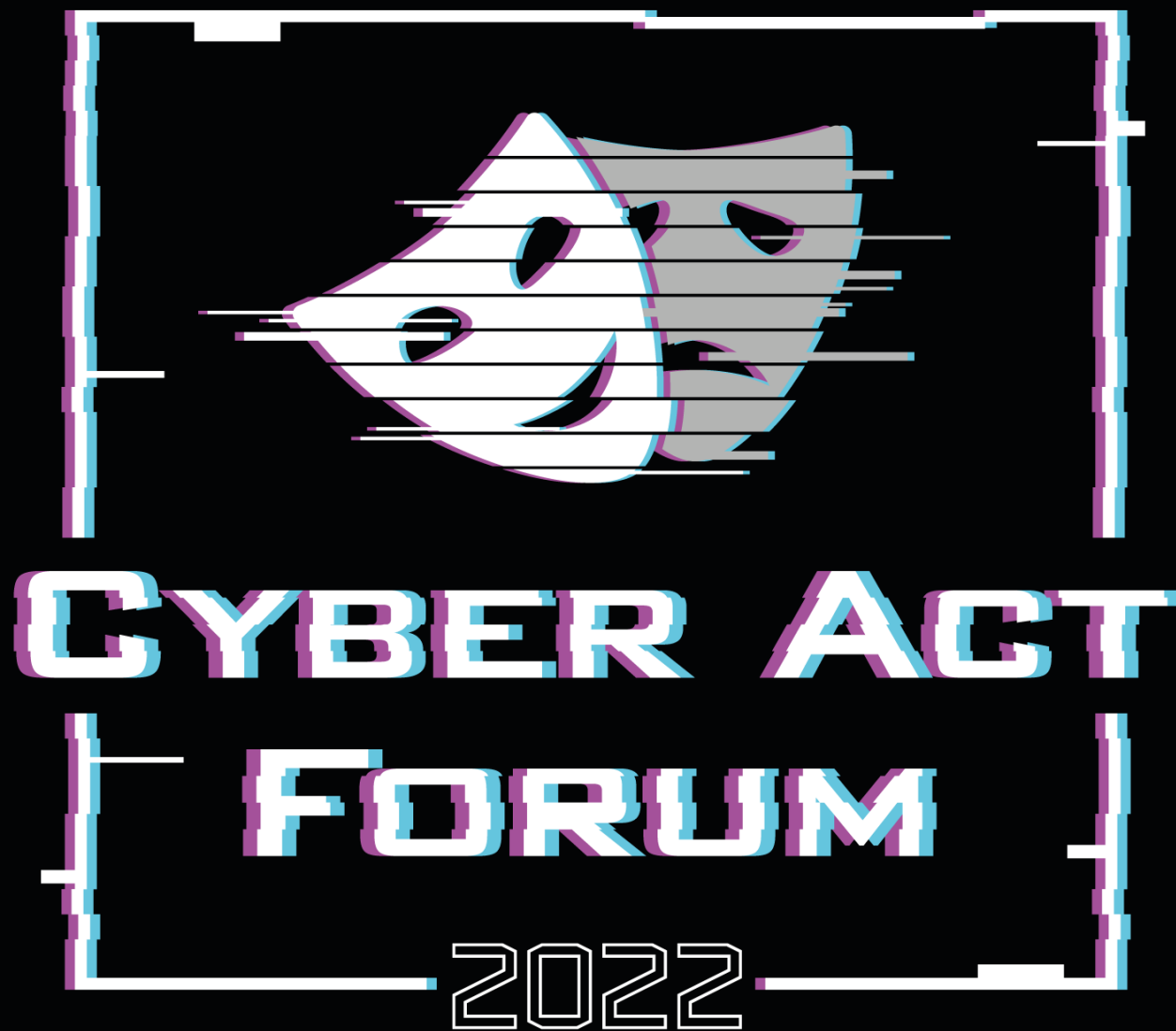




Threat Attribution

Marco Ramilli, PhD





What is
THREAT ATTRIBUTION?

Different meanings

What decision-maker needs

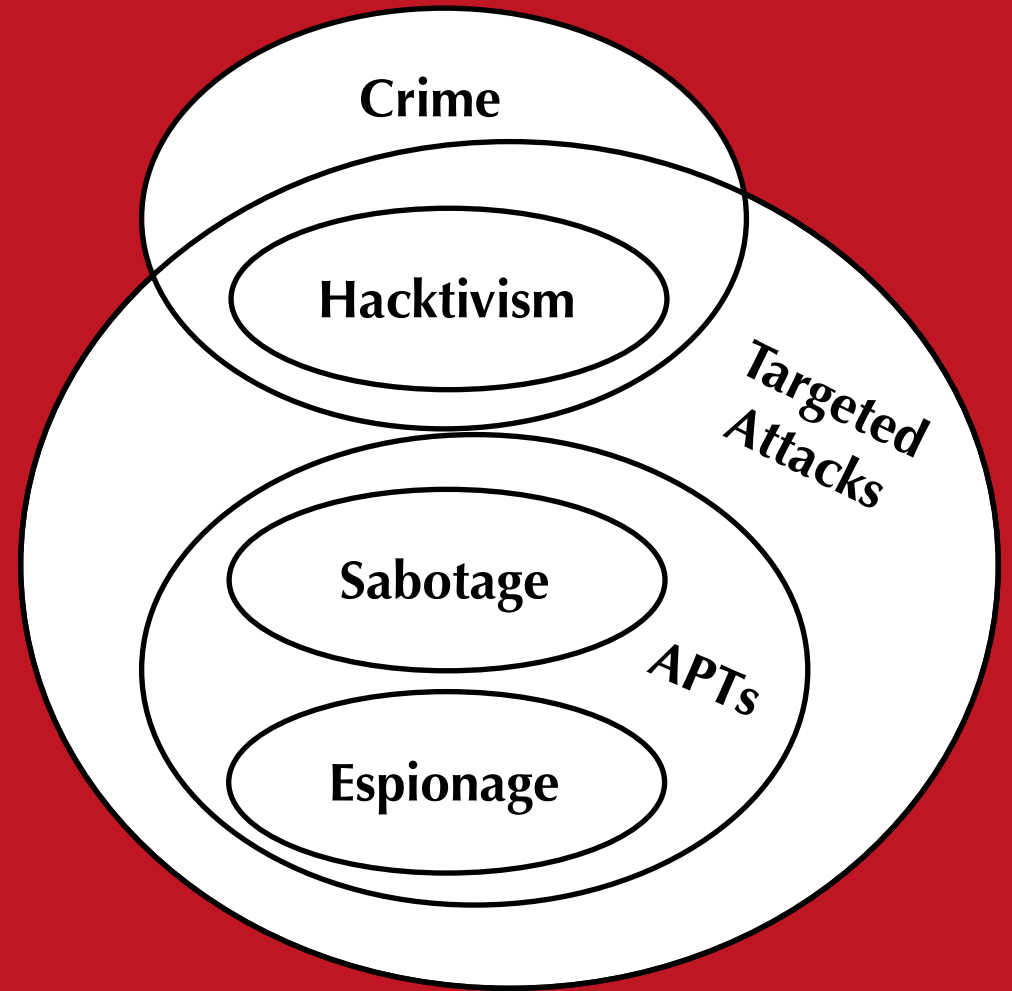
- Attribute to the attacker infrastructure (cutting off, mitigate, eradicate, avoid future attacks)
- Attribute to the man who pressed the keyboard keys (legal activities, countermeasures, employee trust)
- Attribute for the party that is deemed ultimately responsible for the malicious activity (legal implication, political implications, international affairs, activism detection, etc.)

