

Japan Security Analyst Conference 2020
(Opening Talk)

Looking back on the incidents in 2019

JPCERT Coordination Center
Incident Response Group

Takayoshi SHIIGI

January 17th, 2020

**Hello
I am ...**

**Malware
Analyst**

JPCERT **CC**[®]

Japan Security Analyst Conference

Two Major Attack Types

Targeted

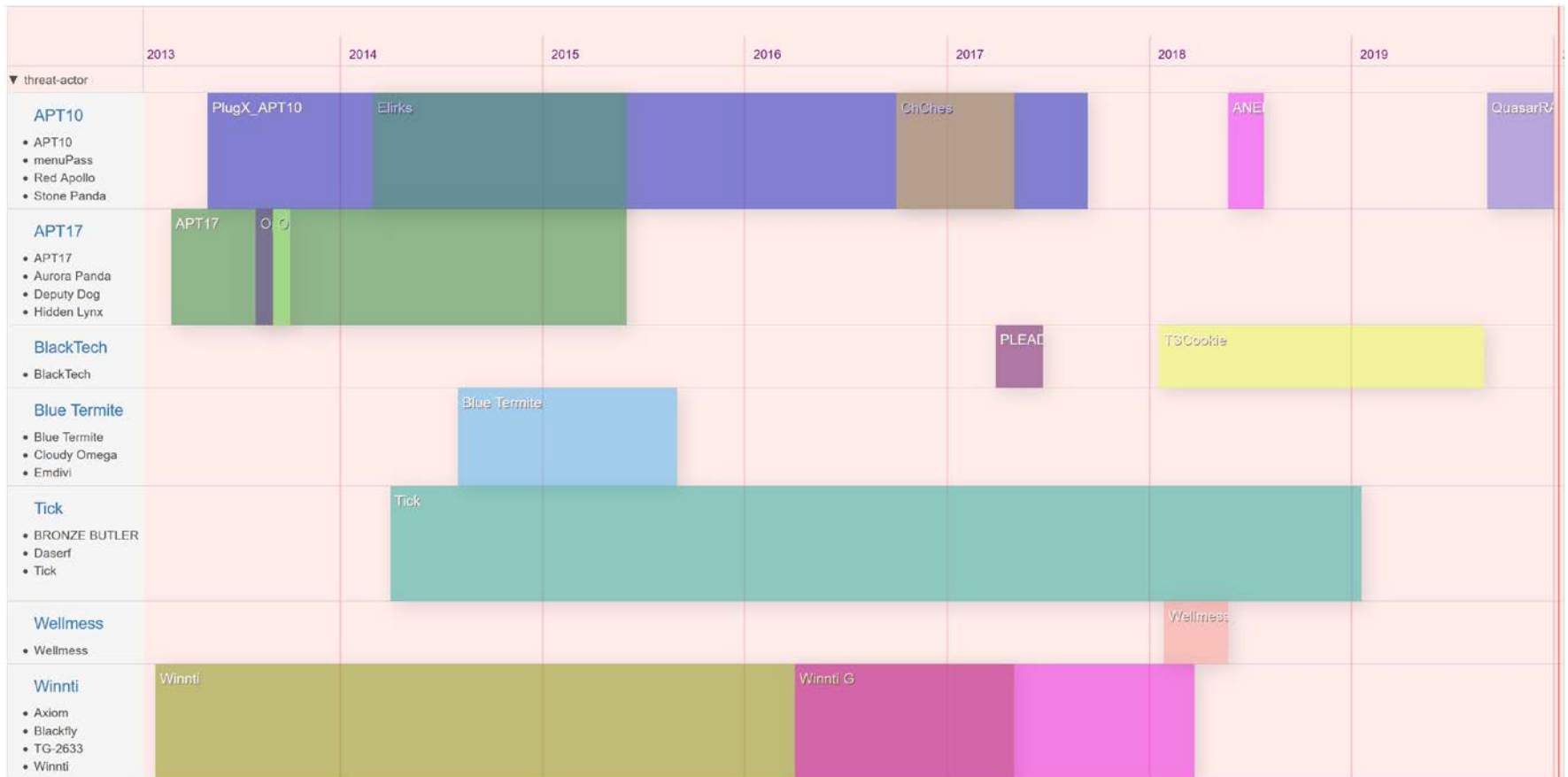
(Attack aimed to steal confidential information)

