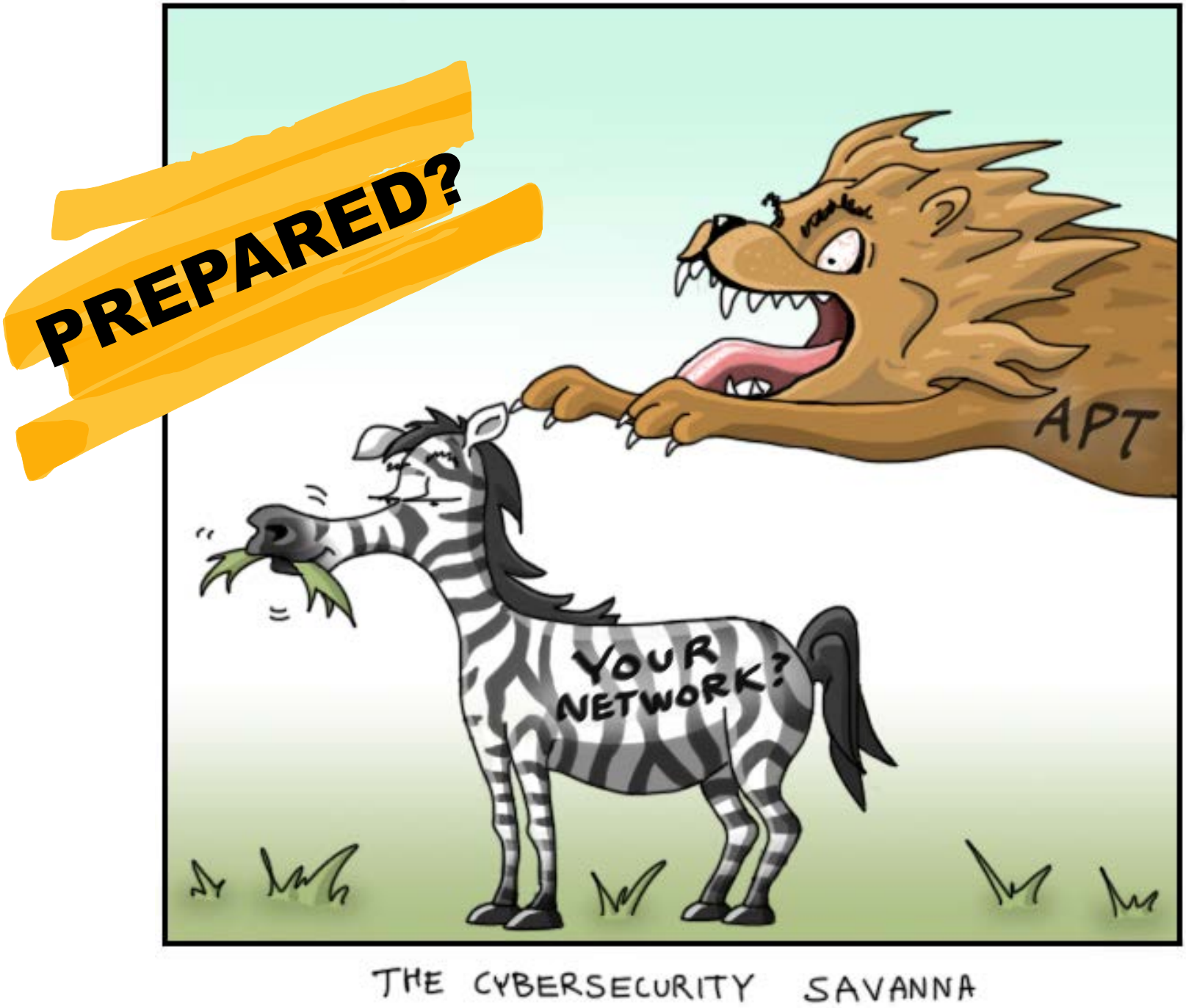
RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

SMALL DATA ANALYSIS

SESSION ID: TRM-T10

Marion Marschalek
Malware Researcher
Cyphort Inc.
@pinkflawd


PREPARED?
APT
YOUR NETWORK?
THE CYBERSECURITY SAVANNA

The Malware Situation

Attack Insights

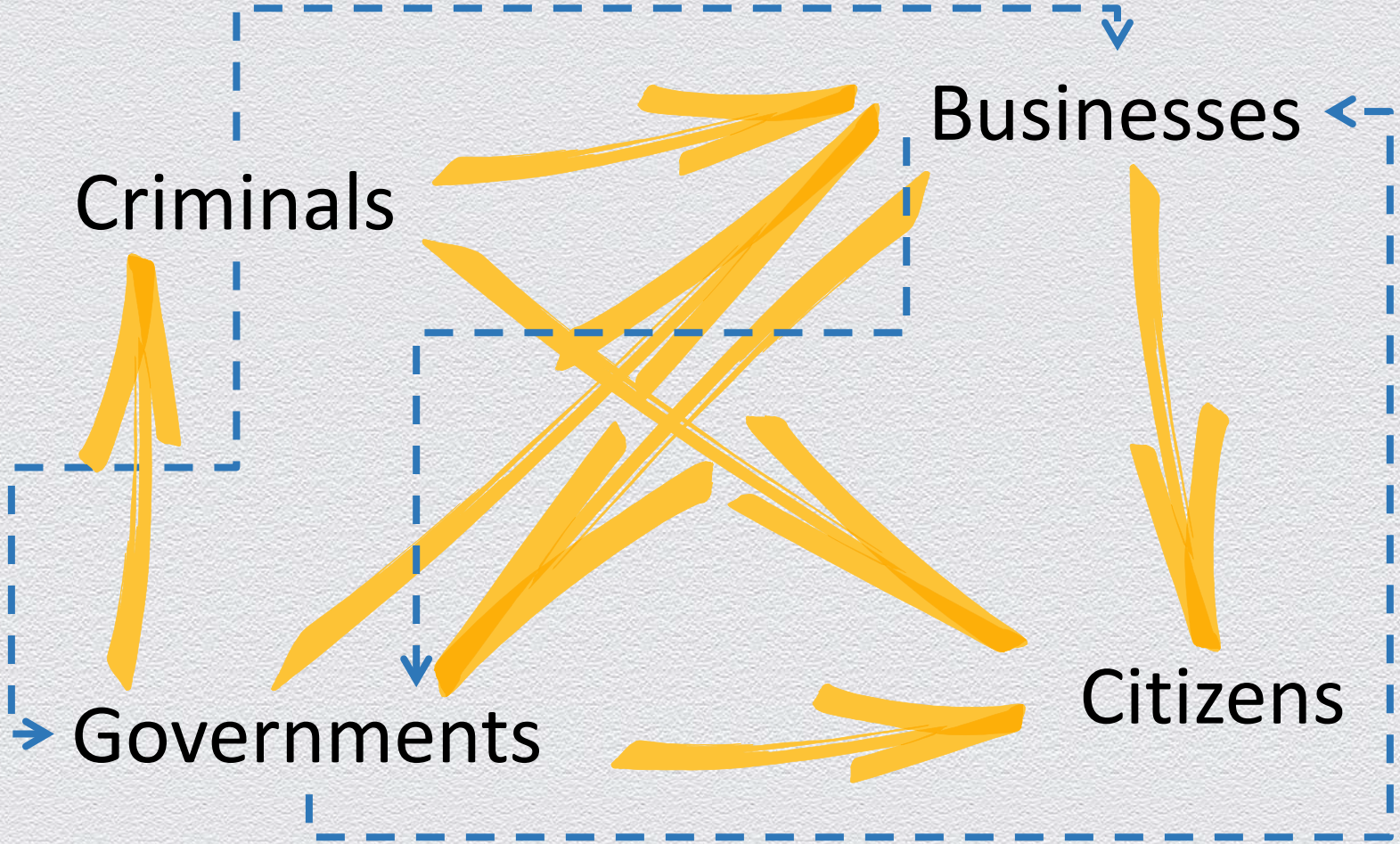
Malware Analyst‘s Bootcamp

Malware in 1998

Malware today

NEXT?

