RSACONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

MALWARE UNDER THE HOOD
KEEPING YOUR INTELLECTUAL PROPERTY SAFE

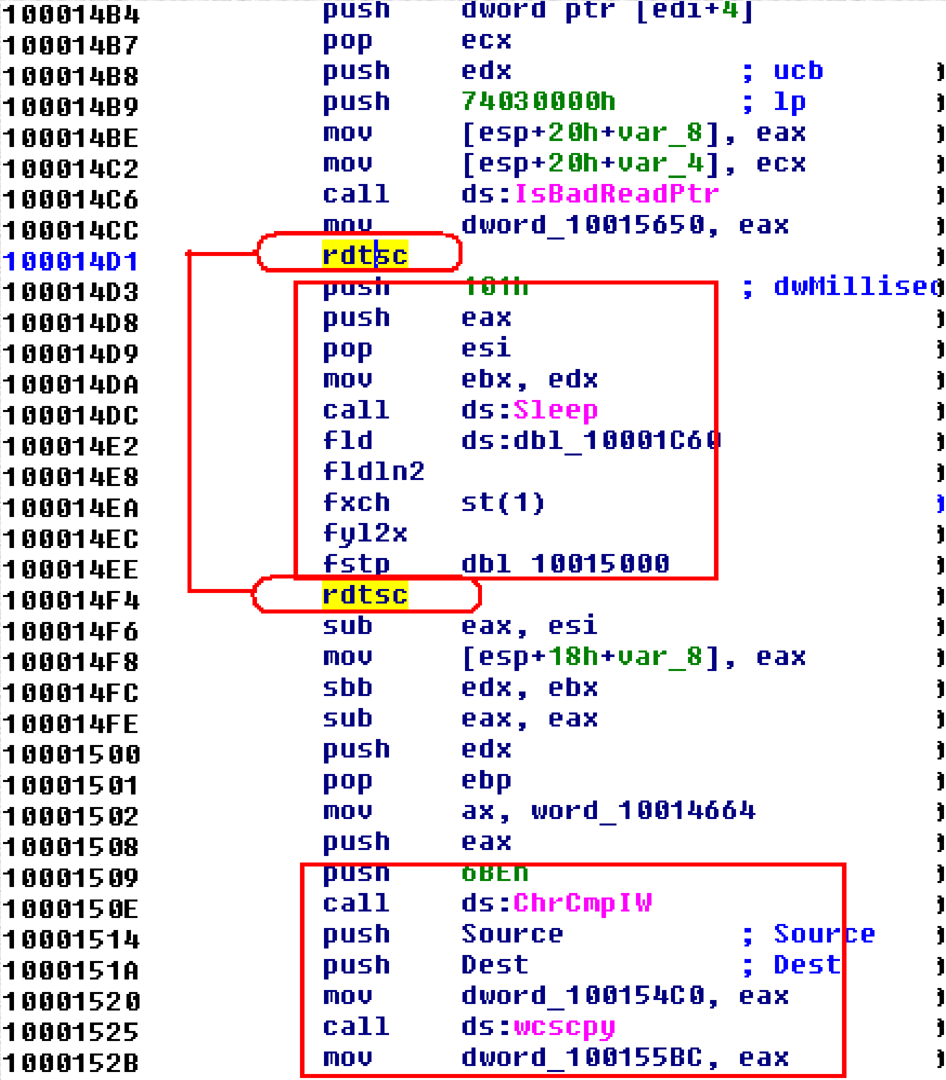
SESSION ID: ANF-F01

Marion Marschalek

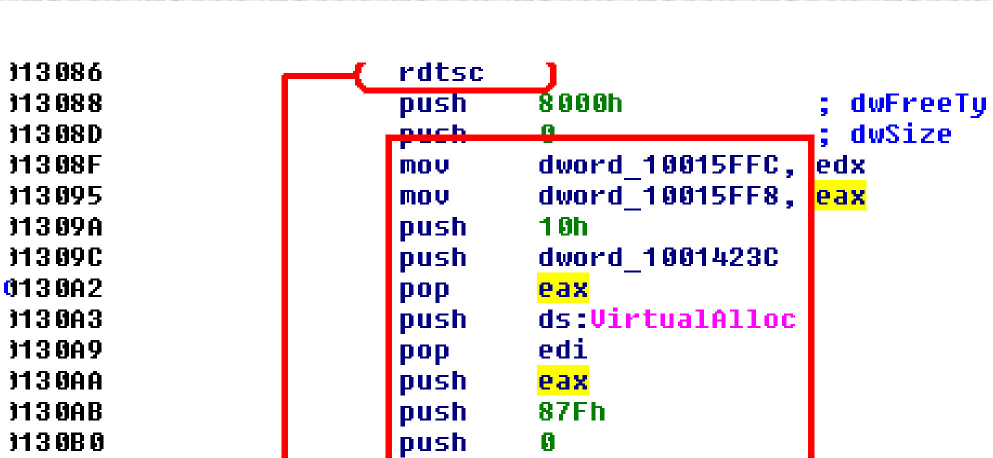
Malware Analyst
IKARUS
@pinkflawd

Mike Kendzierski

Technology Researcher
SHOSHN Ventures



```
100014B4                 push    dword ptr [edi+4]
100014B7                 pop     ecx
100014B8                 push    edx             ; ucb
100014B9                 push    74030000h       ; lp
100014BE                 mov     [esp+20h+var_8], eax
100014C2                 mov     [esp+20h+var_4], ecx
100014C6                 call    ds:IsBadReadPtr
100014CC                 mov     dword_10015650, eax
100014D1                 rdtsc
100014D3                 push    101h            ; dwMillisec
100014D8                 push    eax
100014D9                 pop     esi
100014DA                 mov     ebx, edx
100014DC                 call    ds:Sleep
100014E2                 fld     ds:dbl_10001C60
100014E8                 fldln2
100014EA                 fxch    st(1)
100014EC                 fyl2x
100014EE                 fstp    dbl_10015000
100014F4                 rdtsc
100014F6                 sub     eax, esi
100014F8                 mov     [esp+18h+var_8], eax
100014FC                 sbb     edx, ebx
100014FE                 sub     eax, eax
10001500                 push    edx
10001501                 pop     ebp
10001502                 mov     ax, word_10014664
10001508                 push    eax
10001509                 push    6BEh
1000150E                 call    ds:ChrCmpIW
10001514                 push    Source          ; Source
1000151A                 push    Dest            ; Dest
10001520                 mov     dword_100154C0, eax
10001525                 call    ds:wcscpy
1000152B                 mov     dword_100155BC, eax
```



```
)13086                 rdtsc
)13088                 push    8000h           ; dwFreeTy
)1308D                 push    0               ; dwSize
)1308F                 mov     dword_10015FFC, edx
)13095                 mov     dword_10015FF8, eax
)1309A                 push    10h
)1309C                 push    dword_1001423C
)130A2                 pop     eax
)130A3                 push    ds:VirtualAlloc
)130A9                 pop     edi
)130AA                 push    eax
)130AB                 push    87Fh
)130B0                 push    0
)130B2
)130B4                                                 es
)130B5
)130BB                                                 ab
)130BD                                                 is
)130C2
)130C8
)130CE
)130D0
)130D6
)130D8
)130DE
)130DF
)130E5
)130E7
)130E9
)130EA
)130EB
)130EC                 jmp     loc_10001E34
)130EC _DllMain@12     endp
```

BIG GOALS - ARE YOU MALWARED?

