WHY CORRUPTED (?) SAMPLES IN RECENT APT?
—CASE OF JAPAN AND TAIWAN

By **Suguru Ishimaru**

GREAT

Dec 2016

Introduction

Introduction

$ whoami

Suguru_ISHIMARU

$ whois suguru_ishimaru

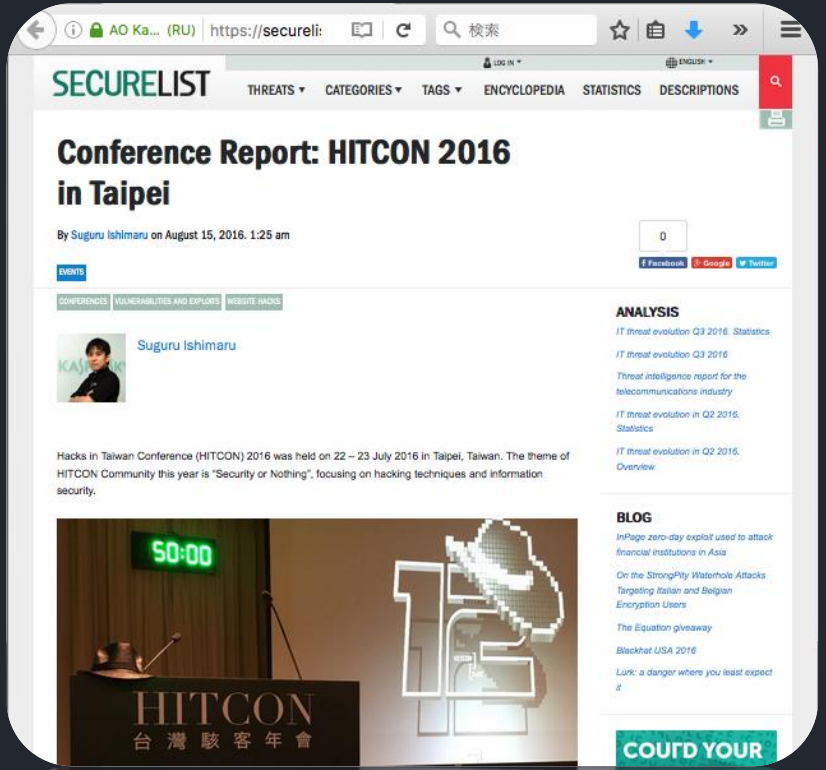
Job_title: Researcher

Department: Global Research Analysis Team

Organization: Kaspersky Labs

E-mail: suguru.ishimaru[at]kaspersky.com

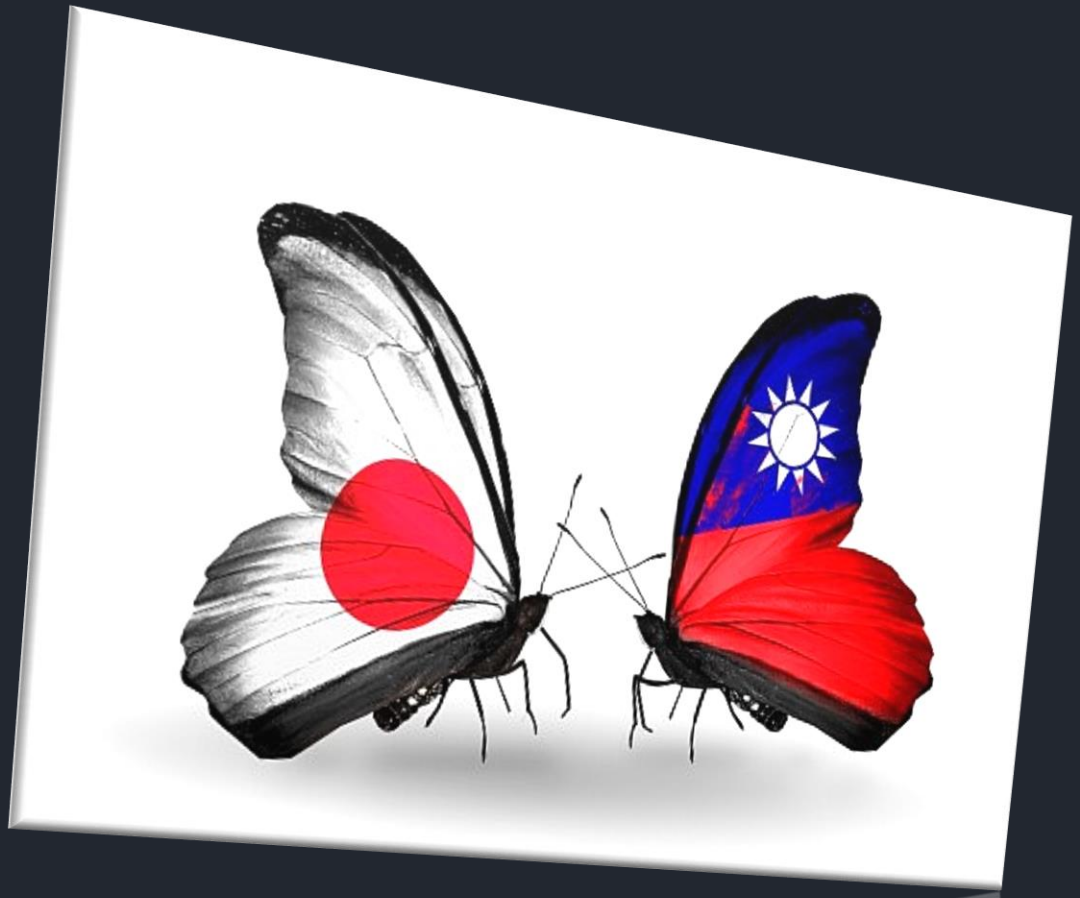
My last blogpost was Conference Report: HITCON 2016 in Taipei



Contents

Contents

$ history | tail -n5



Problem

Problem: A lot of targeted attacks

More than 40 APT

Problem: The biggest issue is...