Good Folks, Bad Folks & Real Life



MALWARE
/ˈmalwɛːɐ̯/

Software that doesn‘t come with an EULA

- Morgan Marquis-Boire

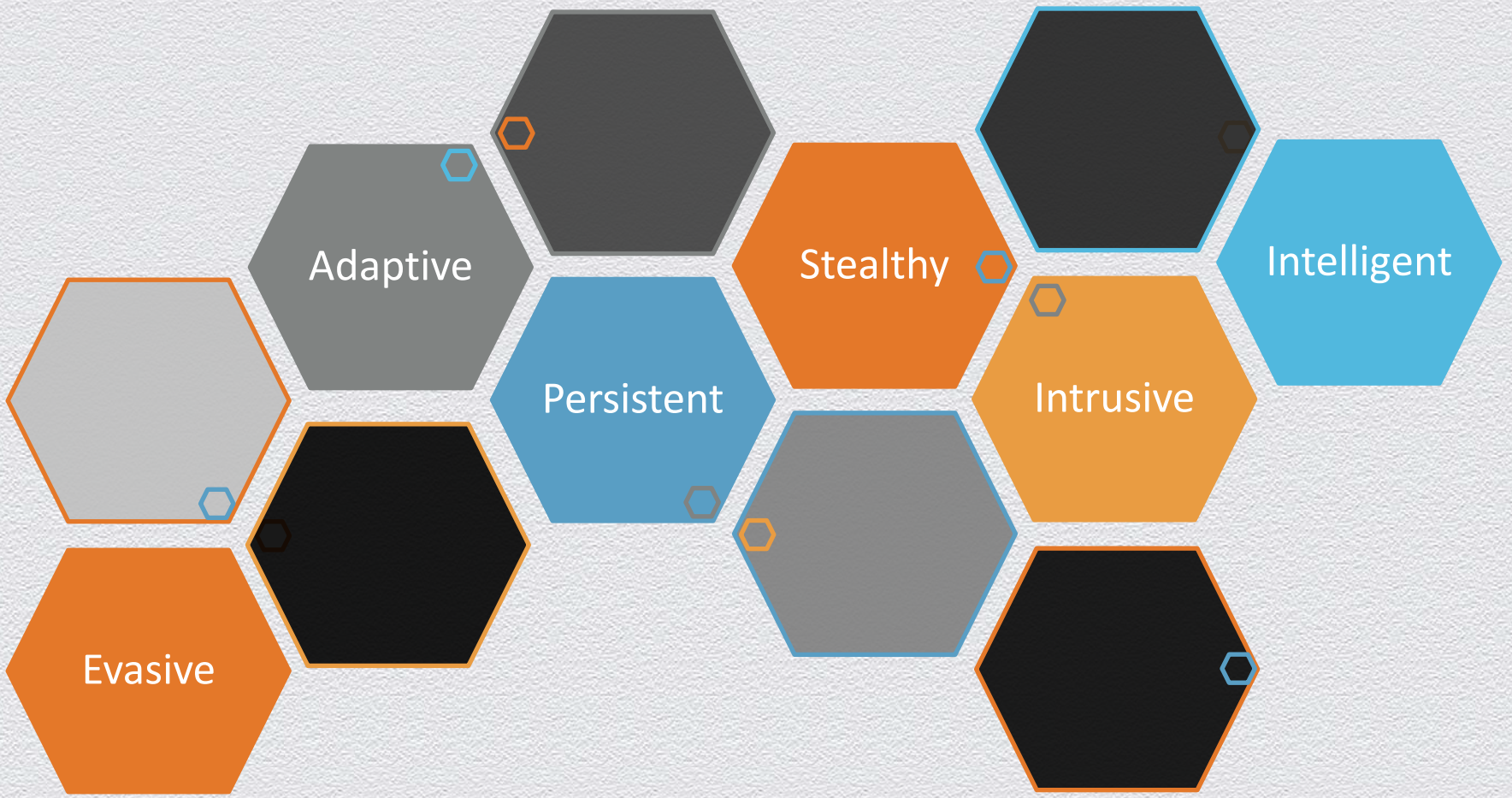
EXPONENTIAL TIMES

- **Botnets** and **mass malware** relaunching
- **Internet** main attack vector – 1.7 billion infections
  - >90% of drive-by infections via Java vulnerabilities!
- **Android malware** getting smarter, more than 300 families
  - >150.000 samples - total growth of 800% since last
- Malware targetting **Linux** servers
  - Operation Windigo affecting 25

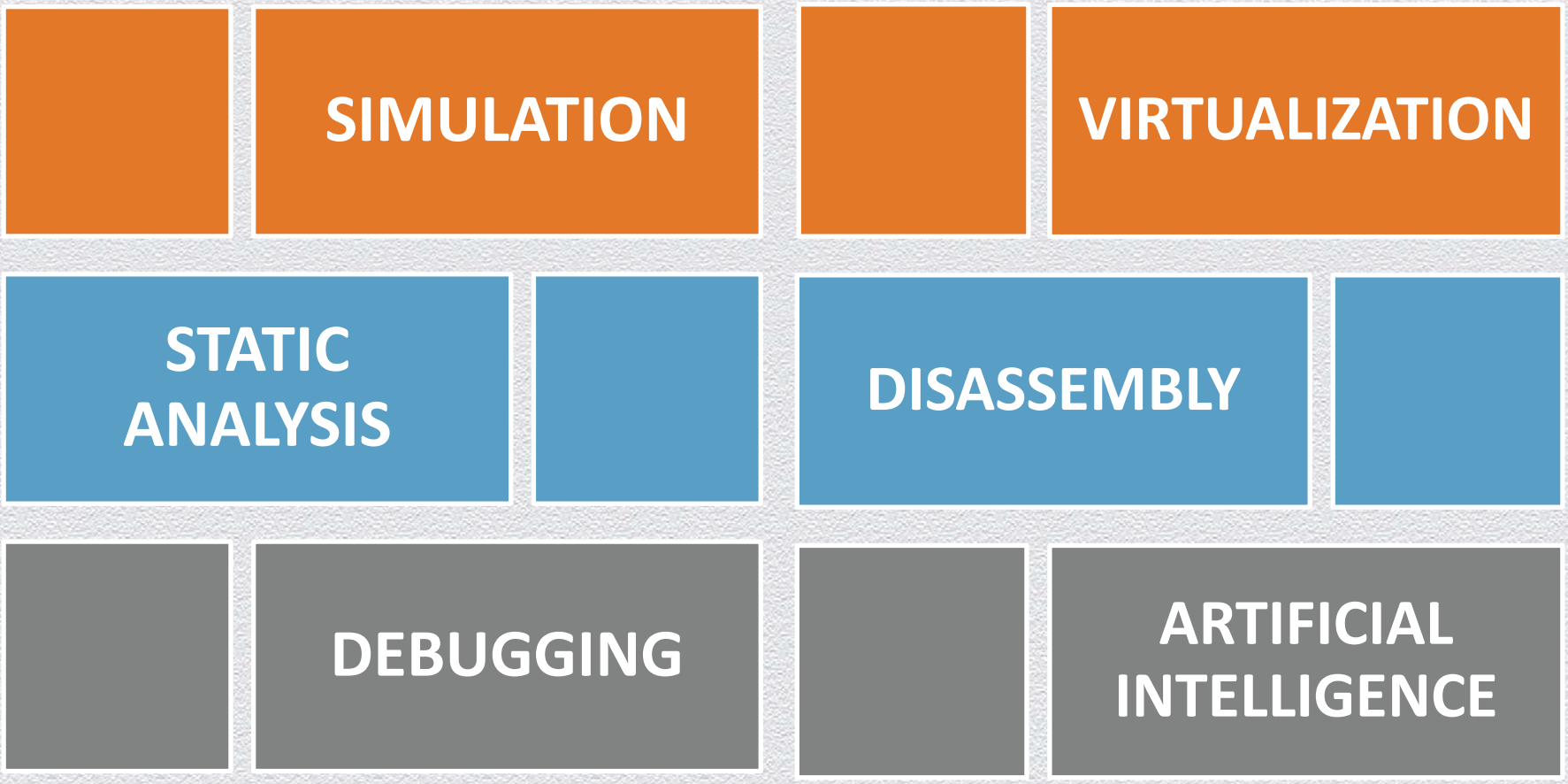
All platforms are at risk!

http://www.securelist.com/en/analysis/204792318/Kaspersk ...statistics_for_2013
http://www.sophos.com/en-us/medialibrary/PDFs/other/s ...port-2014.pdf

