

SMALL DATA ANALYSIS

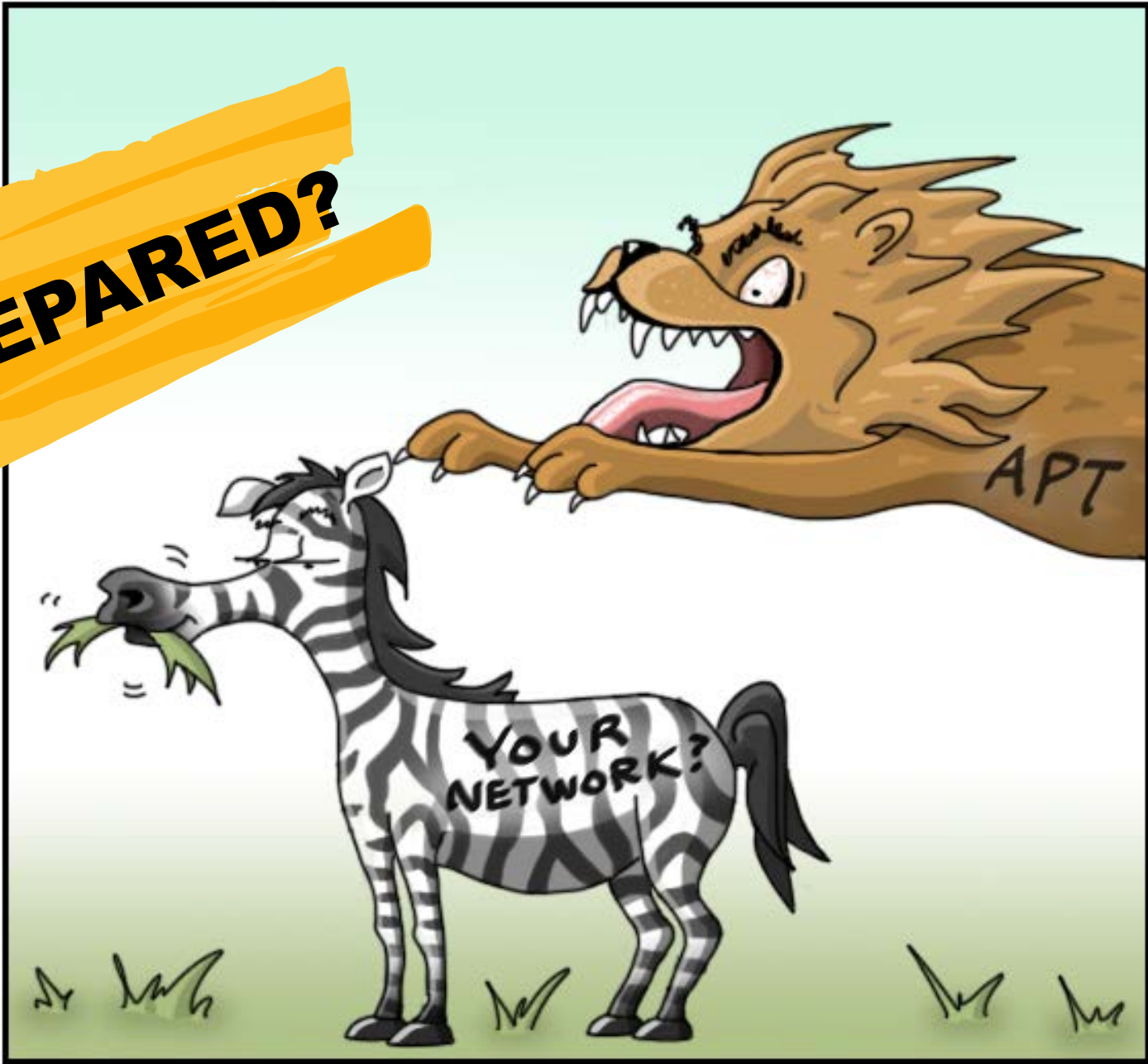
SESSION ID: TRM-T10

Marion Marschalek

Malware Researcher
Cyphort Inc.
@pinkflawd



PREPARED?



THE CYBERSECURITY SAVANNA

The Malware Situation

Attack Insights

Malware Analyst's Bootcamp

Malware in 1998



Malware today



Image Copyright IKARUS Security Software GmdH

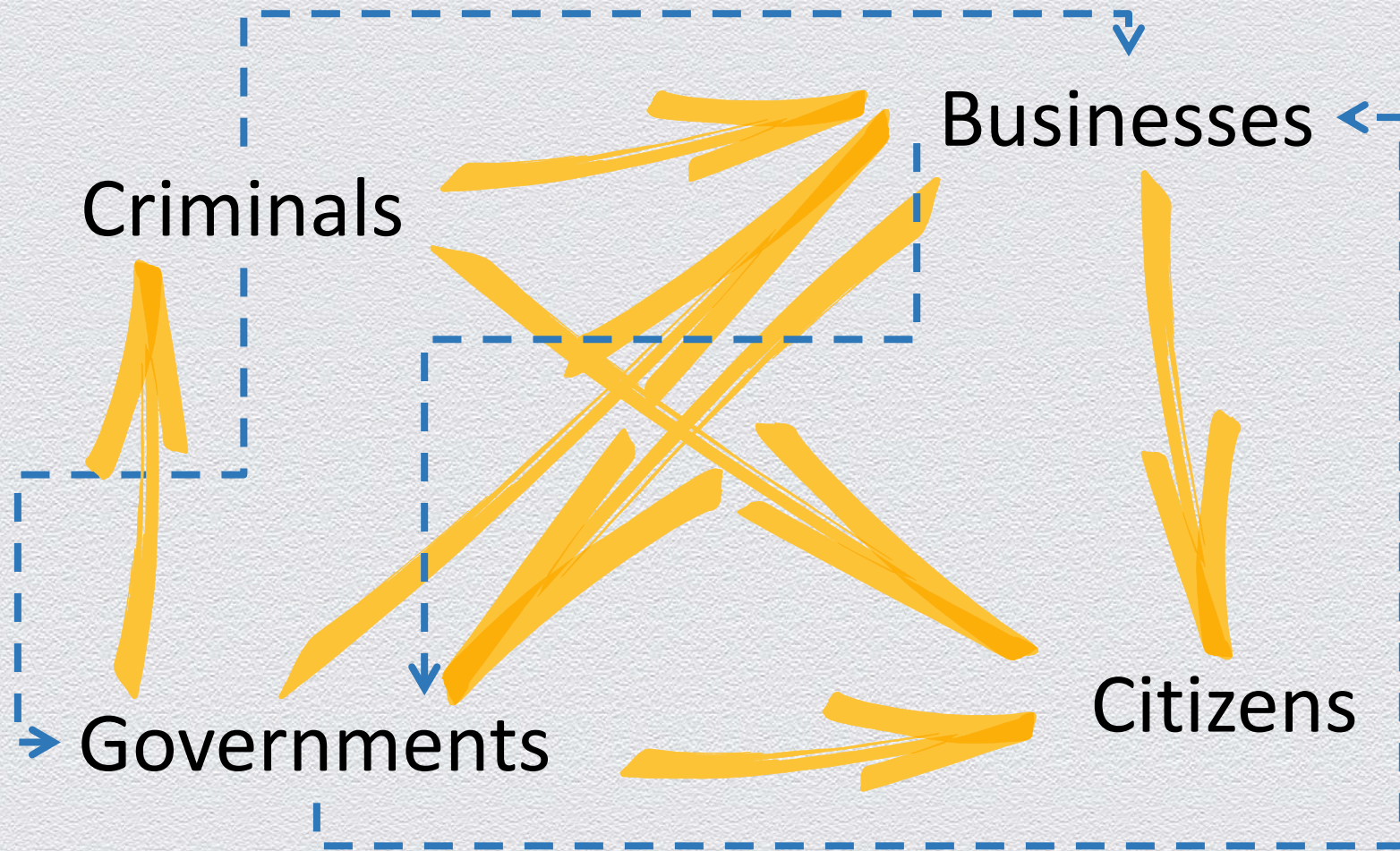
Image Copyright IKARUS Security Software GmdH

NEXT?