Question: What is the biggest problem in APT seen from antivirus side?

Hard work | **No sample** | **No detect**

We collect mass spread samples. However, we could not get APT samples easily. Especially, second stage sample is extremely rare.

Problem: Corrupted samples

We found samples, sometimes they were corrupted. That means they are executable but crashing:

1. Memory dump
2. Unknown binary data
3. Broken data
4. Cured by Anti Virus
5. Quarantined file
6. Password encrypted archive without password

Problem: Why corrupted samples?

Question: Why corrupted samples in recent APT?

I will tell you my answer in conclusion

Motivation

Motivation: What should we do?

Question: What should we do when we got corrupted malware in APT?

Just Ignore

Make AV signature

Deep Analysis

1. Checking really corrupted or not
2. Getting information of related others

Motivation: Two recent APT cases

Probably corrupted (?) samples have found in two recent APT.

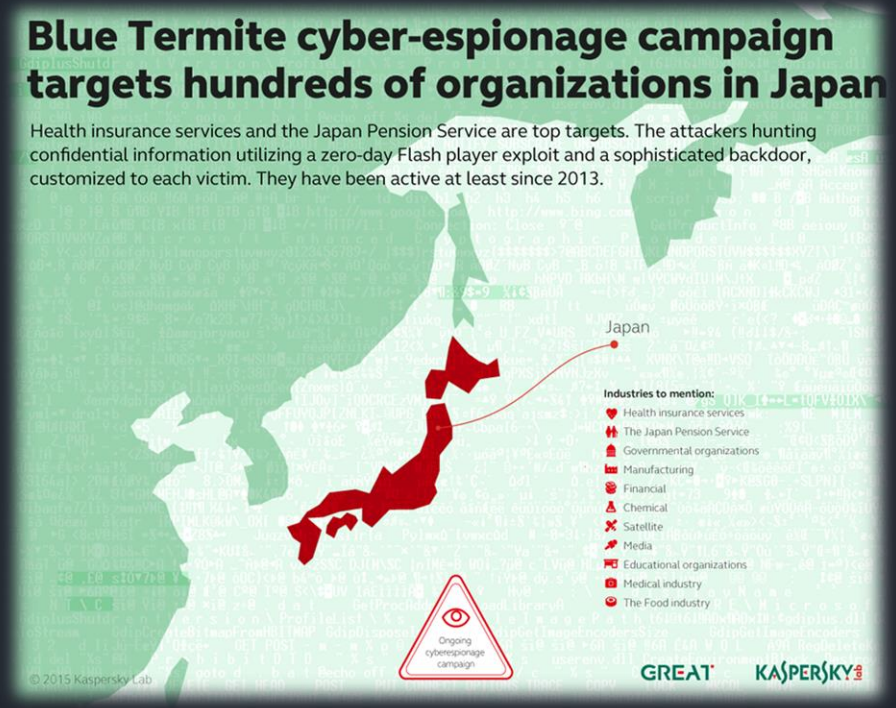
Emdivi

Elirks

Emdivi

Emdivi: Overview

1. The Blue Termite APT campaign
2. Target region is Japan mainly
3. C2s on compromised legitimate sites
4. spear phishing email
5. drive-by dowonload
6. Watering hole attacks
7. CVE-2014-7247
8. CVE-2015-5119



Emdivi: History

JUL 2011 Target to web site in Taiwan

NOV 2013 Oldest sample of Emdivi

NOV 2014 Operation CloudyOmega by Symantec

MAY 2015 Japan pension service Emdivi + PlugX

JUL 2015 Attacks of Flash Player 0day (CVE-2015-5119) by Trendmicro

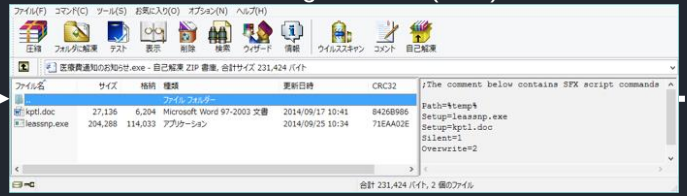
AUG 2015 New activity of the Blue Termite APT by Kaspersky

MAY 2016 Security report about APT (Emdivi) by Macnica

Emdivi: Infection vector

spear phishing e-mail

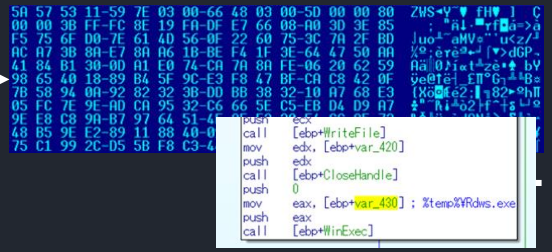
self-extracting archives (SFX) file

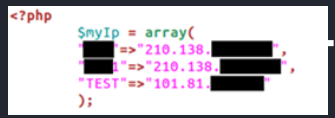


emdivi t17

drive by download

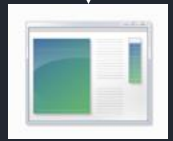
CVE-2015-5119





watering hole attacks

emdivi t20



Emdivi: Target

Regions:

- Japan
- Taiwan

Industries:

1. Government
2. Universities
3. Financial services
4. Energy
5. Food
6. Heavy industry
7. Chemical
8. News media
9. Health care
10. Insurance
11. Security researcher
12. Internet service provider