- Provide Insight
- Demonstrate
- Conclude

Back At You: Questionnaire

NO WE ARE NOT

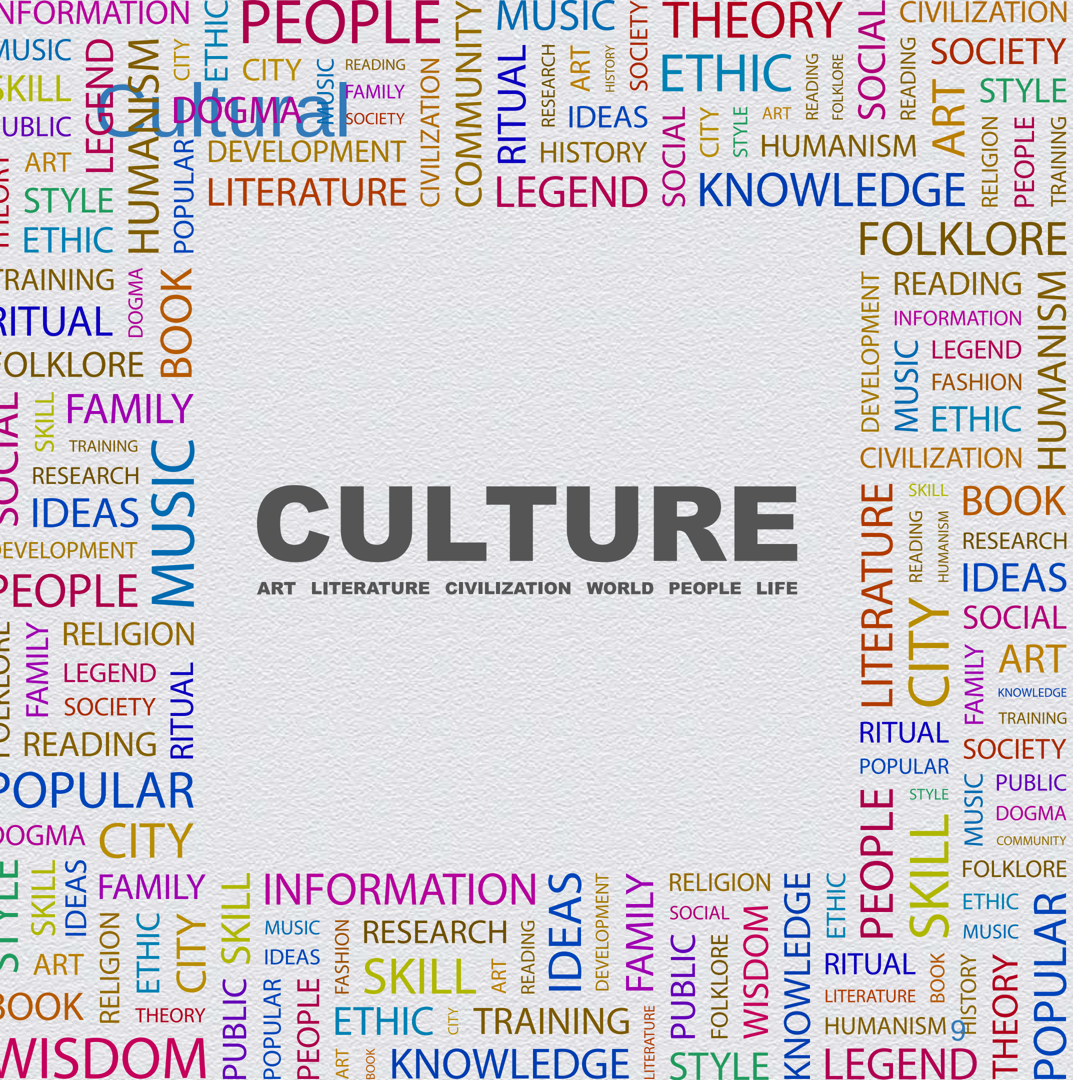
REAL HACKERS.

CALL TO ACTION

- Think and **adapt** as the bad guys do
- Better tools to **identify** and **attribute** malware
- Use **threat intelligence**
- Win the **war** – not the battle

YOUR TRADE SECRETS

ECONOMIC SHORTCUTS



NOT ALL CULTURES VALUE INTELLECTUAL PROPERTY

85% OF BREACHES involve the use of MALICIOUS SOFTWARE

WORLD has become scarier in 2014

- The number of malicious websites grew nearly 600%
- 85% of these sites on legitimate hosts
- Social media is increasingly used for spreading of malware
- Attacks become more targetted
- Growth of mobile malware of nearly 800% in 2013
- Malware adapts to the host it is infecting

http://www.websense.com/assets/reports/websense-2013-threat-report.pdf
http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

WORLD has become scarier in 2014

- The number of malicious websites grew nearly 600%
- 85% of these sites on legitimate hosts
- Social media is increasing
- Attacks become more
- Growth of mobile
- Malware adapts to the

ARE YOU PREPARED?