#RSAC

RSACONFERENCE 2014
ASIA PACIFIC & JAPAN

Good Folks, Bad Folks & Real Life



MALWARE

/ˈmɒlwɛːə/

Software that
doesn't come
with an EULA

- Morgan Marquis-Boire

EXPONENTIAL TIMES

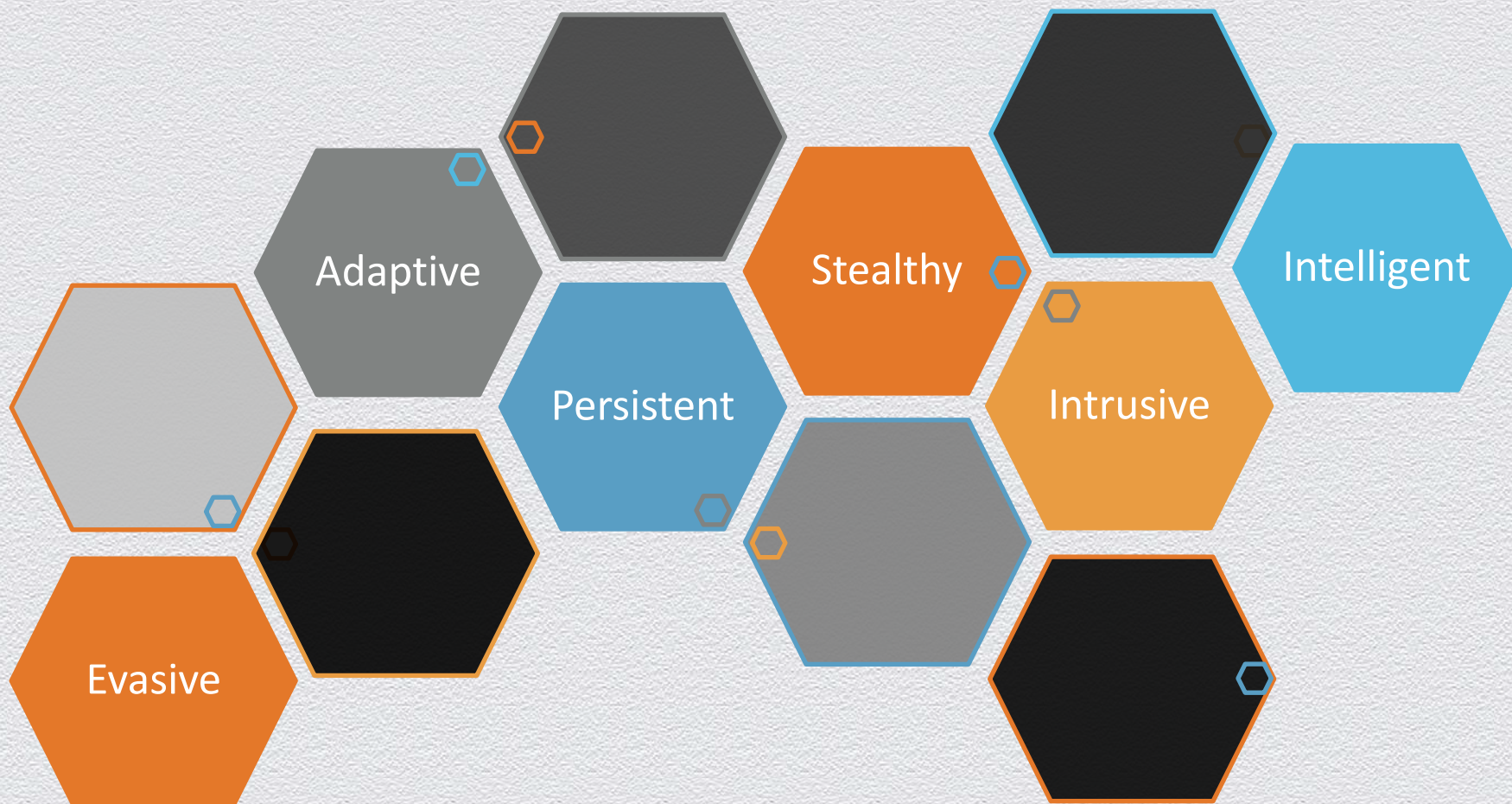
- ◆ **Botnets and mass malware** relaunching
- ◆ **Internet** main attack vector – 1.7 billion infections
 - ◆ >90% of drive-by infections via Java vulnerabilities!
- ◆ **Android malware** getting smarter, more than 300 families
 - ◆ >150.000 samples - total growth of 800% since last year
- ◆ Malware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

**All platforms
are at risk!**

http://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Report_Statistics_for_2013

<http://www.sophos.com/en-us/medialibrary/PDFs/other/operation-windigo-report-2014.pdf>

