFileResponse),
69         typeof(GetSystemInfoResponse),
70         typeof(GetMonitorsResponse),
71         typeof(object),
72         typeof(object),
73         typeof(DoShellExecuteResponse),
74         typeof(object),
75         typeof(object),
76         typeof(object),
77         typeof(GetRegistryKeysResponse),
78         typeof(GetCreateRegistryKeyResponse),
79         typeof(GetDeleteRegistryKeyResponse),
80         typeof(GetRenameRegistryKeyResponse),
81         typeof(GetCreateRegistryValueResponse),
82         typeof(GetDeleteRegistryValueResponse),
83         typeof(GetRenameRegistryValueResponse),
84         typeof(GetChangeRegistryValueResponse),
85         typeof(ReverseProxyConnect),
86         typeof(ReverseProxyConnectResponse),
87         typeof(ReverseProxyData),
88         typeof(ReverseProxyDisconnect),
89         typeof(object),
90         typeof(DoPluginResponse),
91         typeof(DoPlugin)
92     };
93 }
```

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、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、加工された 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、加工されたメッセージを処理することによって、スタックバンプ/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。

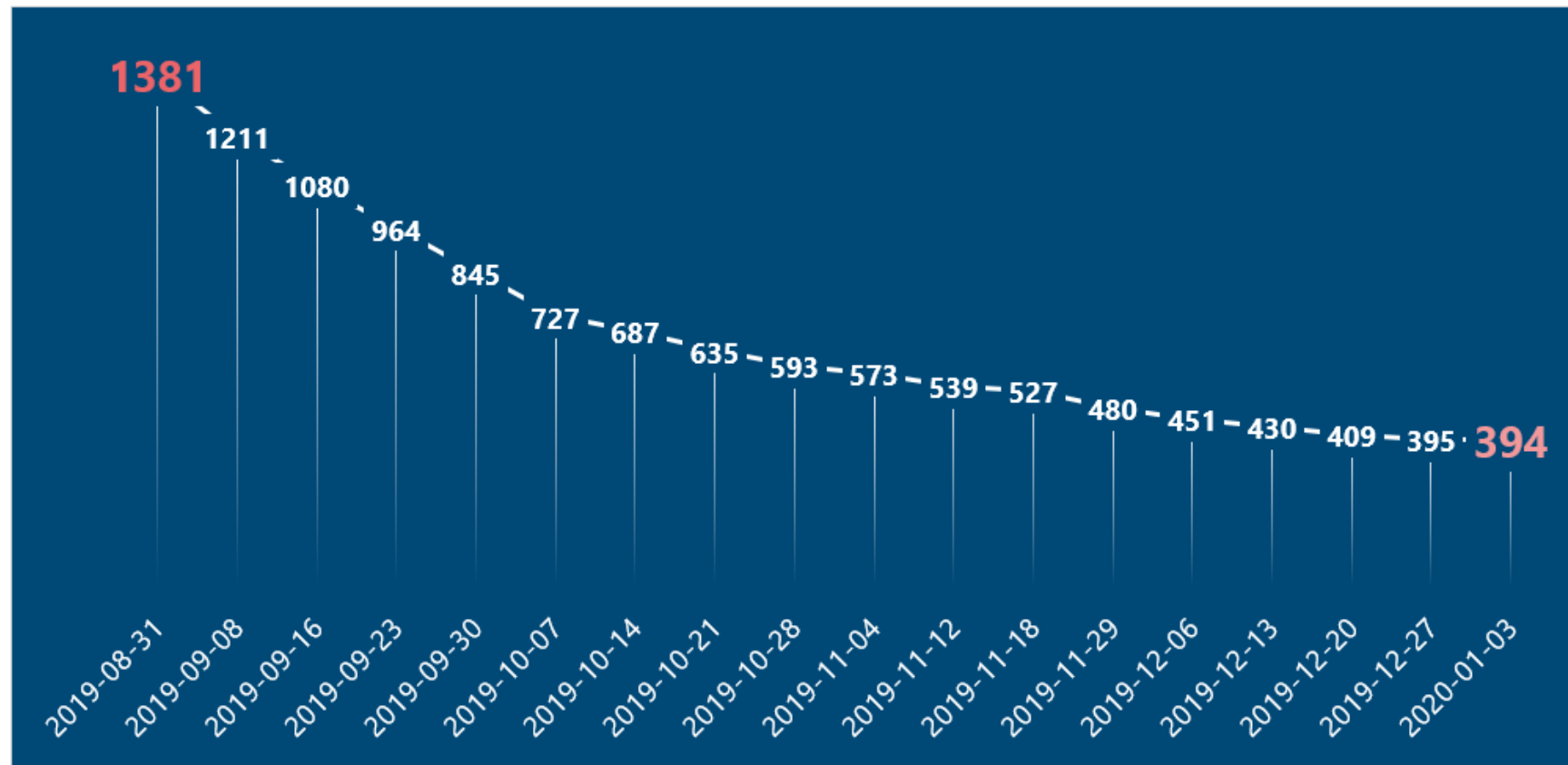
CVE-2019-11539

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

マルウェア Emotet の感染に関する注意喚起

マルウェア Emotet の感染活動について

最終更新: 2019-12-02

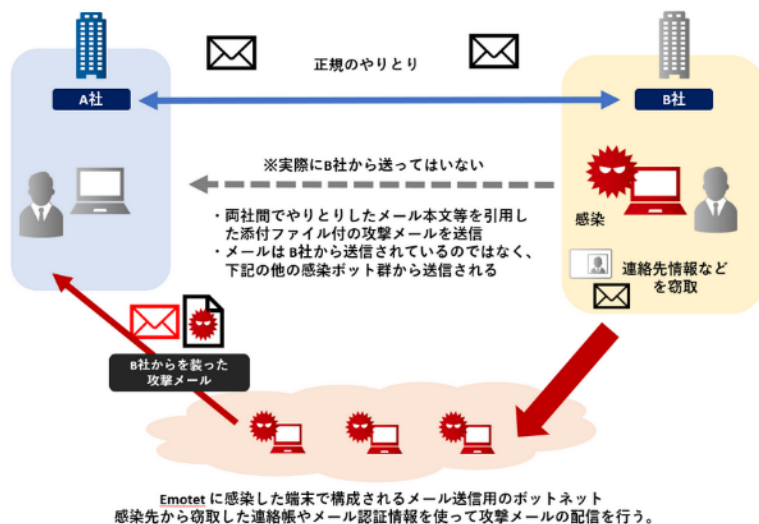
ツイート メール

CyberNewsFlash一覧

JPCERT/CC では、2019年10月後半より、マルウェア 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】



佐藤 研(Ken Sajo)

2019/12/02

マルウェア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>

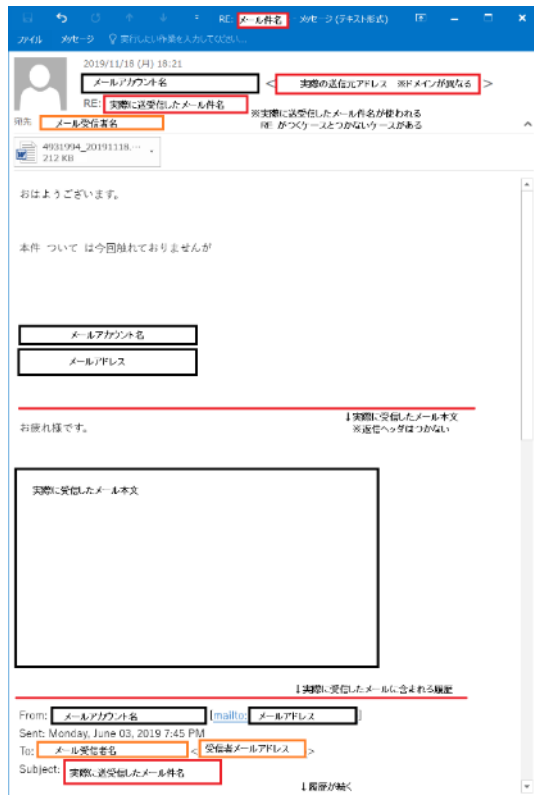
本ブログでは、2019年12月時点のEmotetに感染した疑いがある場合の確認方法や、感染が確認された場合の対処方法など、Emotetに関するFAQを掲載しています。なお、ここに記載されている調査方法がわからない場合は、専門のセキュリティベンダーへの相談を検討してください。

参考: JNSAサイバーインシデント緊急対応企業一覧

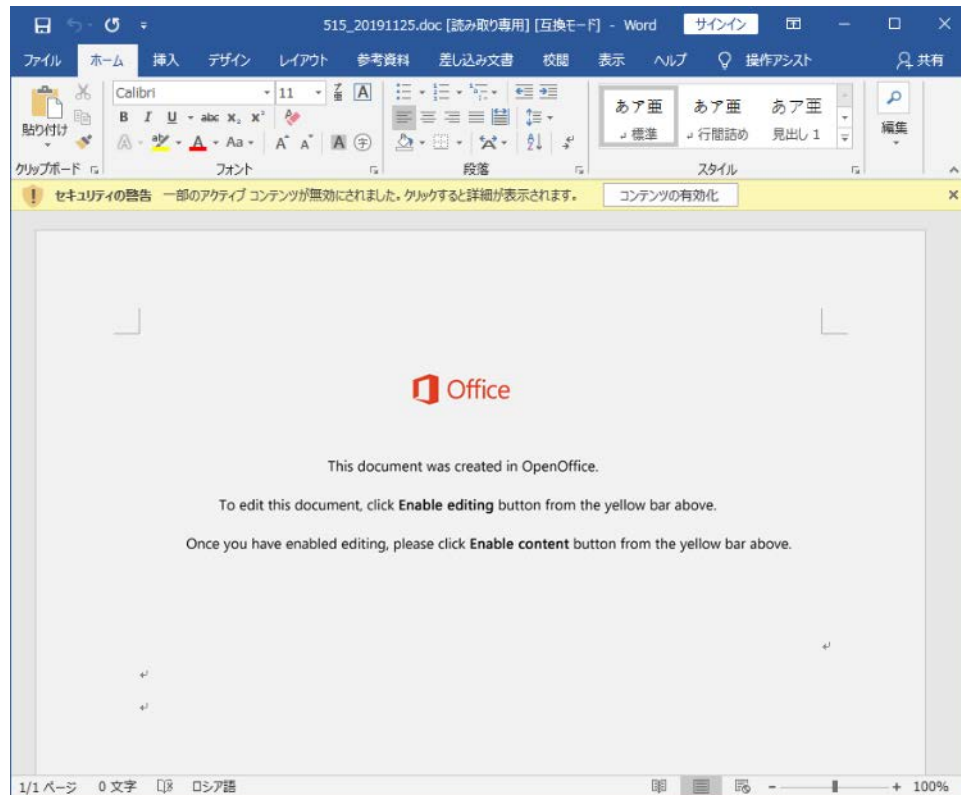
https://www.jnsa.org/emergency_response/

攻撃メールの例

メール本文

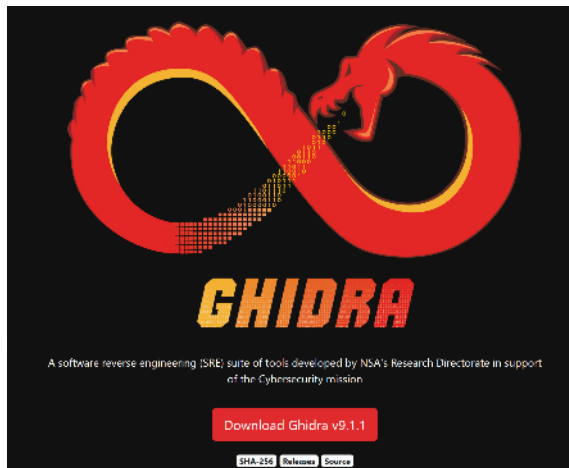


添付ファイル



分析ツール

Ghidra



<https://ghidra-sre.org/>

NationalSecurityAgency / ghidra

Watch 762 Star 18.9k Fork 2.4k

Code Issues 457 Pull requests 50 Actions Projects 0 Wiki Security Insights

Ghidra is a software reverse engineering (SRE) framework <https://www.nsa.gov/ghidra>