with the right skills

holistic security solutions

http://ww se-2013-threat-report.pdf

http://www.sophos. tary/PDFs/other/sophos-security-threat-report-2014.pdf

Copyright 1975 Universal Studios

YESTERDAY

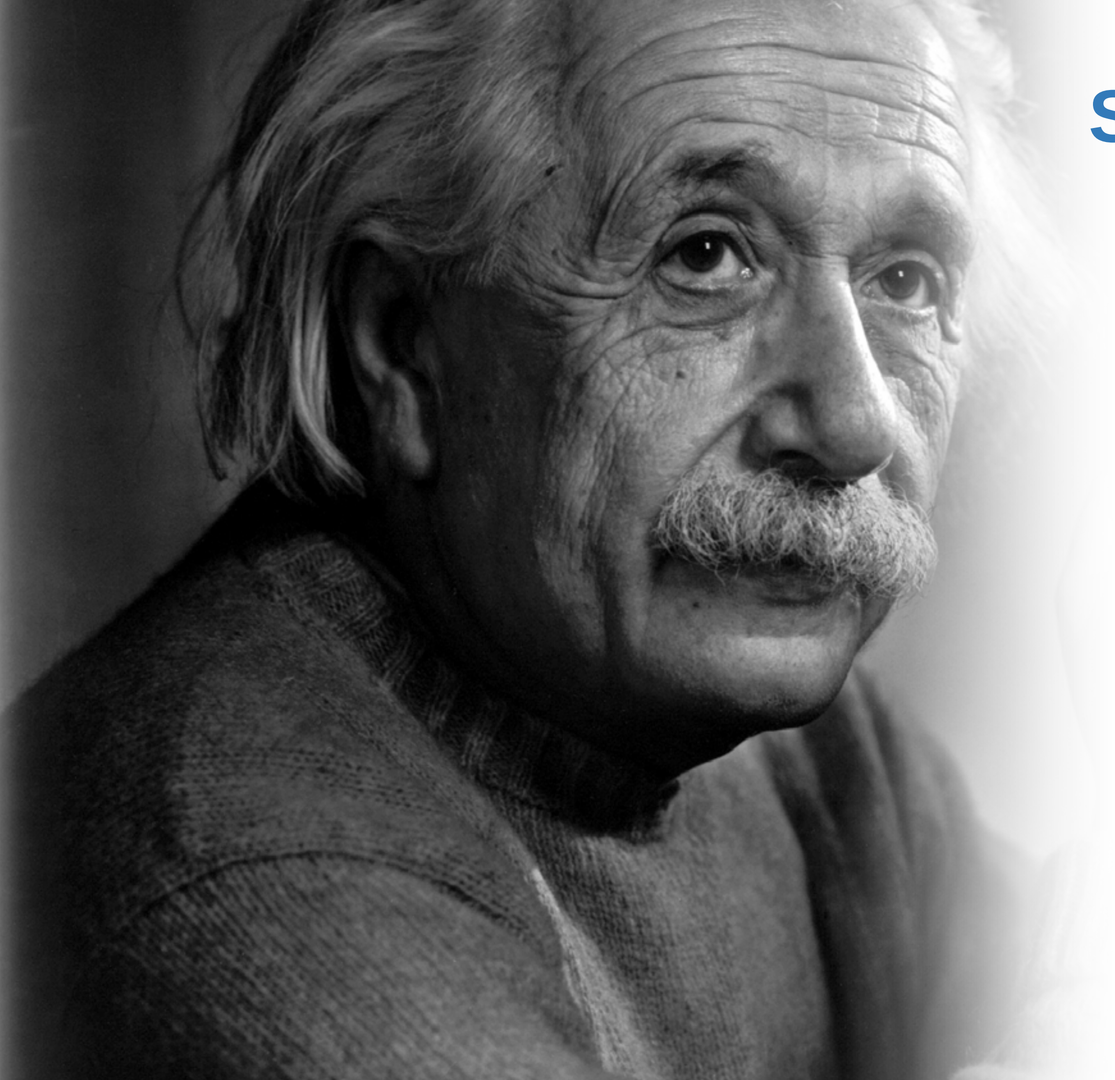
- FOCUSED
- SIMPLE
- PREDICTABLE
- EASY DETECTION

TODAY

- COMPLEX
- STEALTHY
- HIGHLY SOPHISTICATED
- ENOUGH SAID!

mass malware
for the masses

SOPHISTICATED MALWARE FOR THE BIG FISH



SOPHISTICATED

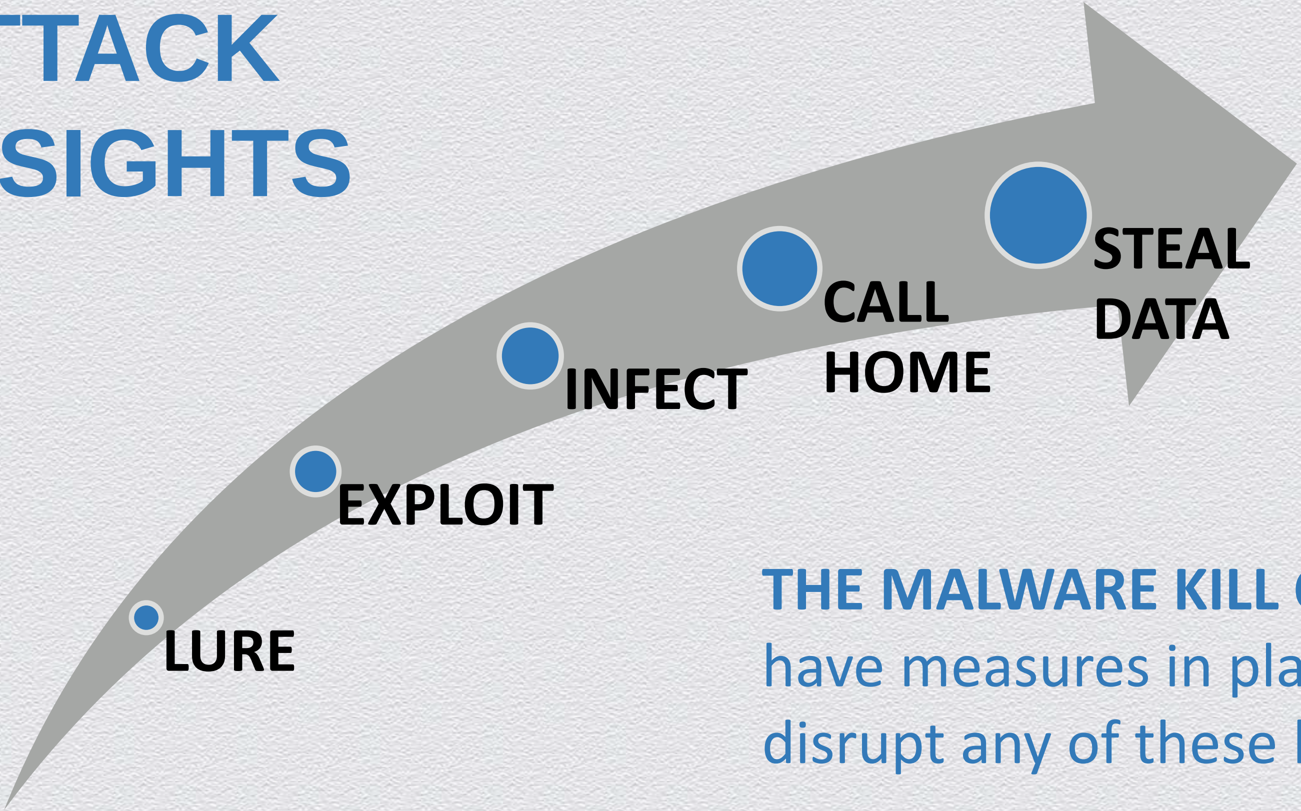
/səˈfistiˌkātid/ *adjective*

“If you can’t explain it simply, you don’t understand it well enough”

