Malware Forensics

Sukwha Kyung

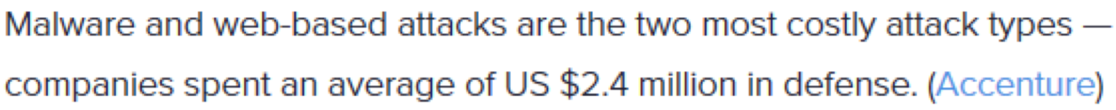
Common Types of Attacks

- Phishing
- Malware
- SQLi
- XSS
- MITM
- DoS
- Brute-force & Dictionary attacks
- …

Common Types of Attacks

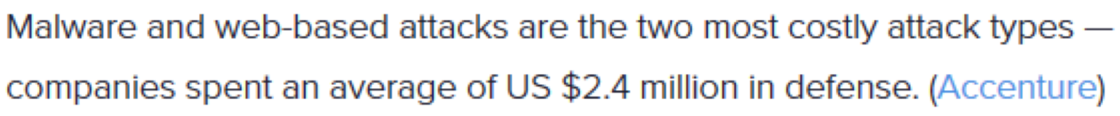
- Phishing
- Malware
- SQLi
- XSS
- MITM
- DoS
- Brute-force & Dictionary attacks
- …

Current Status

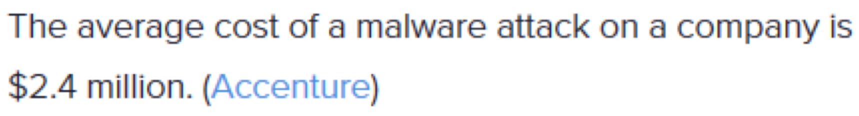


Malware and web-based attacks are the two most costly attack types — companies spent an average of US $2.4 million in defense. (Accenture)

Current Status

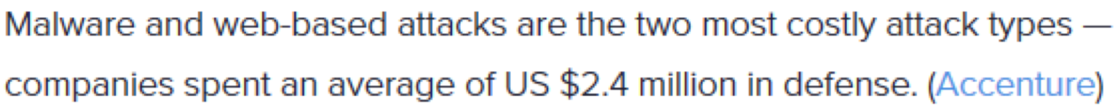


Malware and web-based attacks are the two most costly attack types — companies spent an average of US $2.4 million in defense. (Accenture)

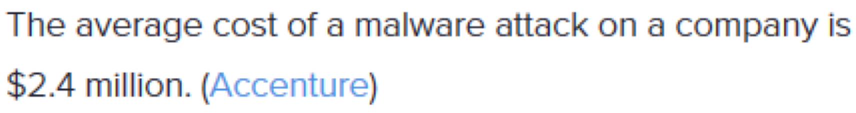


The average cost of a malware attack on a company is $2.4 million. (Accenture)

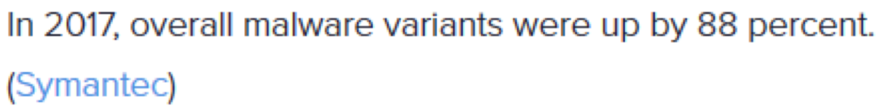
Current Status



Malware and web-based attacks are the two most costly attack types — companies spent an average of US $2.4 million in defense. (Accenture)

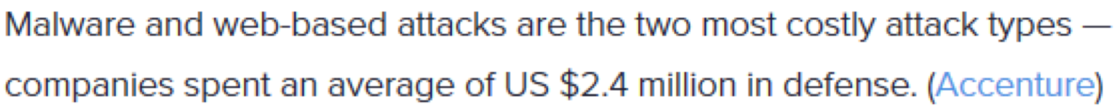


The average cost of a malware attack on a company is $2.4 million. (Accenture)

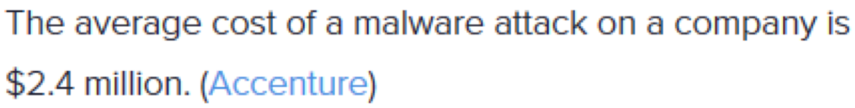


In 2017, overall malware variants were up by 88 percent. (Symantec)