MULTIFUNCTIONAL THREATS



SMARTER ANALYSTS

SIMULATION

VIRTUALIZATION

**STATIC
ANALYSIS**

DISASSEMBLY

DEBUGGING

**ARTIFICIAL
INTELLIGENCE**

SIMULATION

VIRTUALIZATION

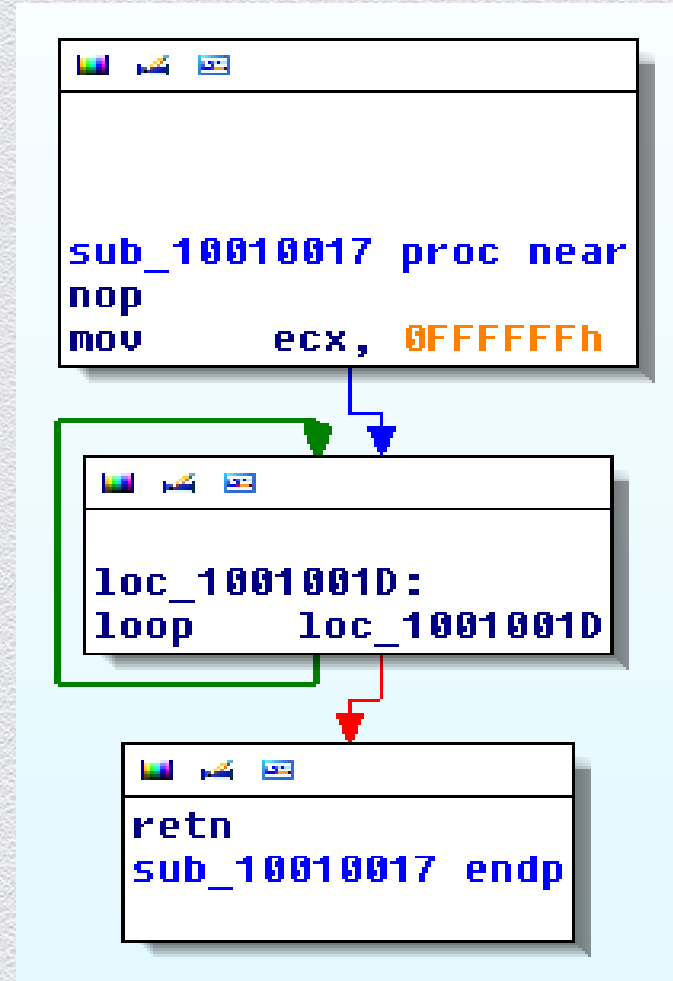
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
2:003F2610 mov [ebp+var_44], 'U'
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], 'h'
```


SIMULATION

VIRTUALIZATION

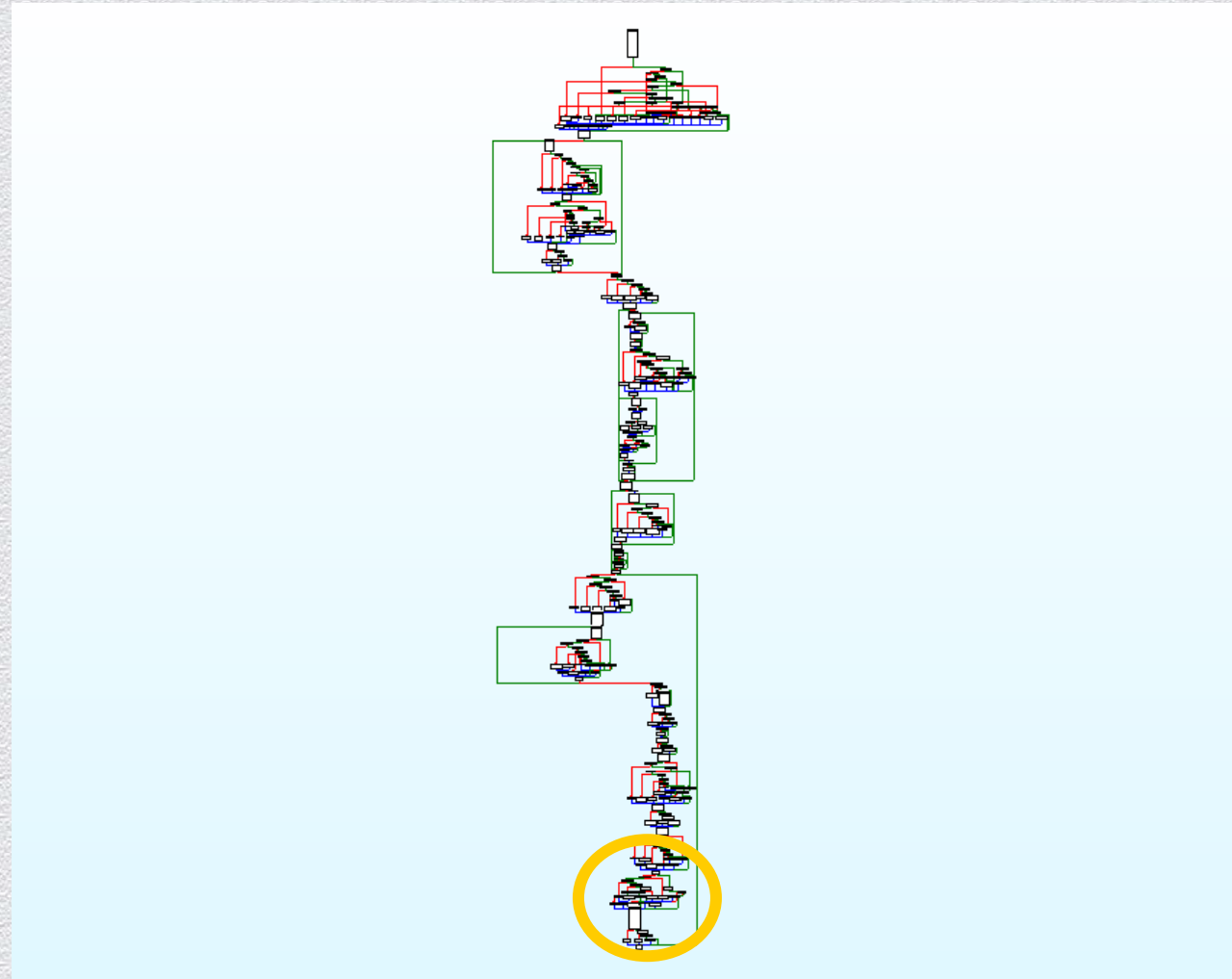
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
01047 0F 84 FF FF FF FF jz near ptr loc_401047+5
01040 00 68 43 add [eax+43h], ch
01050 22 15 90 58 31 05 and dl, ds:5315890h
01056 00 30 add [eax+0], dh
01058 40 inc eax
01059 00 B9 00 00 00 10 add [ecx+10000000h], bh

01045 3B C0 cmp eax, eax
01045 -----
01047 0F db 0Fh
01048 84 FF FF FF dd 0FFFFFF84h
0104C -----
0104C FF 00 inc dword ptr [eax]
0104E 68 02 22 15 00 push 00152212h
01053 58 pop eax
01054 31 05 00 30 40 00 xor dword_403000, eax
0105A B9 00 00 00 10 mov ecx, 10000000h
```


SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
00401C80 push    ebp
00401C81 mov     ebp, esp
00401C83 push    0FFFFFFFh
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
```


SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN




ATTACK INSIGHTS

WOLF IN SHEEP OUTFIT

20KB of Wolf

Ihre Amazon.de Bestellung


If there are problems with how this message is displayed, click here to view it in a web browser.

Sent: So 22.12.2013 12:00

To: 

 Message  Invoice (21 KB)

WOLF

amazon.de

[Amazon Shopping-App](#) | [Mein Konto](#) | [Amazon.de](#)

Bestellbestätigung

Bestellung: #304-0678313-0972324

Guten Tag,

vielen Dank für Ihre Bestellung. Wir werden Sie benachrichtigen, sobald Ihr(e) Artikel versandt wurde(n).

Sie finden das voraussichtliche Lieferdatum weiter unten. Um Ihre Bestellung anzusehen oder zu verändern, besuchen Sie [Meine Bestellungen](#) auf unserer Website.

Lieferung voraussichtlich:

Donnerstag, 9. Dezember 2013


Samstag, 11. Dezember 2013

Versandart:

Standard-Versand

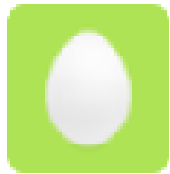
[Bestelldetails](#)

Die Bestellung geht an:


Wien, 1050

Österreich

A STEP BACK IN TIME ...



Tasha Kalley @tashikaami

jetzt

so happy, just finished ordering all my christmas presents on
[#Amazon](#) :)

Öffnen

← Antworten

🗑 Löschen

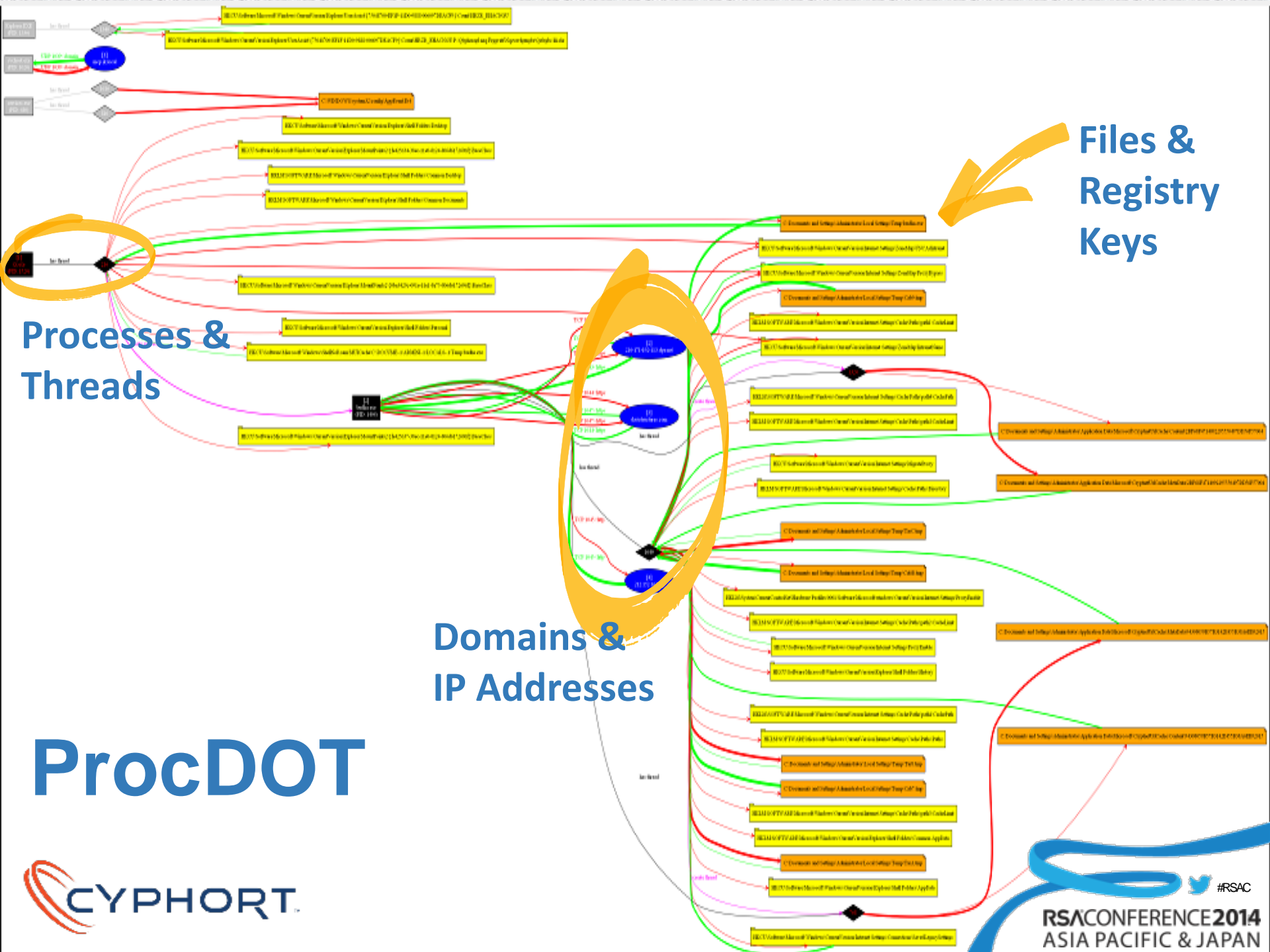
★ Favorisieren

⋮ Mehr

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



EVIL!



Processes & Threads

Files & Registry Keys

Domains & IP Addresses

ProcDOT



Quick Overview

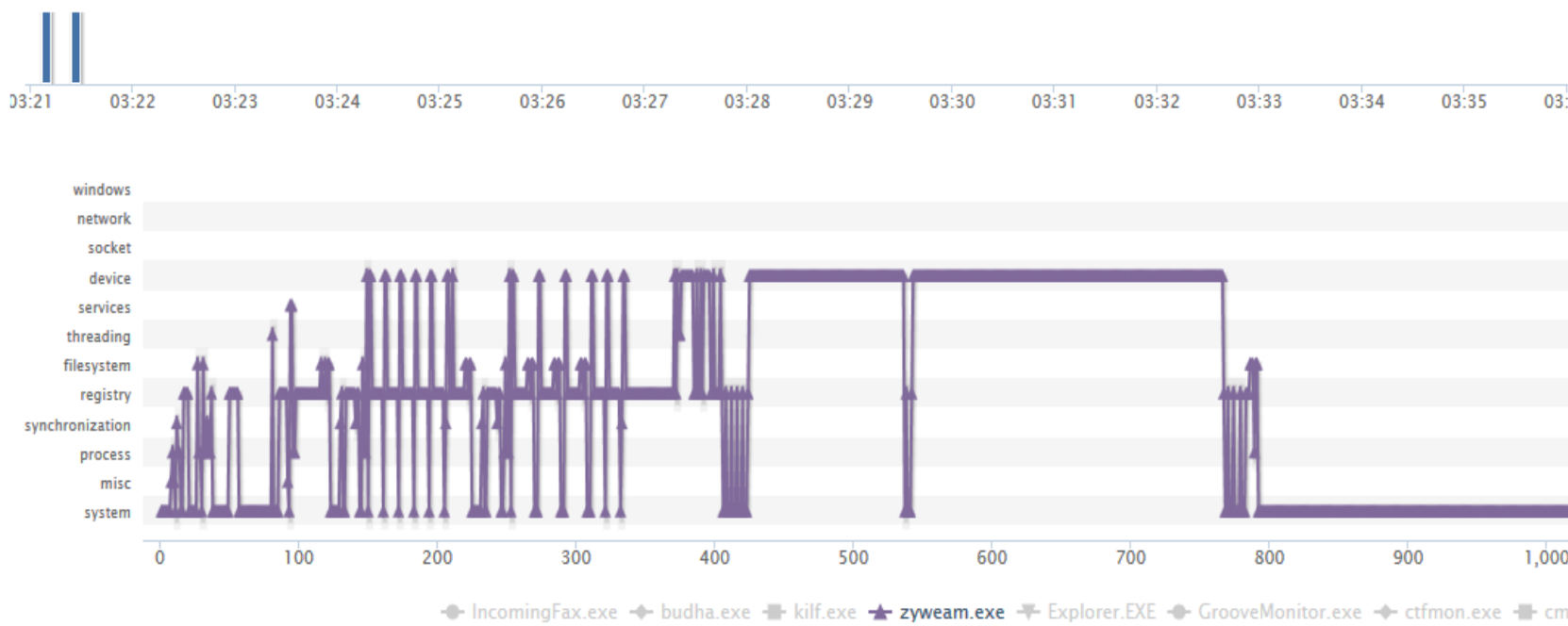
Static Analysis

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

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



**DIG THE
SMALL
DATA ...**

IDA - C:\Documents and Settings\Administrator\Desktop\ida.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_401680
- sub_401688
- sub_401690
- sub_401698
- sub_4016A0
- sub_4016A8
- sub_4016B0
- sub_4016B8
- sub_4016C0
- sub_4016C8
- sub_4016D0
- sub_4016D8
- sub_4016E0
- sub_4016E8
- sub_4016F0
- sub_4016F8
- sub_401700
- sub_401708
- sub_401710
- sub_401718
- sub_401720
- sub_401728
- sub_401730
- sub_401738
- sub_401740
- sub_401748
- sub_401750
- sub_401758
- sub_401760
- sub_401768
- sub_401770
- sub_401778
- sub_401780
- sub_401788
- sub_401790
- sub_401798
- sub_4017A0
- sub_4017A8
- sub_4017B0
- sub_4017B8
- sub_4017C0
- sub_4017C8
- sub_4017D0
- sub_4017D8
- sub_4017E0
- sub_4017E8
- sub_4017F0
- sub_4017F8
- sub_401800
- sub_401808
- sub_401810
- sub_401818
- sub_401820
- sub_401828
- sub_401830
- sub_401838
- sub_401840
- sub_401848
- sub_401850
- sub_401858
- sub_401860
- sub_401868
- sub_401870
- sub_401878
- sub_401880
- sub_401888
- sub_401890
- sub_401898
- sub_4018A0
- sub_4018A8
- sub_4018B0
- sub_4018B8
- sub_4018C0
- sub_4018C8
- sub_4018D0
- sub_4018D8
- sub_4018E0
- sub_4018E8
- sub_4018F0
- sub_4018F8
- sub_401900
- sub_401908
- sub_401910
- sub_401918
- sub_401920
- sub_401928
- sub_401930
- sub_401938
- sub_401940
- sub_401948
- sub_401950
- sub_401958
- sub_401960
- sub_401968
- sub_401970
- sub_401978
- sub_401980
- sub_401988
- sub_401990
- sub_401998
- sub_4019A0
- sub_4019A8
- sub_4019B0
- sub_4019B8
- sub_4019C0
- sub_4019C8
- sub_4019D0
- sub_4019D8
- sub_4019E0
- sub_4019E8
- sub_4019F0
- sub_4019F8
- sub_401A00
- sub_401A08
- sub_401A10
- sub_401A18
- sub_401A20
- sub_401A28
- sub_401A30
- sub_401A38
- sub_401A40
- sub_401A48
- sub_401A50
- sub_401A58
- sub_401A60
- sub_401A68
- sub_401A70
- sub_401A78
- sub_401A80
- sub_401A88
- sub_401A90
- sub_401A98
- sub_401AA0
- sub_401AA8
- sub_401AB0
- sub_401AB8
- sub_401AC0
- sub_401AC8
- sub_401AD0
- sub_401AD8
- sub_401AE0
- sub_401AE8
- sub_401AF0
- sub_401AF8
- sub_401B00
- sub_401B08
- sub_401B10
- sub_401B18
- sub_401B20
- sub_401B28
- sub_401B30
- sub_401B38
- sub_401B40
- sub_401B48
- sub_401B50
- sub_401B58
- sub_401B60
- sub_401B68
- sub_401B70
- sub_401B78
- sub_401B80
- sub_401B88
- sub_401B90
- sub_401B98
- sub_401BA0
- sub_401BA8
- sub_401BB0
- sub_401BB8
- sub_401BC0
- sub_401BC8
- sub_401BD0
- sub_401BD8
- sub_401BE0
- sub_401BE8
- sub_401BF0
- sub_401BF8
- sub_401C00
- sub_401C08
- sub_401C10
- sub_401C18
- sub_401C20
- sub_401C28
- sub_401C30
- sub_401C38
- sub_401C40
- sub_401C48
- sub_401C50
- sub_401C58
- sub_401C60
- sub_401C68
- sub_401C70
- sub_401C78
- sub_401C80
- sub_401C88
- sub_401C90
- sub_401C98
- sub_401CA0
- sub_401CA8
- sub_401CB0
- sub_401CB8
- sub_401CC0
- sub_401CC8
- sub_401CD0
- sub_401CD8
- sub_401CE0
- sub_401CE8
- sub_401CF0
- sub_401CF8
- sub_401D00
- sub_401D08
- sub_401D10
- sub_401D18
- sub_401D20
- sub_401D28
- sub_401D30
- sub_401D38
- sub_401D40
- sub_401D48
- sub_401D50
- sub_401D58
- sub_401D60
- sub_401D68
- sub_401D70
- sub_401D78
- sub_401D80
- sub_401D88
- sub_401D90
- sub_401D98
- sub_401DA0
- sub_401DA8
- sub_401DB0
- sub_401DB8
- sub_401DC0
- sub_401DC8
- sub_401DD0
- sub_401DD8
- sub_401DE0
- sub_401DE8
- sub_401DF0
- sub_401DF8
- sub_401E00
- sub_401E08
- sub_401E10
- sub_401E18
- sub_401E20
- sub_401E28
- sub_401E30
- sub_401E38
- sub_401E40
- sub_401E48
- sub_401E50
- sub_401E58
- sub_401E60
- sub_401E68
- sub_401E70
- sub_401E78
- sub_401E80
- sub_401E88
- sub_401E90
- sub_401E98
- sub_401EA0
- sub_401EA8
- sub_401EB0
- sub_401EB8
- sub_401EC0
- sub_401EC8
- sub_401ED0
- sub_401ED8
- sub_401EE0
- sub_401EE8
- sub_401EF0
- sub_401EF8
- sub_401F00
- sub_401F08
- sub_401F10
- sub_401F18
- sub_401F20
- sub_401F28
- sub_401F30
- sub_401F38
- sub_401F40
- sub_401F48
- sub_401F50
- sub_401F58
- sub_401F60
- sub_401F68
- sub_401F70
- sub_401F78
- sub_401F80
- sub_401F88
- sub_401F90
- sub_401F98
- sub_401FA0
- sub_401FA8
- sub_401FB0
- sub_401FB8
- sub_401FC0
- sub_401FC8
- sub_401FD0
- sub_401FD8
- sub_401FE0
- sub_401FE8
- sub_401FF0
- sub_401FF8

IDA View-A

Hex View

Structures

Enums

Graph overview

Line 2 of 49

63.77% (-57,470) (986,574) 00000710 00401110: sub_401110

SMALL DATA ANALYSIS
 Win32.Upatre
 Win32.Zbot