- Albert Einstein

UNDER THE HOOD

ATTACK INSIGHTS



THE MALWARE KILL CHAIN

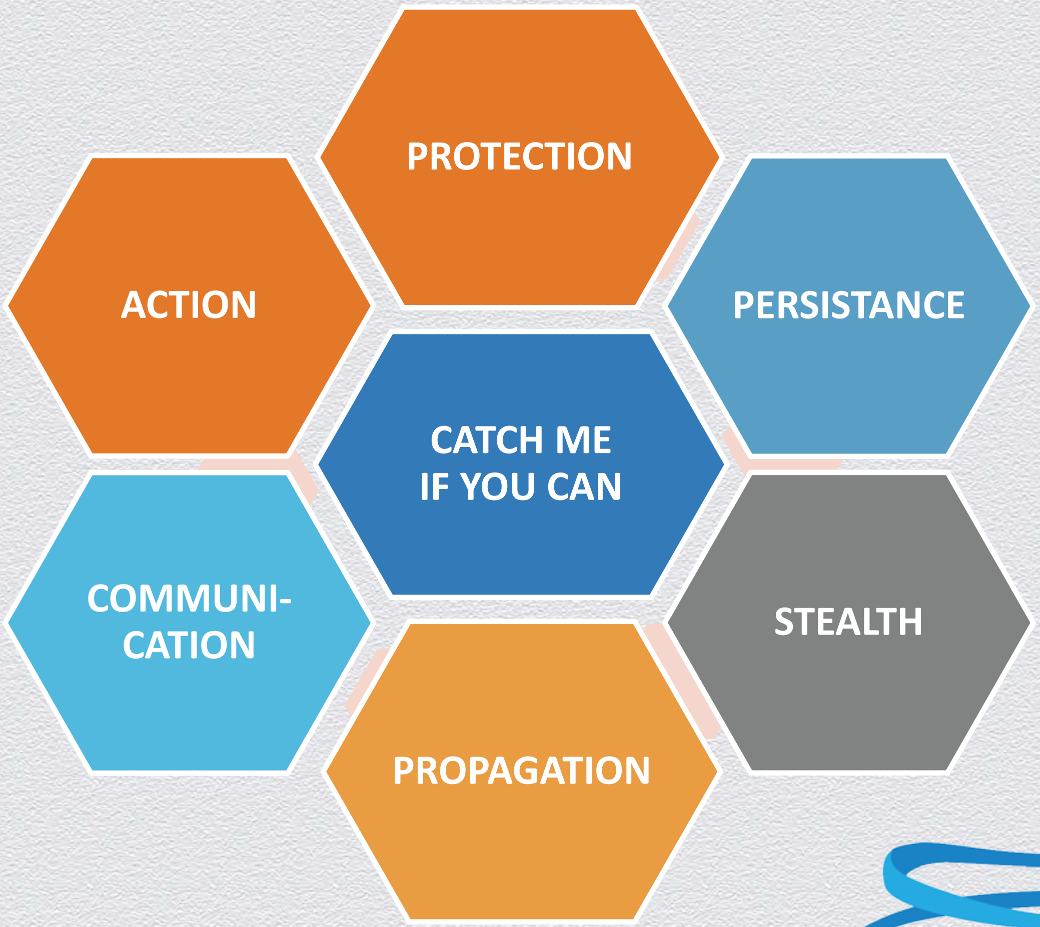
have measures in place to disrupt any of these links

INFECTION VECTORS

- Social Engineering
- Spear Phishing
- Web Drive-By
- Waterholing Attacks
- E-Mail
- Old School Hacking

Understanding is the first crucial step towards **protection**!

MALWARE CORE MODULES



ANALYSIS BOOTCAMP

HANDS ON

- Google Aided Reversing
- From Amazon With Malware
- The Big Evil In Small Pieces

#1 GOOGLE RESPONDED MY INCIDENT

- Malwared Hard Disk: Trojan.Win32.Skynet & Java CVE-2012-4681

1. String search in memory at runtime
2. Let Google do the rest…
3. Hit at blogpost from rapid7 with FUL

TOOLS RECOMMENDATION:

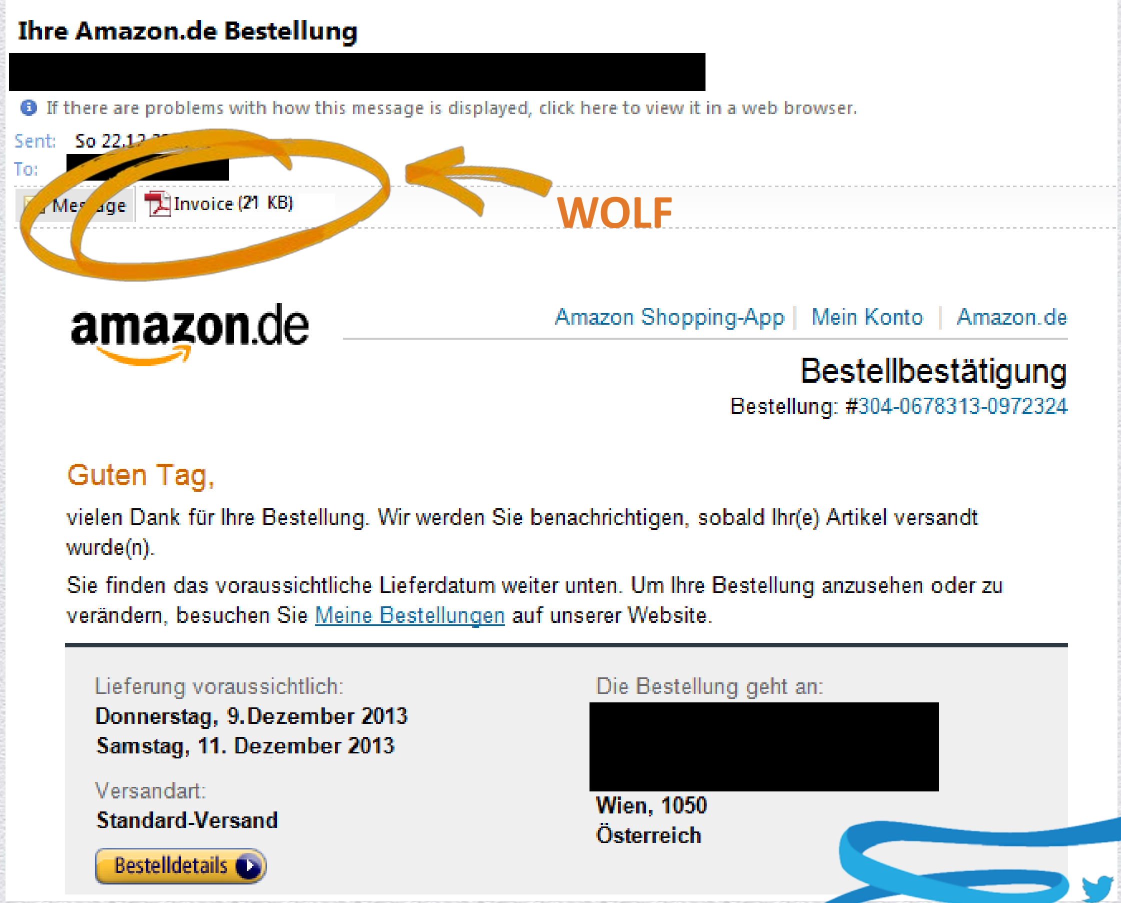
Virtual Machine

Sysinternals Toolsuite

Search Engine of Choice

#2 WOLF IN SHEEP OUTFIT

20KB of Wolf



Ihre Amazon.de Bestellung

[redacted]

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

Sent: So 22.12.

