2024年度後期「ログ分析」報告書

診断日程：2024/12/02～2025/01/20

診断対象：Boss of the SOC version 1（BOTSv1）

使用ツール：Splunk 9.3.1

目次

サイバーキルチェーンの段階	説明
偵察 (Reconnaissance)	対象者に関する情報を事前調査・情報収集する。
武器化 (Weaponization)	エクスプロイトコードやマルウェアを作成し、添付ファイルなどに格納する。
配送 (Delivery)	マルウェアやエクスプロイトコードを添付したメールなどを対象者へ送付する。
攻撃実行 (Exploitation)	対象者が添付ファイルを開くことで、マルウェアやエクスプロイトコードが実行される。
インストール (Installation)	対象者のPCにマルウェアがインストールされる。
遠隔制御 (Command and Control)	C&Cサーバ経由でマルウェアを操作し、内部情報を収集する。
目的の実行 (Actions on Objective)	内部情報を圧縮・暗号化し、外部へ持ち出す。

調査対象：Botsv1 ログ
目的：USBメモリを経由したランサムウェア感染の調査と、感染経路および被害範囲の特定

1.偵察(Reconnaissance)

目的:不審な動きをするアカウントの特定

実施内容

●ログ内の特権変更履歴を調査するために、以下のクエリを実行した結果

Splunk > SPL

```
index=botsv1 sourcetype="wineventlog" EventCode=4672
| stats count by Account_Name, ComputerName
| sort - count
```

●特権変更が複数件発生していることを確認した

```
Administrator                    we8105desk.waynecorpinc.local                    1200
```

　名前がAdministratorになっているアカウントが存在し、多くがパソコンの名前なのに対して不自然だと感じたため

●不審なユーザーwe8105deskをさらに追加サーチした結果

ある特定の期間にしかアクセスしていないことが分かった

●日時を絞り検索した結果(2016/08/24 0:00~2016/08/26 0:00)

Splunk > SPL

```
1  index=botsv1 we8105desk
```

sourcetypeが以下の結果になった

sourcetype

8 値, 100% のイベント　　選択済み　はい　いいえ

レポート

トップ値　　時間別トップ値　　レア値

このフィールドを持つイベント

値	カウント	%
xmlwineventlog	104,360	89.332%
wineventlog	10,028	8.584%
stream:smb	1,528	1.308%
stream:ldap	746	0.638%
stream:dns	111	0.095%
nessus:scan	24	0.02%
suricata	23	0.02%
WinRegistry	3	0.002%

●xmlwineventlogのカウントが異常な数値と感じたためさらに深堀してみた結果

Splunk > SPL

```
1  index=botsv1 we8105desk sourcetype="xmlwineventlog"
```

上記の検索によりどこからの通信が多かったを調べることができた

SourceIp

6 値, 50.262% のイベント　　選択済み　はい　いいえ

レポート

トップ値　時間別トップ値　レア値

このフィールドを持つイベント

値	カウント	%
192.168.250.100	52,270	99.649%
192.168.250.255	69	0.132%
127.0.0.1	66	0.126%
0.0.0.0	42	0.08%
224.0.0.252	6	0.011%
192.168.250.70	1	0.002%

結果"192.168.250.100"がホストのIPアドレスであると推測できる

●初期段階のログ分析中、不審なアカウントや特権変更の履歴を確認していた際、通常のシステムプロセスとして動作するはずの『WUDFHost.exe』が頻繁にイベントに記録されていたため深堀して検索してみることにした結果

Splunk > SPL

```
1  index=botsv1 host=we8105desk sourcetype=WinRegistry WUDFHost.exe
```

18件のイベントがヒットした

✓ 18件のイベント (2016/08/24 9:00:00.000～2016/08/25 9:00:00.000)

イベント (18)　パターン　統計情報　視覚エフェクト

タイムラインのフォーマット ▾　－ズームアウト　＋選択項目に

WUDFHost.exe は通常デバイスドライバー関連のプロセスですが、悪用の可能性があると判断しました。

考察

●この段階では、外部から攻撃者がUSBメモリを使用してデバイスを偵察していた可能性が高いと推測されます。

2.武器化（Weaponization）

目的:攻撃に使用されたエクスプロイドコードやマルウェアの特定

実施内容

●WUDFHost.exe のプロセスチェーンを詳細に分析するため、以下のクエリを実行しました。

Splunk > SPL

```
index=botsv1 host=we8105desk sourcetype=WinRegistry WUDFHost.exe
```