```

== GUID-Finder plug-in: v: 1.0A - Dec 20 2007, By Sirmabus ==
-----
Python 2.6.5 (x265:79096, 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 summary is has been finalized.
<Default debugger> - incmpat - loaded 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
  
```



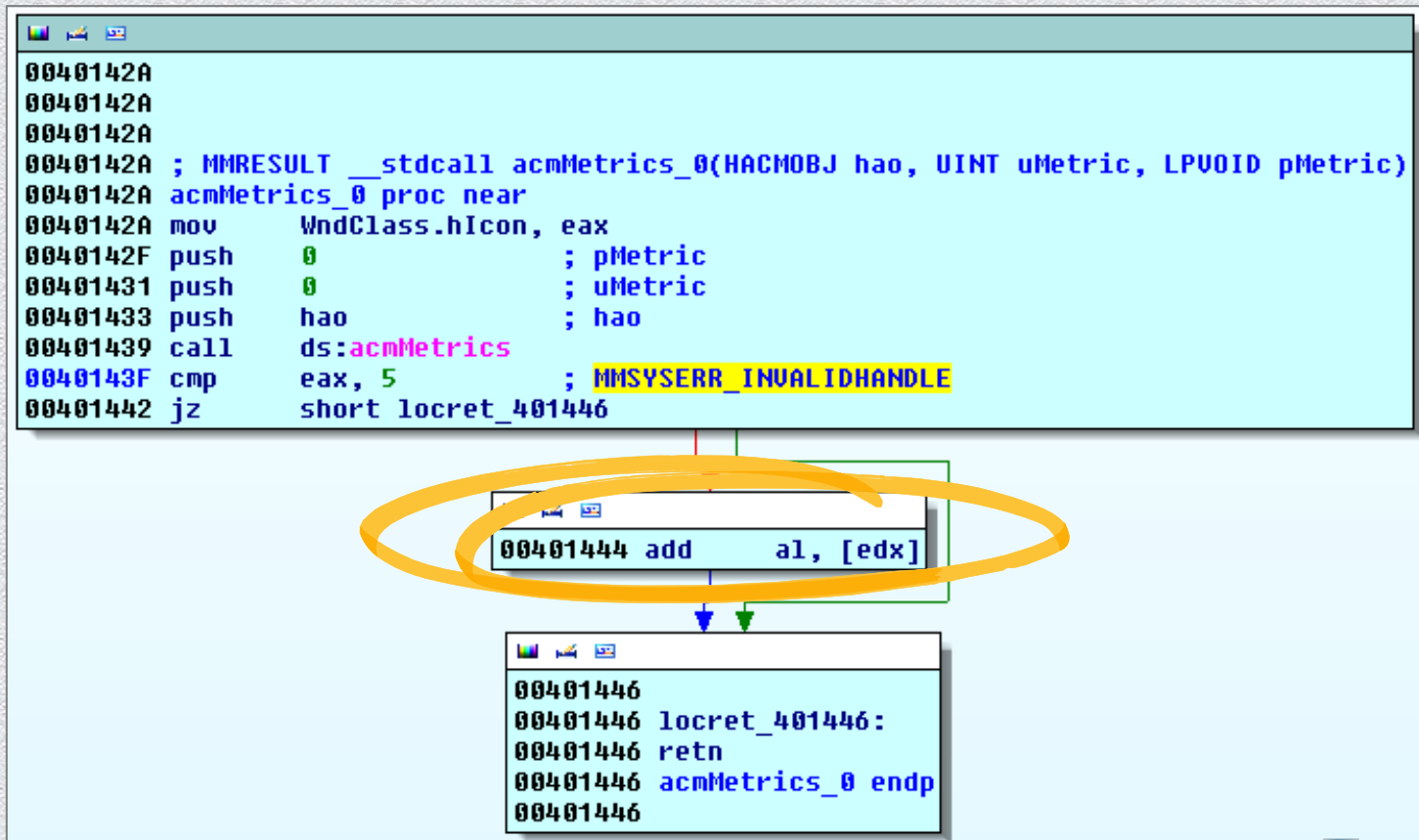
WIN32.UPATRE

Protected
Packed
Downloader.



PROTECTION

ANTI SIMULATION



PROTECTION

BREAKPOINT DETECTION