To: [redacted]

Message | Invoice (21 KB)

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).

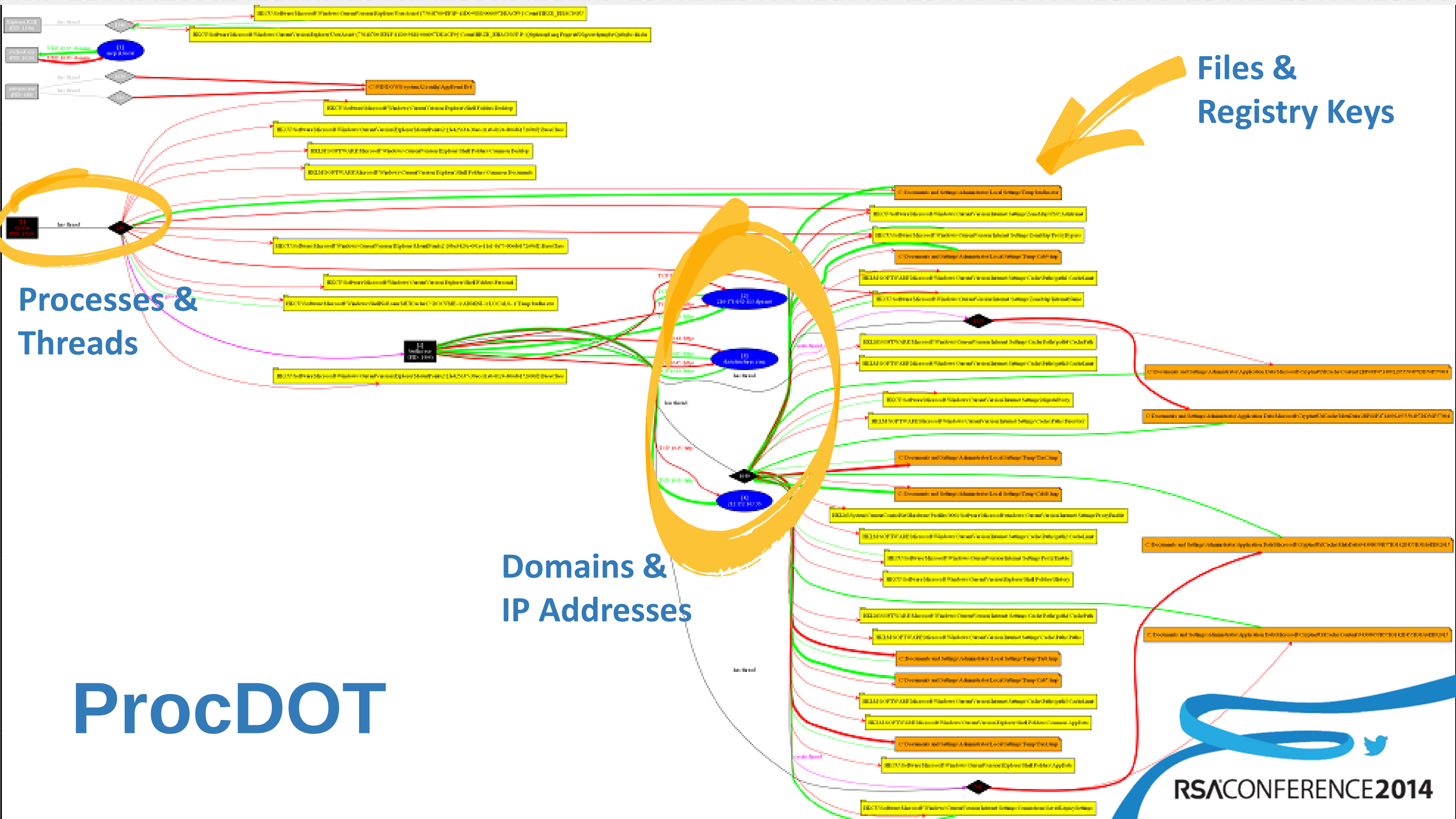
Sie finden das voraussichtliche Lieferdatum weiter unten. Um Ihre Bestellung anzusehen oder zu verändern, besuchen Sie Meine Bestellungen auf unserer Website.

Lieferung voraussichtlich:
Donnerstag, 9.Dezember 2013
Samstag, 11. Dezember 2013