software-analysis disassembler reverse-engineering

1,990 commits 3 branches 0 packages 6 releases 84 contributors Apache-2.0

Branch: master New pull request

Create new file Upload files Find file Clone or download

ryanmkurtz Merge remote-tracking branch		Latest commit 7bf041c Jan 8, 2020
.github/ISSUE_TEMPLATE	Text Improvements	Apr 4, 2019
GPL	Merge remote-tracking branch 'origin/patch'	Dec 5, 2019
Ghidra	Merge remote-tracking branch	Jan 8, 2020
GhidraBuild	GT-3328 minor revisions to sleigh options processing per review	Nov 26, 2019
GhidraDocs	GT-3301: Updating InstallationGuide.	Nov 14, 2019
eclipse	updated eclipse formatter settings	Sep 27, 2019
gradle	Merge branch 'GT-3404_ryanmkurtz_PR-1351_marcogross_sha'	Dec 18, 2019
licenses	Major refactoring of the gradle build system.	Apr 24, 2019
.gitattributes	Candidate release of source code.	Mar 27, 2019
.gitignore	Merge remote-tracking branch 'origin/ghidra1_Emulator'	Jul 13, 2019
.gitlab-ci.yml	allow tests to be initiated via web interface	Oct 10, 2019

<https://github.com/NationalSecurityAgency/ghidra>

IDA: Undo