●結果「friendlyname」が「MIRANDA_PRI」である USB メモリが接続されていることを確認しました。

Log file

```
keypath="HKLM\software\microsoft\windows portable
devices\devices\wpdbusenumroot#umb#2&37c186b&0&storage #volume #??
usbstor #disk &ven_generic&prodflash_disk&rev_8.07#7d961196&0#\
friendlyname
```

●USB メモリ内には疑わしい Word ファイル「Miranda_Tate_unveiled.dotm」が存在していました。

考察

●マルウェアが武器化された形でUSBメモリに格納され、標的に配布された可能性が考えられます。

3. 配送（Delivery）

目的: 攻撃対象へのマルウェア配送手段の特定

実施内容

●USB デバイスのドライブ文字を特定するため、以下のクエリを使用しました。

Splunk > SPL

```
1  index=botsv1 sourcetype=XmlWinEventLog host=we8105desk "d:\\"
```

●結果
USB メモリ「MIRANDA_PRI」が D ドライブとして認識され、そこからマルウェアが実行されていることを確認しました。（マルウェアが実行されていたことは次に確認）

その後、ファイルが共有されていないか確認してみたところ

Splunk > SPL

```
1  index=botsv1 sourcetype=winregistry host=we8105desk fileshare
```

IPアドレス192.168.250.20とファイルシェアをしていることが分かった。

4.攻撃実行（Exploitation）

目的: マルウェアの実行状況の特定

実施内容

●Dドライブから実行されたプロセスを調査しました

Splunk > SPL

```
index=botsv1 sourcetype=XmlWinEventLog *.dotm CommandLine=*
host=we8105desk
| eval length=len(CommandLine)
| table CommandLine length
| sort - length
```

●結果
Word テンプレートファイル「Miranda_Tate_unveiled.dotm」が実行されていたことがわかりました。

```
e14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"
```

このことからDドライブで実行されたコマンドがないか検索した結果

Splunk > SPL

```
index=botsv1 sourcetype=XmlWinEventLog CommandLine=* "/d"| table
CommandLine ProcessId ParentProcessId ParentCommandLine
```

```
/d /c taskkill /t /f /im "121214.tmp" &gt; NUL &amp; ping -n
1 127.0.0.1 &gt; NUL &amp; del
"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"
&gt; NUL
```

Dドライブからtaskkillされていることがわかりtaskkillされていたtmpファイルを調査した結果

Splunk > SPL

```
index=botsv1 sourcetype=XmlWinEventLog 121214.tmp CommandLine=* | table
CommandLine ProcessId ParentProcessId ParentCommandLine |reverse
```

"C:\Windows\System32\cmd.exe" /C START "" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"	1476	3968	"C:\Windows\System32\WScript.exe" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\20429.vbs"
"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\{35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe"	3836	3828	"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"

考察

- 「osk.exe」が本来のディレクトリ（C:\Windows\System32）ではなく、ユーザーの AppData フォルダ内に存在しているため、攻撃者が改ざんしたものであると推測されます。

5. インストール（Installation）

目的: 感染範囲の特定

実施内容

●感染範囲を確認するため以下を実行した

Splunk > SPL

```
index=botsv1 sourcetype=stream:DNS src=192.168.250.100 record_type=A NOT (query{}=*.microsoft.com OR query{}=*.waynecorpinc.local OR query{}=*.bing.com) | stats count by query{} | sort - 10 count
```

50件/ページ ▾　フォーマット　プレビュー ▾

query{}
wpad
isatap
cerberhhyed5frqa.xmfir0.win
dns.msftncsi.com
ipinfo.io
shell.windows.com
solidaritedeproximite.org

●結果
不審なサイトとの接続を確認できました。

●不審なサイトへのアクセスがあったためstream:httpで検索してみた

37.187.37.150	1	http://solidaritedeproximite.org/mhtr.jpg
54.148.194.58	1	http://ipinfo.io/json
67.132.183.25	5	http://shell.windows.com/0409/fileassoc.css http://shell.windows.com/HeaderSlice.jpg http://shell.windows.com/fileassoc/fileassoc.asp
92.222.104.182	1	http://92.222.104.182/mhtr.jpg

●結果
複数の外部サイトからmhtr.jpgが見つかりその一部にsolidaritedeproximite.orgが存在し、以上のことからこの外部経由でjpgがダウンロードされた可能性があると考えた。

●感染したマルウェアがダウンロードしたファイルであるかを特定するため、以下のクエリを実行しました。

Splunk > SPL

```
index=botsv1 sourcetype=stream:http src=192.168.250.100 url=*mhtr.jpg*
| table _time src dest url
```