It's not a technical issue

- Technical forensics, human intelligence, signal intelligence, history, geopolitics.
- Every attribution comes with a uncertainty percentage

Why is so important?

To DEFEND yourself



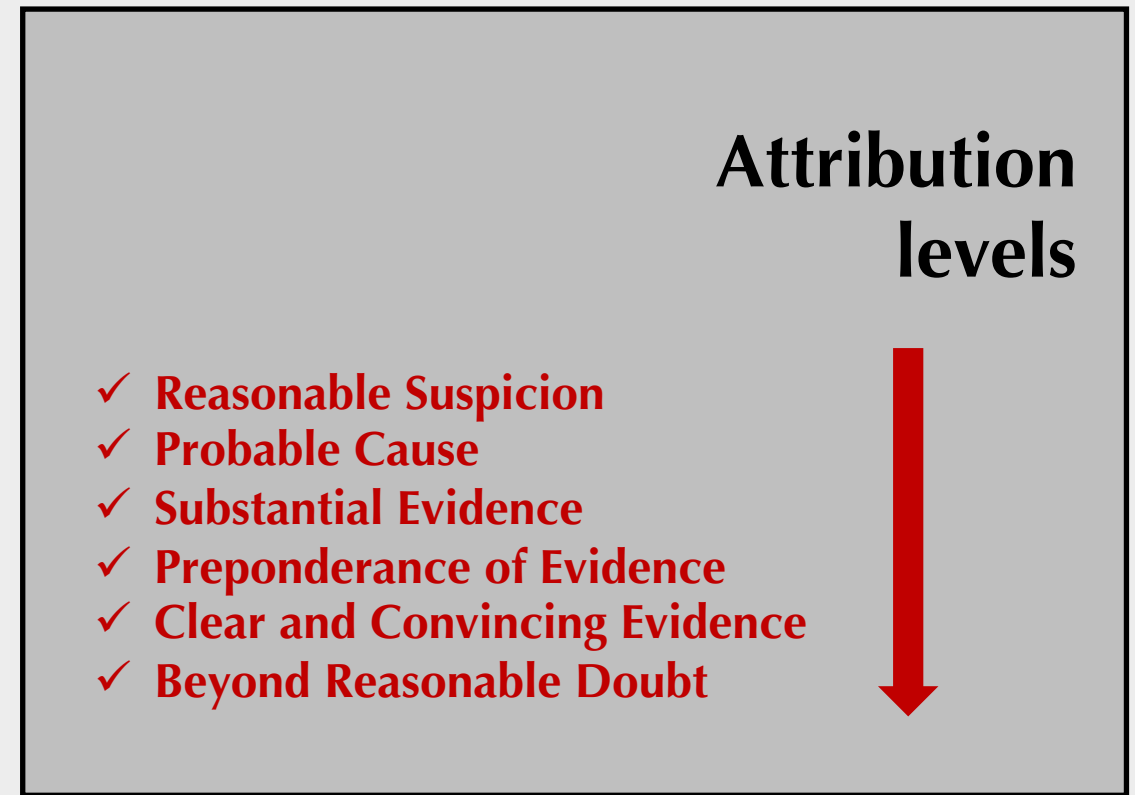
Responsibility



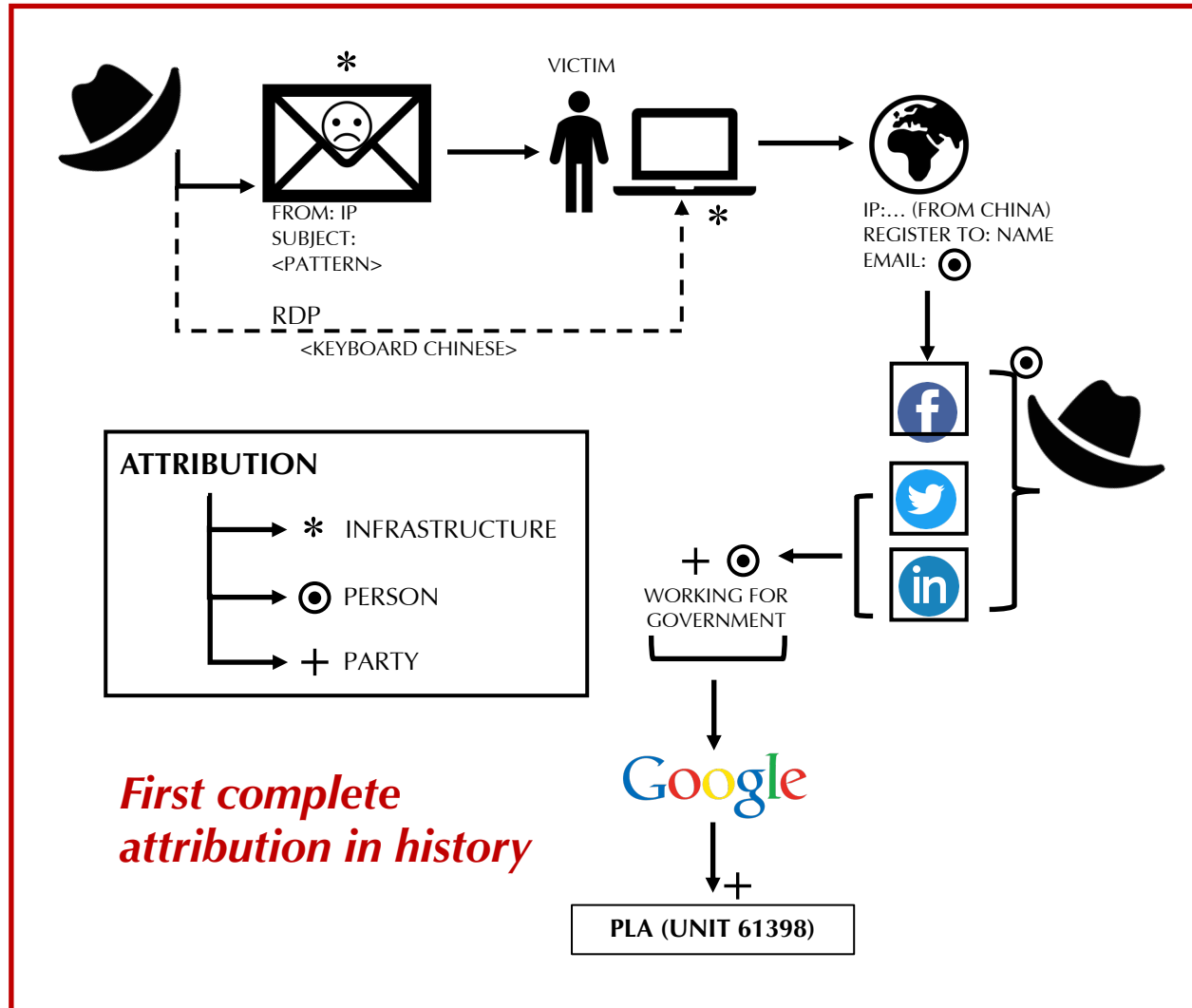
Accountability

Main Attribution Levels

- A «determination» is rarely definitive. God may know who «really» did it, but our determinations of who did it will be associated with some degree of uncertainty or confidence about it.