Versandart:
Standard-Versand

Bestelldetails

Die Bestellung geht an:
[redacted]
Wien, 1050
Österreich

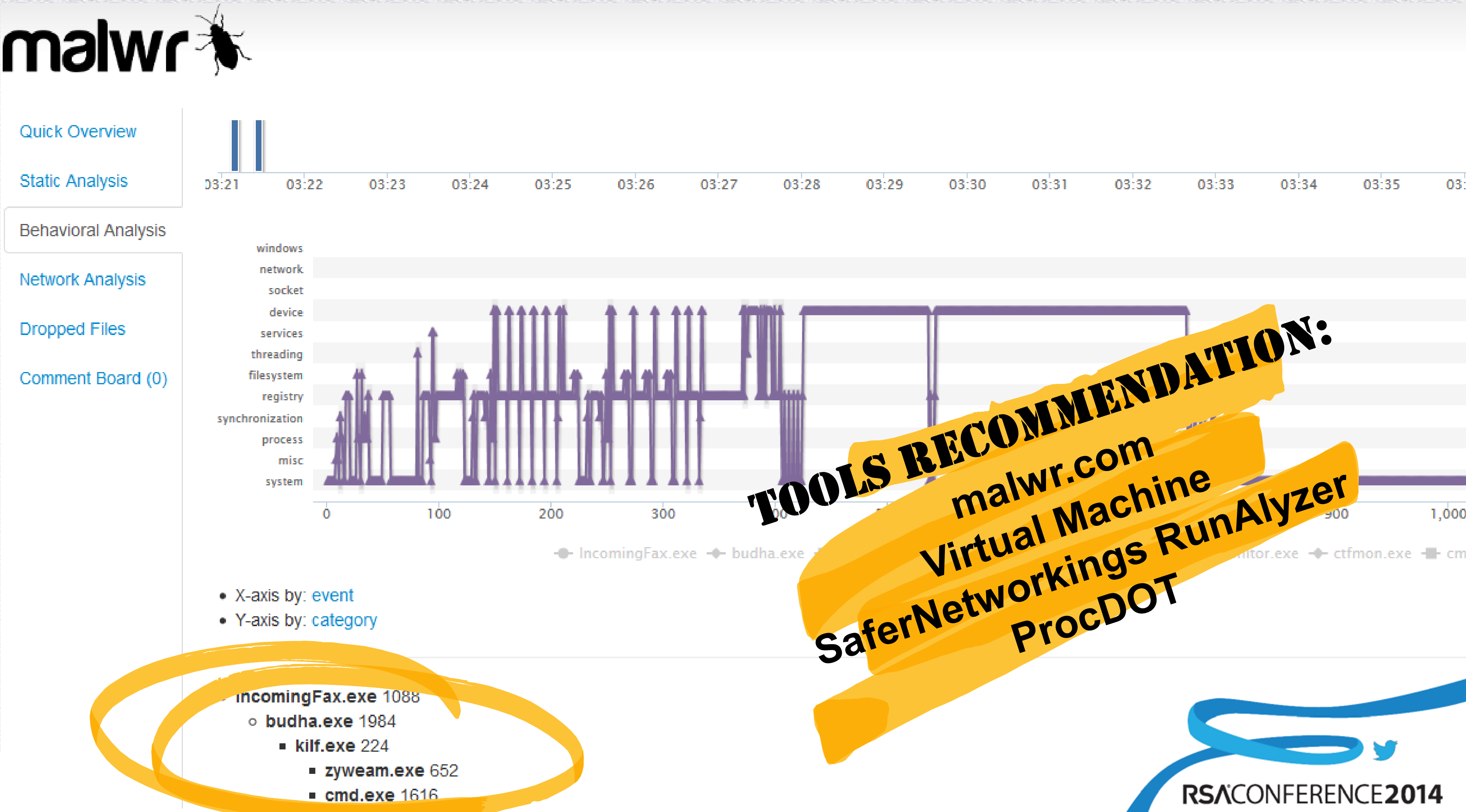


Files & Registry Keys

Processes & Threads

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

TOOLS RECOMMENDATION:

malwr.com

Virtual Machine

SaferNetworkings RunAlyzer

ProcDOT

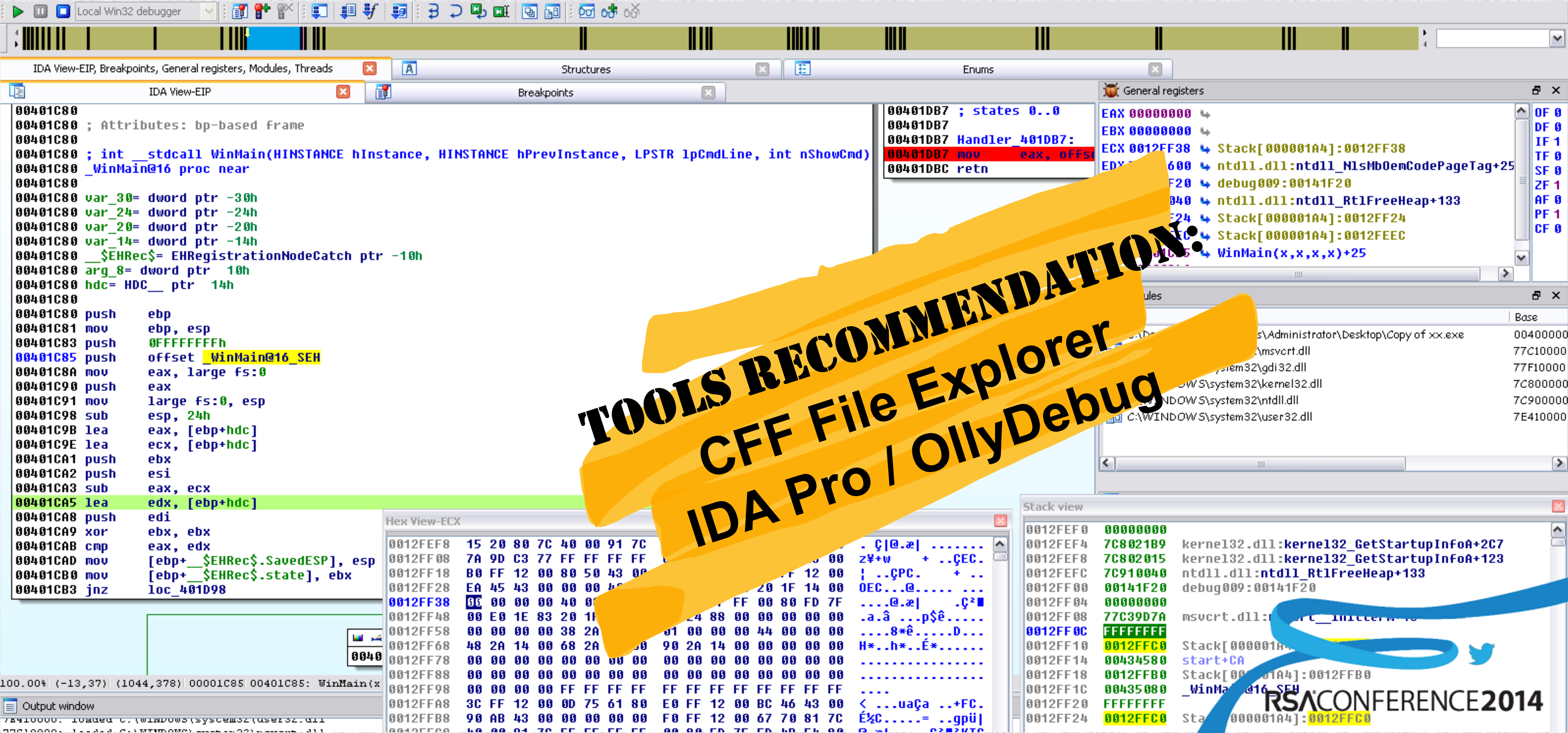
#3 THE BIG EVIL IN SMALL PIECES

- Google didn’t prove helpful this time.
- Dynamic Analysis didn’t give any useful insight.
- Reverse Engineering proved to be painful.

It is never possible to entirely prevent reversing.