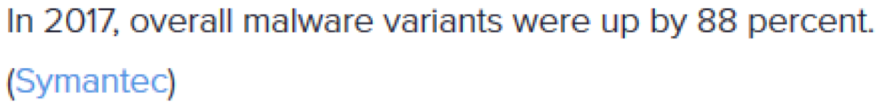
Current Status



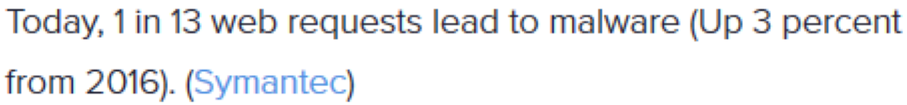
Malware and web-based attacks are the two most costly attack types — companies spent an average of US $2.4 million in defense. (Accenture)



The average cost of a malware attack on a company is $2.4 million. (Accenture)

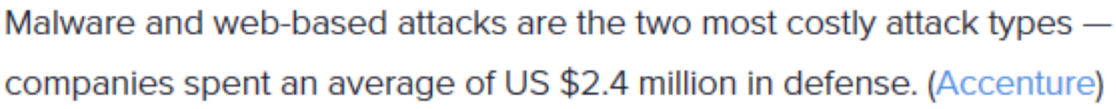


In 2017, overall malware variants were up by 88 percent. (Symantec)

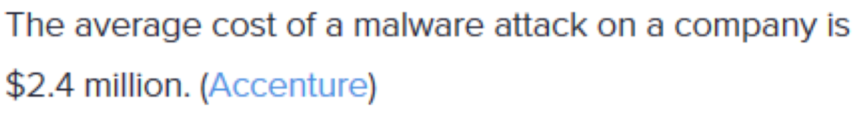


Today, 1 in 13 web requests lead to malware (Up 3 percent from 2016). (Symantec)

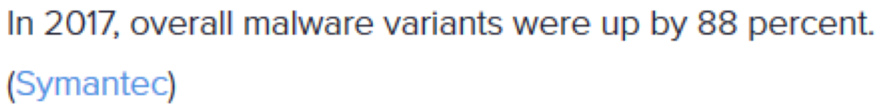
Current Status



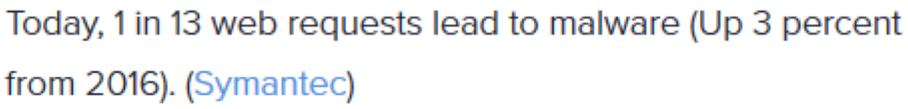
Malware and web-based attacks are the two most costly attack types — companies spent an average of US $2.4 million in defense. (Accenture)



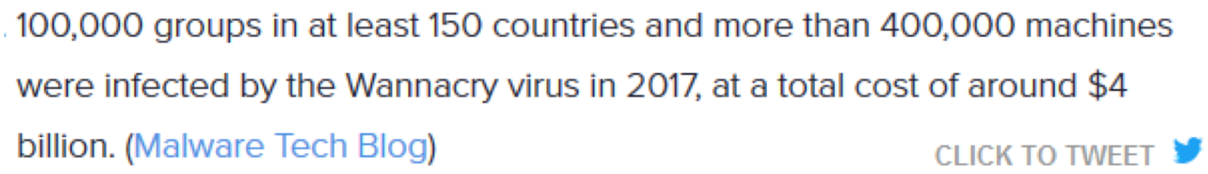
The average cost of a malware attack on a company is $2.4 million. (Accenture)



In 2017, overall malware variants were up by 88 percent. (Symantec)



Today, 1 in 13 web requests lead to malware (Up 3 percent from 2016). (Symantec)



100,000 groups in at least 150 countries and more than 400,000 machines were infected by the Wannacry virus in 2017, at a total cost of around $4 billion. (Malware Tech Blog)

Malware

- A set of instructions (CPU instructions, commands/scripts) that run on victim's computer and make the system do what an attacker wants it to do.