- The necessary degree of confidence in an attribution judgment depends on the nature of the malicious activity being attributed and the action that is contemplated in its aftermath.



Simple but significative case: APT1 (2013)



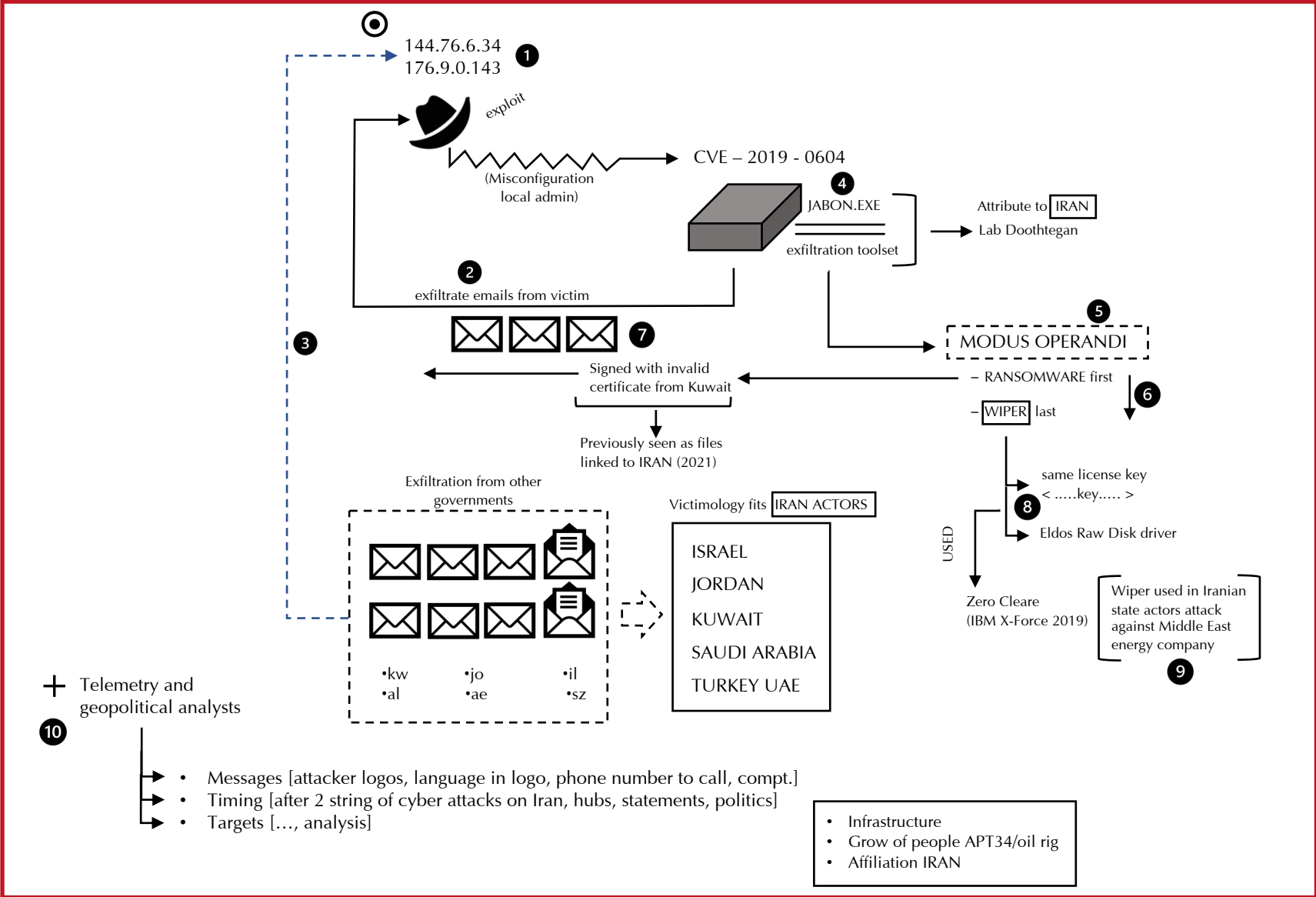
From 2013 many things changed...

- Threat Actors are much more sophisticated
- Many new techniques are used as false flags
- Many Anti Analysis technique have been adopted