_time	src	dest	url
2016/08/25 01:48:13.285	192.168.250.100	37.187.37.150	http://solidaritedeproxim
2016/08/25 01:48:14.620	192.168.250.100	92.222.104.182	http://92.222.104.182/mht

_time	src	dest	http.hostname
2016/08/25 01:48:14.620	192.168.250.100	92.222.104.182	92.222.104.18
2016/08/25 01:48:13.492	192.168.250.100	solidaritedeproximite.org	solidaritedep

結果

●ランサムウェア関連ファイル「mhtr.jpg」がネットワーク経由でダウンロードされたことが確認されました。

6.遠隔制御（Command and Control）

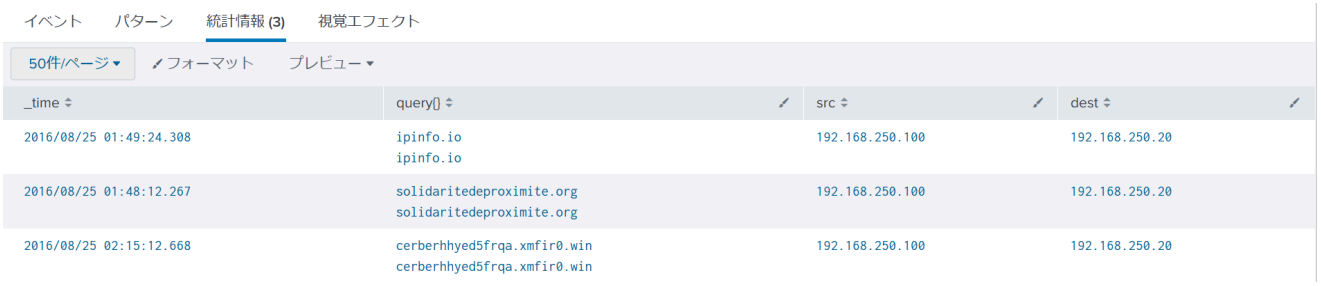
目的: C&C 通信の有無を確認

実施内容

●感染デバイスからの DNS クエリを調査し、不審な通信を特定しました。

Splunk > SPL

```
index=botsv1 sourcetype=stream:DNS src=192.168.250.100 record_type=A NOT
(query{}=*.microsoft.com OR query{}=*.waynecorpinc.local OR
query{}=*.bing.com OR query{}=isatap OR query{}=wpad OR
query{}=*.windows.com OR query{}=*.msftncsi.com)
| table _time query{} src dest
```



イベント　パターン　統計情報 (3)　視覚エフェクト

50件/ページ　フォーマット　プレビュー

_time	query{}	src	dest
2016/08/25 01:49:24.308	ipinfo.io ipinfo.io	192.168.250.100	192.168.250.20
2016/08/25 01:48:12.267	solidaritedeproximite.org solidaritedeproximite.org	192.168.250.100	192.168.250.20
2016/08/25 02:15:12.668	cerberhhyed5frqa.xmfir0.win cerberhhyed5frqa.xmfir0.win	192.168.250.100	192.168.250.20

結果

「cerber(セルバー）」と関連する不審なドメインが複数回通信されていることを検出しました。
cerberについて調べてみた結果、ランサムウェア関連の記事が多数見られこれにより solidaritedeproximite.org を経由して外部通信が確認され、ランサムウェア 'Cerber' が感染の原因であると予測します。

7.目的の実行（Actions on Objective）

目的: データ暗号化と情報漏洩の確認

実施内容

●暗号化されたファイルの範囲を調査しました。

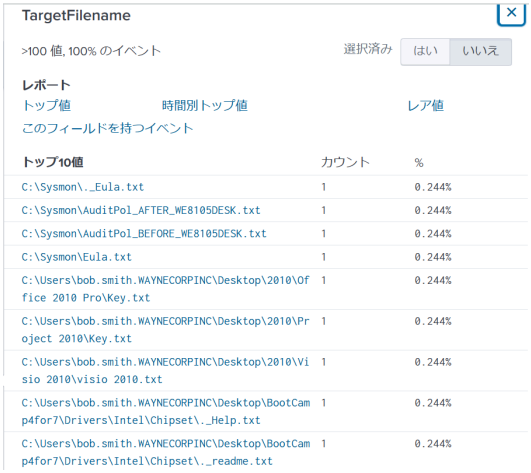
Splunk > SPL

```
index=botsv1 sourcetype=XmlWinEventLog host=we8105desk *.txt
```