MULTIFUNTIONAL THREATS



SMARTER ANALYSTS



SIMULATION

VIRTUALIZATION

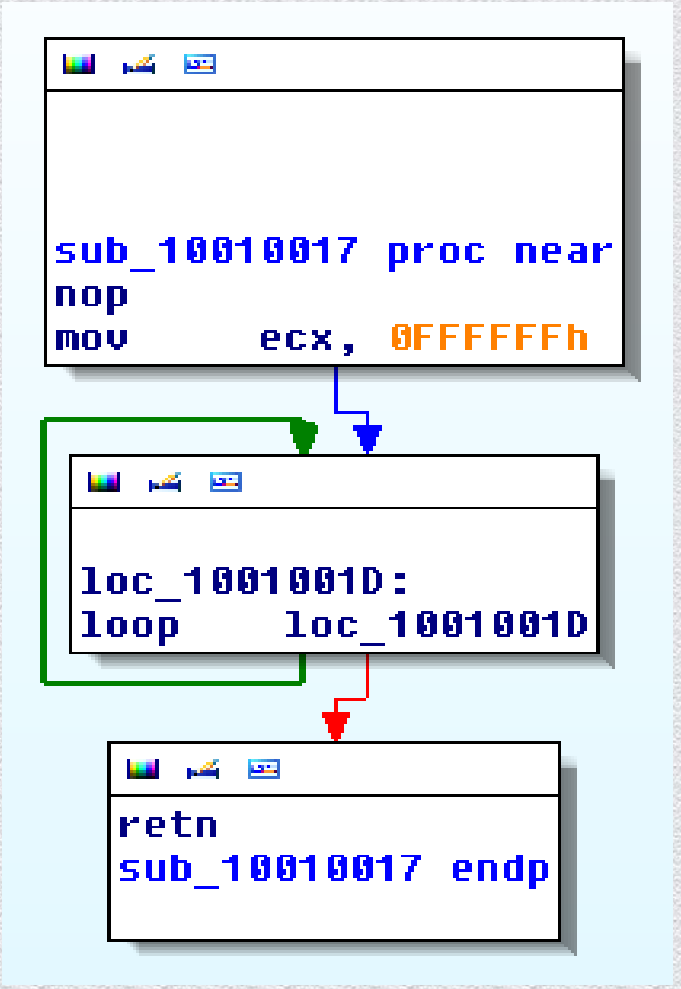
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
2:003F2610 mov     [ebp+var_44], 'V'
2:003F2614 mov     [ebp+var_43], 'B'
2:003F2618 mov     [ebp+var_42], 'o'
2:003F261C mov     [ebp+var_41], 'x'
2:003F2620 mov     [ebp+var_40], 'S'
2:003F2624 mov     [ebp+var_3F], 'e'
2:003F2628 mov     [ebp+var_3E], 'r'
2:003F262C mov     [ebp+var_3D], 'v'
2:003F2630 mov     [ebp+var_3C], 'i'
2:003F2634 mov     [ebp+var_3B], 'c'
2:003F2638 mov     [ebp+var_3A], 'e'
2:003F263C mov     [ebp+var_39], '.'
2:003F2640 mov     [ebp+var_38], 'e'
2:003F2644 mov     [ebp+var_37], 'x'
2:003F2648 mov     [ebp+var_36], 'e'
2:003F264C mov     [ebp+var_35], bl
2:003F264F mov     byte ptr [ebp+var_2C], 'v'
2:003F2653 mov     byte ptr [ebp+var_2C+1], 'm'
2:003F2657 mov     byte ptr [ebp+var_2C+2], 't'
2:003F265B mov     byte ptr [ebp+var_2C+3], 'o'
2:003F265F mov     byte ptr [ebp+var_28], 'o'
2:003F2663 mov     byte ptr [ebp+var_28+1], 'l'
2:003F2667 mov     byte ptr [ebp+var_26], 's'
2:003F266B mov     byte ptr [ebp+var_26+1], 'd'
2:003F266F mov     byte ptr [ebp+var_24], '.'
2:003F2673 mov     byte ptr [ebp+var_24+1], 'e'
2:003F2677 mov     byte ptr [ebp+var_22], 'x'
2:003F267B mov     byte ptr [ebp+var_22+1], 'e'
2:003F267F mov     byte ptr [ebp+var_20], bl
```

SIMULATION

VIRTUALIZATION

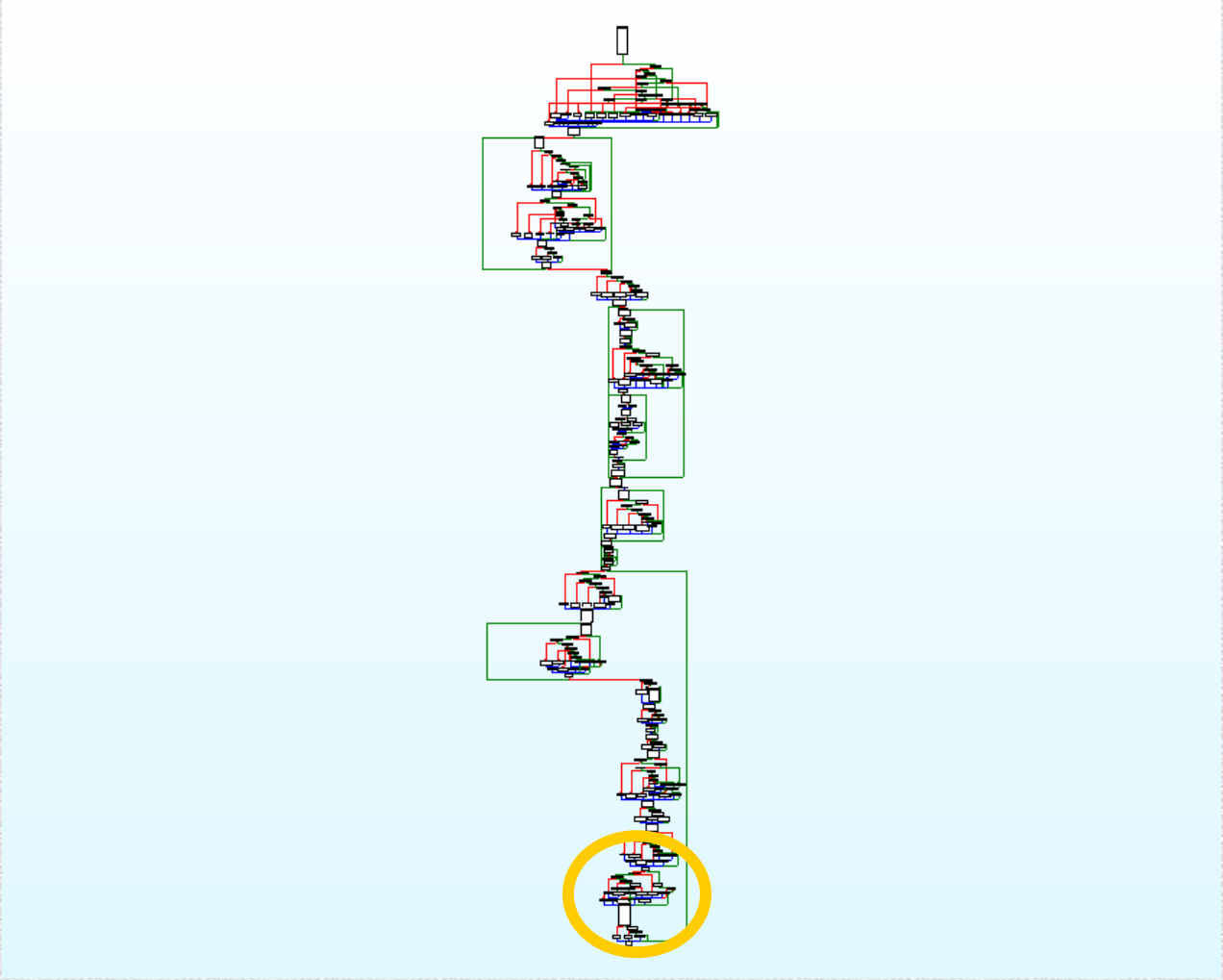
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

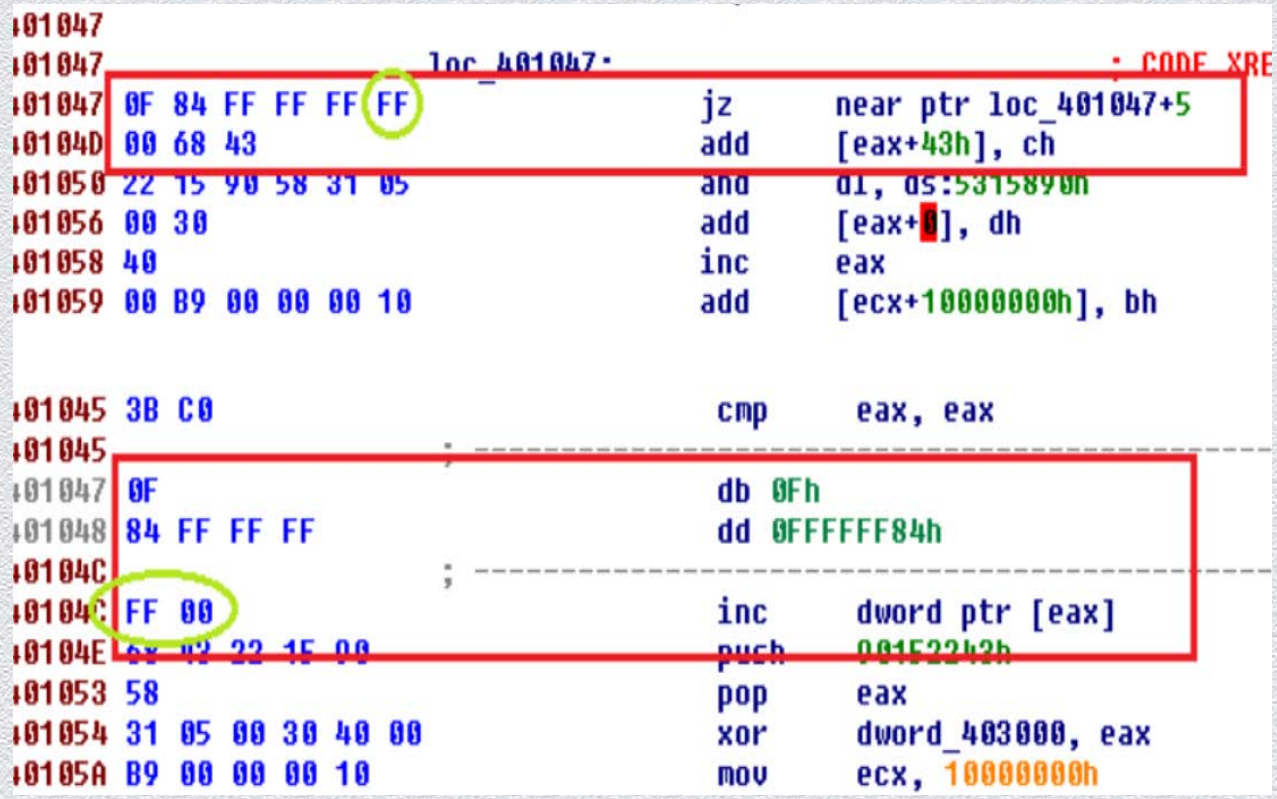
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
00401C80 push    ebp
00401C81 mov     ebp, esp
00401C83 push    0FFFFFFFFh
00401C85 push    offset _WinMain@16_SEH
00401C8A mov     eax, large fs:0
00401C90 push    eax
00401C91 mov     large fs:0, esp
00401C98 sub     esp, 24h
```