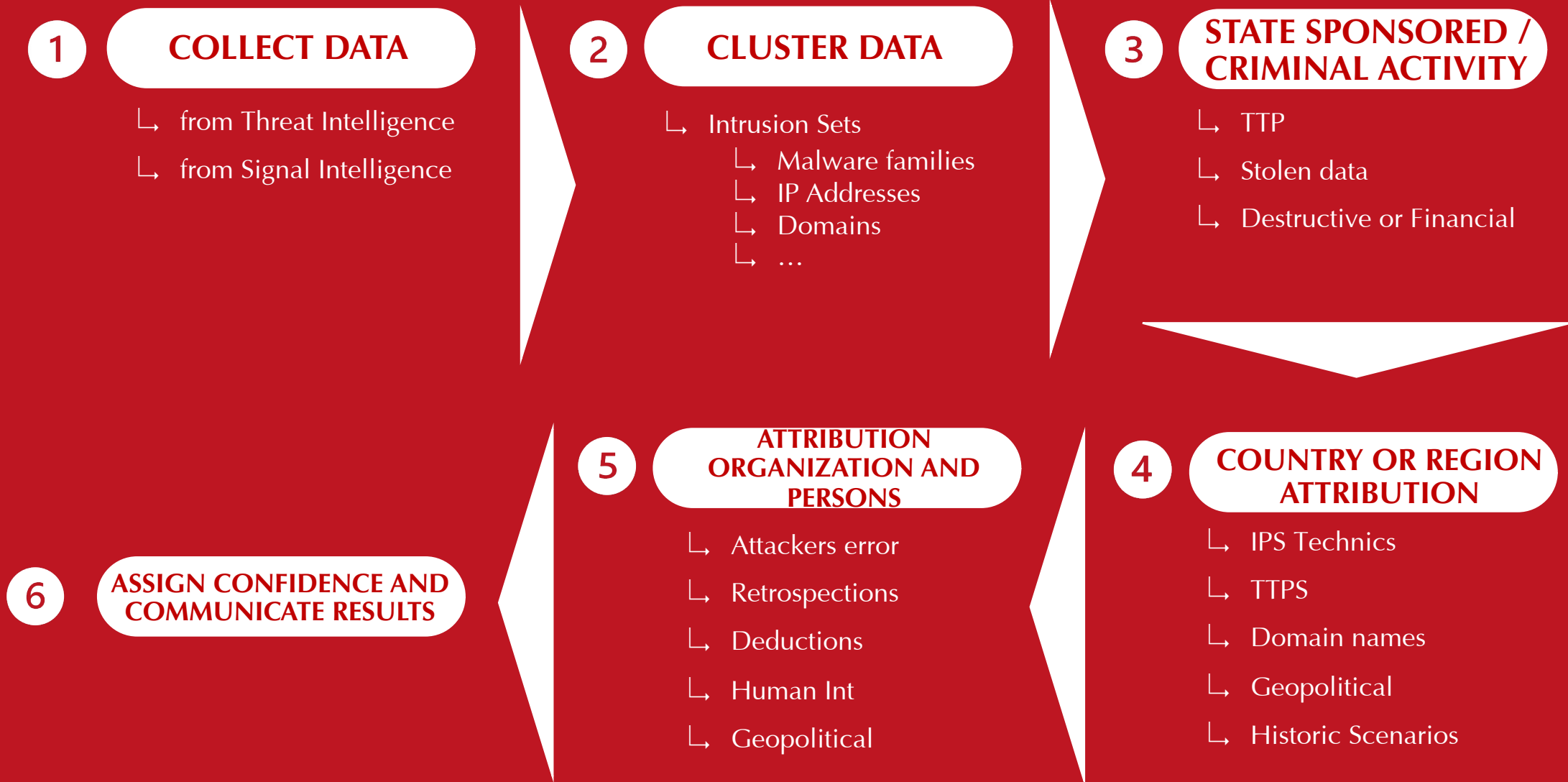
... but still many threat actors behave in the same way

- They like to be identified (Ransom Notes, Splashscreen,..)
- They like to be tracked
- They don't re-write their own code
- They reuse infrastructure

Another case: APT34



Attribution phases



Attribution Framework MICTIC

	ASPECT	EXAMPLE EVIDENCE
M	MALWARE	Language settings, timestamps, hases, strings, functions, behaviour, used libraries
I	INFRASTRUCTURE	Whois data, links, host, domain names, url, cdn patterns
C	CONTROL SERVERS (COMMAND & CONTROL)	Source code, logs, sized hard drives, memory swapping, installed software
T	TELEMETRY	Working hours, malware generations, social engineering, email campaigns
I	INTELLIGENCE	Intercepted Communication, IoCs, Certificates
C	CUI BONO	Geopolitical analysis, History, International Affairs, International partnerships

MALWARE: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Code similarity	Crypto implementation C&C protocol Obfuscation techniques Code reuse	Clustering Clustering Clustering Clustering
Contro Servers	Domains Ips Url Patterns	Clustering Clustering Clustering
Rich Header	Environment Setup Environment Similarities Environment Diversities	Clustering Clustering Clustering
Linker and Compiler Timesteps	Time zones Working weeks Unusual holidays	Country Country Country
PDB Path	Naming patterns Project names OS language Person or organization names	Clustering Clustering Country Person or Organization
Language Sources	Codepage IDs	Country
Strings	Keywords Language Grammatical characteristics	Clustering Country Country

INFRASTRUCTURE: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Public Information	Timestamps RDP configuration Source Ips (attacker connections) C&C patterns Source IP (victimology/cui bono) Private surfing	Clustering Clustering Clustering Clustering Clustering
Active Scanning	Certificates Banners Handshakes Directories and Files	Clustering Clustering Clustering Clustering
Additional Analysis	Certificate timestamps Whois overlap to non-attacker websites pDNS overlap with non-attacker websites	Country Organization and Person Organization and Person

C2: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Network traffic	Timestamps RDP configuration Source Ips (attacker connections) C&C patterns Source IP (victimology/cui bono) Private surfing	Country Country Country, Organization Clustering Person Person
Hard Disk	Scripts (comments, function names,..) GUI Language OS Configuration Access logs (attacker connections) Access logs (victimology) Malware samples Tools Target lists notes, manuals Self-infection of attacker Source code Installed libraries	Clustering, organization Country Country Country, organization Country Clustering Clustering Country, organization Country, organization, persona Country Clustering

TELEMETRY: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Samples	Malware Attribution	All
Prevalence	Regions, Actors	Country
Co-occurrence	Other malware and tools, legitimate software of machine	Clustering Country
Behaviour	Code similarity TTPS C&C addresses Timestamps	Clustering Clustering Country Country
Previous Attribution	Other malware and tools attributed to	Clustering and Organization

INTELLIGENCE: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
OSINT	See Geopolitical Aspect	All
General SIGINT	Communication about tasking, contact, information	Organization, person
Cyberspecific SIGINT	Traffic from victim Trojan horse Traffic to C2 Telecommunication providers	Country Organization Organization Organization
HUMINT	Recruiting sources close to operation Recruiting intelligence consumers	Organization, person Organization
Offensive Operations	C2 servers Home-networks of attackers Telecos providers	Organization Person, organization Organization
Request to Providers	Email and chat communication Login logs C2 servers	Organization, person All All