検索したところ423件のイベントが引っかかり、感染したユーザーがtxtに関与したことが分かったがこれだけでは何が起きたかわからないためさらに絞り込むことにした
絞り込む方法としてファイル作成時間であるイベントコード２で検索をさらに絞り込み
TaretFilenameで作成された場所を検索した

Splunk > SPL

```
index=botsv1 sourcetype=XmlWinEventLog host=we8105desk *.txt EventCode=2
```

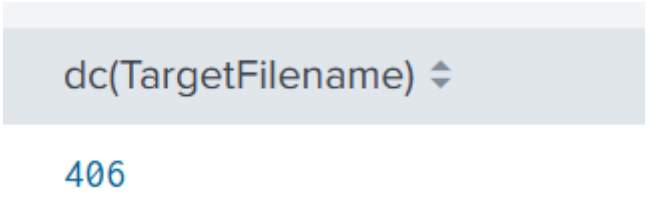

TargetFilename

>100 値, 100% のイベント　選択済み　はい　いいえ

レポート
トップ値　時間別トップ値　レア値
このフィールドを持つイベント

トップ10値	カウント	%
C:\Sysmon\._Eula.txt	1	0.244%
C:\Sysmon\AuditPol_AFTER_WE8105DESK.txt	1	0.244%
C:\Sysmon\AuditPol_BEFORE_WE8105DESK.txt	1	0.244%
C:\Sysmon\Eula.txt	1	0.244%
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Office 2010 Pro\Key.txt	1	0.244%
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Project 2010\Key.txt	1	0.244%
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Visio 2010\visio 2010.txt	1	0.244%
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\._Help.txt	1	0.244%
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\._readme.txt	1	0.244%

●結果C:\Users\bob.smithでの作成が多く確認された
先ほどの結果を含めてstatsを使い暗号化されたファイルの数を調べた結果


dc(TargetFilename)

406

結果

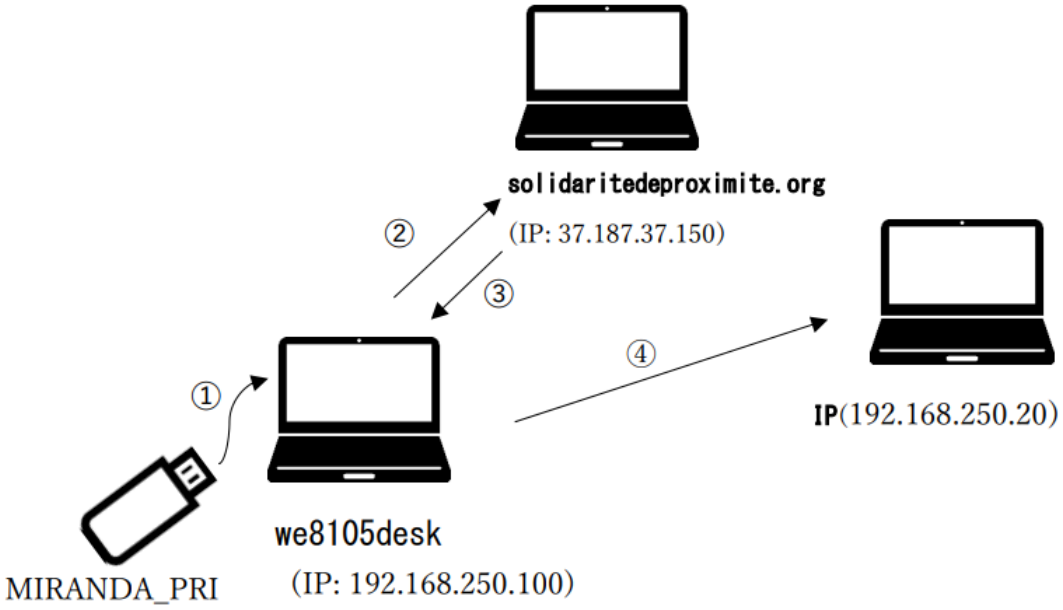
ローカルおよび共有ディスク上で 423 件の .txt ファイルが暗号化されていることを確認しました。

結論

● USB メモリを経由したランサムウェア感染の可能性が高いことが判明しました。
● 攻撃の痕跡として、特定のマルウェア（Cerber）に関連する通信と暗号化が確認されました。
●暗号化されたファイルがあることからランサムウェアによる脅迫が行われたと思われます。

推奨対策:

- USBメモリ使用制限: 特定のデバイスID以外のUSB接続を無効化。
- 通信監視: Cerber関連ドメイン（例: solidaritedeproximite.org）への通信をファイアウォールで遮断。



