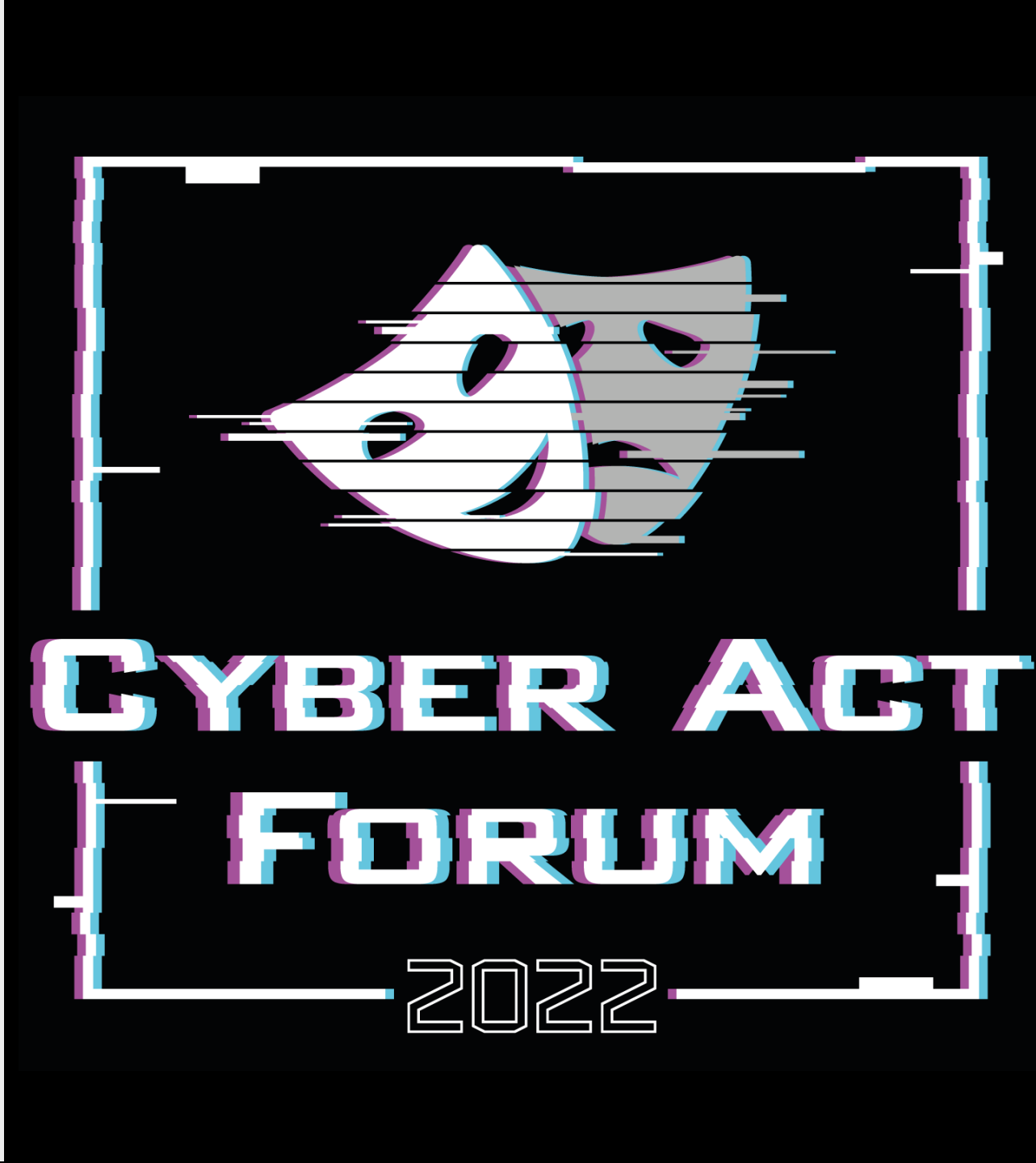
YOROI®

TINEXTA GROUP

Threat Attribution

Marco Ramilli, PhD



What is THREAT ATTRIBUTION?

Different meanings

What decision-maker needs

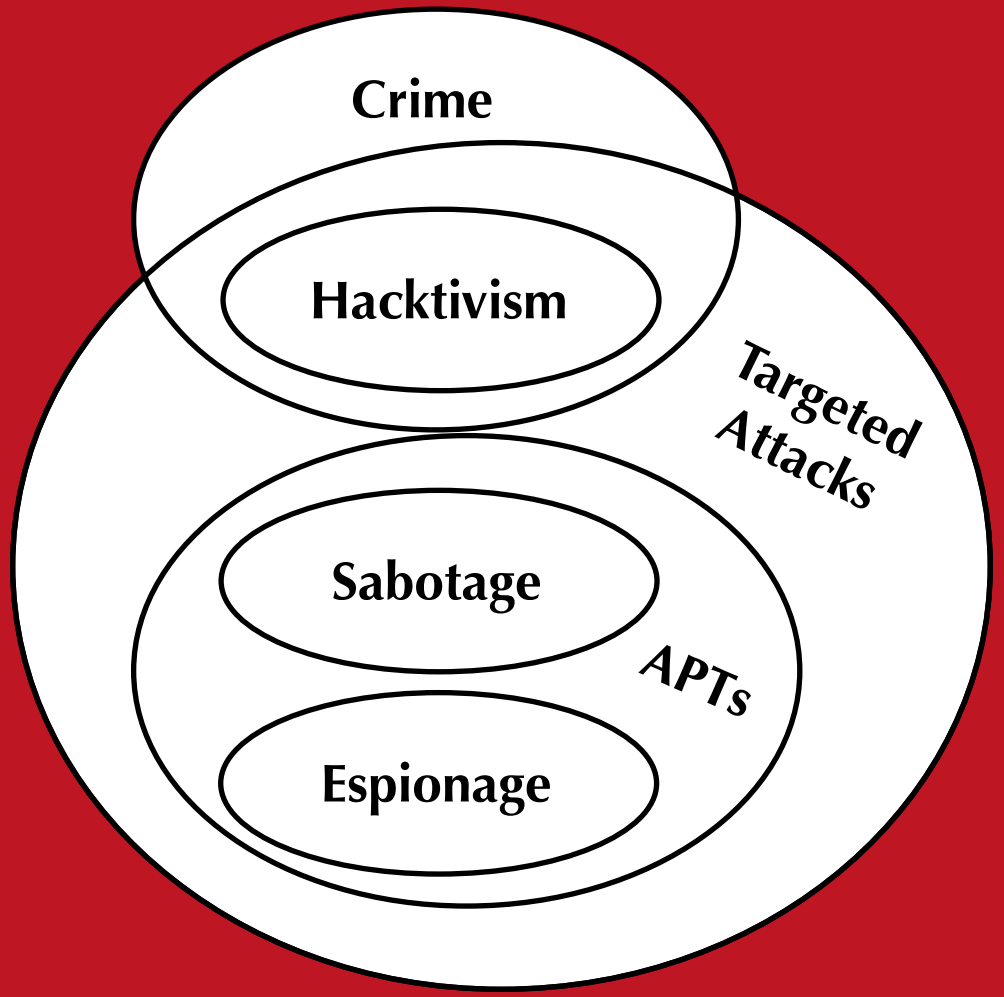
- Attribute to the attacker infrastructure (cutting off, mitigate, eradicate, avoid future attacks)
- Attribute to the man who pressed the kyboard keys (legal activities, contermeasures, employee trust)
- Attribute for the party that is deemed ultimately responsible for the malicious activity (legal 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 uncertanty percentage

Why is so important?