Widespread

(Attack aimed to steal money)

Targeted Attack

Targeted Attack Campaigns (confirmed by JPCERT/CC)



Trends in Recent Targeted Attack

Leverage Cloud services

- Microsoft Azure
- Google Cloud etc.

Leverage Generic tools

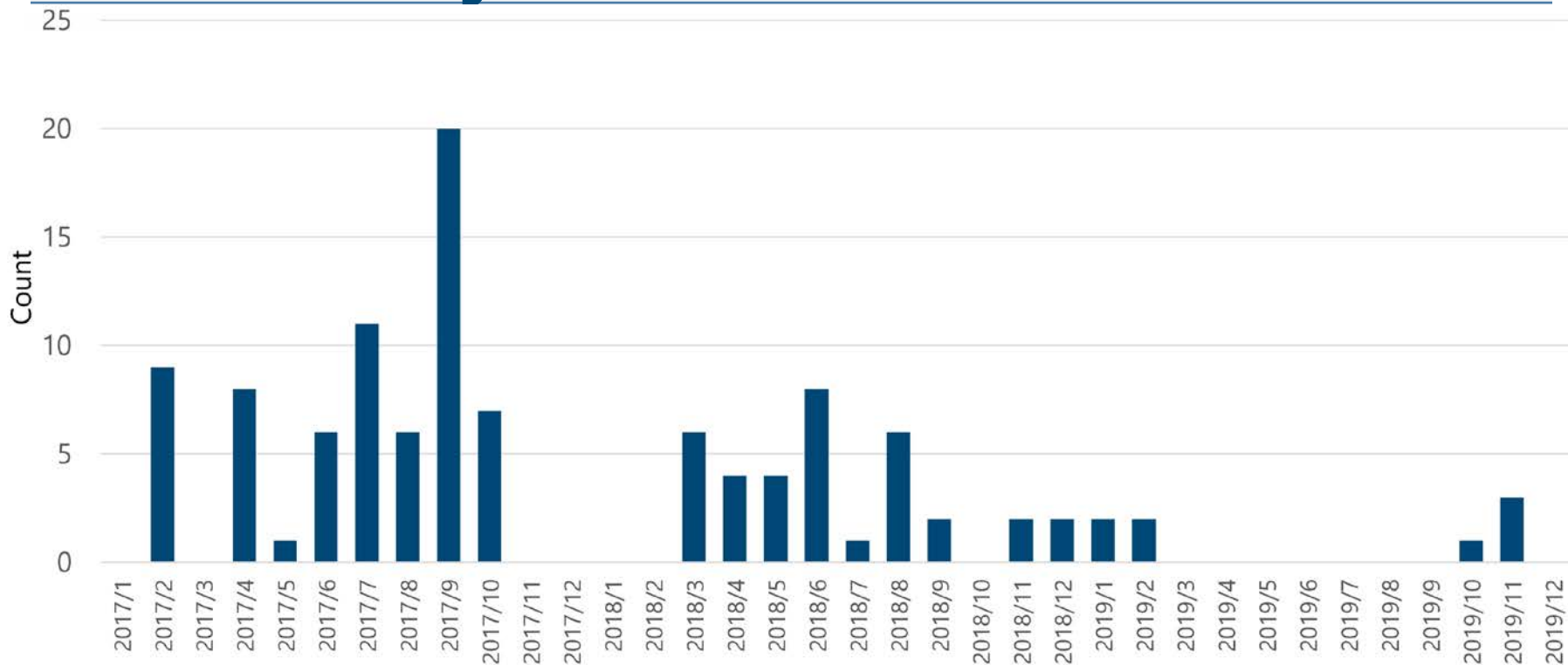
- Open source tools
 - PoshC2
 - PowerShell Empire
 - QuasarRAT etc.
- OS commands