CUI BONO: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Political News	Summits Negotiations Strategic events Domestic conflict International conflicts	Country Country Country Country Country
Economic News	Strategies on economic growth Trading agreements Stock status Investments on specific regions or sectors	Country Country Country Country Country
Agencies Mission	Laws Unit names and designators Job posting Reports on achievements Research papers Won grants	Organization Organization Organization Organization Organization Organization



our credo in YOROI

Defence
belongs
to humans



YOROI
SECURITY



La presenza Yoroi nel mondo dei Social Media e nella Blogosfera

Linkedin



Youtube



Twitter



Blog Yoroi



Blog M. Ramilli



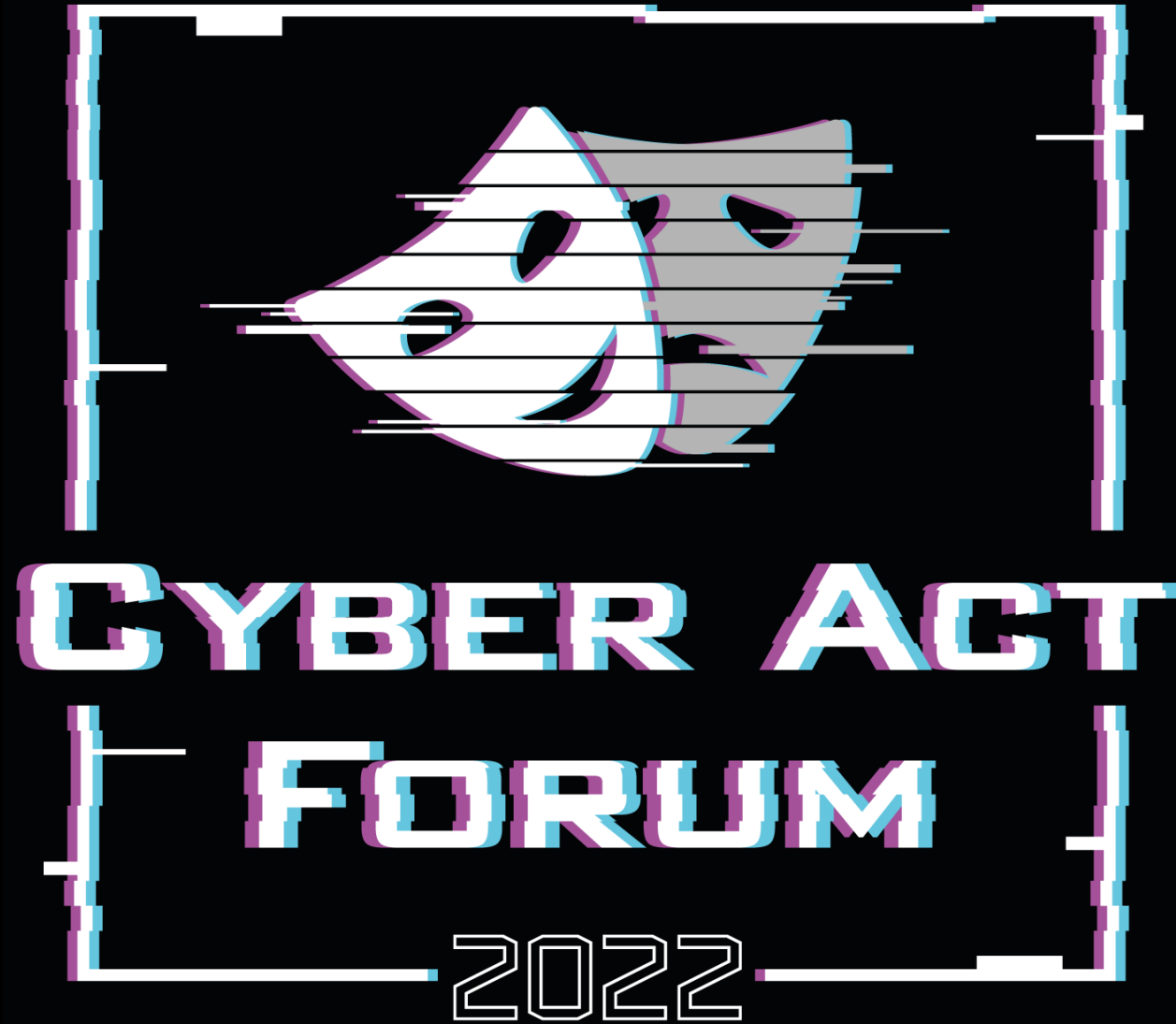
Yoroi® è un marchio registrato | Registrazione N°: 016792947





TINEXTA GROUP

yoroi.company



Case Study: Chinese APT



```
6E 74 65 72 Parameters\Inter
72 61 63 74 active).Interact
56 61 6C 75 ive.RegQueryValu
7E 73 5C 70 eEx(Parameters\p
72 61 6D 00 rogram).program.
6E 74 43 6F SYSTEM\CurrentCo
76 69 63 65 ntrolSet\Service
6E 72 73 00 \*\*\Parameters
7E 65 00 00 SvcHostDLL.exe
0A 00 00 00 sleep...exit...
6E 69 6C 65 read remote file
6E 69 6C 65 error!#...file
64 21 23 00 download end!#.
64 61 74 61 downend.downdata
2E 64 00 00 ....datasize%d .
```

dargoner

化变为题

积分: 6

贴数: 5

日期 2005-3-10 8:35:50

```
#include <stdio.h>
#include <windows.h>
#include <time.h>
```

```
#define DEFAULT_SERVICE "IPREP"
#define MY_EXECUTE_NAME "SvcHostDLL.exe"
```

```
//main service process function
void __stdcall ServiceMain( int argc, wchar_t* argv[] ):
```

2005 posting of similar source code,
includes poster's handle.

Case Study: Chinese APT

#define MY_EXECUTE_NAME "SvcHostDLL.exe"

Search

About 426 results (0.56 seconds)

[Advanced search](#)

Tip: [Search for English results only](#). You can specify your search language in [Preferences](#)

[svchostdll.rar svchostdll.cpp](#)

... #define DEFAULT_SERVICE "IPRIP" #define MY_EXECUTE_NAME "SvcHostDLL.exe"
DWORD ... see svchostdll.h for the class definition CSvchostdll.CSvchostdll() ...
[read.pudn.com/downloads54/sourcecode/.../svchostdll.cpp_.htm](#) - [Cached](#)

[SvcHostDll.dll--补天论坛::补天网::Patching.net::0day-exploits::网...](#)

Mar 10, 2005 ... #define DEFAULT_SERVICE "IPRIP" #define MY_EXECUTE_NAME
"SvcHostDLL.exe" //main service process function void __stdcall ServiceMain(int ...
[www.patching.net/bbs/viewdoc_43201_2.html](#) - [Cached](#) - [Similar](#)

[svchost难题，请高手清进- VC/MFC / 进程/线程/DLL - \[Translate this page \]](#)