```
00401451
00401451
00401451 decrypt_n_jumptab ptr
00401451
00401451 var_4= dword ptr
00401451
00401451 xor     esi, esi
00401453 add     esi, offset unk_40100F
00401459 xor     edi, edi
0040145B add     edi, esi
0040145D mov     ebx, eax
0040145F add     ebx, 6
00401462 mov     eax, 30h
00401467 mov     edx, fs:[eax]
0040146A push   edx
0040146B push   0
0040146D mov     ecx, 34Ch

00401472 loc_401472: ; start 40100F
00401473 mov     al, [esi]
00401474 sub     al, bl
00401476 stosb
00401477 add
00401478 mov     ecx
0040147B cmp     ecx, 0
0040147E jnz     short loc_401472
```


PROTECTION

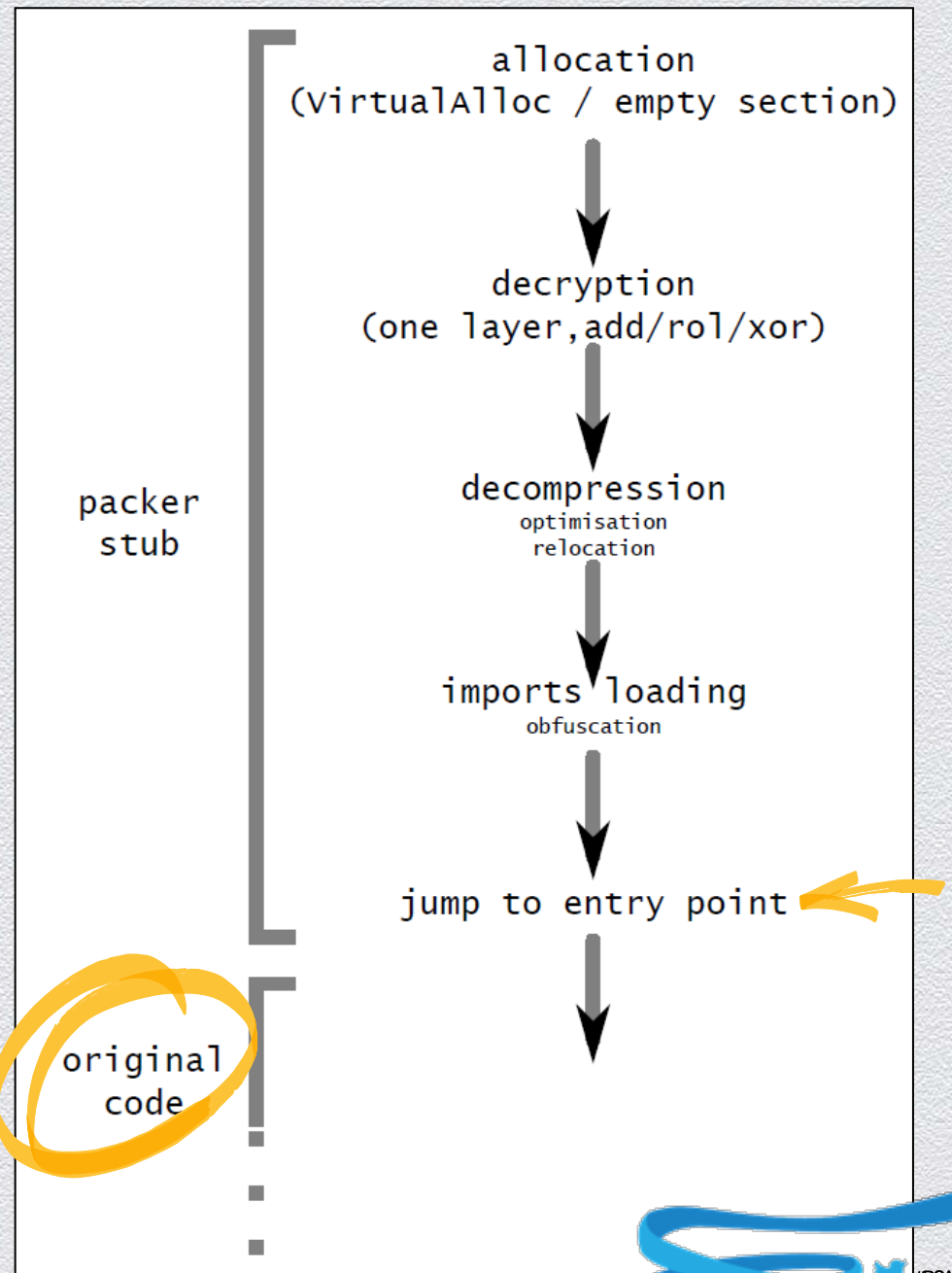
TIMING

DEFENCE