Complex Malware

- File less
- Modular architecture
- Multiple stages

Tick

Scan Activity



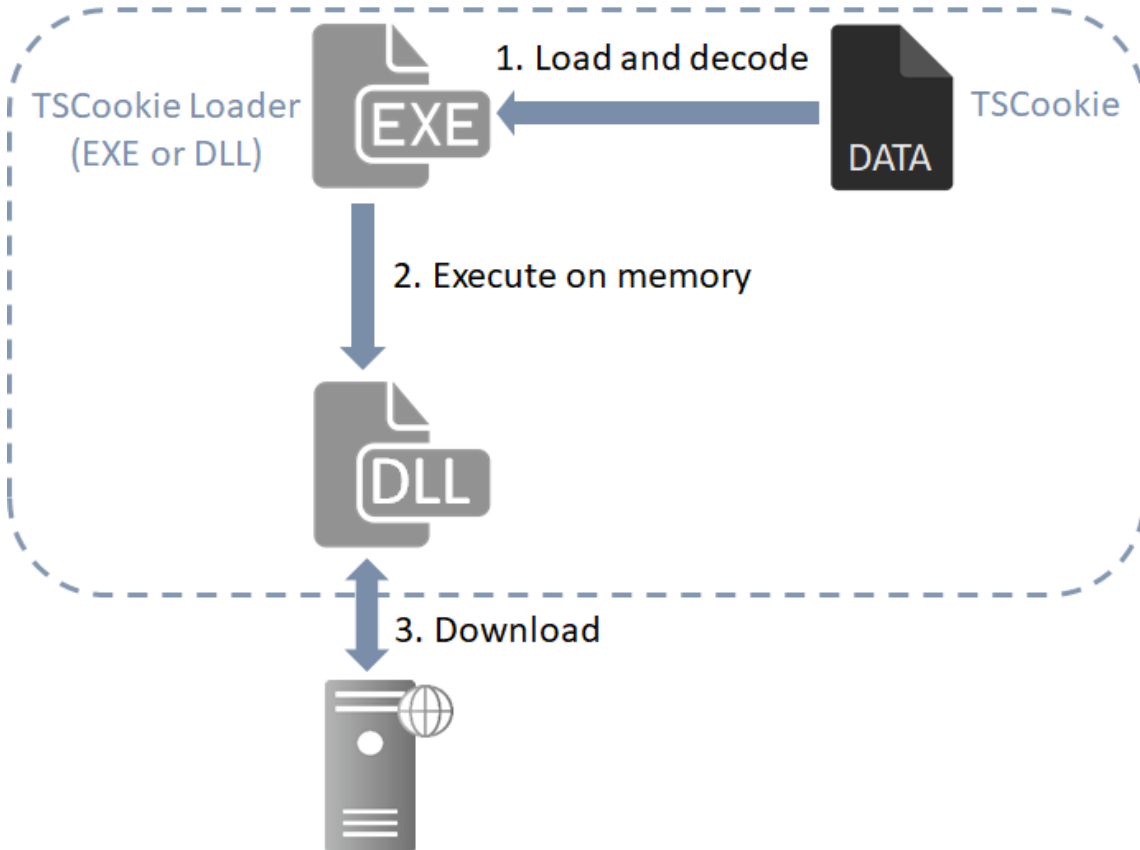
Observation of scan activities for exploiting the asset management software
(Source: TSUBAME(Internet monitoring system): Jan, 2017~Dec, 2019)