2006年7月12日 ... #define DEFAULT_SERVICE "IPRIP" #define MY_EXECUTE_NAME
"SvcHostDll.exe" HANDLE hDll=NULL; SERVICE_STATUS_HANDLE hSvc, DWORD
dwCurrState; ...
[topic.csdn.net/t/20060712/01/4874487.html](#) [China](#) [Cached](#)

[svchost 服务怎么写? - \[Translate this page \]](#)

8 posts - 5 authors - Last post: Jun 25, 2009

... #define DEFAULT_SERVICE "IPRIP" #define MY_EXECUTE_NAME "SvcHostDLL.exe"
__declspec(dllexport) void __stdcall ServiceMain(int argc, ...
[topic.csdn.net/.../521632*b-abe3-4197-bbf6-9417592b7e7c.html](#) - [China](#) - [Cached](#)

[Show more results from topic.csdn.net](#)

[XFOCUS Security Forums -> Re: bingle 请进，关于哪个svchost启动服...](#)
[务...](#) [Translate this page]

#define MY_EXECUTE_NAME "SvcHostDll.exe" HANDLE hDll=NULL,
SERVICE_STATUS_HANDLE hSvc, DWORD dwCurrState; void __stdcall ServiceMain(int
argc, wchar_t* ...
[https://www.xfocus.org/bbs/index.php?act=SE&f=3&t=60693&p...](#)

Case Study: Chinese APT

```
00 6D 73 65 77 6D 76 00 %s\%s.%s.msewnv.
6C 6C 51 2F 34 2E 30 20 200.Mozilla/4.0
62 6C 55 3B 20 4D 53 49 (comPatIble; MSI
69 6E 54 6F 77 73 20 4E E 9.0; Windows N
4E 45 54 20 43 4C 52 28 T 8.8; .NET CLR
29 00 57 54 68 74 74 70 1.1.4322).WTh:tp
2F 25 54 25 30 34 64 00 ://%s:%d/%d%04d.
64 61 74 00 44 65 66 61 %s\%05d.dat.Defa
74 61 31 00 50 72 6F 68 alt.WinStat1.Floc
0D 0A 25 73 20 25 73 0D eee0427 %e %e
64 2D 25 30 32 64 2D 28 ... [%04d-%02d-%
3A 25 30 32 64 3A 25 30 02d %02d:%02d:%0
5B 46 31 31 5D 00 00 00 2d].hke.[F11]...
5B 46 31 32 5D 00 00 00 [F9]....[F12]...
5B 46 38 5D 00 00 00 00 [F10]...[F8]....
5B 46 37 5D 00 00 00 00 [F5]....[F7]....
5B 46 34 5D 00 00 00 00 [F6]...[F4]....
```

Format Strings are written by humans
so great opportunity for uniqueness

Case Study: Chinese APT

```
6E 6B 6E ivileqe. ...Unkn
00 00 00 own type! ....
44 2D 52 Ramdisk ....CD-R
69 6E 64 OM .Remote .find
20 00 00 %c:\ %dM/%dM ..
6E 61 62 Removable ..Unab
6E 65 2E le to determine.
79 73 74 ...%c:\....syst
75 73 65 en mem: %dM use
46 69 6C d: %d%% PageFil
25 64 4D e. %dM free. %dM
77 65 72 ...System Power
68 6F 75 on time: %f hou
6E 65 20 re.....machine
63 2E 0A type: maybe pc..
79 70 65 ....machine type
70 21 0A : maybe Laptop!..
6F 6E 3A .....version:
69 6C 64 %s v%d.%d build
73 20 6F %d%s...Win32s o
00 00 00 n Windows 3.1
```

- Logging Strings such as:
 - "Unable to determine"
 - "Unknown type!"
- Reveals source code reuse! (BO2k)

Case Study: Chinese APT

Google code search Search [Advanced Code Search](#)

labs

Code

[boxp_beta7/srv_system/main.h](#) - 1 identical

```
81: char *sRplmeminfo; // Reply: "Memory: %dM in use: %d%% Page file: %dM free: %dM\n"
82: char *sRplerrdisk; // Reply: "Unable to determine.\n"
83: char *sRpldiskrmv; // Reply: "Removable\n"

87: char *oRpldiskram; // Reply: "Ramdisk\n"
88: char *sRpldiskuk; // Reply: "Unknown type!\n"
89: char *sRpldiskinfo; // Reply: " Bytes free: %u MB(%s)/%u MB(%s)\n"
```

[prdownloads.sourceforge.net/boxp/boxp_beta7_src.zip](#) - GPL - C - [More from boxp_beta7_src.zip](#) »

[boxp_beta6/srv_system/cmd_system.cpp](#) - 1 identical

```
510: case 0:
511:     api->plstrcat(svReply, "Unable to determine.\n");
512:     break;

548: default:
549:     api->plstrcat(svReply, "Unknown type!\n");
550:     break;
```

[prdownloads.sourceforge.net/boxp/boxp_beta6_src.zip](#) - LGPL - C++

[srv_system/cmd_system.cpp](#) - 2 identical

```
334: case 0:
335:     lstrcat(svReply, "Unable to determine.\n");
336:     break;

360: default:
361:     lstrcat(svReply, "Unknown type!\n");
362:     break;
```

[prdownloads.sourceforge.net/bu2k/bu2kdev_src_1-1-1.zip](#) - LGPL - C++

Logging Strings such as:

- "Unable to determine"
- "Unknown type!"

Reveals source code reuse! (BO2k)

Case Study: Chinese APT

5C 25 73 00 00 00 C0	\Services\s....
2E 25 73 00 00 00 C0	rb..%s%\s.%s....
41 59 00 44 65 66 61	tmp.DISPLAY.Defa
61 30 00 50 4F 53 54	ult.WinSta0.POST
00 00 00 4D 6F 7A 69	%d%s....Mozi
63 6F 6D 70 61 74 69	lla/4.0 (compati
20 36 2E 30 3B 20 57	ble: MSIE 6.0; W
20 35 2E 30 3B 20 2E	indows NT 5.0; .
2E 31 2E 34 33 32 34	NET CLR 1.1.4324
74 2E 75 69 64 00 66	...v\smr...uid.f
00 20 00 68 6B 65 C0	PsKey400...hke.
30 30 30 31 2E 74 6D	...f...001.tm
00 00 00 25 73 5C 73	p...%s%\s...%s\s
65 20 2D 6B 20 6E 65	vchost.exe -k ne
63 68 65 64 75 6C 65	tsvcs...Schedule

73 6	10006A1F	call _CreateMutexA:
65 5	10006A1F	mov eax,dword ptr [ebp+0x24]
67 6	10006A22	add esp,0x14
6F 7	10006A25	shr eax,1
72 7	10006A27	push 0x10013F0:lpName_PsKey400
00 0	10006A2C	push 0x0:bIn...
	10006A2E	push 0x0:lpMutexAttributes
	10006A30	mov ebx,0x1
	10006A35	mov dword ptr [ebp+0x24],eax
	10006A38	call dword ptr [0x100100D8] // __imp_KERNEL32.dll!CreateMutexA[000120D6]

Mutex names remain consistent at least for one infection-push, as they are designed to prevent multiple-infections for the same malware.