```
.text:00401117 mov     edi, ds:byte_40118F
.text:00401119 rdtsc
.text:0040111B 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:00401137 descryption_rdtsc endp
.text:00401137
.text:00401137 rdtsc
.text:00401139 pop     edx
.text:0040113B sub     eax, edx
.text:0040113D sub     esp, 18h
.text:0040113F push   0
.text:00401141 push   heap_403040
.text:00401143 call   dword ptr ds:acmStreamOpen
```


PACKER

What is a packer?
How to identify it?



PACKER

3 Stages

- ◆ Data Compression
- ◆ Decryption
- ◆ Decompression with
RtlDecompressBuffer

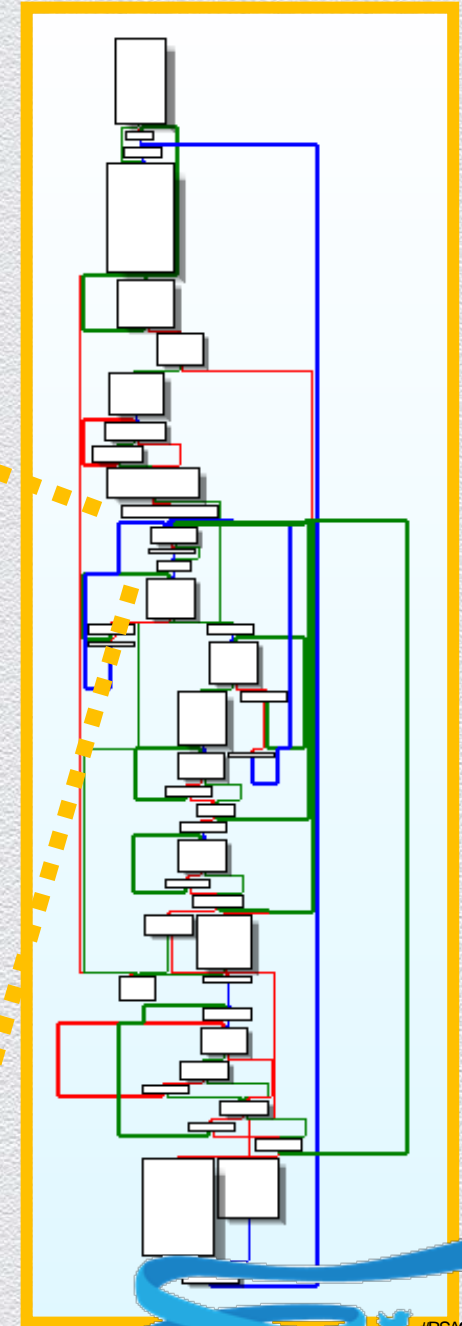
```
1  WORD key_modifier = AC601330h
2  WORD sub_key = E25ED5B0h
3  WORD xor_key = 86E53278h
4  (WORD*) code = [offset_buffer]
5  int memsize = [size_buffer]
6
7  for (i=0; i<10; i++)
8  {
9      xor_key -= key_modifier          // underflow
10 }
11
12 for (i=0; i<memsize; i++)
13 {
14     code[i] =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


DOWNLOADER

```
00B111EA
00B111EA loc_B111EA:
00B111EA push  esi
00B111EB push  esi
00B111EC push  esi
00B111ED push  esi
00B111EE push  offset aUpdatesDownlader ; "Updates downloader"
00B111F3 call  off_B1206C
00B111F9 mov   [ebp+var_1C], eax
00B111FC cmp   eax, esi
00B111FE jz    loc_B110BD
```

```
00B11204 or    [ebp+var_8], 0FFFFFFFh
00B11208 mov  [ebp+var_34], offset aText ; "text/*"
00B1120F mov  [ebp+var_30], offset aApplication ; "application/*"
00B11216 mov  [ebp+var_2C], esi
```

```
00B11219
00B11219 loc_B11219:
00B11219 inc   [ebp+var_8]
00B1121C cmp   [ebp+var_8], 1
00B11220 jle  short loc_B11225
```