...

```
00401D98
00401D98 loc_401D98:
00401D98 mov     ecx, 69805h
00401D9D call    ecx
00401D9F mov     eax, 69805h
00401DA4 mov     ecx, [ebp+__$EHRec$.pNext]
00401DA7 mov     large fs:0, ecx
00401DAE pop     edi
00401DAF pop     esi
00401DB0 pop     ebx
00401DB1 mov     esp, ebp
00401DB3 pop     ebp
00401DB4 retn    10h
```

CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

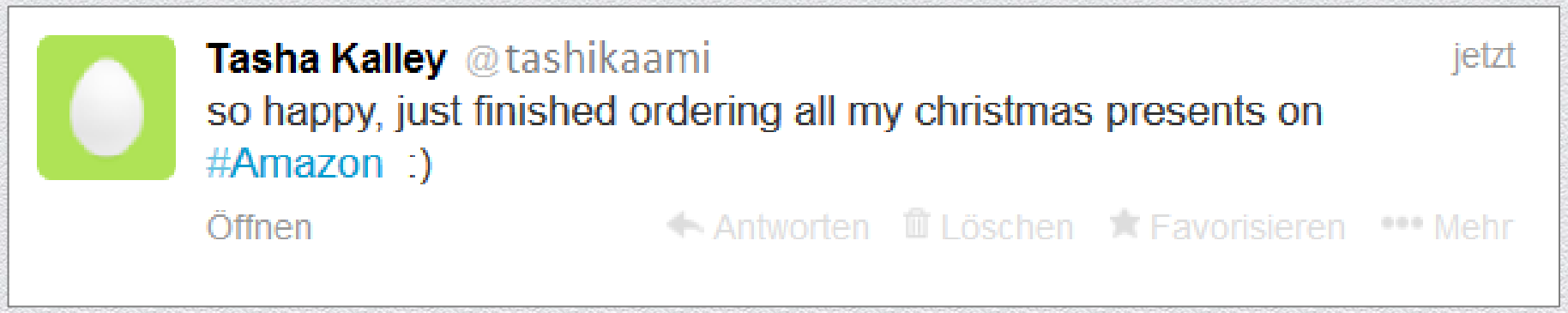
RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

ATTACK INSIGHTS

WOLF IN SHEEP OUTFIT

20KB of Wolf

A STEP BACK IN TIME ...

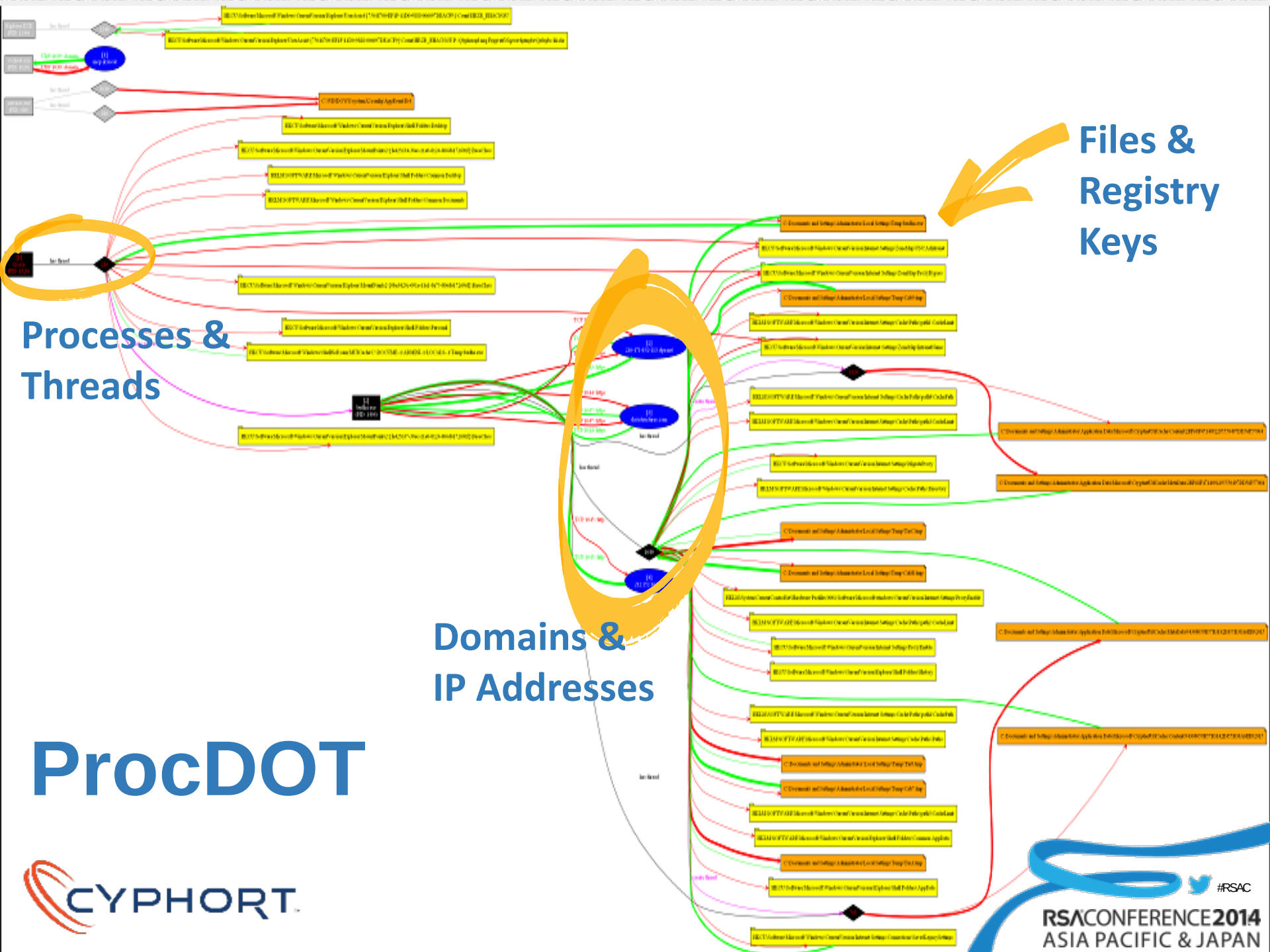


Train employees to identify sensitive personal information and how to handle social networking sites correctly!

CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN



ProcDOT

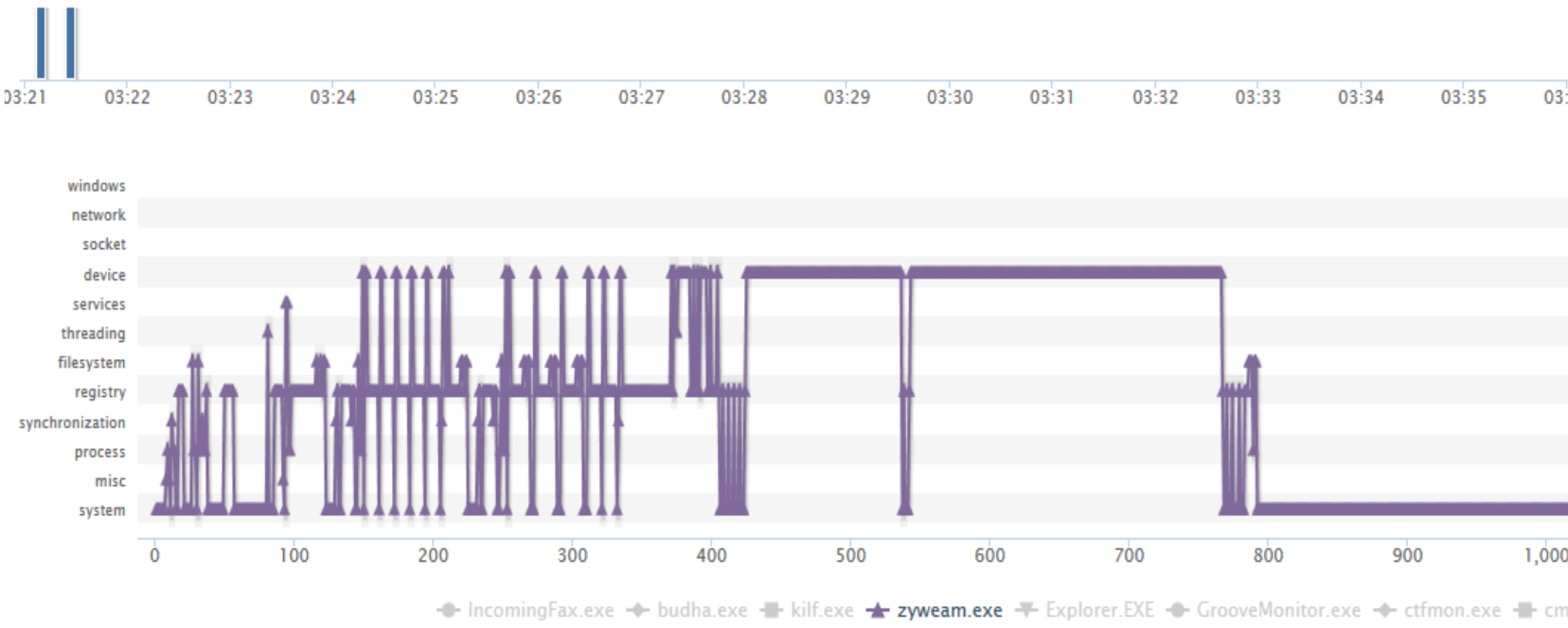
CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

malwr

- Quick Overview
- Static Analysis
- Behavioral Analysis
- Network Analysis
- Dropped Files
- Comment Board (0)