To DEFEND yourself



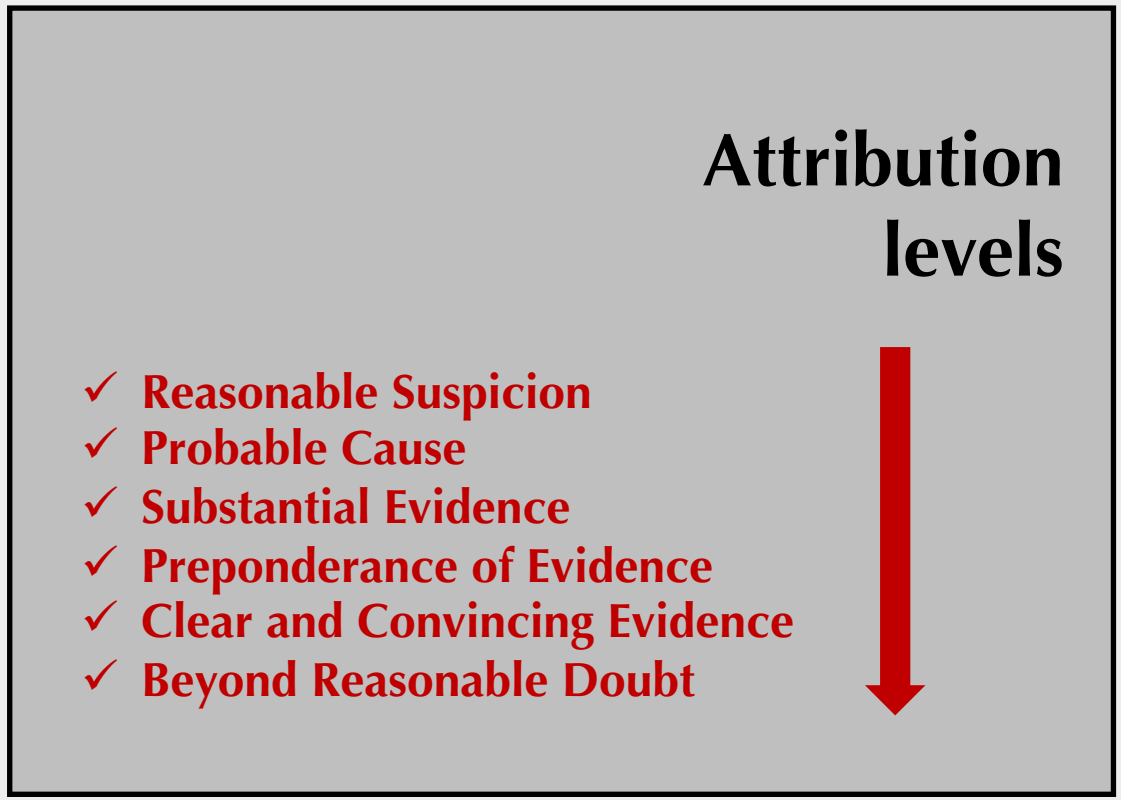
Responsibility

Accountability

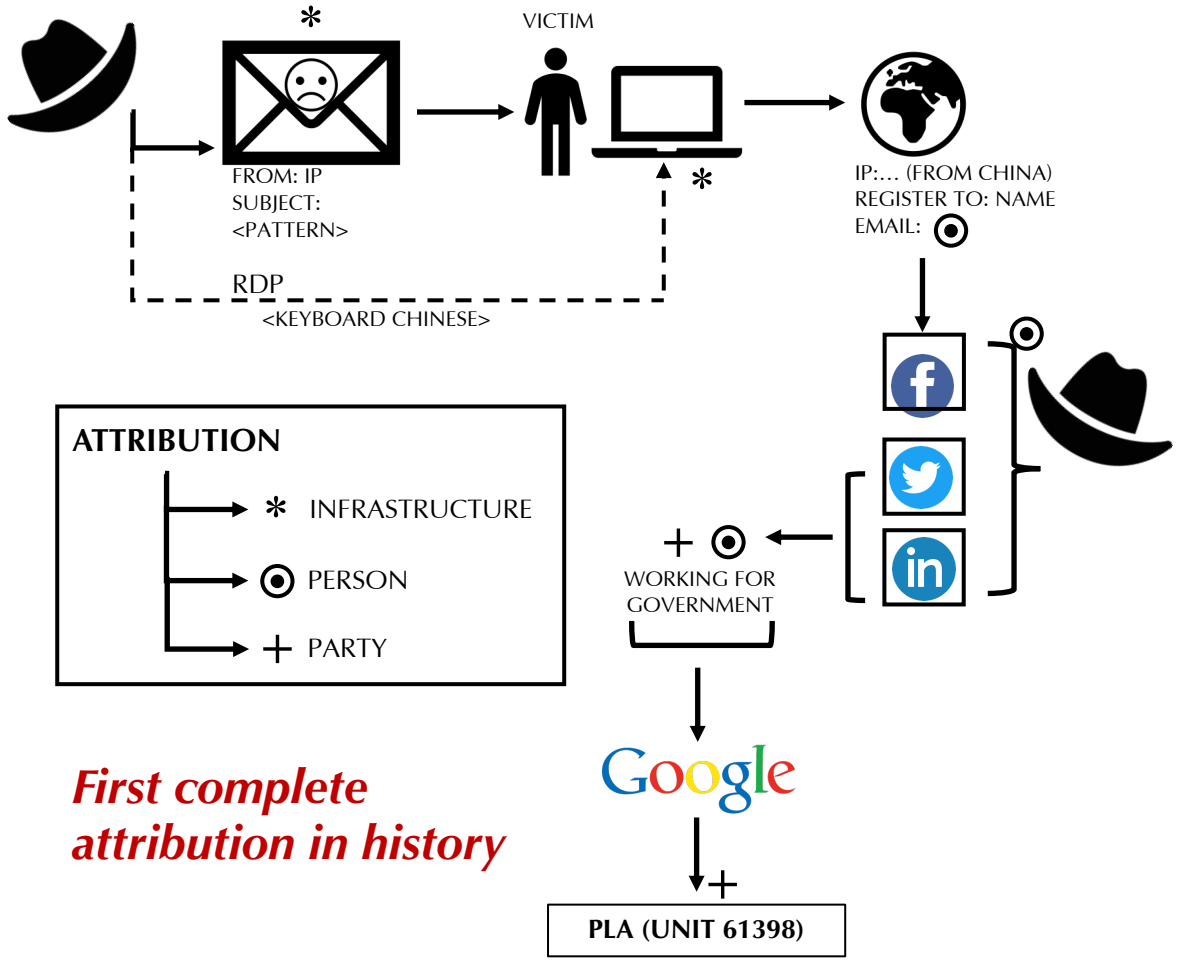
Main Attribution Levels

- A «determination» is rarely definitive. God may know who «really» did it, but our determinations of who did it will be associate with some degree of uncertainty or confidence about it.