Malware

- A set of instructions (CPU instructions, commands/scripts) that run on victim's computer and make the system do what an attacker wants it to do.
- Purpose of malware:
  - Machine level: steal, delete files/information
  - Large scale: spam, relay

Malware Forensics

- Conducting forensic analysis on malicious code
  - Static Analysis: investigating of execution file without running
  - Dynamic Analysis: observing malware's activities by running it

Malware Forensics

- Conducting forensic analysis on malicious code
  - Static Analysis: investigating of execution file without running
  - Dynamic Analysis: observing malware's activities by running it
- Not only WHAT, but also HOW:
  - Malware forensics often involves how the victim's system got infected by malware (Network Forensics).

History

- Melissa (1999)
- SQL Slammer (2003)
- Mydoom (2004)
- Zeus (2007)
- Operation Aurora (2009)
- Stuxnet (2010)
- CryptoLocker (2013)
- Sony Pictures hack (2014)
- Mirai (2016)
- WannaCry (2017)

Types of Malware

- Virus
- Worm
- Trojan
- Backdoor
- Rootkit
- Adware
- Browser Hijacker
- Ransomware

Mitigation

- Anti-malware software
  - Intrusion Detection Systems (IDS): Detect & Report
  - Intrusion Prevention Systems (IPS): Detect, Block & Report
- What is the most naïve way to create malware signature?

Anti-Malware Software

- What is the most naïve way to create malware signature?
  - MD5/SHA256sum?

Anti-Malware Software

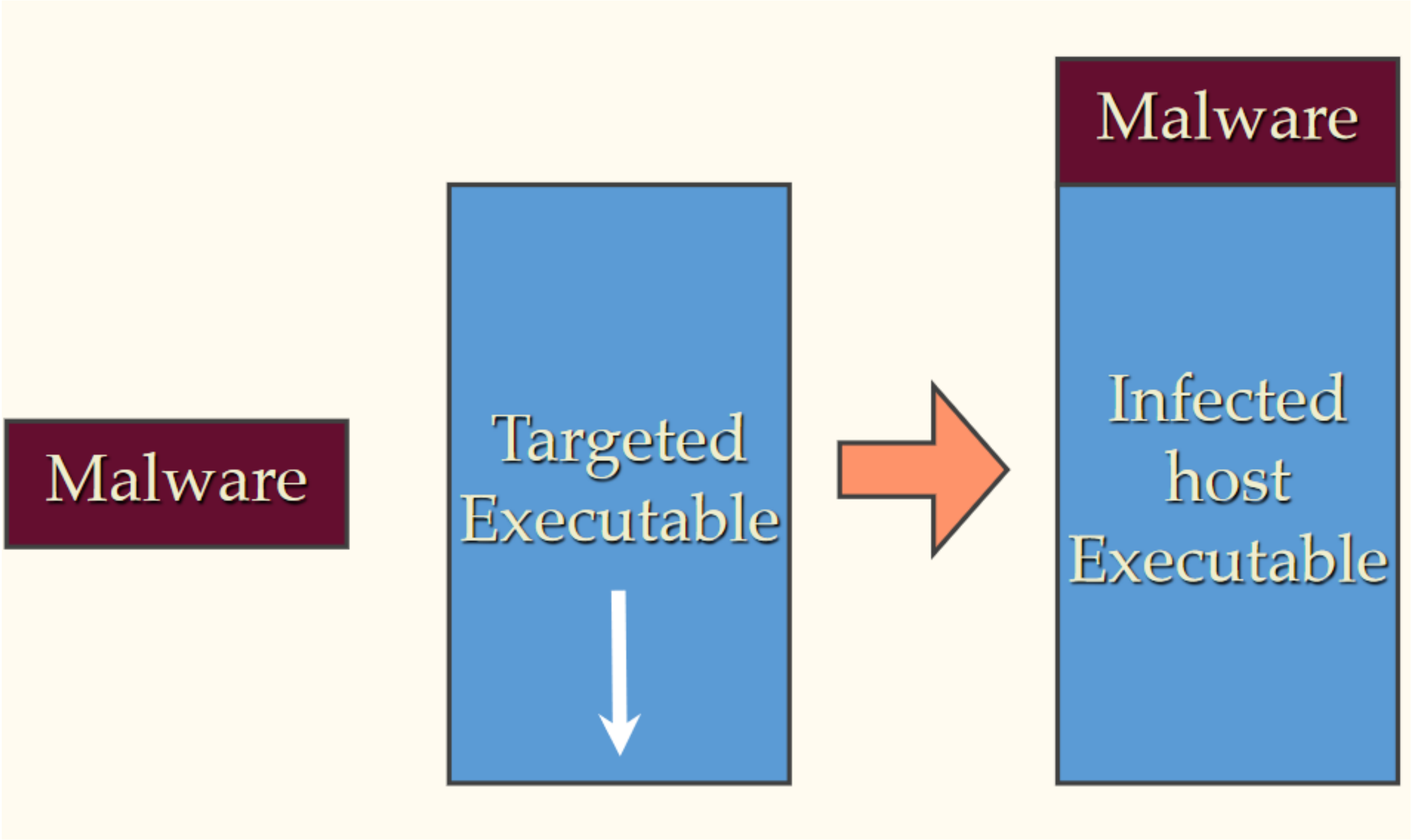
- What is the most naïve way to create malware signature?
  - MD5/SHA256sum?
  - Attacker can create infinite number of the same malware with different signature by just changing one bit.