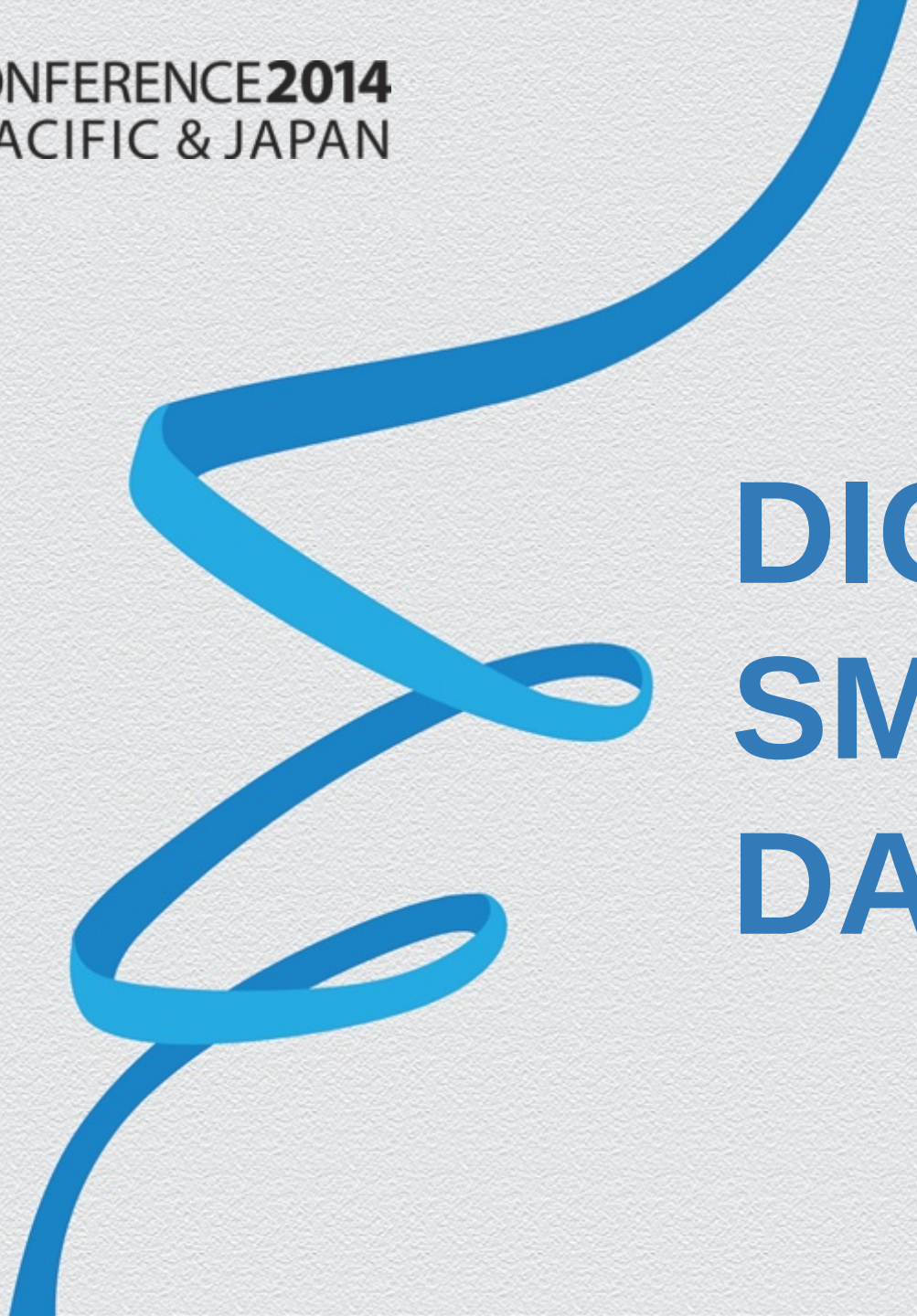
- X-axis by: event
- Y-axis by: category

- **IncomingFax.exe** 1088
  - **budha.exe** 1984
    - **kilf.exe** 224
      - **zyweam.exe** 652
      - **cmd.exe** 1616

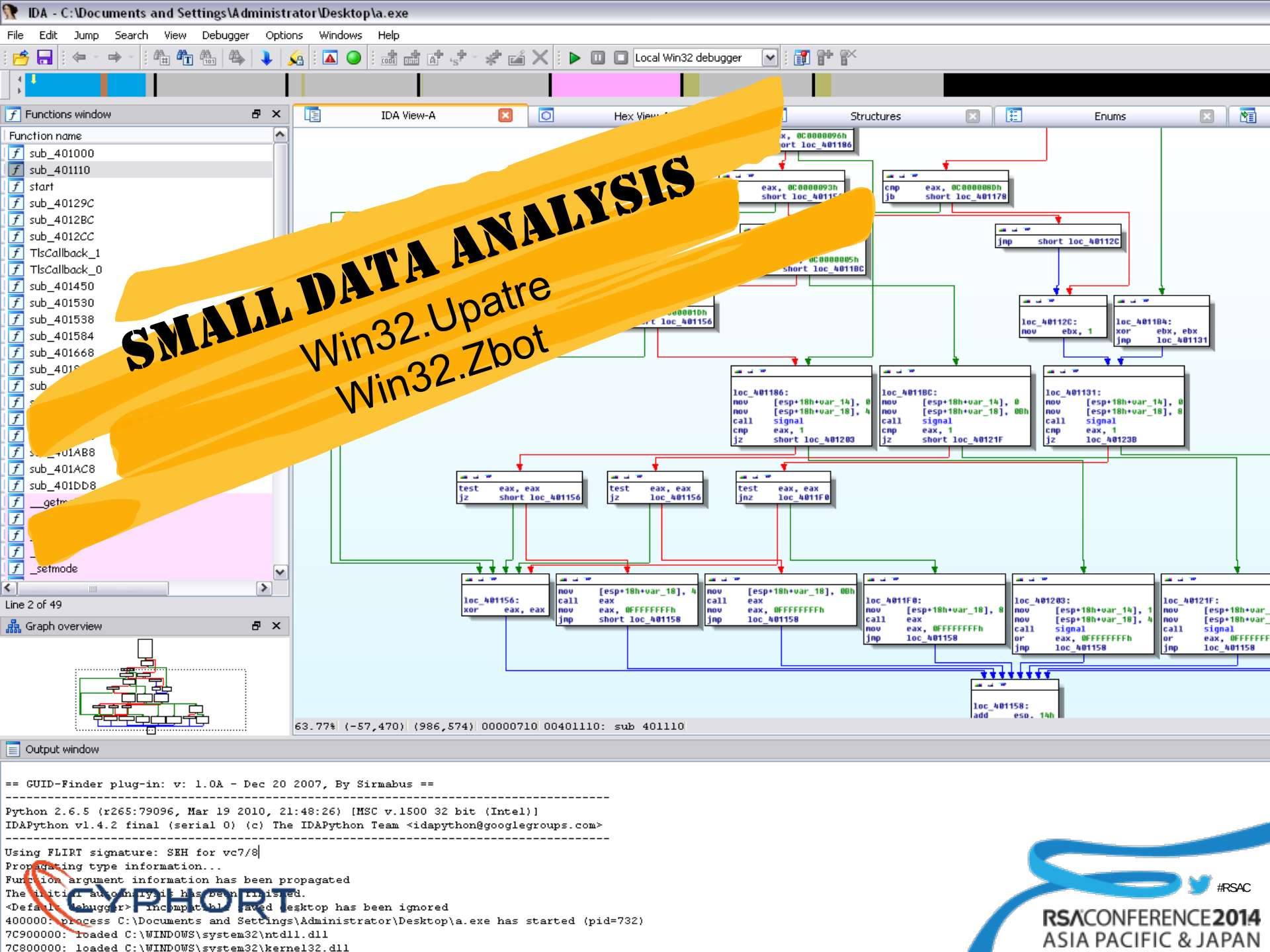
CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN



DIG THE SMALL DATA …


IDA - C:\Documents and Settings\Administrator\Desktop\a.exe
File Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
Functions window
Function name
sub_401000
sub_401110
start
sub_40129C
sub_4012BC
sub_4012CC
TlsCallback_1
TlsCallback_0
sub_401450
sub_401530
sub_401538
sub_401584
sub_401668
sub_401AB8
sub_401AC8
sub_401DD8
_setmode
Line 2 of 49
Graph overview
IDA View-A
Hex View
Structures
Enums
SMALL DATA ANALYSIS
Win32.Upatre
Win32.Zbot
63.77% (-57,470) (986,574) 00000710 00401110: sub_401110
Output window
== GUID-Finder plug-in: v: 1.0A - Dec 20 2007, By Sirmabus ==
Python 2.6.5 (r265:79096, Mar 19 2010, 21:48:26) [MSC v.1500 32 bit (Intel)]
IDAPython v1.4.2 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
Using FLIRT signature: SEH for vc7/8
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
<Default Debugger> - Incompatible saved desktop has been ignored
400000: process C:\Documents and Settings\Administrator\Desktop\a.exe has started (pid=732)
7C900000: loaded C:\WINDOWS\system32\ntdll.dll
7C800000: loaded C:\WINDOWS\system32\kernel32.dll
CYPHORT
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

WIN32.UPATRE

Protected

Packed

Downloader.