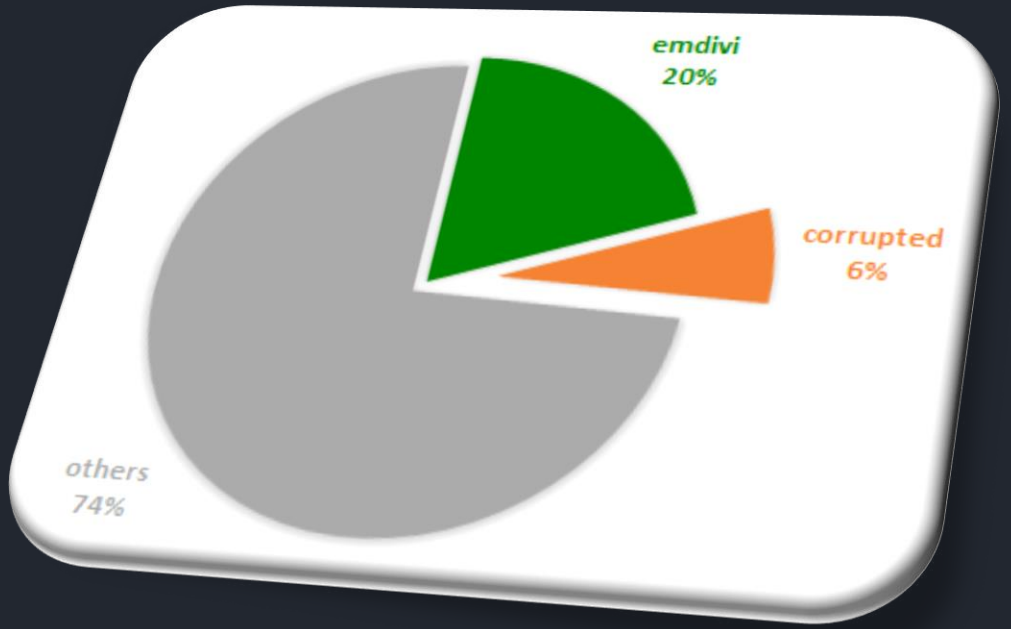
To create infrastructure

Japan Hosting provider

Taiwan web site

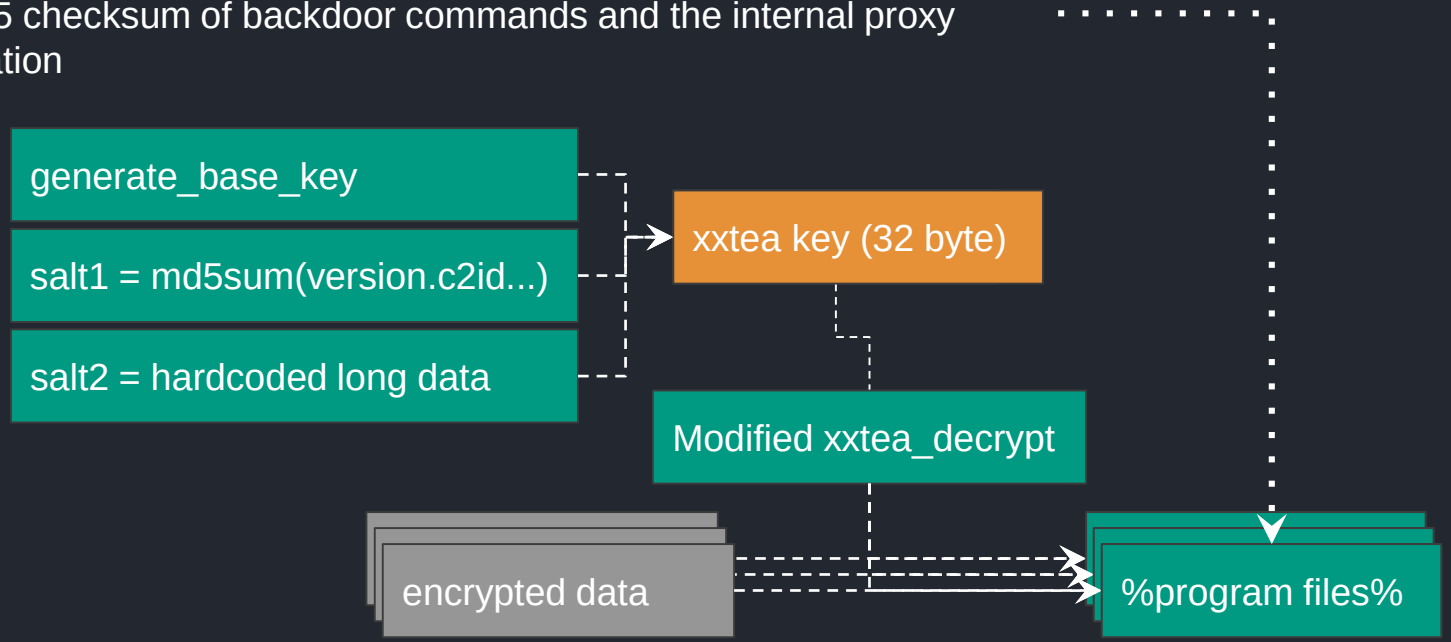
Emdivi: Corrupted (?) samples

We collected more than 600 samples related to this attacks, around 25 percents were Emdivi samples.
Among them, 6 percents did not work.