- “REVERSING Secrets of Reverse Engineering” by Eldad Eilam

#3 THE BIG EVIL IN SMALL PIECES



```
00401C80
00401C80 ; Attributes: bp-based frame
00401C80
00401C80 ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
00401C80 _WinMain@16 proc near
00401C80
00401C80 var_30= dword ptr -30h
00401C80 var_24= dword ptr -24h
00401C80 var_20= dword ptr -20h
00401C80 var_14= dword ptr -14h
00401C80 __$EHRec$= EHRegistrationNodeCatch ptr -10h
00401C80 arg_8= dword ptr  10h
00401C80 hdc= HDC__ ptr  14h
00401C80
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
00401C9B lea     eax, [ebp+hdc]
00401C9E lea     ecx, [ebp+hdc]
00401CA1 push    ebx
00401CA2 push    esi
00401CA3 sub     eax, ecx
00401CA5 lea     edx, [ebp+hdc]
00401CA8 push    edi
00401CA9 xor     ebx, ebx
00401CAB cmp     eax, edx
00401CAD mov     [ebp+__$EHRec$.SavedESP], esp
00401CB0 mov     [ebp+__$EHRec$.state], ebx
00401CB3 jnz     loc_401D98
```

```
100.00% (-13,37) (1044,378) 00001C85 00401C85: WinMain(x
```

```
00401DB7 ; states 0..0
00401DB7
00401DB7 Handler_401DB7:
00401DB7 mov     eax, offse
00401DBC retn
```

```
EAX 00000000
EBX 00000000
ECX 0012FF38   Stack[000001A4]:0012FF38
EDX        600  ntdll.dll:ntdll_NlsMbOemCodePageTag+25
           F20  debug009:00141F20
           040  ntdll.dll:ntdll_RtlFreeHeap+133
           F24  Stack[000001A4]:0012FF24
            EC  Stack[000001A4]:0012FEEC
           1C85 WinMain(x,x,x,x)+25

OF 0
DF 0
IF 1
TF 0
SF 0
ZF 1
AF 0
PF 1
CF 0
```

```
                                                 Base
s\Administrator\Desktop\Copy of xx.exe           00400000
\msvcrt.dll                                      77C10000
em32\gdi32.dll                                   77F10000
WS\system32\kernel32.dll                         7C800000
NDOWS\system32\ntdll.dll                         7C900000
C:\WINDOWS\system32\user32.dll                   7E410000
```

```
0012FEF8  15 20 80 7C 40 00 91 7C                          . Ç|@.æ| .......
0012FF08  7A 9D C3 77 FF FF FF FF                       00  z¥+w    + ..ÇEC.
0012FF18  B0 FF 12 00 80 50 43 00                   12 00  ¦ ..ÇPC.    + ..
0012FF28  EA 45 43 00 00 00               20 1F 14 00  OEC...@..... ...
0012FF38  00 00 00 00 40 0             FF 00 80 FD 7F  ....@.æ|    .Ç²■
0012FF48  00 E0 1E 83 20 1          24 88 00 00 00 00 00  .a.â ...p$ê.....
0012FF58  00 00 00 00 38 2A        01 00 00 00 44 00 00 00  ....8*ê.....D...
0012FF68  48 2A 14 00 68 2A        90 2A 14 00 00 00 00 00  H*..h*..É*......
0012FF78  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0012FF88  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0012FF98  00 00 00 00 FF FF FF FF  FF FF FF FF FF FF FF FF  ....
0012FFA8  3C FF 12 00 0D 75 61 80  E0 FF 12 00 BC 46 43 00  < ...uaÇa ..+FC.
0012FFB8  90 AB 43 00 00 00 00 00  F0 FF 12 00 67 70 81 7C  É½C.....= ..gpü|
```

```
0012FEF0  00000000
0012FEF4  7C8021B9  kernel32.dll:kernel32_GetStartupInfoA+2C7
0012FEF8  7C802015  kernel32.dll:kernel32_GetStartupInfoA+123
0012FEFC  7C910040  ntdll.dll:ntdll_RtlFreeHeap+133
0012FF00  00141F20  debug009:00141F20
0012FF04  00000000
0012FF08  77C39D7A  msvcrt.dll:
0012FF0C  FFFFFFFF
0012FF10  0012FFC0  Stack[000001A
0012FF14  00434580  start+CA
0012FF18  0012FFB0  Stack[00  1A4]:0012FFB0
0012FF1C  00435080  _WinMa  @16_SEH
0012FF20  FFFFFFFF
0012FF24  0012FFC0  Sta  000001A4]:0012FFC0
```

TOOLS RECOMMENDATION:

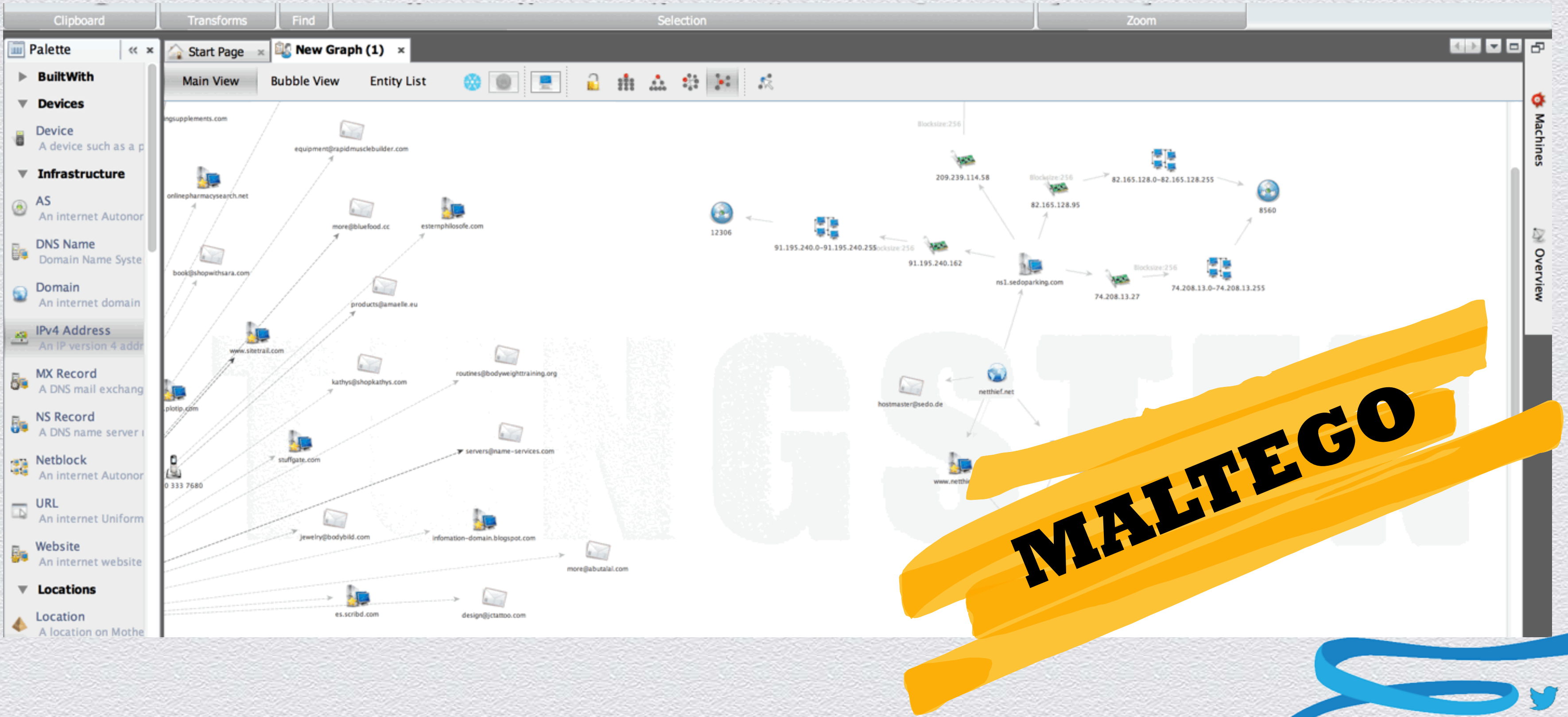
CFF File Explorer

IDA Pro / OllyDebug

#3 THE BIG EVIL IN SMALL PIECES

- Clearly targeted
- Complex software
- Author had good understanding of AV internals
- Related to other malware