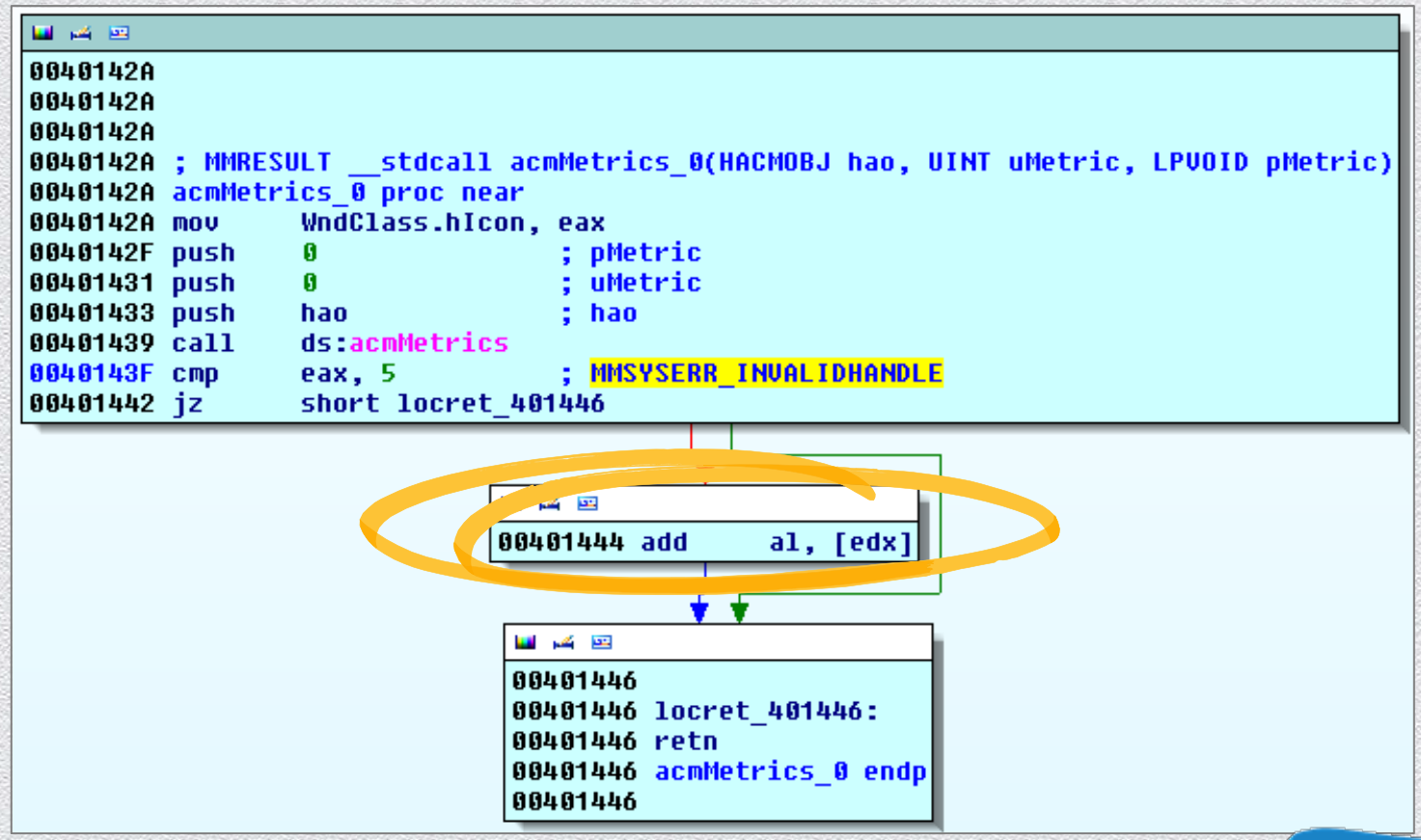
CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

PROTECTION

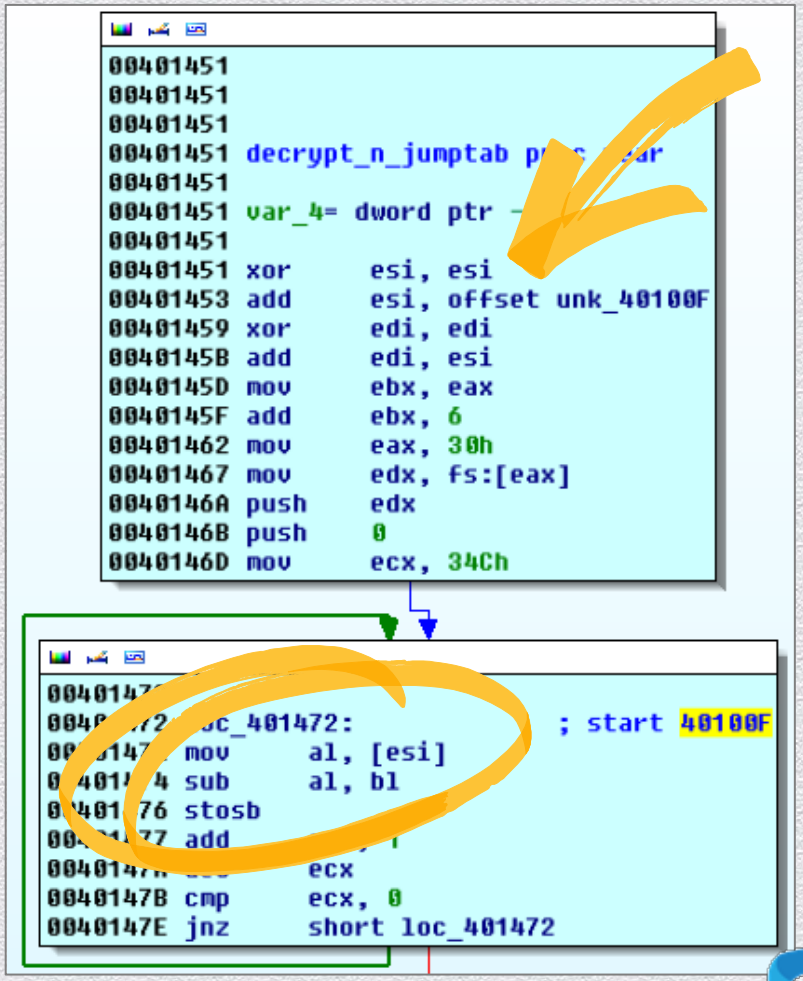
ANTI SIMULATION



PROTECTION

BREAKPOINT

DETECTION



PROTECTION

TIMING

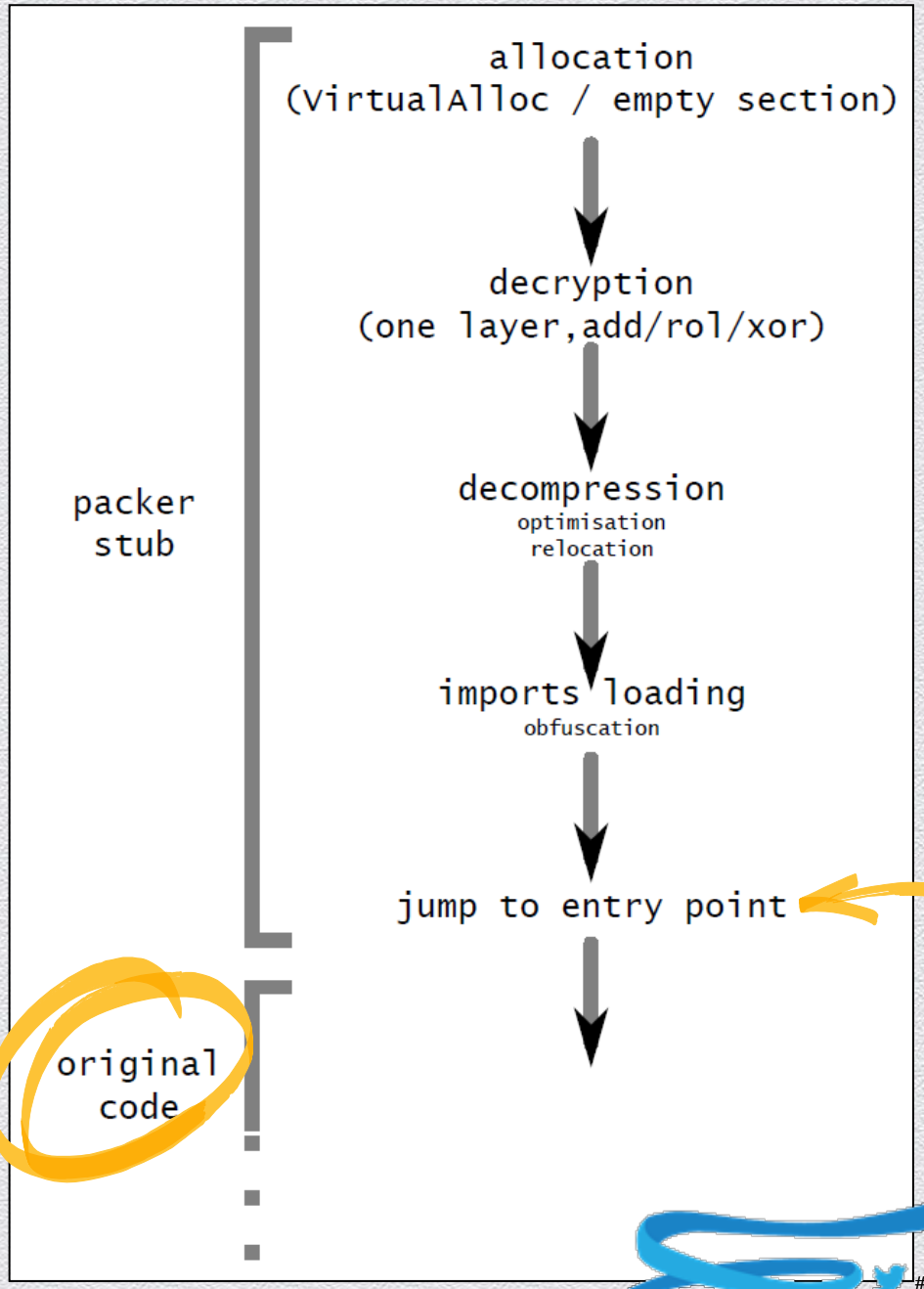
DEFENCE

```
.text:0040111  mov     l, ds:byte_40118F
.text:0040111  rdtsc
.text:0040111  push    eax
.text:00401123 mov     bh, [esi]
.text:00401125 mov     [edi], bh
.text:00401127 inc     edi
.text:00401128
.text:00401128 loc_401128:
.text:00401128 inc     esi
.text:00401129 inc     esi
.text:0040112A inc     esi
.text:0040112B push    eax
.text:0040112C mov     al, [esi]
.text:0040112E stosb
.text:0040112F
.text:0040112F loc_40112F:
.text:0040112F add     [edi-1], bl
.text:00401132 pop     eax
.text:00401133 loop    loc_401128
.text:00401  destruction_rdtsc endp
.text:00401
.text:00401  rdtsc
.text:00401  pop     edx
.text:00401138 sub     eax, edx
.text:0040113A sub     esp, 18h
.text:0040113D push    0
.text:0040113F push    heap_40304D
.text:00401145 call    dword ptr ds:acmStreamOpen
```