Netis製ルータ(53413番ポート)

脆弱性についての説明

Netis製(中国製)のルータに関する脆弱性を発見した。
デフォルトで UDP の 53413ポートが開放されています。
このポートはパスワードで保護されていますが、すべての製品で共通であり、パスワードを入手すれば誰でも簡単に不正アクセスが可能になります。

> 本ブログでも既報の通り、「Netis」は中国国内で人気のネットワーク機器メーカ「Netcore」社の中国国外向けのブランド名です。ほとんどの Netis製ルータにはデフォルトで UDP の 53413ポートが開放されており、WAN側から接続可能になっています。この 53413ポートはファームウェア上でハードコードされた単体のパスワードで「保護」されていますが、それこそが脆弱性の本体です。すでにこのパスワードは明らかになっており、パスワードを入手した人物は誰でも外部から Netis製ルータに接続し不正アクセスが可能です。JPCERT／CC によれば、この 6月に観測された日本における 53413ポートへの通信増加は、まさにこのルータの脆弱性を狙い遠隔操作のためのボットを感染させる目的の攻撃であったようです。
>
> インターネット定点観測レポート(2015年 10～12月)
> ルータの脆弱性を狙う通信の増加をJPCERT/CCが報告 |

source_typeごとの件数を調べる

Splunk > SPL

```
index=botsv1 dest_port=53413
| stats count by sourcetype
| sort -count
```

実行結果

sourcetype	count
fortigate_traffic	66556
suricata	2

fortigate_trafficのactionフィールドを調べる

actionフィールドを見ることでリクエストが拒否されたかどうかがわかる。
よってsourcetype=fortigate_trafficであるログの数とaction=blockedの数が同じであればすべてのリクエストが拒否されていることがわかる。

実行したSPL

Splunk > SPL

```
index=botsv1 dest_port=53413 sourcetype=fortigate_traffic
```

Splunk > SPL

```
index=botsv1 dest_port=53413 sourcetype=fortigate_traffic action=blocked
```

実行結果

source_typeがfortigate_trafficであるログはすべてactionがblockedである。
よってsource_typeがfortigate_trafficのログに関しては、53413番ポートに対する攻撃は防がれていることが分かる。

suricataのログを調べる

実行したSPL

Splunk > SPL

```
index=botsv1 dest_port=53413 sourcetype=suricata
```

上記のSPLでログが2件合致し、日付は2016/8/11と2016/8/25でした。

- **2016/8/11のログ**

Log file

```
{"timestamp":"2016-08-10T15:58:23.791919-
0600","flow_id":3724372038,"in_iface":"eth1","event_type":"dns","src_ip":"
{"type":"answer","id":41232,"rcode":"NOERROR","rrname":"55.58.203.23.in-ad
55.deploy.static.akamaitechnologies.com"}}
```

src_ip: 8.8.8.8やsrc_port: 53とあります。
このIPアドレスとポート番号からGoogle Public DNSサーバーからクエリを送っていることがわかります。
rcode: "NOERROR":やrrname: "55.58.203.23.in-addr.arpa":とあります。
これらからリバースDNSクエリ(IPアドレスからホスト名を引く)であり、対象のIPアドレスは 23.203.58.55である。

rdata: "a23-203-58-55.deploy.static.akamaitechnologies.com"
rdata(Resource Data)は、DNS(Domain Name System)でリソースレコード(RR: Resource Record)のデータ部分を指します。

rdataの内容からIPアドレス23.203.58.55の逆引きを行い、それがAkamaiの静的コンテンツ配信サーバーであることがわかりました。
Akamai Technologiesは、世界的なCDNのリーダー企業でありWAFなどを提供しています。
これらの要素からAkamaiの静的コンテンツ配信サーバーに対する正常な通信であると思われます。

- **2016/8/25のログ**

Log file

```
1  {"timestamp":"2016-08-24T10:49:57.043008-
   0600","flow_id":3724372038,"in_iface":"eth1","event_type":"dns","src_ip":"
   {"type":"answer","id":6010,"rcode":"NOERROR","rrname":"147.24.93.85.in-add
```

8/11のログと同じくsrc_ip: 8.8.8.8やsrc_port: 53とあり、Google Public DNSサーバーからクエリを送っていることがわかります。

rrname: "147.24.93.85.in-addr.arpa":
とあるので、リバースDNSクエリ(IPアドレスからホスト名を引く)で対象のIPアドレスは85.93.24.147であることがわかります。
rdata: "dashmallicy.xyz":
なのでIPアドレス 85.93.24.147 のP逆引きレコードに対応するホスト名です。