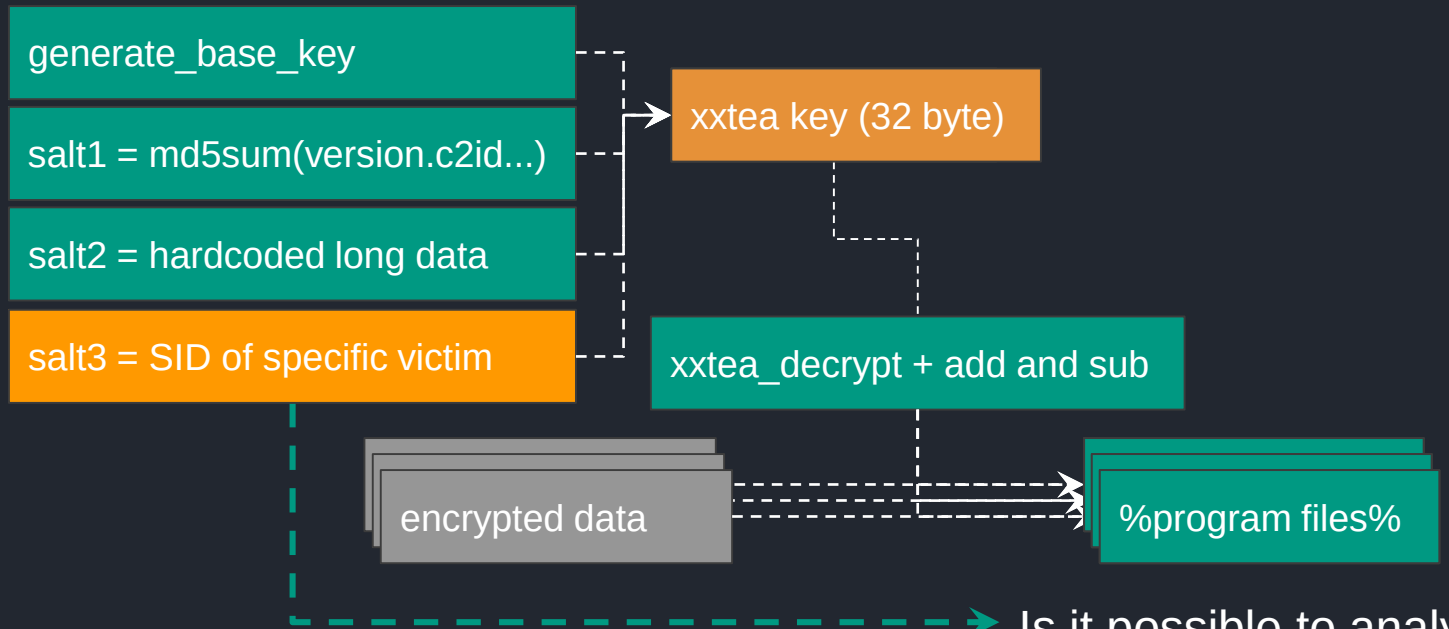


Emdivi: Important data was encrypted

Emdivi family stores encrypted important data:
C2, API name, strings for anti-analysis, value of mutexes, as well as the md5 checksum of backdoor commands and the internal proxy information



Emdivi: C~~orrupted (?)~~ ustomized samples



Emdivi: Corrupted (?) customized samples

SECURELIST

LOG IN

THREATS ▾ CATEGORIES ▾ TAGS ▾ ENCYCLOPEDIA ST

In early July 2015, however, Kaspersky Lab found a sample that creates a decryption key with Salt1, Salt2, and Salt3. Salt3 is the security identifier (SID) from a compromised PC.

The flow of decryption key generation (with additional Salt3):

```
rep stosb
mov     esi, [esi]      ; salt1 = 't20.22.1.8750.2081.4209.0'
mov     ecx, [ebp+var_10]
push    ebx
mov     eax, esi
call    base64_enc      ; base64(salt1)
xor     esi, esi
push    esi
push    [ebp+var_10]
lea     eax, [ebp+var_20]
push    eax
call    md5sum          ; md5(base64(salt1))
push    [ebp+var_10]    ; void *
mov     [ebp+var_4], esi
call    j__j__free
push    esi
lea     eax, [ebp+var_30]
push    offset salt2    ; "ynva+sL198PGeY504ZjbY00TX3R8v0unu00065i"...
push    eax
call    md5sum          ; md5(salt2)
add     esp, 24h
mov     byte ptr [ebp+var_4], 1
push    dword ptr [eax+4]
lea     ebx, [ebp+var_20]
push    dword ptr [eax]
call    strcat          ; md5(base64(salt1)) + md5(salt2)
lea     esi, [ebp+var_30]
mov     byte ptr [ebp+var_4], 0
call    free
lea     eax, [ebp+var_30]
push    eax
call    _getSID         ; salt3 = 'S-1-5-21-XXXXXXXXXX-YYYYYYYYYY-ZZZZZZZZZ'
pop     ecx
mov     byte ptr [ebp+var_4], 2
push    dword ptr [eax+4]
push    dword ptr [eax]
call    strcat          ; md5(base64(salt1)) + md5(salt2) + salt3
lea     esi, [ebp+var_30]
mov     byte ptr [ebp+var_4], 0
call    free
lea     eax, [ebp+var_30]
push    eax
lea     eax, [ebp+var_20]
call    _md5sum         ; md5(md5(base64(salt1)) + md5(salt2) + salt3)
pop     ecx
```

In other words, the sample works only on its target PCs. Without knowing the victim's SID, the decryption key will not be generated successfully, making it difficult to decrypt important data. This means it's not possible to analyze the malware in detail.

We published the details as a blog in securelist.com

Summary

From early June, when the cyber-attack on the Japan Pension Service started to be reported widely, various Japanese organizations would have started to deploy protection measures. However, the attackers from Blue Termite, who it seems kept a close eye on them, started to employ new attack methods and successfully expanded their operation. While writing this article, another sample of emdivi t20 has been found. It employs AES in addition to SID tricks, making it difficult to decrypt sensitive data. In order to fight back against this cyber-espionage, Kaspersky Lab will continue its research.

Kaspersky products detect emdivi t17, emdivi t20, and the flash exploits using the verdicts below:

- Backdoor.Win32.Emdivi.*
- Backdoor.Win64.Agent.*

→ Is it possible to analyze?