PACKER

What is a packer?

How to identify it?



PACKER

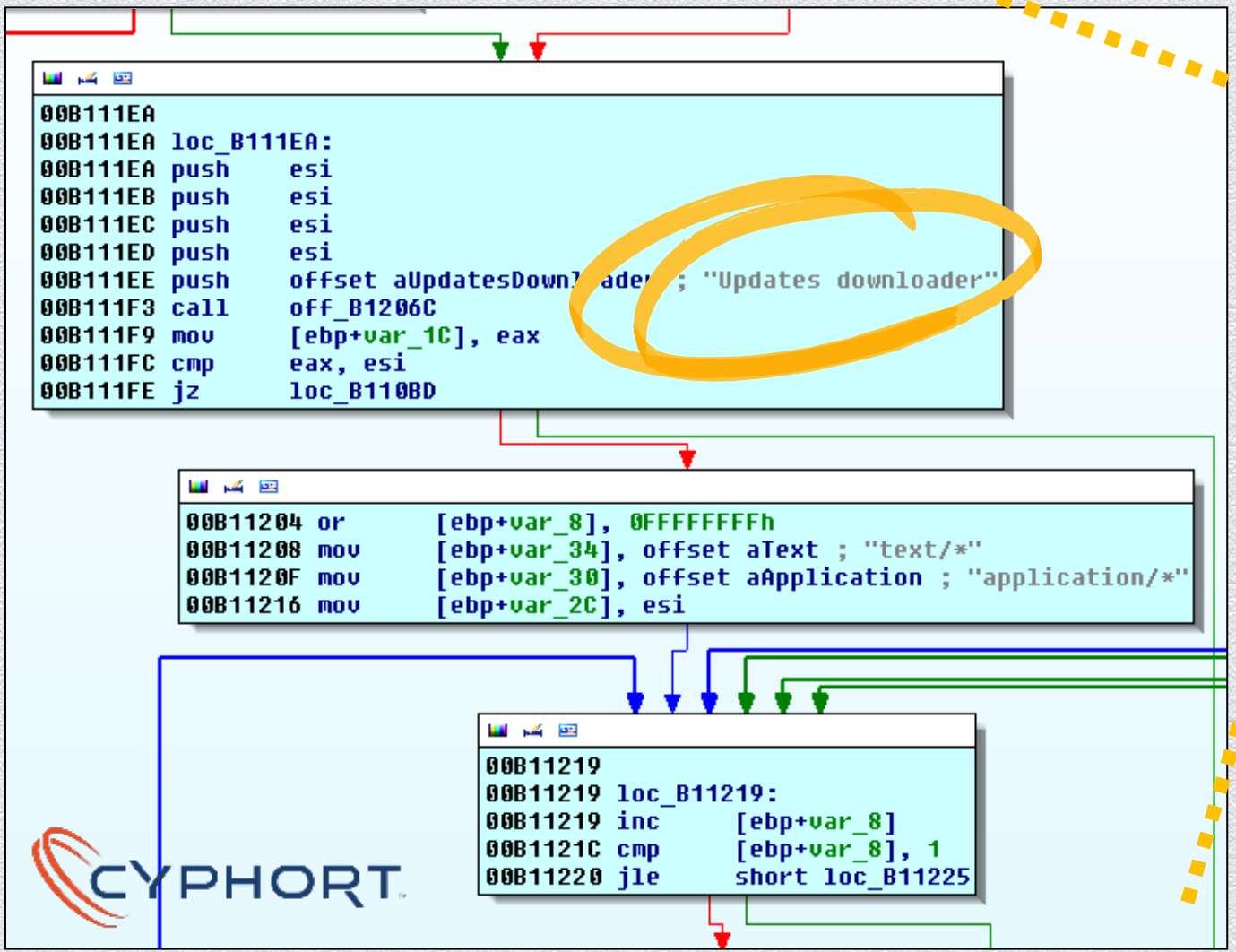
3 Stages

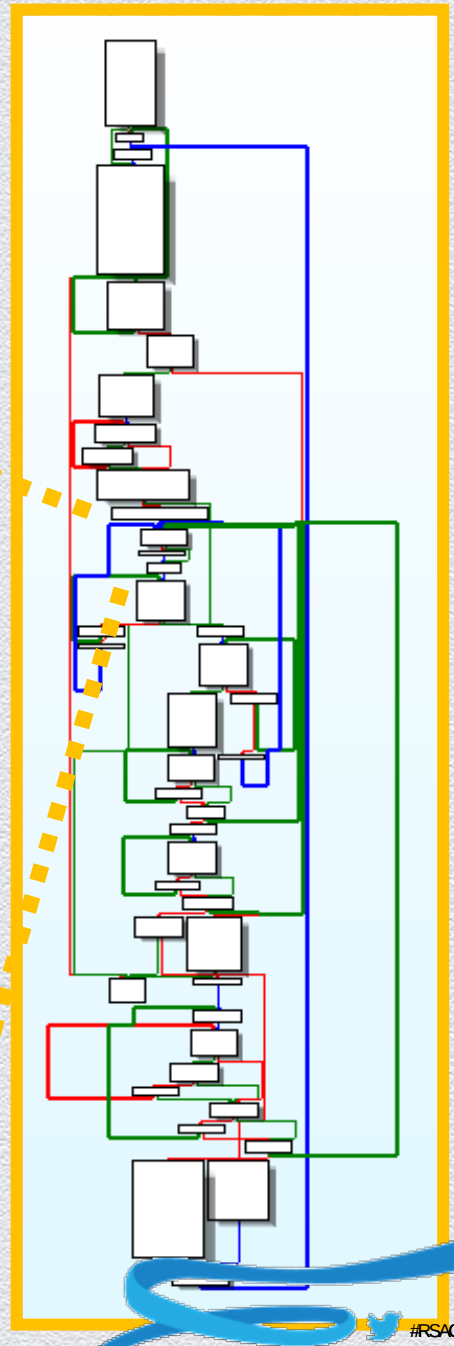
- Data Compression
- Decryption
- Decompression with RtlDecompressBuffer

```
1  WORD key_modifier = AC601330h
2  WORD sub_key = E25ED5B0h
3  WORD xor_key = 86E53278h
4  (WORD*) code = [offset_buffer]
5  int memsize = [size_buffer]
6
7  for (i=0; i<10; i++)
8  {
9      xor_key -= key_modifier          // underflow
10 }
11
12 for (i=0; i<memsize; i++)
13 {
14     code[i] = code[i] XOR xor_key    // modify data
15     code[i] -= sub_key
16
17     sub_key -= xor_key               // modify keys
18     ROR(xor_key)
19 }
```