```
sub_429105 proc near ; CODE XREF: WinMain(x,x,x,x)+10:r
arg_0      = dword ptr 4
arg_4      = dword ptr 8
arg_8      = dword ptr 0Ch
arg_C      = dword ptr 10h

push ebx
push esi
push edi
or ebx, 0FFFFFFFh
call 7AfxGetThread@YGPAVCWinThread@@XZ ; AfxGetThread(void)
mov esi, eax
call 7AfxGetModuleState@YGPAVAFX_MODULE_STATE@@XZ ; AfxGetModuleState(
push [esp+0Ch+arg_C]
mov edi, [eax+4]
push [esp+10h+arg_8]
push [esp+14h+arg_4]
push [esp+18h+arg_0]
call sub_439E1C ; 7AfxWinInit@YGHPAUIINSTANCE__@@@XZ ; AfxWinInit(
; doubtful name

test eax, eax
jz short loc_42916E
test edi, edi
jz short loc_429145
mov eax, [edi]
mov ecx, edi
call dword ptr [eax+84h]
test eax, eax
jz short loc_42916E

loc_429145: ; CODE XREF: sub_429105+30:r
mov ecx, [esi]
mov ecx, esi
call dword ptr [eax+50h]
test eax, eax
jnz short loc_429165
mov ecx, [esi+1Ch]
test ecx, ecx
jz short loc_42915C
mov eax, [ecx]
call dword ptr [eax+58h]

loc_42915C: ; CODE XREF: sub_429105+50:r
mov eax, [esi]
mov ecx, esi
call dword ptr [eax+68h]
jmp short loc_42916C

loc_429165: ; CODE XREF: sub_429105+49:r
mov eax, [esi]
mov ecx, esi
call dword ptr [eax+54h]

loc_42916C: ; CODE XREF: sub_429105+5E:r
mov ebx, eax

loc_42916E: ; CODE XREF: sub_429105+2C:r
; sub_429105+3E:r
call 7AfxWinTerm@YGXXZ ; AfxWinTerm(void)
pop edi
mov eax, ebx
pop esi
pop ebx
ret 10h
sub_429105 endp
```



```
unk_429105 db 53h ; S ; CODE XREF: WinMain(x,x,x,x)+10:r
db 56h ; V
db 57h ; W
db 63h ; J
db 0CBh ; E
db 0FFh ; Y
db 0E8h ; e
db 17h ;
db 007h ; e
db 0FFh ; Y
db 0FFh ; Y
db 0FFh ; Y
db 88h ; i
db 0F0h ; o
db 0E8h ; e
db 82h ; i
db 0E5h ; A
db 0 ;
db 0 ;
db 0FFh ; Y
db 74h ; t
db 24h ; S
db 1Ch ;
db 88h ; i
db 74h ; t
db 4 ;
db 0FFh ; Y
db 74h ; t
db 24h ; S
db 1Ch ;
db 0FFh ; Y
db 74h ; t
db 24h ; S
db 1Ch ;
db 0E8h ; e
db 0E0h ; i
db 0Ch ;
db 1 ;
db 0 ;
db 85h ; ...
db 0C0h ; A
db 74h ; t
db 38h ; i
db 85h ; ...
db 0FFh ; Y
db 74h ; t
db 0Eh ;
db 88h ; i
db 7 ;
db 88h ; i
db 0CFh ; i
db 0FFh ; Y
db 90h ;
db 84h ; ..
db 0 ;
db 0 ;
db 0 ;
db 85h ; ...
db 0C0h ; A
db 74h ; t
db 29h ; j
db 88h ; i
db 6 ;
db 88h ; i
```



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] マルウェア関連 [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 コーヒーブレイク / Coffee break



Thank you!