No

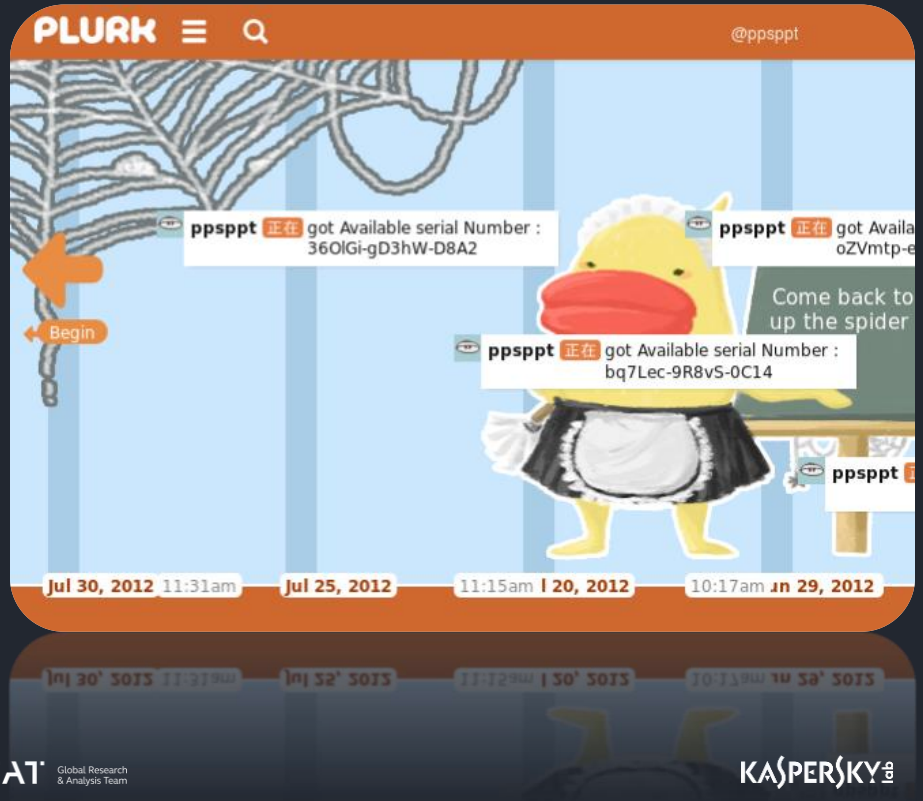
Emdivi: DEMO

Emdivi t20 AES + SID

Elirks

Elirks: Overview

1. As known as PLURK
2. The Elirks APT campaign
3. Unique schema to connect real C2
4. Target Regions are Taiwan, Japan
5. Trojan dropper is fake folder icon
6. Decoys were sometimes airline e-ticket



This group uses several types of malware Elirks, Ymailer, Ymailer-mini and Micrass. This presentation is forcusing Elirks

Elirks: History

MAR 2010 Oldest Elirks sample

JUL 2012 Chasing Advanced Persistent Threats (APT) by SecureWorks

JUL 2013 Hunting the Shadows by Fyodor Yarochkin, Pei Kan PK Tsung, Ming-Chang Jeremy Chiu, Ming-Wei Benson Wu

AUG 2015 Let's Play Hide and Seek In the Cloudby Ashley, Belinda

MAR 2016 Japan Tourist Bureau (JTB) Elirks + PlugX

JUN 2016 Tracking Elirks Variants in Japan: Similarities to Previous Attacks by paloalto

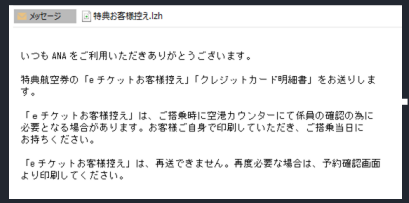
SEP 2016 MILE TEA: Cyber Espionage Campaign Targets Asia Pacific Businesses and Government Agencies by paloalto

OCT 2016 BLACKGEAR Espionage Campaign Evolves by trendmicro

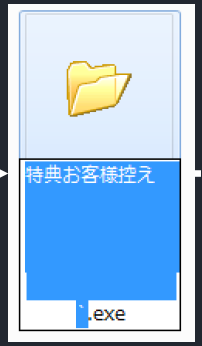
NOV 2016 Japan Business Federation Elirks + PlugX

Elirks: Infection vector

spear phishing e-mail



Trojan dropper spoofing folder icon



fake folder icon: 78 %

create dir, decoy and delete it self

Name	PID	CPU	I/O tot...	Private ...	Description
System Idle Process	0	98.84		0	
csrss.exe	352			1.93 MB	クライアント サーバー ラン...
wininit.exe	404			1.35 MB	Windows スタートアップ ア...
csrss.exe	412	0.05		10.19 MB	クライアント サーバー ラン...
winlogon.exe	468			2.26 MB	Windows ログオン アプリケ...
explorer.exe	2092	0.05		117.37 ...	エクスプローラー
vmtoolsd.exe	2188	0.03		13.74 MB	VMware Tools Core Service
ProcessHacker.exe	1916	0.25		8.96 MB	Process Hacker
svchost.exe	2672	0.17		2.13 MB	

Elirks malware

Elirks: Target

Regions:

- Taiwan
- Japan

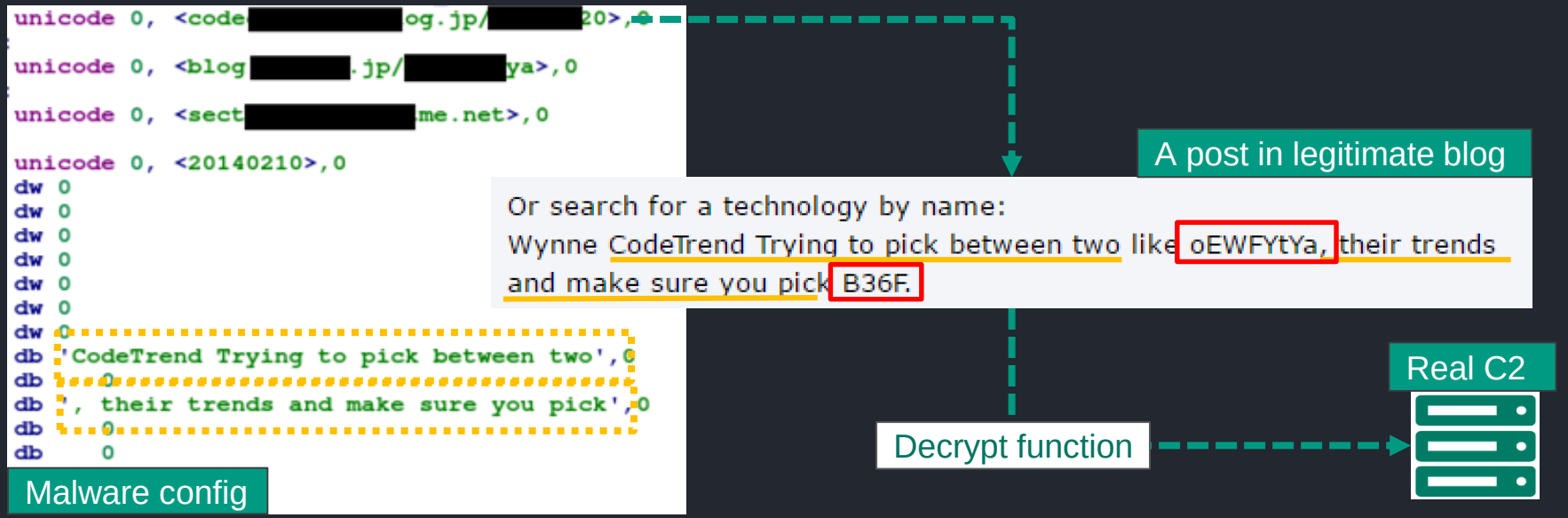
Industries:

1. Government
2. Universities
3. Heavy industry
4. News media
5. Trading
6. Airline
7. Travel agency

Decoys of airline e-ticket

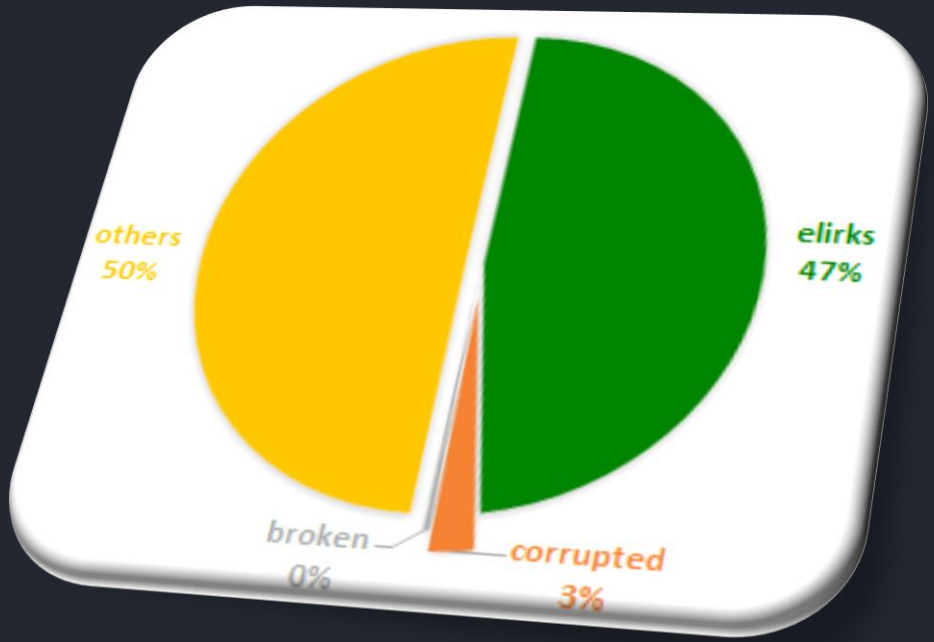
Elirks: Unique schema to connect real C2

The Elirks malware has unique schema to connect real C2. It connects blogpost of legitimate site getting encrypted real C2 information.