- The necessary degree of cnfidence in an attribution judgment depends on the nature of the malicious activity bein attributed and the action that is contemplated in its aftermath.



Simple but significative case: APT1 (2013)



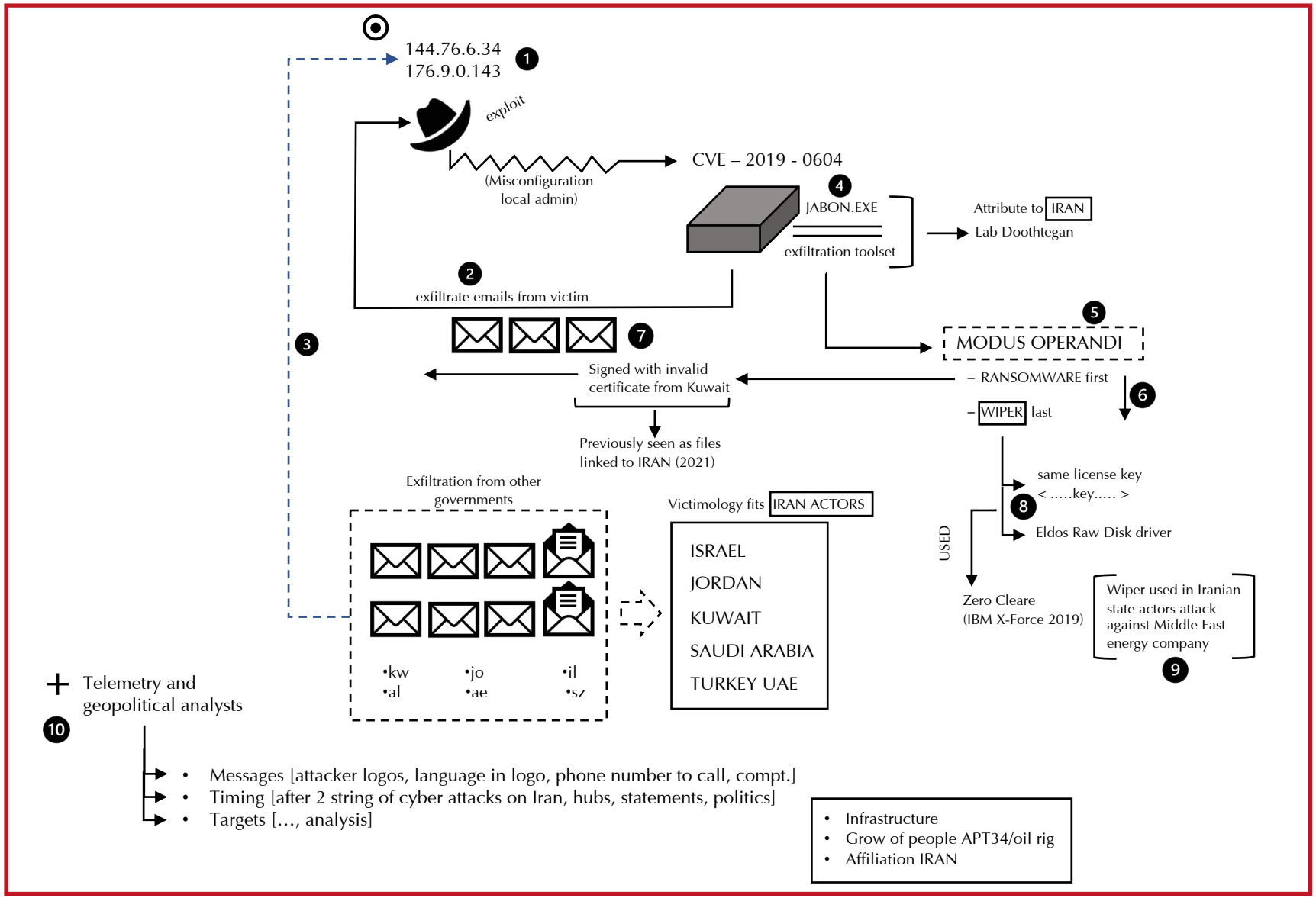
From 2013 many things changed…

- 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, Splashcreen,..)
- They like to be tracked
- They don't re-write their own code
- They reuse infrastructure

Another case: APT34



Attribution phases

1. **COLLECT DATA**
   - from Threat Intelligence
   - from Signal Intelligence
2. **CLUSTER DATA**
   - Intrusion Sets
     - Malware families
     - IP Addresses
     - Domains
     - …
3. **STATE SPONSORED / CRIMINAL ACTIVITY**
   - TTP
   - Stolen data
   - Destructive or Financial
4. **COUNTRY OR REGION ATTRIBUTION**
   - IPS Technics
   - TTPS
   - Domain names
   - Geopolitical
   - Historic Scenarios
5. **ATTRIBUTION ORGANIZATION AND PERSONS**
   - Attackers error
   - Retrospections
   - Deductions
   - Human Int
   - Geopolitical
6. **ASSIGN CONFIDENCE AND COMMUNICATE RESULTS**