Malware(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
```

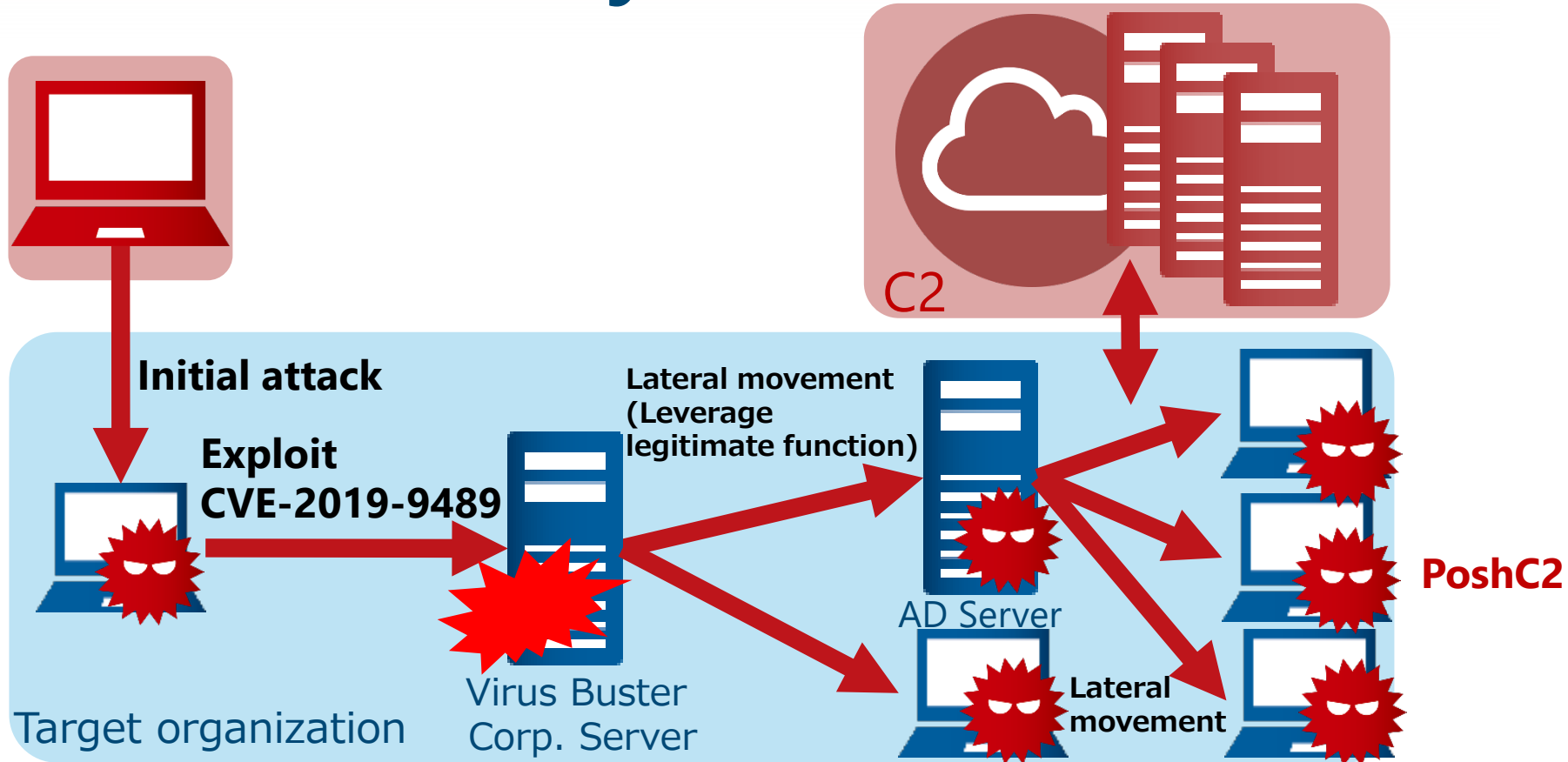
BlackTech

TSCookie Loader & TSCookie



Attack Exploiting Specific Product (CVE-2019-9489)

Attack Summary



QuasarRAT (APT10)

Execution Flow

Service start





Loader



Encoded QuasarRAT

Config Value

Config Value

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

Function