#3 THE BIG EVIL IN SMALL PIECES



#3 THE BIG EVIL IN SMALL PIECES

KEY FINDINGS

- Domain Name
- IP-Address
- E-Mail Address
- Name, for what its worth
- Geo Location
- Related Malware
- Infection Mechanism
- Stealth Mechanism
- Communication Protocol
- Data Compression
- Hint which Data was stolen

LESSONS LEARNED

RE-Tool #1: google.com

Online Analysis Tools

Virtual Machine / Sandbox

SysInternals Toolsuite

Wireshark

RunAlyzer

IDA Pro / OllyDebug

Step 1

Gather Information

Step 2

Use this Information to gather more Information

Step 3

Build the BIG PICTURE

IN A NUTSHELL

Accept culturally different viewpoints on IP

Acquire the right skills

Adapt just like the bad guys do

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

MALWARE UNDER THE HOOD
KEEPING YOUR IP SAFE

SESSION ID: ANF-F01

Marion Marschalek

Malware Analyst
IKARUS
@pinkflawd

Mike Kendzierski

Technology Researcher
SHOSHN Ventures

RESOURCES

- http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ – **Target Data Breach Dec. 2013**
- http://www.washingtonpost.com/business/technology/hackers-break-into-washington-post-servers/2013/12/18/dff8c362-682c-11 – **Washington Post Hack Dec. 2013**
- http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf – **Sophos Threat Report 2014**
- http://www.websense.com/assets/reports/websense-2013-threat-report.pdf – **Websense Threat Report 2013**
- http://www.microsoft.com/security/sir/story/default.aspx?_escaped_fragment_=10year_malware#!10year_malware – **Malware Evolution, MMPC**

RESOURCES

- http://0x1338.blogspot.co.at – write-up of case study #2
- https://docs.google.com/file/d/0B5hBKwgSgYFaVmxTaFk3OXl4cjg/edit?usp=sharing – analysis report of case study #3
- https://malwr.com/ – online malware analysis platform running cuckoo sandbox
- http://anubis.iseclab.org/ – online malware analysis platform
- http://zeltser.com/reverse-malware/ – link to SANS course and list of tools
- http://technet.microsoft.com/de-de/sysinternals/bb545021.aspx - Sysinternals Tools

BACK AT YOU: QUESTIONNAIRE

YOUR INTELLECTUAL PROPERTY

1. Have you identified your **Intellectual Property** & data classification strategy?

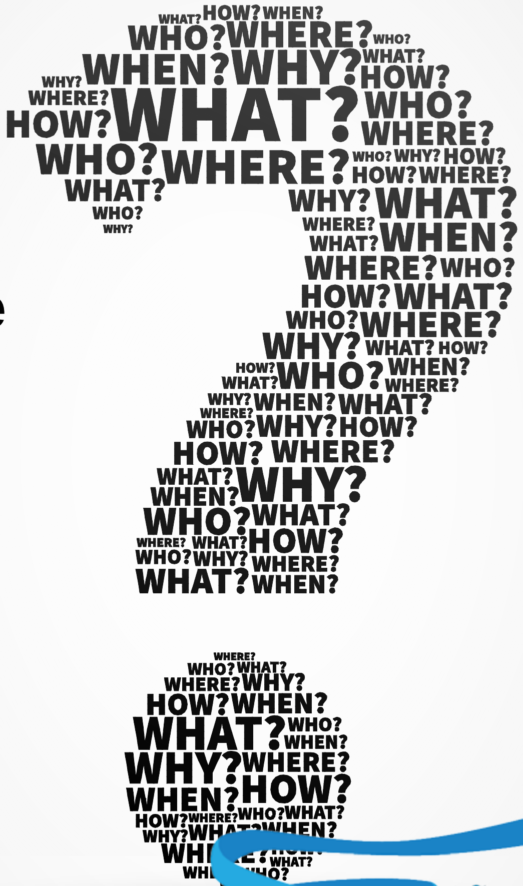
2. Do you know exactly **where it resides**?

3. Do you know what systems and individuals **access it**?

MOBILE DEVICES

4. Do you have measures in place to **monitor access** to your company data **from outside** your company network?

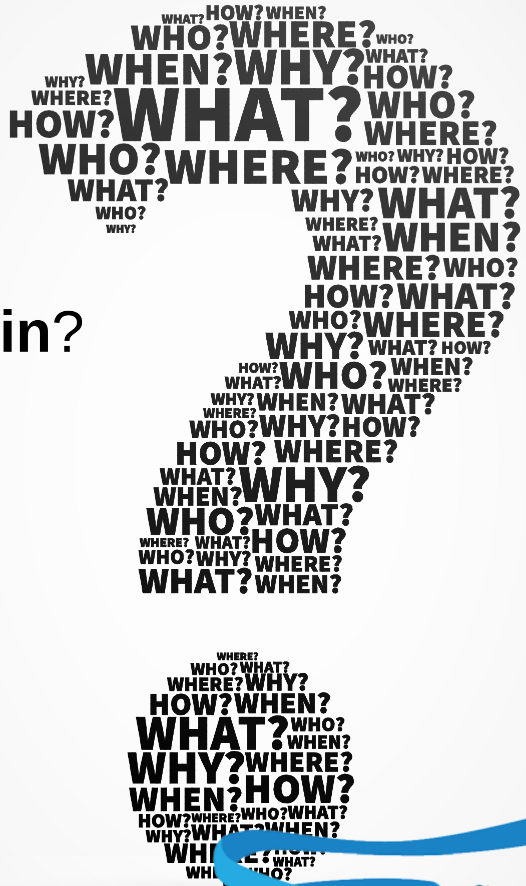
5. Do you still have **control over your companies mobile devices**, even when they get lost/stolen?



WEB & E-MAIL SECURITY

6. Do you have security measures that secure every link in the **malware infection kill-chain**?

7. Do your security systems incorporate intelligence data to identify **compromised web links in real-time**?



INFRASTRUCTURE

8. Do you have **data encryption** in place where it is needed? And even there where you don’t yet think it is necessary?

9. Is your **system’s documentation** safe?

ALL COMES DOWN TO THE PEOPLE

10. Are your employees trained on what personal or **company related information** to keep confidential?

11. Do you have someone on your team who knows how to react in case of a **malware incident**?

12. Does he know how to **analyze** malware?