このドメイン"dashmallicy.xyz"をVirusTotal - Homeで調べてみた結果危険だという報告はありませんでした。

サイバーキルチェーン

ここまでの情報から、ポートスキャンを行っており、サイバーキルチェーンの偵察段階のログであることが分かります。

対策

このメーカーのルータにしかない脆弱性なので別製品に乗り換える。
ポートフィルタリングの設定を見直す。

Apache Log4j(8089番ポート)

実行したSPL

1つ目と同様に、宛先ポートが怪しいログを調べ8089番に辿り着いた。

下記のSPLで一意にログを特定できました。

Splunk > SPL

```
index=botsv1 src_port=61746 dest_port=8089 flow_id=948947464
```

Log file

```
{"timestamp":"2016-08-28T12:00:37.000085-
0600","flow_id":948947464,"event_type":"flow","src_ip":"192.168.225.173","
{"pkts_toserver":20,"pkts_toclient":20,"bytes_toserver":3604,"bytes_toclie
0600","age":28,"state":"closed","reason":"timeout"},"tcp":
{"tcp_flags":"1f","tcp_flags_ts":"1f","tcp_flags_tc":"1b","syn":true,"fin"
```

脆弱性についての説明

宛先ポート番号が8089であるログが多くあり、不審な点が見つかった。

> ポート8089について参考記事
> 検証用AWSアカウントでGuardDutyと闘う話 ～不用意にポート開けるな編～ #EC2 - Qiita
> 【セキュリティ ニュース】「Log4Shell」攻撃、対象ポートが拡大中 - 警察庁観測（1ページ目 / 全1ページ） ：Security NEXT

8089ポートに関連する脆弱性がないか調べてみたところ、「CVE-2021-44228」や「CVE-2021-45046」が見つかった。
この脆弱性は「Apache Log4j」により、リモート攻撃が可能となるものである。

> Log4jはApacheソフトウェア財団のプロジェクトである「Apache Logging」で開発されたオープンソースソフトウェアの1つであり、Javaで開発したプログラムに対してログを記録・出力するための機能を提供します。

> Apache Log4jについて参考記事
> Apache Log4jに見つかった脆弱性「Log4Shell」とは | ドコモビジネス | NTTコミュニケーションズ 法人のお客さま
> 初心者でも分かるLog4jとその脆弱性、影響範囲から対策方法のすべて - ペンタPRO：ペンタセキュリティが提供するセキュリティ情報まとめサイト

攻撃の仕組み

> 1. 攻撃者は脆弱性を利用できるようにするため、特殊な文字列を含ませたhttpリクエスト（データ）をサーバに送信する
> 2. サーバに脆弱性がある場合、Javaアプリケーションは送られてきたデータを処理した結果を、そのままログに書き込んでしまう
> 3. ログに書き込まれたデータに特殊な変数が含まれていると、JDNI Lookup機能がそれを実行してしまう
> 4. Log4j が、ダウンロードした悪意のあるプログラムを読み込み、実行してしまう
>
> この文字列がログに書き込まれ、JNDI Lookup機能により実行された場合、アクセスを受けたLDAPサーバ（ldap://xxxxx.com/a）は、悪意のあるJava ClassファイルのURLを応答します。するとLog4jは、応答されたURLに配置されている悪意のあるJava Classファイルをダウンロード、メモリ内に読み込み実行してしまうというわけです。
>
> 初心者でも分かるLog4jとその脆弱性、影響範囲から対策方法のすべて - ペンタPRO：ペンタセキュリティが提供するセキュリティ情報まとめサイト

> Log4jに見つかった深刻な脆弱性であるLog4Shellを利用すれば、任意のコードをリモートで実行する、RCE（Remote Code Execution：リモートコード実行）が可能です。背景にあるのはLookupと呼ばれる機能やJNDI（Java Naming and Directory Interface）と呼ばれる仕組みの処理にある問題で、攻撃者が送信した文字列をLog4jがログとして記録すると、その文字列に記述された通信先やサーバー内部のファイルからjava classファイルと呼ばれるファイルを読み込んで実行してしまうというものです。
> Apache Log4jに見つかった脆弱性「Log4Shell」とは | ドコモビジネス | NTTコミュニケーションズ 法人のお客さま