```
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 }
```

Widespread Attack

Attack Exploiting Vulnerabilities in SSL VPN Products

Alert & Advisory

[Updated] Alert Regarding Vulnerabilities in Multiple SSL VPN Products

last update: 2019-09-06



JPCERT-AT-2019-0033

JPCERT/CC

2019-09-02(Initial)

2019-09-06(Update)

I. Overview

JPCERT/CC confirmed details of vulnerabilities in multiple SSL VPN products including Proof-of-Concept code have been made public.

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



公開日: 2019/10/17 最終更新日: 2019/10/17

JVNNU#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、修正された 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 アプリケーション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、修正されたメッセージを処理することによって、スタッフバフアオーバーフローが発生する可能性があります。

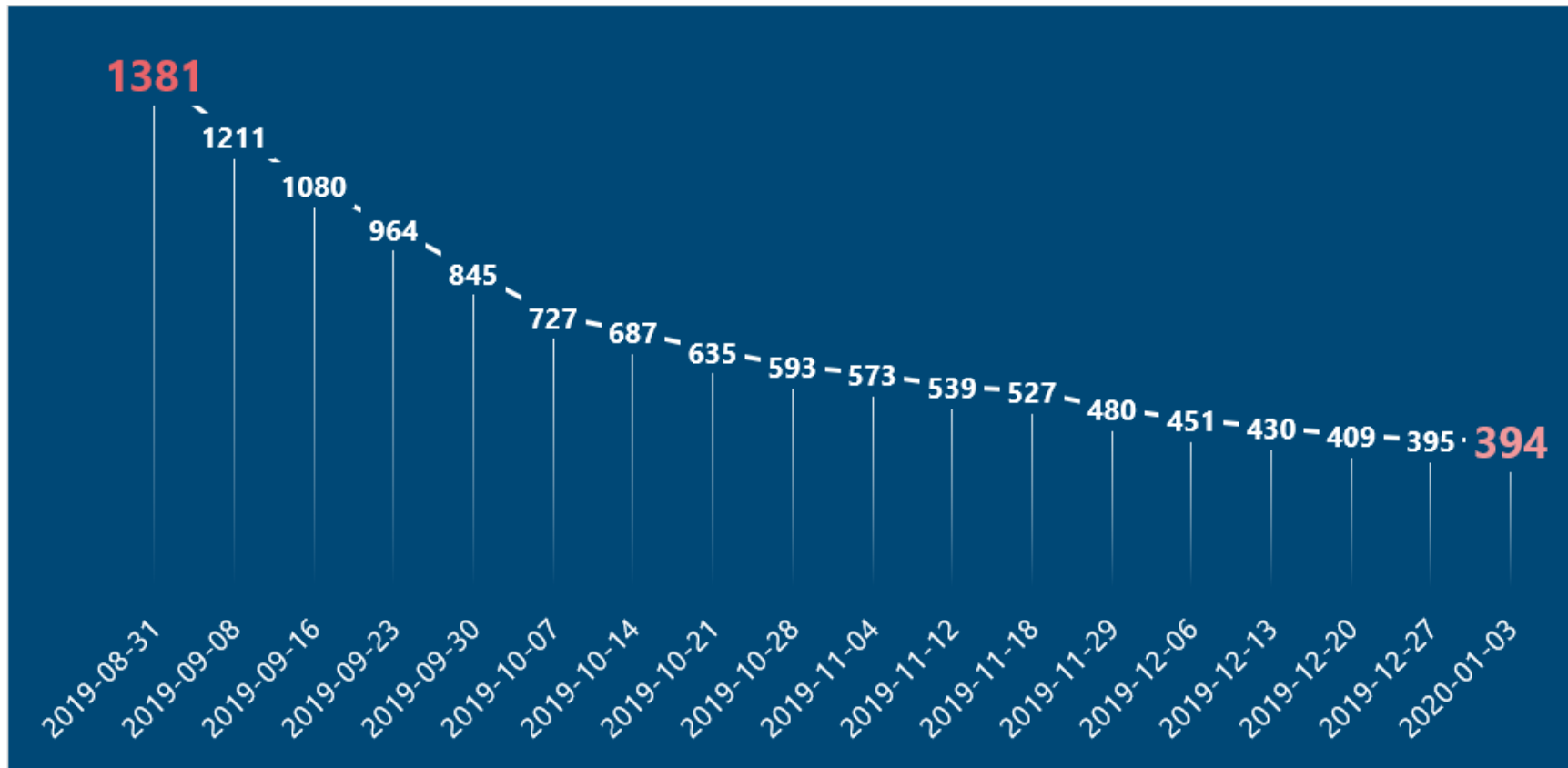
CVE-2019-11541
Reuse Existing NC (Pulse) Session オプションで SAML 認証を使用しているユーザの認証情報が漏えいする可能性があります。

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。

Vulnerable Pulse Secure VPN hosts in Japan (CVE-2019-11510)



Emotet

Publication

[Updated] Alert Regarding Emotet Malware Infection

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】

- ・両社間でやりとりしたメール本文等を引用した添付ファイル付の攻撃メールを送信
- ・メールはB社から送信されているのではなく、下記の他の感染ボット群から送信される

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)

December 4, 2019

How to Respond to Emotet Infection (FAQ)



Since October 2019, there has been a growing number of Emotet infection cases in Japan. JPCERT/CC issued a security alert as follows:

Alert Regarding Emotet Malware Infection

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

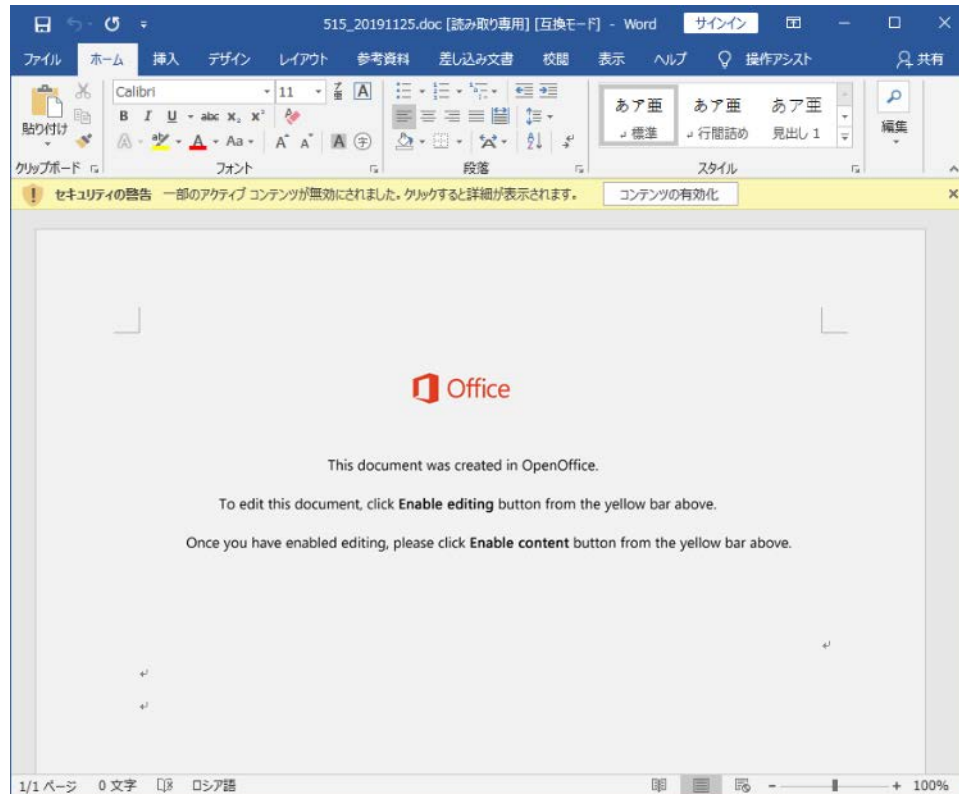
The purpose of this entry is to provide instructions on how to check if you are infected with Emotet and what you can do in case of infection (based on the information available as of December 2019). If you are not familiar with the detailed investigation methods described here, it is recommended that you consult with security vendors who can assist you.

Malicious Mail Example

Mail

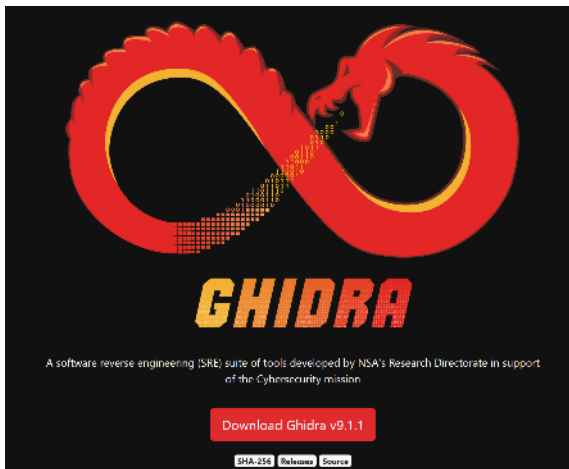


Attachment



Analysis Tool

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)+101p
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@YGPAVCInThread@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@YGHPPAUHINSTANCE_0@0P
; 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+301j
mov       eax, [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+501j
mov       eax, [esi]
mov       ecx, esi
call      dword ptr [eax+68h]
jmp       short loc_42916C

loc_429165: ; CODE XREF: sub_429105+491j
mov       eax, [esi]
mov       ecx, esi
call      dword ptr [eax+54h]

loc_42916C: ; CODE XREF: sub_429105+5E1j
mov       ebx, eax

loc_42916E: ; CODE XREF: sub_429105+2C1j
; sub_429105+3E1j
call      7AfxWinTerm@YGXXZ ; AfxWinTerm(void)
pop       edi
mov       eax, ebx
pop       esi
pop       ebx
retn     10h
sub_429105 endp
```