CYPHORT

DOWNLOADER





CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

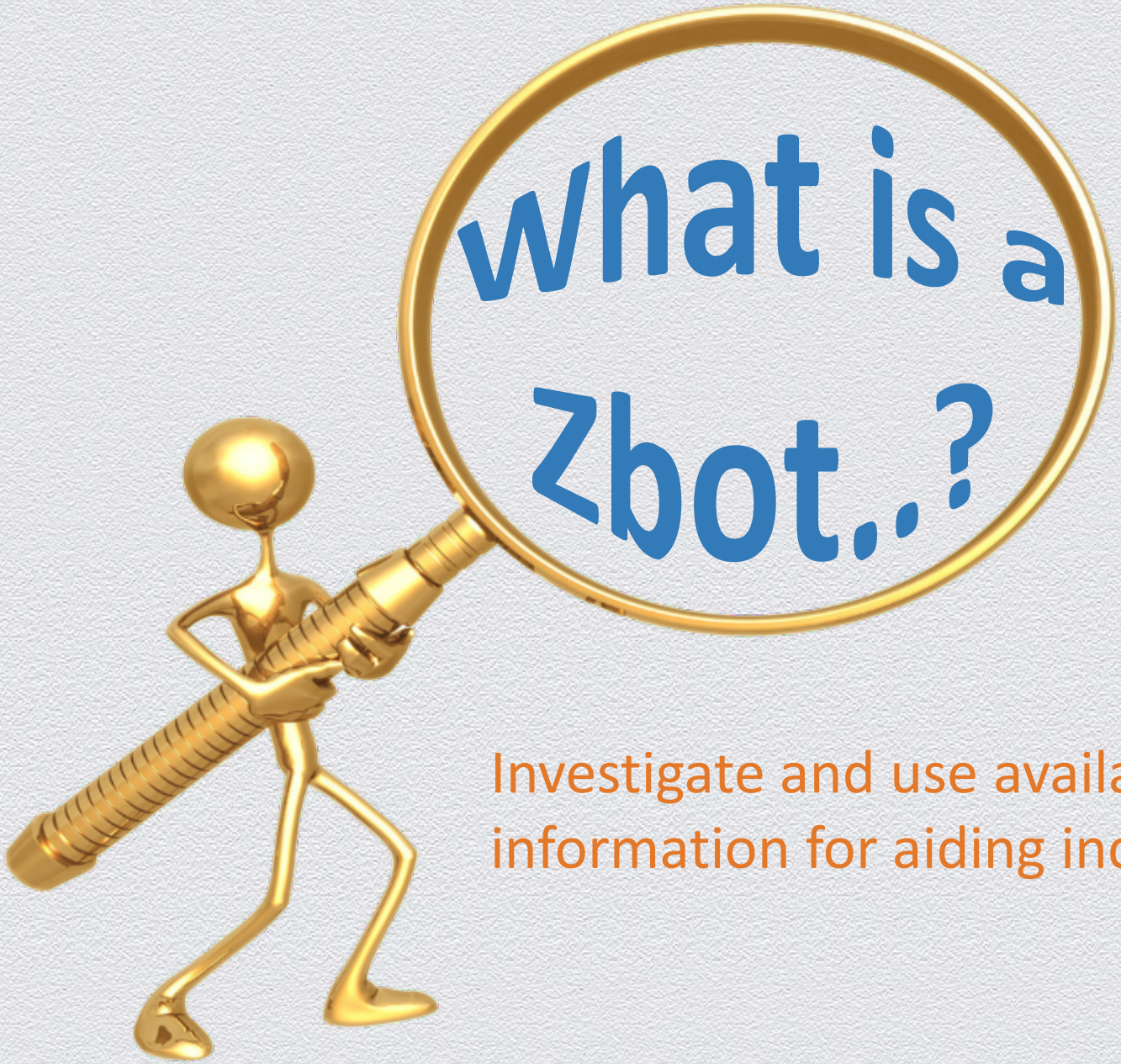
DOWNLOADER

C&C Information

mentoringgroup.com	216.171.192.113
davistructures.com	173.255.128.30

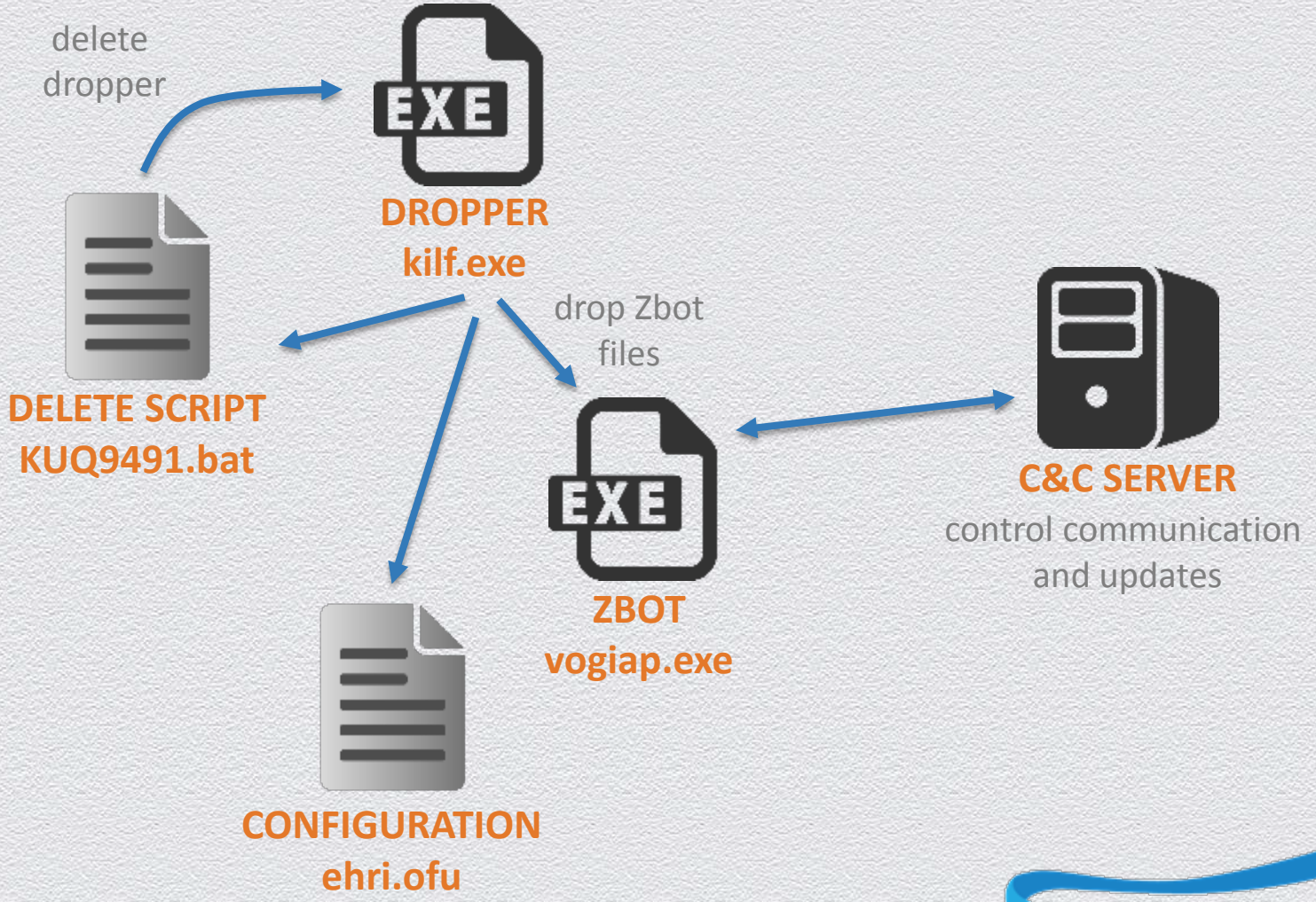
Dropped Malware: Win32.Zbot

kilf.exe	378.00 KB (387072 bytes)
vogiap.exe	378.00 KB (387072 bytes)
KUQ9491.bat	174 bytes
ehri.ofu	482 bytes



Investigate and use available threat information for aiding incident response!

Win32.Zbot


delete
dropper
EXE
DROPPER
kilf.exe
drop Zbot
files
DELETE SCRIPT
KUQ9491.bat
EXE
ZBOT
vogiap.exe
C&C SERVER
control communication
and updates
CONFIGURATION
ehri.ofu

STEALTH & PERSISTANCE

- Persistance via Windows Registry

Keyname	HKU\...\Software\Microsoft\Windows\CurrentVersion\Run\Gerwilo
Keyvalue	C:\Documents and Settings\...\Application Data\Wihoxq\vogiap.exe

- DLL-Injection on Startup
- Infection of system process
- On-the-fly updates

BEHAVIOR ONCE RESIDENT

- API Hooks in Userland:
  wininet.dll, user32.dll, ws2_32.dll,...

```
…..
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!InternetCloseHandle
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpQueryInfoA
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpOpenRequestA
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpOpenRequestW
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!InternetReadFile
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpSendRequestA
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpSendRequestExW
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpEndRequestA
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!HttpSendRequestW
.text   C:\WINDOWS\Explorer.EXE[1320] WININET.dll!InternetReadFileExA
....
```

ATTACK TIMELINE

Malicious E-Mail

Win32.Upatre Downloader

Persistance

Win32.Zbot

Data Exfiltration

BE SMARTER

Employee Awareness / E-Mail Filter

Perimeter Security

Intelligent Endpoint Protection

Threat Intelligence Correlati

Data Leak Prevention

Malicious E-Mail

Win32.Upatre Downloader

stance

Zbot

a Exfiltration

CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Keep track of the threats that target you!

CYPHORT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

SMALL DATA ANALYSIS

SESSION ID: TRM-T10

Thank you for your attention!

Marion Marschalek
Malware Researcher
Cyphort Inc.
@pinkflawd

Resources

- https://drive.google.com/file/d/0B9Mrr-en8FX4MS1HdjBjNEhYWk0/edit?usp=sharing
  “Upatre Technical Paper” by Marion Marschalek
- http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013
  “Kaspersky Security Bulletin 2013” by Kaspersky Labs
- http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
  “Sophos Security Threat Report 2014” by Sophos Labs
- http://www.sophos.com/medialibrary/PDFs/technical%20papers/Sophos%20what%20is%20zeus%20tp.pdf
  “What is Zeus?” By Sophos Labs
- http://threatgeek.typepad.com/.a/6a0147e41f3c0a970b017d3be346ef970c-pi
  Threat Toons