TCPのフラグについて

先程示したログのフィールドにtcp_flags:1f(0001.1111)というものがあります。これはTCPヘッダのフラグを示すものです。

10ビット目	9ビット目	8ビット目	7ビット目	6ビット目
Reserved	Accurate ECN	Congestion	ECN-Echo	Urgent

5ビット目	4ビット目	3ビット目	2ビット目	1ビット目
Acknowledgment	Push	Reset	SYN	FIN

- tcp_flags:1f(0001.1111)がどういう意味なのか

立っていたフラグ	説明
FIN(Finish)	接続の終了を要求するフラグ。通信を終了する際に使用される。
SYN(Synchronize)	接続の確立を要求するフラグ。シーケンス番号の同期に使用。
RST(Reset)	接続をリセットするフラグ。異常な接続やエラー時に使用。
PSH(Push)	即座にデータを受信側にプッシュすることを要求するフラグ。
ACK	データの受信確認を行うフラグ。

FIN、SYN、RSTが同時に立っているのは明らかにおかしいと感じたのでさらに調べるとクリスマスツリー攻撃であることが分かりました。

※クリスマスツリー攻撃とは

> TCPパケットの複数のフラグがオンになった異常ものを送り込むことで、プロトコルを適切に処理できないデバイスやコンフィグレーションに対して予期しない動作を誘発することが可能
>
> クリスマスツリー攻撃とは？概要から対策まで徹底解説

サイバーキルチェーン

ここまでの情報から、サイバーキルチェーンの偵察段階のログであることが分かります。

対策

- Apache Log4j
  最新版へアップデートを行いましょう。
  バージョンアップしない場合の具体的な対策方法については、JPCERT/CCのページをご覧ください。

> 参考:
> Apache Log4j の脆弱性対策について(CVE-2021-44228) | アーカイブ | IPA 独立行政法人 情報処理推進機構
> 「Log4j」の脆弱性とは？ リスクや対策など | 株式会社 日立ソリューションズ・クリエイト
> Apache Log4jの任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起

- クリスマスツリー攻撃
  ファイアウォールの設定を見直し、適切なポートフィルタリングを行う

> 参考:
> クリスマスツリー攻撃とは？概要から対策まで徹底解説

Memcached DDoS攻撃(11211番ポート)

脆弱性についての説明

引き続き特定のポートに問題がないか調べると、11211番ポートに関連した製品の深刻な脆弱性を発見しました。
Memcachedサーバの脆弱性を利用したDDoS攻撃です。

> Memcached とは？
>
> Memcached は、オープンソースの高性能分散型のメモリー／データベースキャッシュシステムです。多くの場合にキー値を使用し、アクセスの多いデータをメモリーにキャッシュすることで、動的な Web サイトや Web アプリケーションを高速化します。
> Memcached は、Facebook、Twitter、YouTube などの企業で広く使用されています。
> UDP もサポートされ、 攻撃ベクトルに利用される大きな要因となっています。
>
> Memcached DDoS 攻撃とは？| Akamai

攻撃の仕組み

> memcached攻撃は次の4つのステップで発生します：
> 1.攻撃者は公開されたmemcachedサーバーにデータの大きなペイロード*を埋め込みます。
> 2.次に、攻撃者は標的となる被害者のIPアドレスで HTTP GETリクエストを偽装します。
> 3.リクエストを受信する脆弱なmemcachedサーバーは、応答することで役立てようとしているため、標的に大量の応答を送信します。
> 4.標的のサーバーまたはその周囲のインフラストラクチャは、memcachedサーバーから送信された大量のデータを処理できないため、正当なリクエストに対する過負荷とサービス拒否が発生します。
>
> memchachedを利用したDDoS攻撃 | Cloudflare

実行したSPL

- ポート番号だけで絞り込み

Splunk > SPL

```
index=botsv1 dstport=11211
| sort _time
```

- DDos攻撃が疑われるので、1分以内に10件以上のトラフィックが存在するログを絞り込む

Splunk > SPL

```
index=botsv1
dstport=11211
| bin _time span=1m
| stats count by _time, srcip, dstip, srcport, dstport
| where count > 10
```

実行結果
それぞれの実行結果を見てみると、どちらも623件です。
通信を試みたログが短時間に集中していることがわかります。

Splunk > SPL

```
index=botsv1 dstport=11211 action=blocked
| sort _time
```

623件であり、すべて防がれていることがわかります。

サイバーキルチェーン

Memcached DDoS 攻撃を行うための準備としてポートスキャンを行っており、サイバーキルチェーンでは偵察段階に当たります。

対策

不要なポートである場合は閉じる。

> - **Memcached DDoS の直接のターゲット**: この種の攻撃には、クラウド型の DDoS 対策を活用します。増幅係数が高く、オープンな Memcached サーバーが多いことから、データセンターのローカルな対策では、キャパシティの問題が生じる可能性があります。
>
> Memcached DDoS 攻撃とは？| Akamai