Ctrl+Z



```
unk_429105 db 53h ; S
           db 56h ; V
           db 57h ; W
           db 83h ; 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 8Bh ; ;
           db 0F0h ; 0
           db 0E8h ; e
           db 82h ; ;
           db 0E5h ; a
           db 0 ;
           db 0 ;
           db 0FFh ; Y
           db 74h ; t
           db 24h ; S
           db 1Ch ;
           db 8Bh ; ;
           db 78h ; x
           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 0E8h ; e
           db 0Ch ;
           db 1 ;
           db 0 ;
           db 85h ; ;
           db 0C0h ; A
           db 74h ; t
           db 3Bh ; ;
           db 85h ; ;
           db 0FFh ; Y
           db 74h ; t
           db 0Eh ;
           db 8Bh ; ;
           db 7 ;
           db 8Bh ; ;
           db 0CFh ; F
           db 0FFh ; Y
           db 90h ;
           db 84h ;
           db 0 ;
           db 0 ;
           db 0 ;
           db 85h ; ;
           db 0C0h ; A
           db 74h ; t
           db 29h ; ;
           db 8Bh ; ;
           db 0 ;
           db 6 ;
           db 8Bh ; ;
           db 0 ;
```



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		

How to Enjoy JSAC 2020

Sharing Technical Info about Incidents

Topic	Session Title
A	Evil Hidden in Shellcode: The Evolution of Malware DBGPRINT
A/D	Threat Information on the APT Group Conducting "Operation Bitter Biscuit"
B/A	The Implementation and Usage of Artifact Collection Tool and Simple Malware Analysis Sandbox for macOS
B	Developing an Efficient Mac Forensic Tool
C	Is It Wrong to Try to Find APT Techniques in Ransomware Attack?
D	100 more behind cockroaches? or how to hunt IoCs with OSINT
D	Battle Against Ursnif Malspam Campaign targeting Japan
D	An Overhead View of the Royal Road

[A] Malware [C] Incident

[B] Forensics [D] Threat trends, intelligence

Networking

15:00 - 15:30

Coffee break



Thank you!