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

C2: Attribution

INFORMATION TYPE	CHECK FOR	ATTRIBUTION PHASE
Network traffic	Timestamps	Country
	RDP configuration	Country
	Source Ips (attacker connections)	Country, Organization
	C&C patterns	Clustering
	Source IP (victimology/cui bono)	Person
	Private surfing	Person
Hard Disk	Scripts (comments, function names,..)	Clustering, organization
	GUI Language	Country
	OS Configuration	Country
	Access logs (attacker connections)	Country, organization
	Access logs (victimology)	Country
	Malware samples	Clustering
	Tools	Clustering
	Target lists notes, manuals	Country, organization
	Self-infection of attacker	Country, organization, persona
	Source code	Country
	Installed libraries	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	Country
	Negotiations	Country
	Strategic events	Country
	Domestic conflict	Country
	International conflicts	Country
Economic News	Strategies on economic growth	Country
	Trading agreements	Country
	Stock status	Country
	Investments on specific regions or sectors	Country
		Country
Agencies Mission	Laws	Organization
	Unit names and designators	Organization
	Job posting	Organization
	Reports on achievements	Organization
	Research papers	Organization
	Won grants	Organization

our credo in YOROI

Defence belongs to humans


YOROI
SECURITY

YOROI®

TINEXTA GROUP

La presenza Yoroi nel mondo dei Social Media e nella Blogosfera

Linkedin

Youtube

Twitter

Blog Yoroi

Blog M. Ramilli

YOROI®

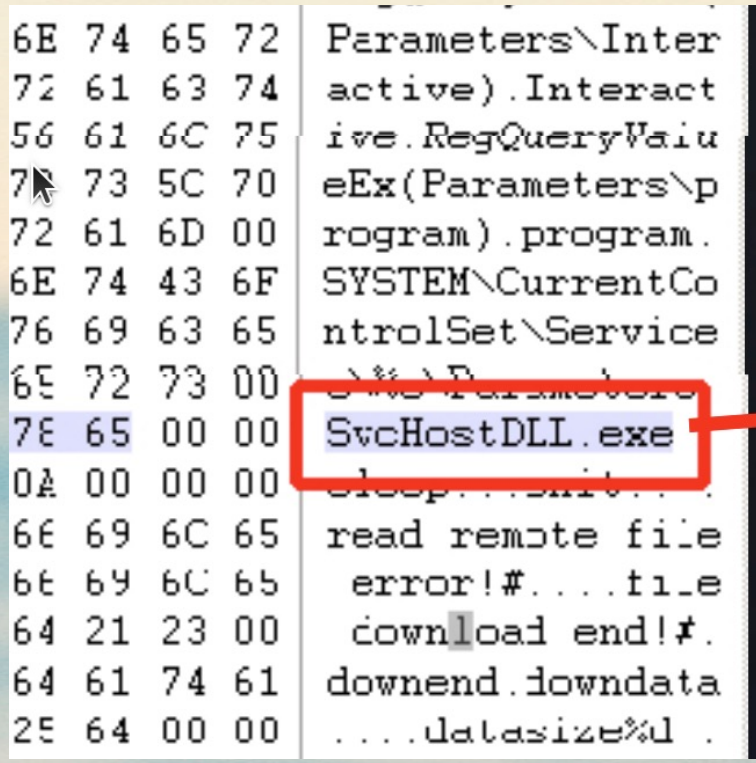
TINEXTA GROUP

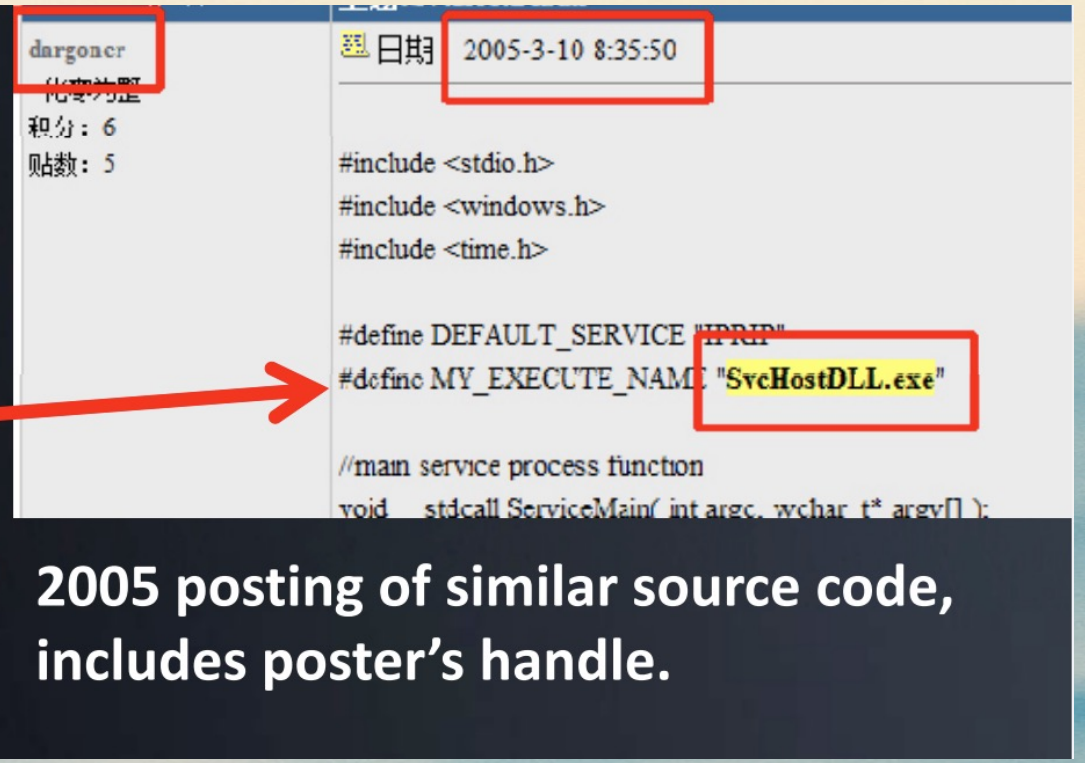
yoroi.company

CYBER ACT FORUM

2022

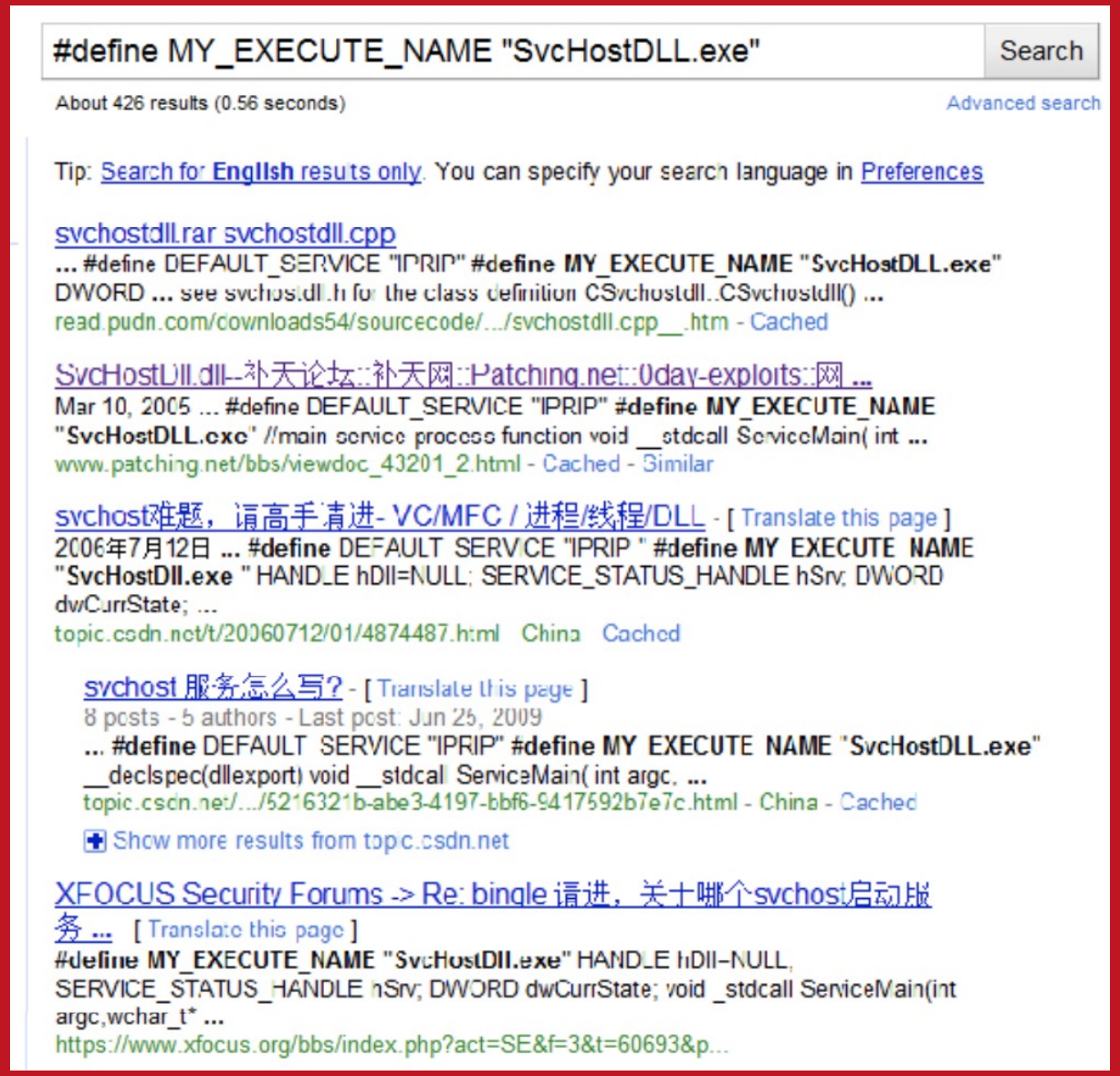
Case Study: Chinese APT



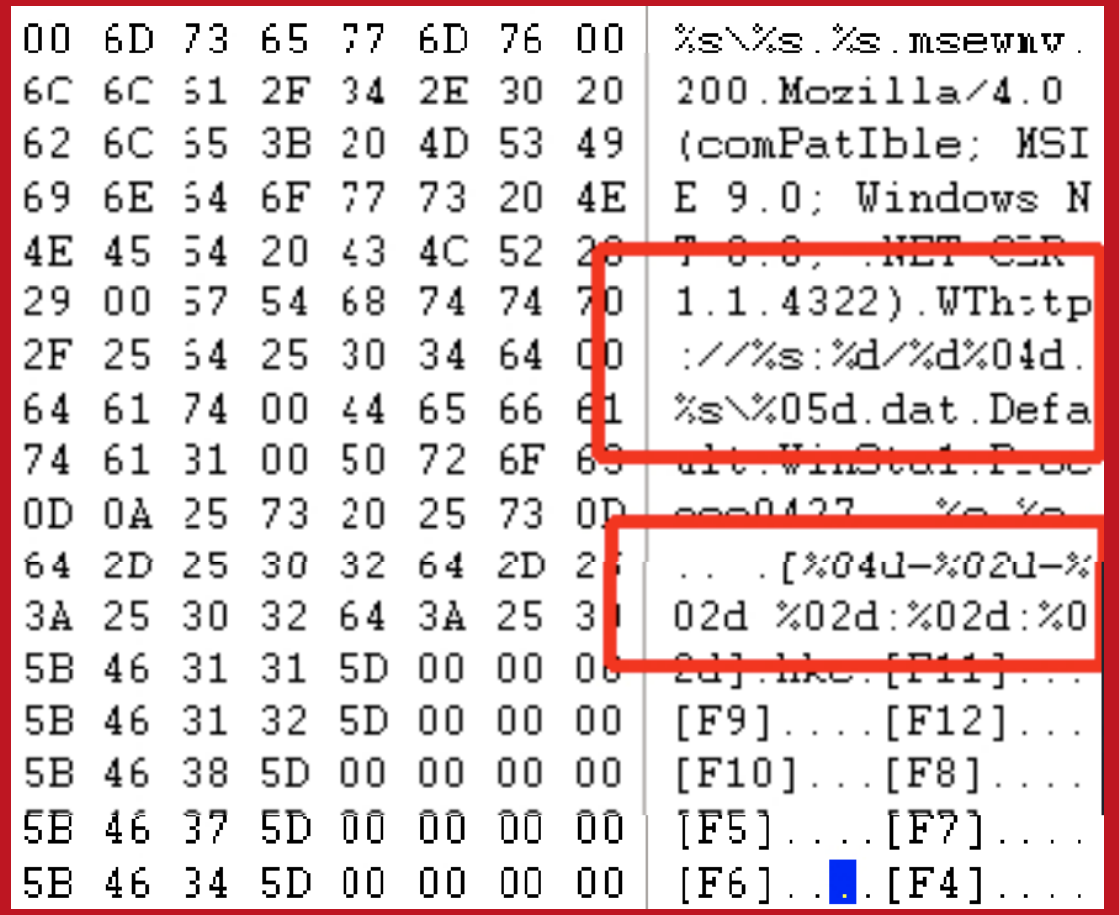


2005 posting of similar source code, includes poster's handle.