My Advice

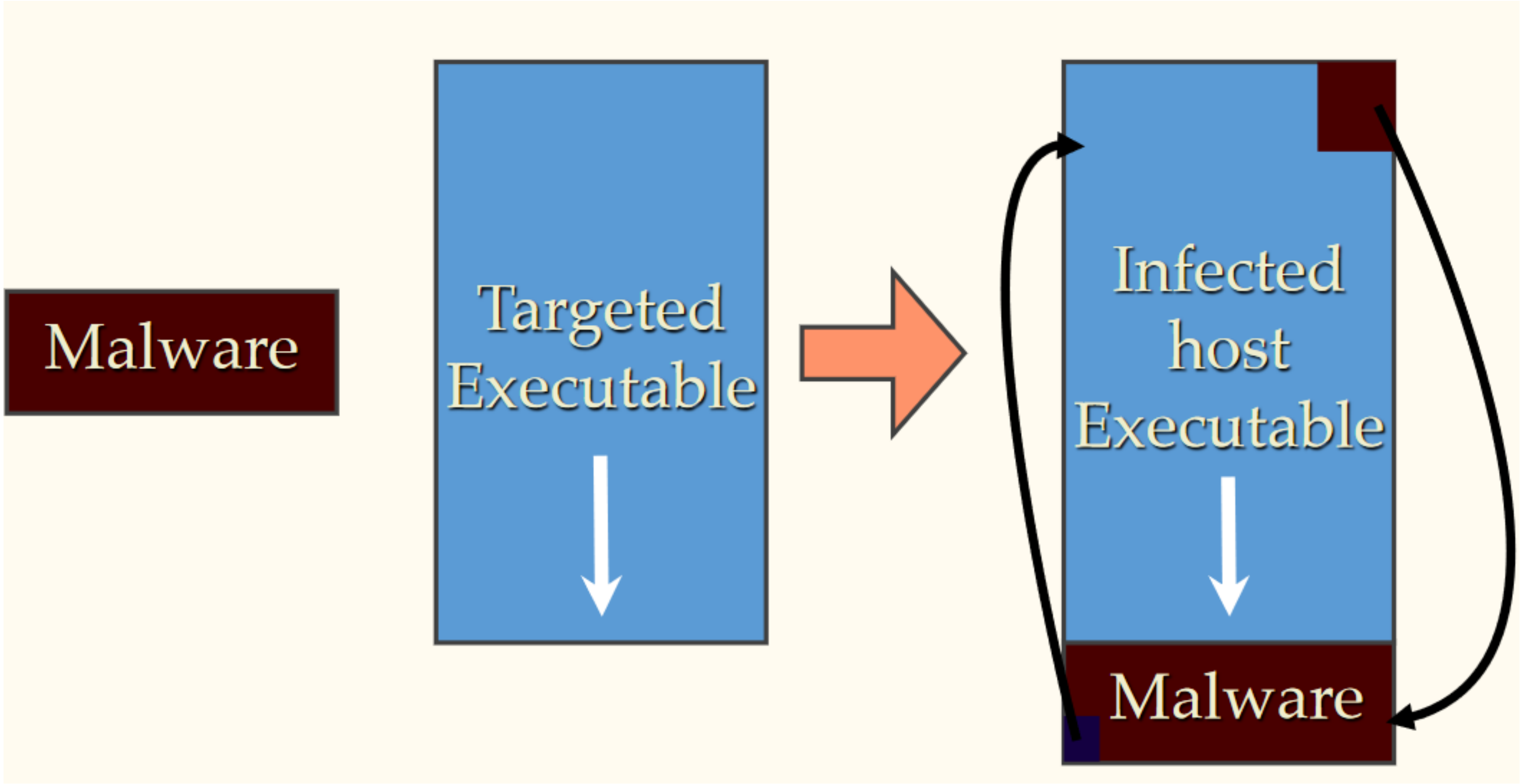
Virus

- A program that can infect other programs by modifying them to include a, possibly evolved, version of itself.
  - Fred Cohen (1983)