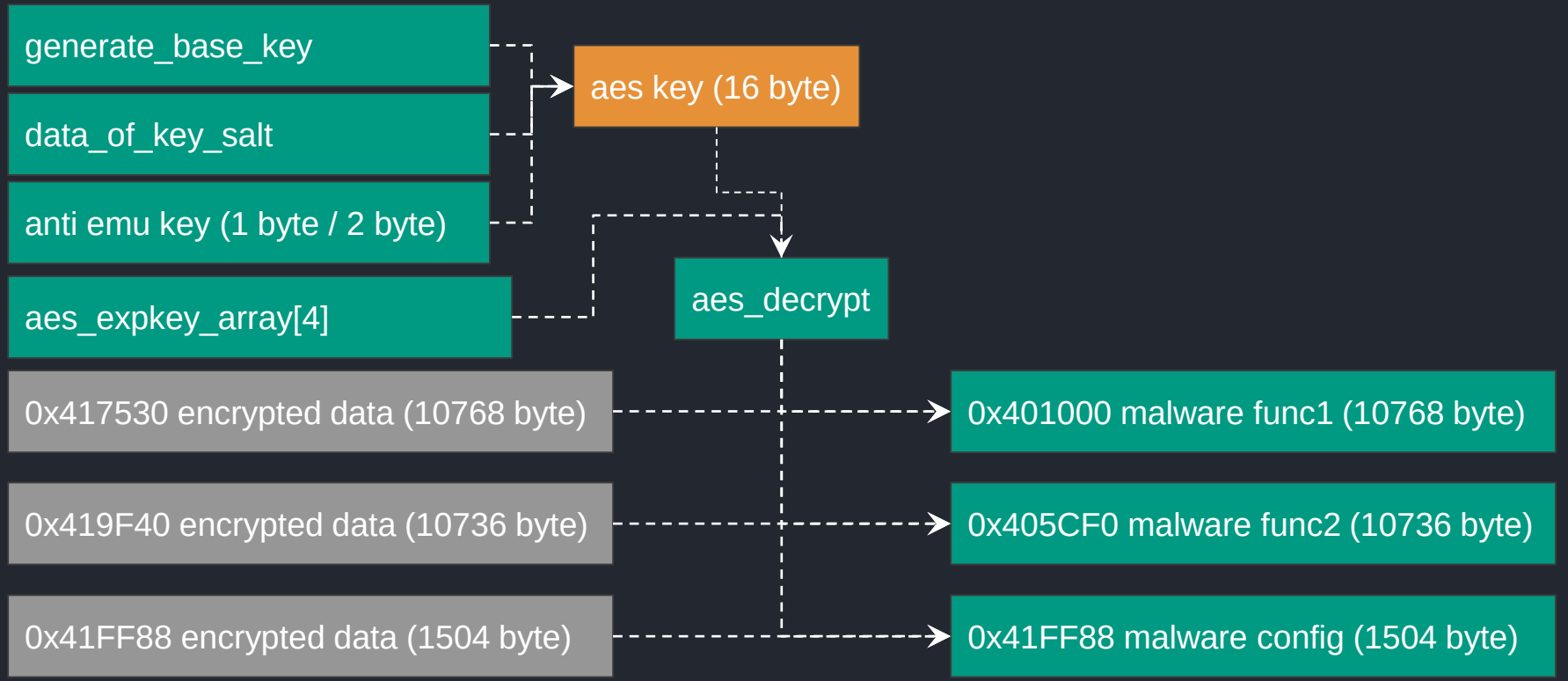


Elirks: Corrupted (?) samples

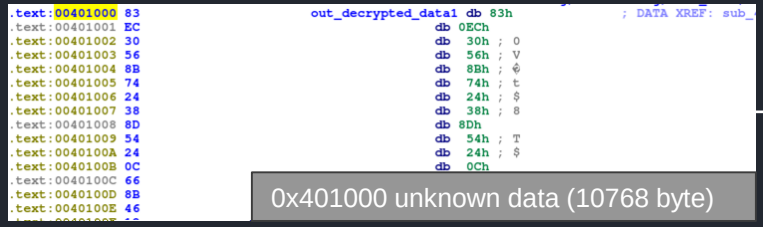
We collected more than 200 samples.
Among them, less than 3 percent were probably corrupted.
Then we confirmed why these samples does not work.