Case Study: Chinese APT

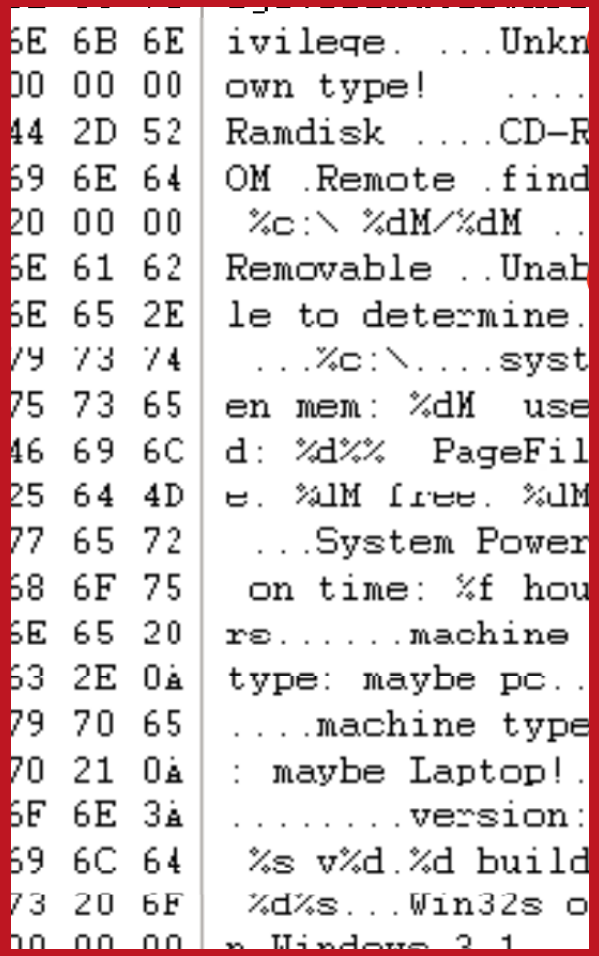


Case Study: Chinese APT



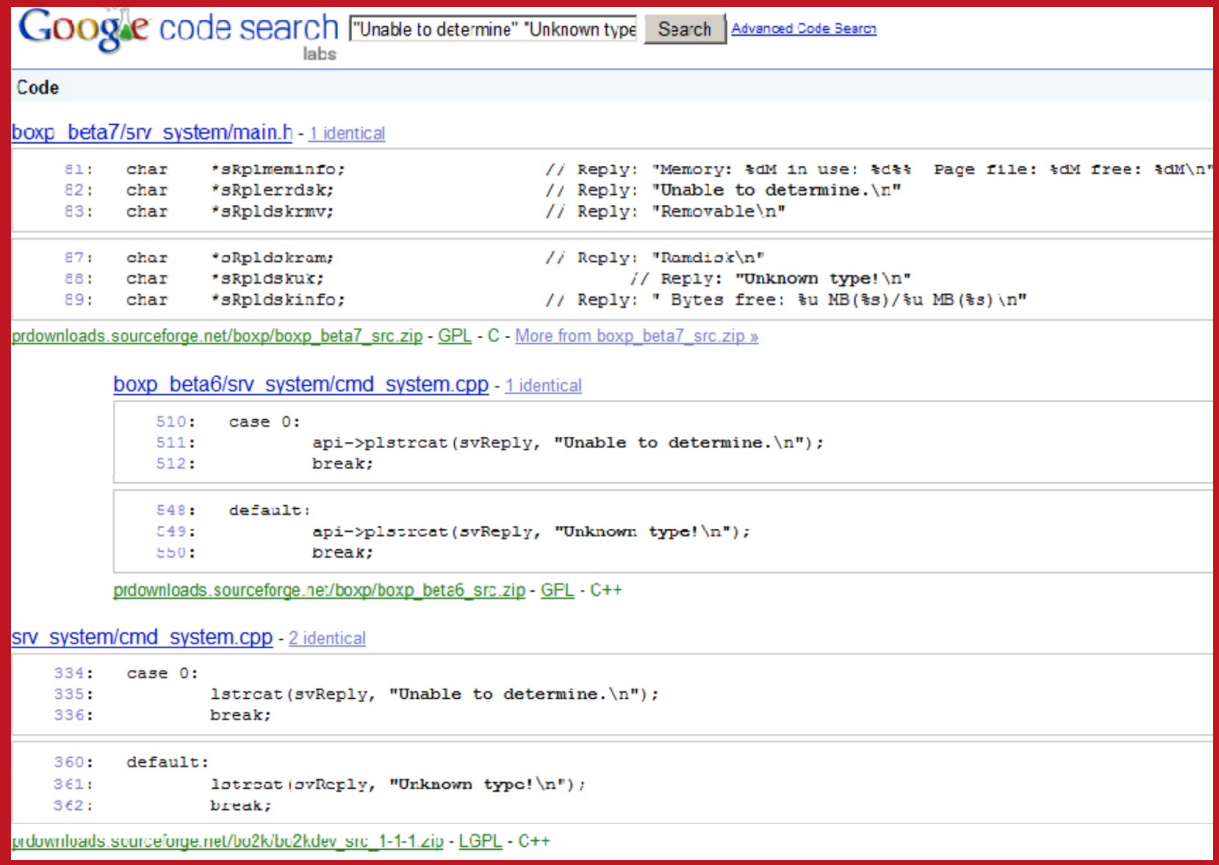
Format Strings are written by humans
so great opportunity for uniqueness