Mutex remain consistent since they need to prevent multiple infections

Case Study: Chinese APT

Copyright and Version Strings

- OpenSSL/0.9.6...
- RAND part of OpenSSL 0.9.8e 23 Feb 2007
- MD5 part of OpenSSL 0.9.8k 25 Mar 2009
- libdes part of OpenSSL 0.9.7b 10 Apr 2003
- inflate 1.2.1 Copyright 1995-2003 Mark Adler
- inflate 1.1.4 Copyright 1995-2002 Mark Adler
- inflate 1.2.3 Copyright 1995-2005 Mark Adler
- inflate 1.0.4 Copyright 1995-1996 Mark Adler
- inflate inflate 1.1.3 Copyright 1995-1998 Mark Adler
- inflate 1.1.2 Copyright 1995-1998 Mark Adler
- inflate 1.2.2 Copyright 1995-2004 Mark Adler



Case Study: Chinese APT

- Every new version of zlib has a unique pattern of bits in the data tables – these are modified for each version specifically
- This pattern is a data constant and can be used even if the copyright notices have been removed

<http://www.enyo.de/fw/security/zlib-fingerprint/zlib.db>

Case Study: Chinese APT

- Not as specific as zlib patterns but can be used to detect the inflate decompressor

<http://www.enyo.de/fw/security/zlib-fingerprint/inflate.db>



Case Study: Chinese APT

FindKernel32:

pushad

and esi, 0FFFF0000h
mov ecx, 100h

Mask off ESI to a page boundary

FK32_Loop:

call TryAddress
jnc FK32_Success
sub esi 010000h
loop FK32_Loop

Load ECX w/ a length to scan backwards from

FK32_Hardcodes:

mov esi, KERNEL32_WIN9X
call TryAddress
jnc FK32_Success

Subtract, try again

mov esi, KERNEL32_WINNT
call TryAddress
jnc FK32_Success

Try a bunch of hard coded offsets if the scan fails

mov esi, KERNEL32_WIN2K
call TryAddress
jnc FK32_Success

mov esi, KERNEL32_WINME
call TryAddress
jnc FK32_Success

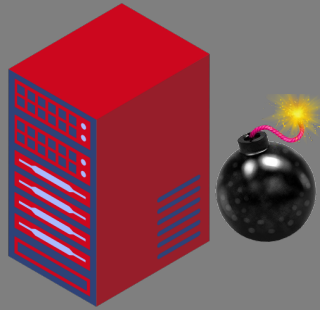
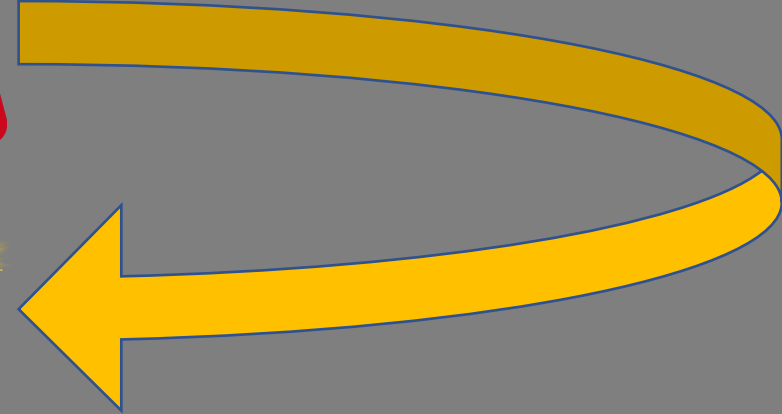
FK32_Fail:

popad
stc
ret

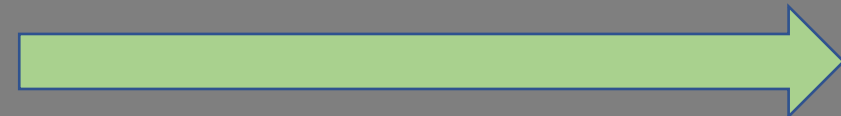
FK32_Success:

mov [ebp + Kernel32], esi
popad
clc
ret

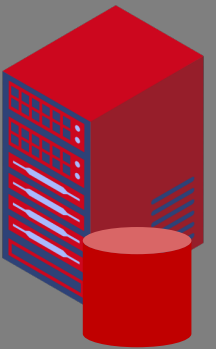
Case Study: Chinese APT



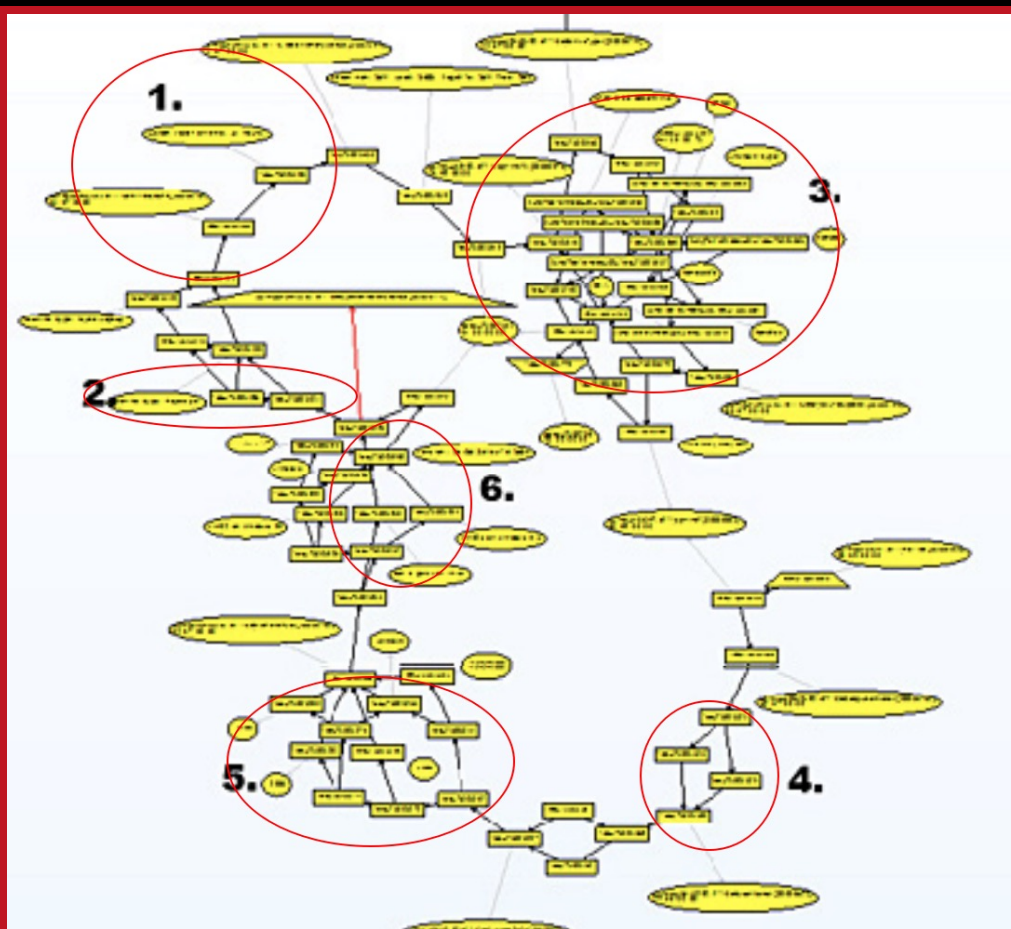
Once installed, the malware phones home...