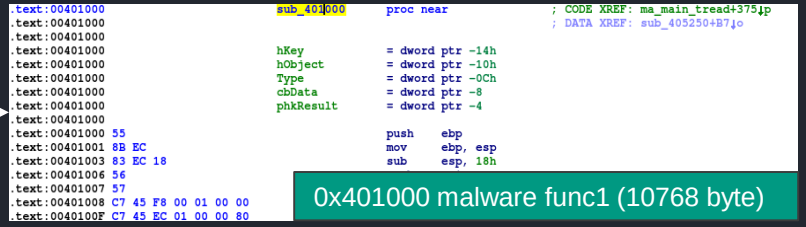


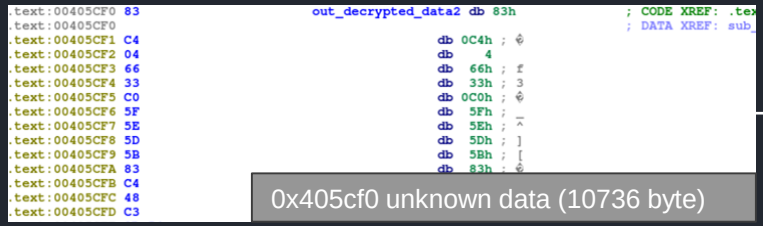
Elirks: Elirks has three encrypted data

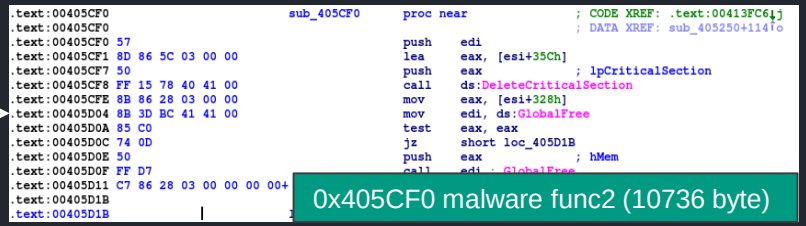


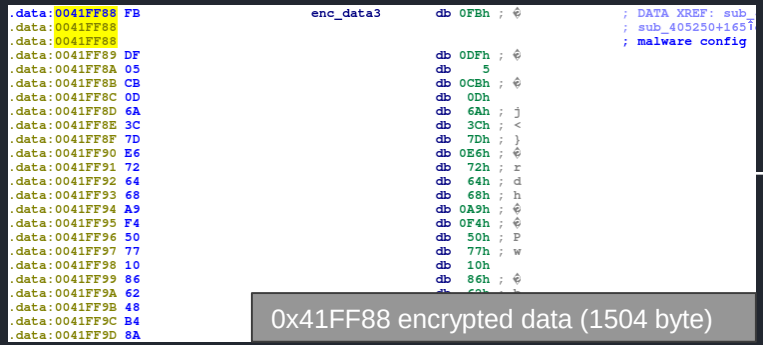
Elirks: Decrypted Elirks

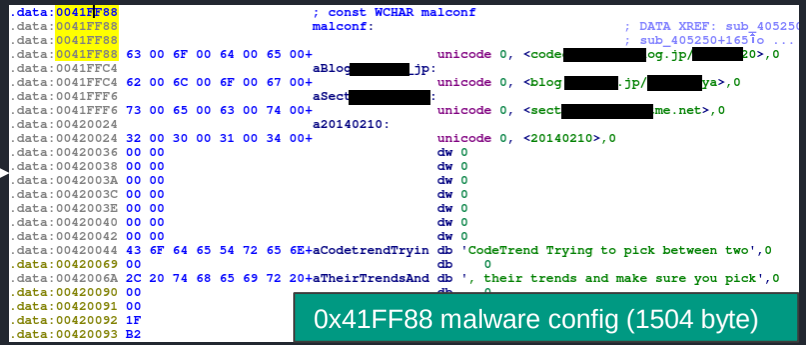












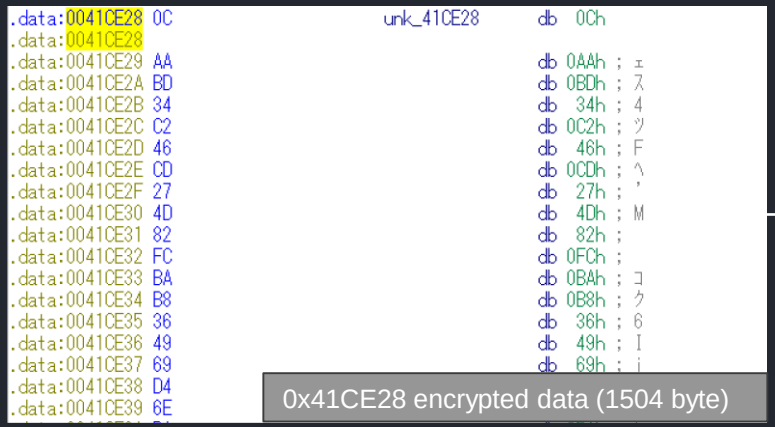
GREAT Global Research & Analysis Team

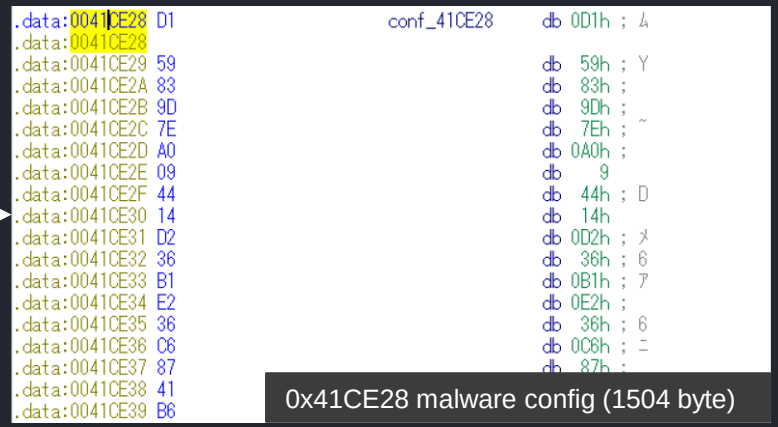
KASPERSKY lab

Elirks: Corrupted (?) samples

A corrupted (?) sample does not decrypt malware config.

That means does not work and can not analyze.





Elirks: DEMO

Elirks probably corrupted (?) sample

Elirks: C~~orrupted (?)~~ ustomized samples

It was customized sample for specific victims

Compare specific dir and current dir to extract 4 bytes xor key as part of generate AES key

aes key (16 byte)

```
.data:0041CE28 0C                      unk_41CE28      db  0Ch
.data:0041CE28
.data:0041CE29 AA                                      db 0AAh ; ｪ
.data:0041CE2A BD                                      db 0BDh ; ｽ
.data:0041CE2B 34                                      db  34h ; 4
.data:0041CE2C C2                                      db 0C2h ; ﾂ
.data:0041CE2D 46                                      db  46h ; F
.data:0041CE2E CD                                      db 0CDh ; ﾍ
.data:0041CE2F 27                                      db  27h ; '
.data:0041CE30 4D                                      db  4Dh ; M
.data:0041CE31 82                                      db  82h ;
.data:0041CE32 FC                                      db 0FCh ;
.data:0041CE33 BA                                      db 0BAh ; ｺ
.data:0041CE34 B8                                      db 0B8h ; ｸ
.data:0041CE35 36                                      db  36h ; 6
.data:0041CE36 49                                      db  49h ; I
.data:0041CE37 69                                      db  69h ; i
.data:0041CE38 D4
.data:0041CE39 6E
```

0x41CE28 encrypted data (1504 byte)

```
.data:0041CE28 ; const WCHAR String
.data:0041CE28 String:                                 ; DATA XREF: .text:00404
.data:0041CE28                                         ; .text:00404516↑o ...
.data:0041CE28                         unicode 0, <210.209.[redacted]>,0
.data:0041CE46                         dw 0
.data:0041CE48                         dw 0
.data:0041CE4A                         dw 0
.data:0041CE4C aSoftwareMicros:
.data:0041CE4C                         unicode 0, <SOFTWARE¥Microsoft¥Windows¥CurrentVe
.data:0041CE4C                         unicode 0, <ORE.EXE>,0
.data:0041CECE aIexplore_exe_l:
.data:0041CECE                         unicode 0, <¥IEXPLORE.EXE.lnk>,0
.data:0041CEF2                         dw 0
.data:0041CEF4                         dw 0
.data:0041CEF6                         dw 0
.data:0041CEF8                         dw 0
.data:0041CEFA aWinTheCompetio db 'win the competion award',0
.data:0041CF12                 db    0
.data:0041CF13                 db    0
.data:0041CF14 aWellKnownForTh db ', well known for the series of',0
.data:0041CF33                 db    0
.data:0041CF34
.data:0041CF35
```

0x41CE28 malware config (1504 byte)

Conclusion

Conclusion: Answer of my title's question

Question: Why corrupted (?) samples in recent APT?

It's not corrupted.
The attacker developed
customized malware

When you find corrupted sample,
It might to be chance of analysis very interesting APT malware

Conclusion: Whitelist approach in APT

Common malware should work in any environment.

APT malware have to work in specific environment.

This approach and introduced new techniques are very simple ,However it works effectively.

Thank You

suguru.ishimaru[at]kaspersky.com