Case Study: Chinese APT



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

Case Study: Chinese APT

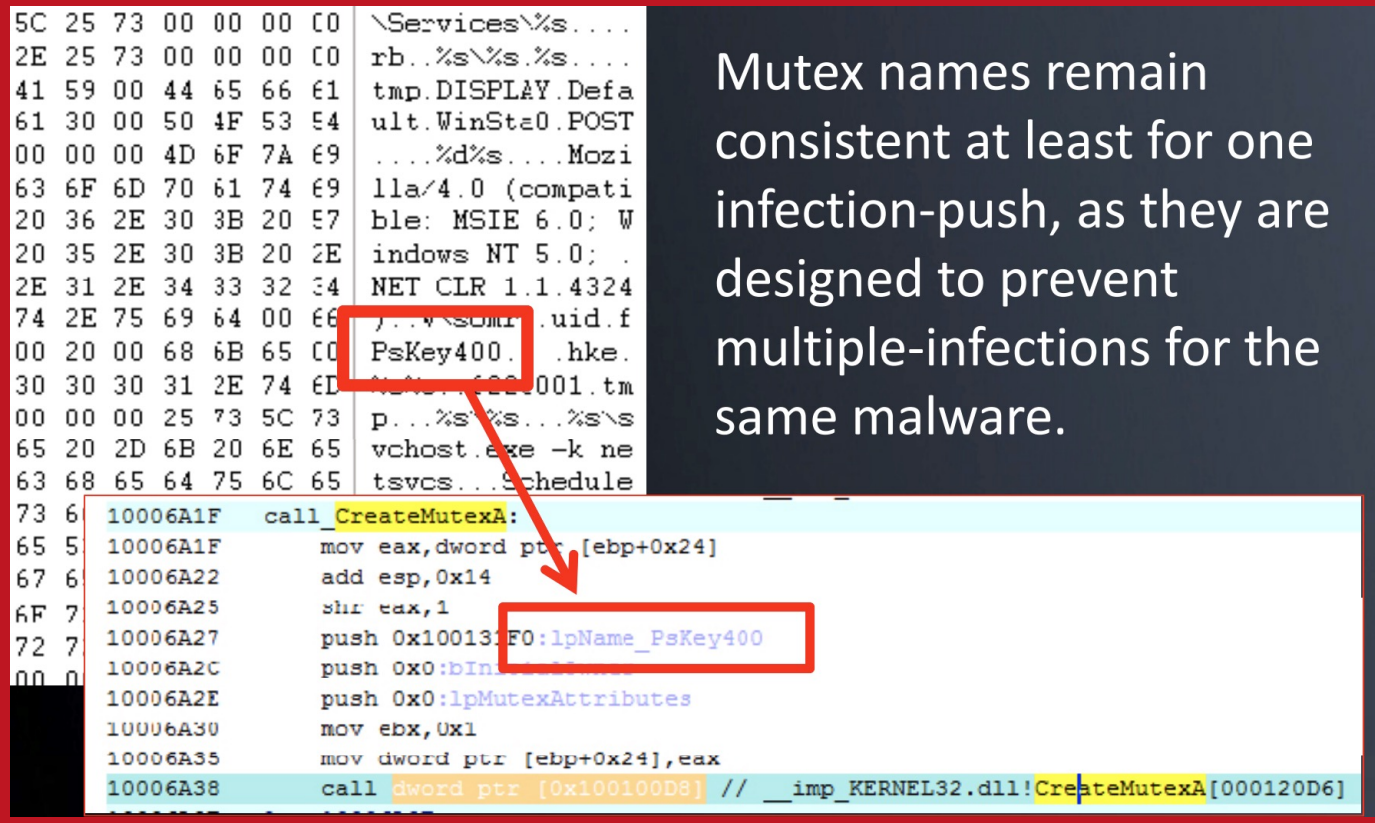


Logging Strings such as:

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

Reveals source code reuse! (BO2k)

Case Study: Chinese APT



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 Copy gri ht 1995-2002 Mark Adler
- inflate 1.2.3 Copyright 1995-2005 Mark Adler
- inflate 1.0.4 Copyright 1995-1996 Mark Adler
- inflate inflate 113 . . Copyright 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 specfically
- 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 specific as zlib patterns 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

FK32_Loop:
                call  TryAddress
                jnc  FK32_Success
                sub  esi 010000h
                loop  FK32_Loop

FK32 Hardcodes:
                mov    esi, KERNEL32_WIN9X
                call     TryAddress
                jnc      FK32_Success

                mov    esi, KERNEL32_WINNT
                call     TryAddress
                jnc      FK32_Success