TIMESTAMP	SOURCE COMPUTER USERNAME	
VICTIM IP	ADMIN?	OS VERSION
HD SERIAL NUMBER		



Case Study: Chinese APT



1. This queries the uptime of the machine...
2. Checks whether it's a laptop or desktop machine...
3. Enumerates all the drives attached to the system, including USB and network...
4. Gets the windows username and computername...
5. Gets the CPU info
6. and finally... the version and build number of windows.

Case Study: Chinese APT

Call IsDebuggerPresent

– Or, read offset 2 from the PEB structure

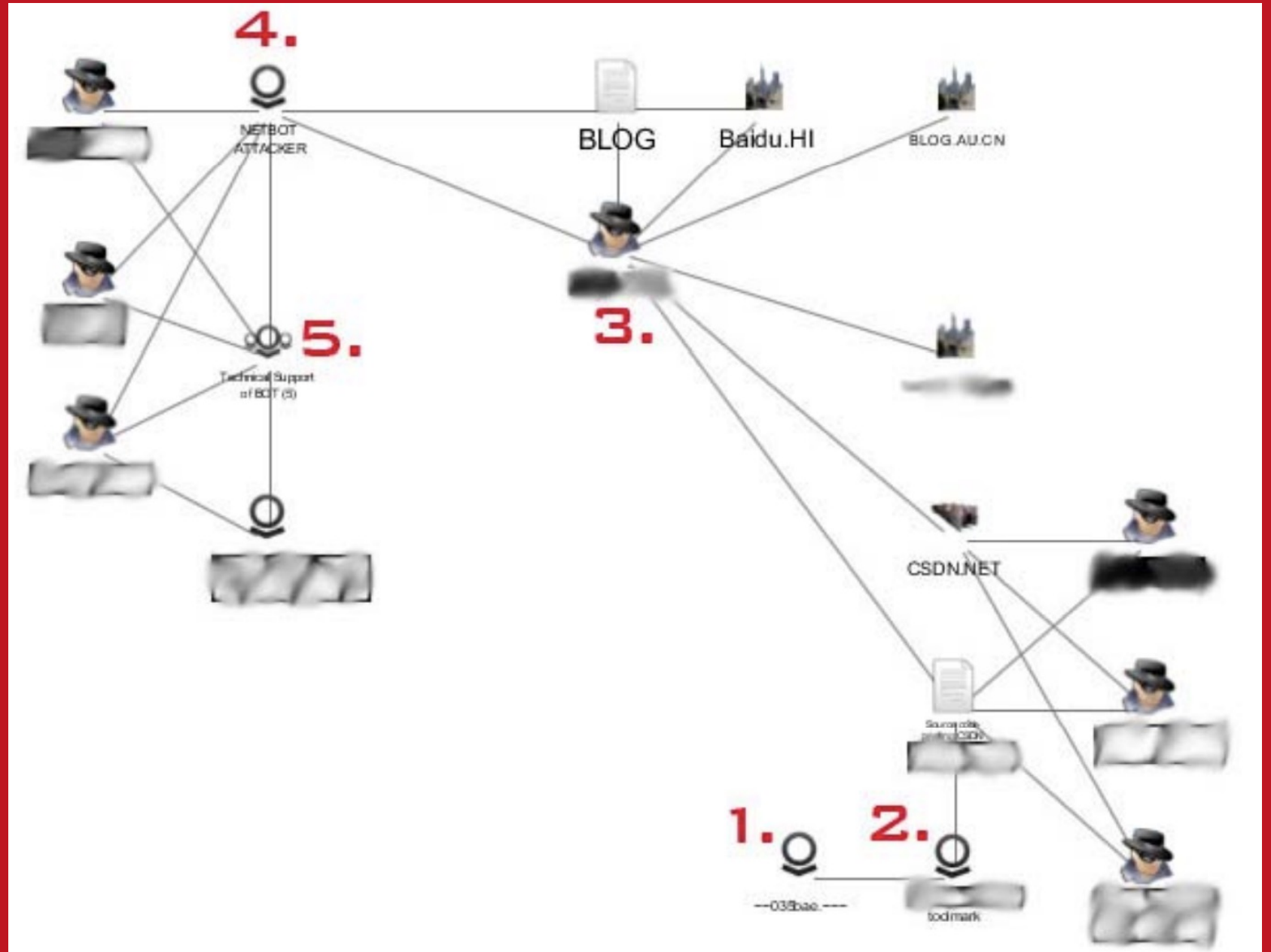
```
mov eax, fs:[30h]
mov eax, byte ptr [eax+2]
test eax, eax
jnz __found_debugger
```

Check the Heap Manipulation Flags in NtGlobalFlags

```
FLG_HEAP_ENABLE_TAIL_CHECK,
FLG_HEAP_ENABLE_FREE_CHECK,
FLG_HEAP_VALIDATE_PARAMETERS
```

Heap Flags, not the same as NtGlobalFlags NtGlobalFlags but affected by the use of
FLG_HEAP_*





Clustering Collections

- Large number of samples
- Need to group self-similar items into “clusters”
 - Like a “ts range att t” rac or”

From the cluster, perform link analysis into social cyberspaces to find “participants”

 Some participants may “resolve” into a developer, user, or other archetype