5000番ポート

脆弱性についての説明

Windows XPでUPnPの実装に問題があり、UPnPサービスの脆弱性を突くものです。

> 5000番ポートはそのようなポート番号の一つで、いくつかの用途に用いられる。よく知られる用途の一つとして、コンピュータからネットワーク上の機器の検知や設定を行うためのUPnP（Universal Plug and Play）で用いられるプロトコルの一つであるSSDP（Simple Service Discovery Protocol）が利用していた。
>
> コンピュータが周辺機器からのイベント通知を受け付けるポート番号としてTCPの5000番が用いられ、Windows XPではUPnPの実装に問題があったため5000番ポートが攻撃の標的となった。現在ではこの用途（SSDP Event Notification）はTCPの2869番が標準のポートとされる。
>
> 5000番ポート（ポート5000 / TCP5000番）とは - IT用語辞典 e-Words
> TCP 5000番ポートへのアクセスが急増，原因は2種類の新種ワーム | 日経クロステック（xTECH）

また、Docker Remote APIやWebサーバー、カスタムサービスで使用されることが多く、特にFlaskサーバのポートとしてよく使われる。
認証が構成されていないDocker APIの場合、コンテナを自由に操作されるリスクがあり危険です。

> **Flask**（フラスク）は、プログラミング言語Python用の、軽量なウェブアプリケーションフレームワークである
>
> 参考:
> Flask - Wikipedia

sourcetypeごとの件数を調べる

Splunk > SPL

```
index=botsv1 dest_port=5000
| stats count by sourcetype
| sort -count
```

上記のSPLで検出されるログは、suricataが5件、stream:tcpが5件、fortigate_trafficが223件ありました。

sourcetype	count
fortigate_traffic	233
stream:tcp	5
suricata	5

suricataのログを調べる

Splunk > SPL

```
index=botsv1 dest_port=5000 sourcetype=suricata
| sort time
```

suricataでのログは5件であり、5件のログのフィールドについて調べたものを表にしてまとめました。

ログ番号	宛先IP	応答	状態	終了理由	送信バイト数	受信バイト数
1	192.168.250.70	なし	syn_sent	timeout	124	0
2	192.168.250.70	なし	syn_sent	timeout	124	0
3	192.168.250.70	なし	syn_sent	timeout	124	0
4	192.168.250.41	あり	closed	timeout	124	120
5	192.168.250.40	あり	closed	timeout	124	120

1つ目~3つ目はsyn_sent状態なのでSYNを受信済みであることが分かります。

4つ目、5つ目のログではSYN,ACK,RSTのフラグが立っておりclosed状態なのでコネクション確立段階でないことが分かります。

> 参考:
> TCPの状態遷移 #Network - Qiita

stream:tcpのログを調べる

Splunk > SPL

```
index=botsv1 dest_port=5000 sourcetype=stream:tcp
| sort time
```

ログ番号	接続先	状態 (tcp_status)	拒否 (refused)	処理時間 (ms)	送信バイト	受信バイト	接続
1	192.168.250.40:5000	拒否 (1)	1	6	60	124	拒否
2	192.168.250.41:5000	拒否 (1)	1	237	60	124	拒否
3	192.168.250.70:5000	成功 (2)	0	1	0	124	成功
4	192.168.250.70:5000	成功 (2)	0	5	0	124	成功
5	192.168.250.70:5000	成功 (2)	0	2	0	124	成功

それぞれのログを表にまとめると上記のようになりました。

また、3~4つ目のログでは接続が成功しているので更なる調査が必要だと思われます。

fortigate_trafficのactionフィールドを調べる

Splunk > SPL

```
index=botsv1 dest_port=5000 sourcetype=fortigate_traffic
```

上記のSPLで233件のログが検出された

Splunk > SPL

```
index=botsv1 dest_port=5000 sourcetype=fortigate_traffic action=blocked
```

先程のSPLで検出された通信が成功していないログがどれだけの数なのかを調べると、
sourcetype=fortigate_trafficであるログはすべてaction=blockedであった。
よって通信は成功していないことが分かります。

サイバーキルチェーン

ここまでの情報から、サイバーキルチェーンの偵察段階のログであることが分かります。

対策

UPnPを使う場合は2869番ポートを使う。
ポートフィルタリングの設定を見直す。