                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
```

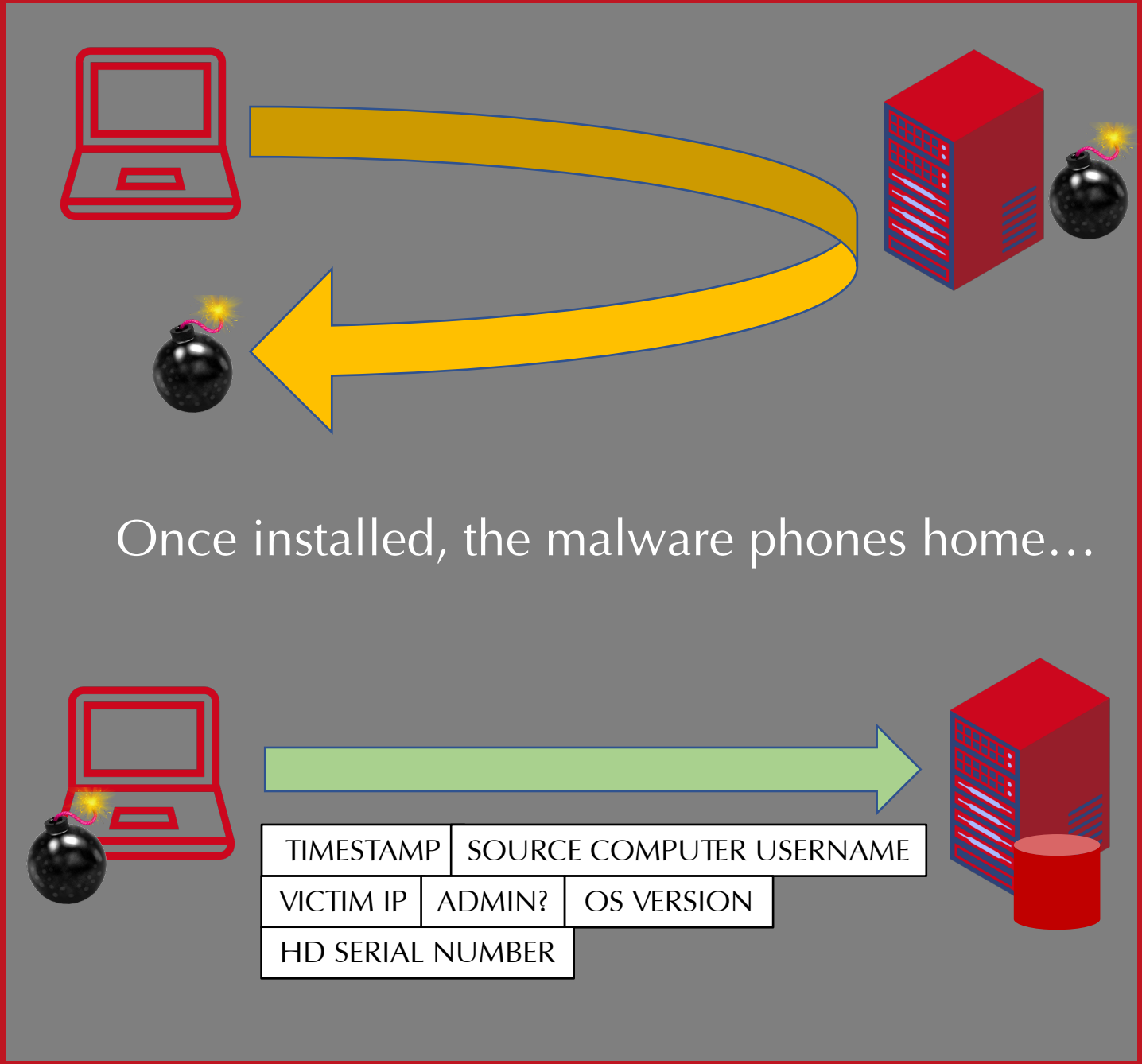
Mask off ESI to a page boundary

Load ECX w/ a length to scan backwards from

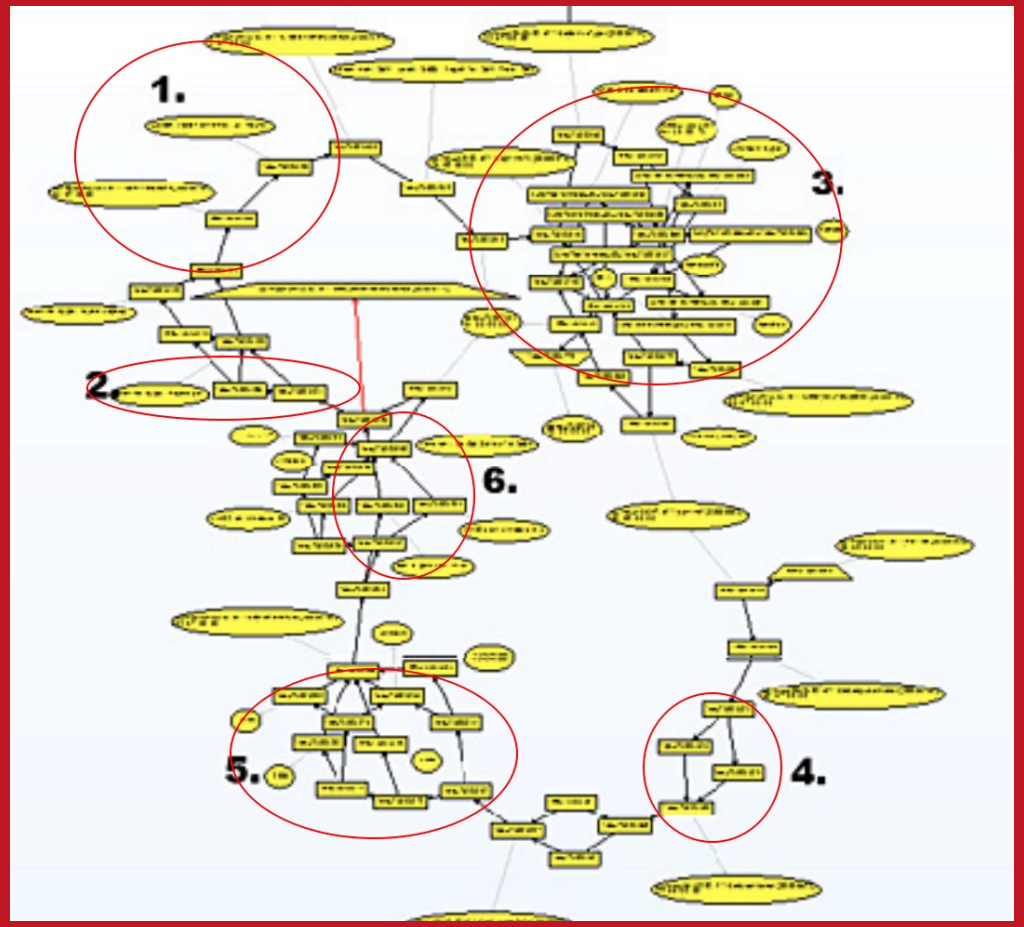
Subtract, try again

Try a bunch of hard coded offsets if the scan fails

Case Study: Chinese APT



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

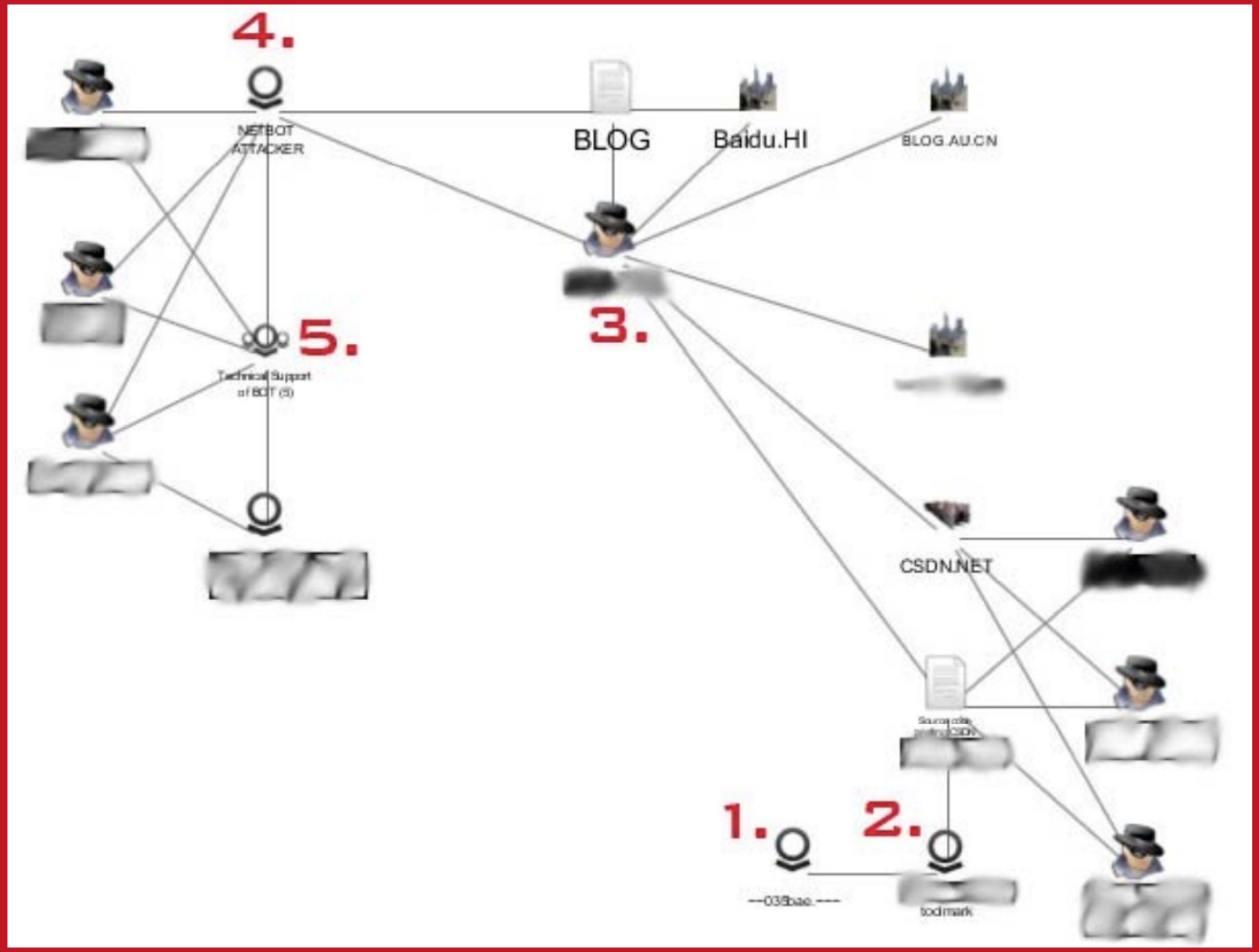
```
mov eax, fs:[30h]
mov eax, byte ptr [eax+2]
test eax, eax
jnz __found_debugger
```

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_*

Example Threat Attribution with PALANTIR



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