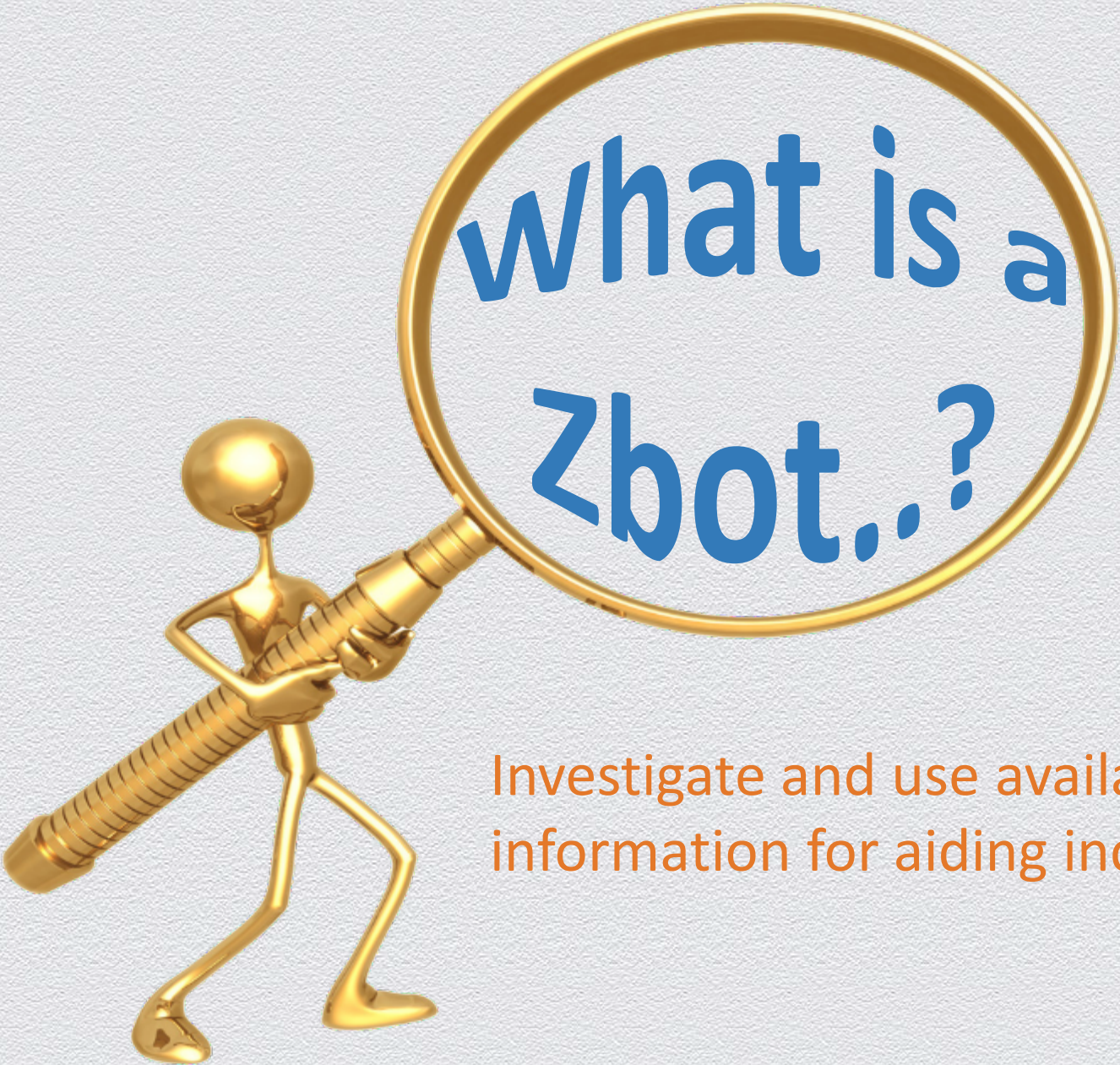
DOWNLOADER

C&C Information

mentoringgroup.com	216.171.192.113
davistructures.com	173.255.128.30

Dropped Malware: Win32.Zbot

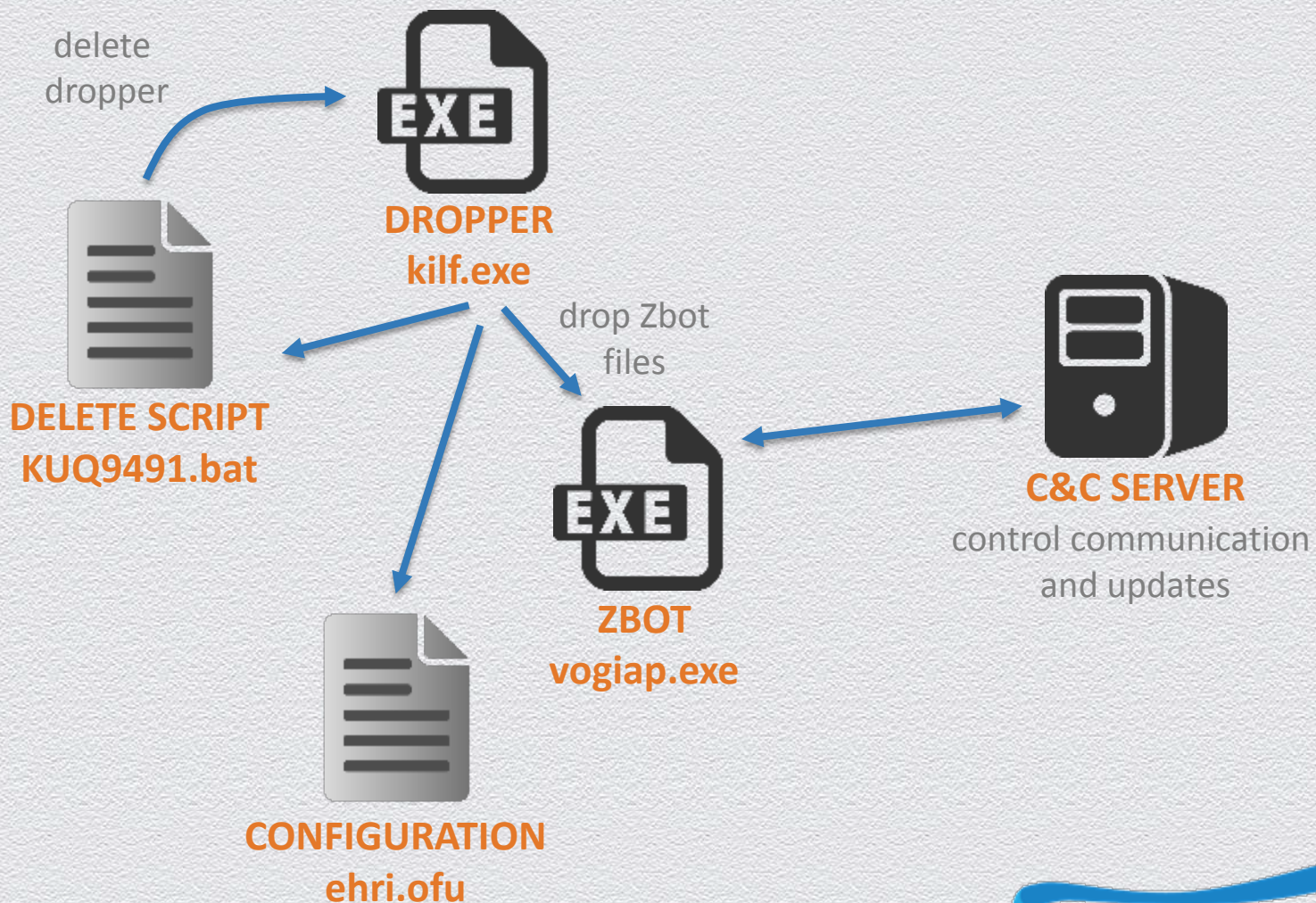
kilf.exe	378.00 KB (387072 bytes)
vogiap.exe	378.00 KB (387072 bytes)
KUQ9491.bat	174 bytes
ehri.ofu	482 bytes



what is a
Zbot..?

Investigate and use available threat information for aiding incident response!

Win32.Zbot



STEALTH & PERSISTENCE

- ◆ Persistence via Windows Registry

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

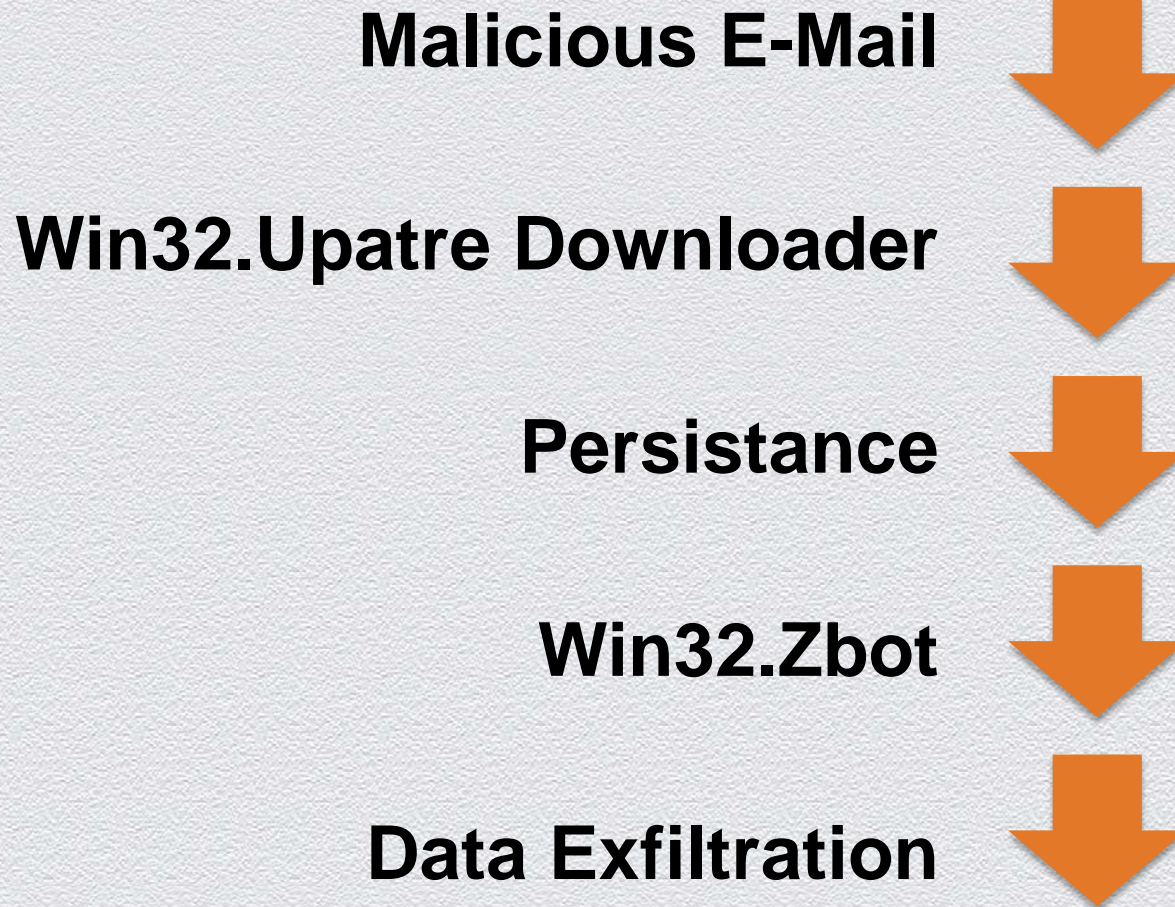
- ◆ DLL-Injection on Startup
- ◆ Infection of system process
- ◆ On-the-fly updates

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



BE SMARTER

Employee Awareness /
E-Mail Filter

Malicious E-Mail

Perimeter Security

Win32.Upatre Downloader

Intelligent Endpoint Protection

Malware Instance


Threat Intelligence Correlation

Bot

Data Leak Prevention

Data Exfiltration

**BREAK
THE
CHAIN**



**Keep track
of the threats
that target you!**

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_Overview_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