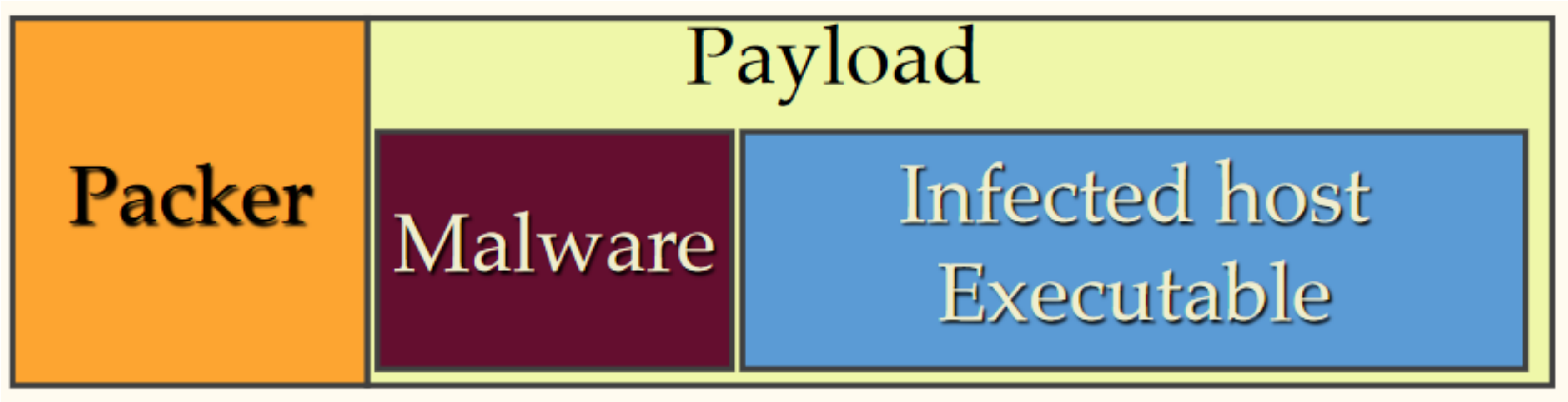
Virus Example



Virus Example



Packers



Packer

Payload

Malware

Infected host Executable

Packers

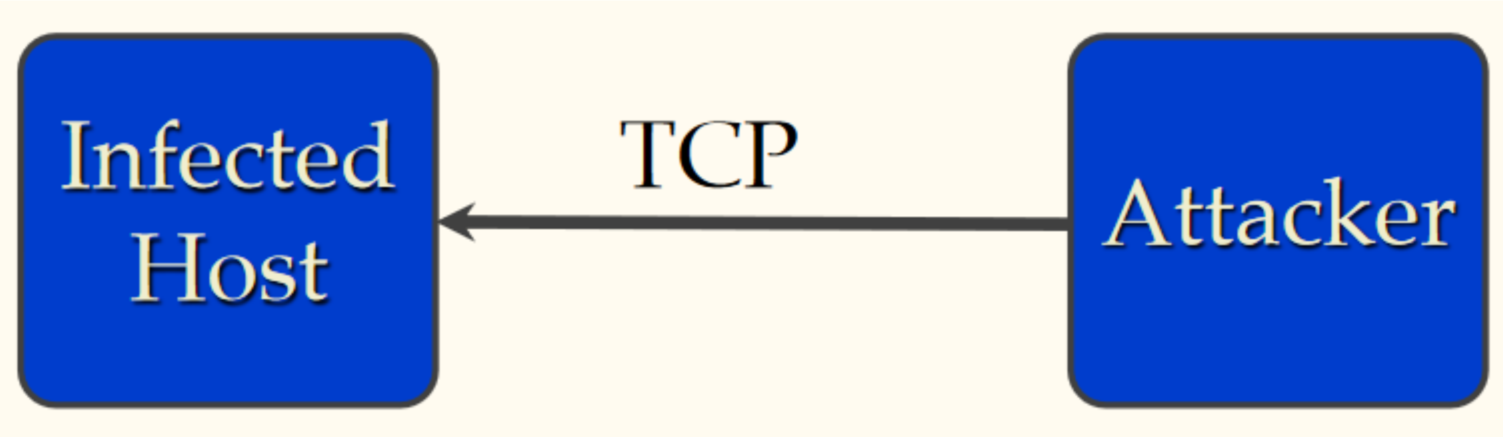
- Not necessarily malicious

- Compress
- Encrypt
- Randomize (Polymorphism)
- Anti-debug Technique (int / fake jmp)
- Add-junk
- Anti-VM
- Virtualization

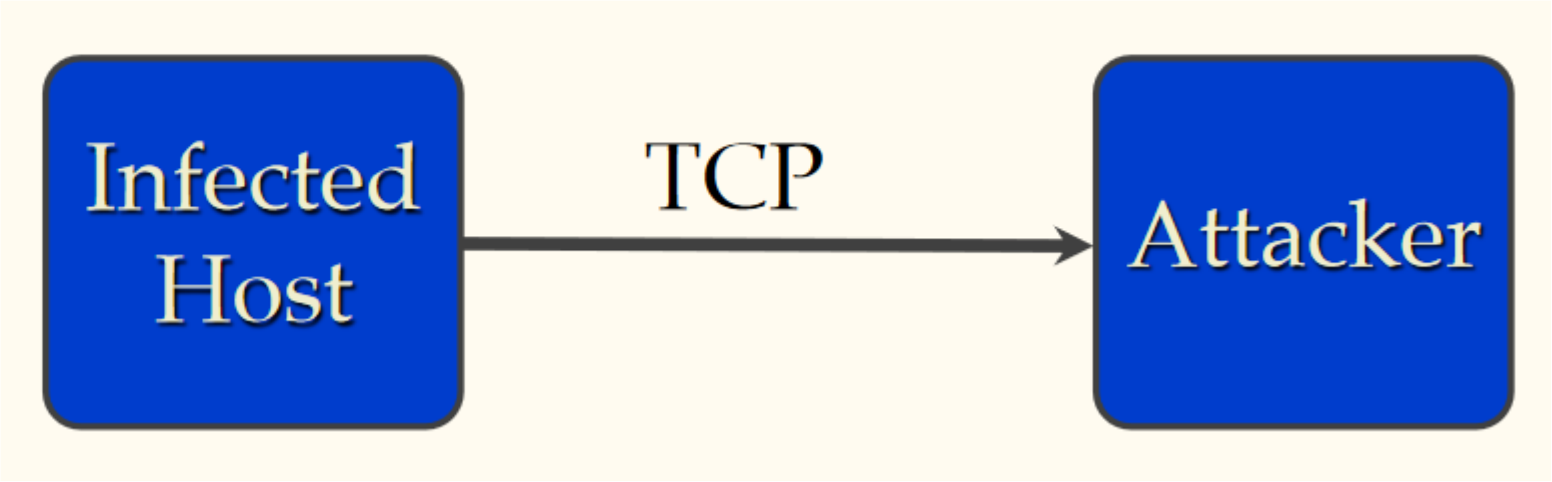
Backdoor

- A secret method to bypass normal authentication or encryption of a system.
    - Hidden part of a program
    - Separate program
    - Default passwords
- E.g.) Clipper chip (1993)

Backdoor



Reverse Backdoor



Trojan

- The class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the victim computer.

Trojan

- E.g.) “waterfalls.scr” – a free waterfall screensaver.
- When run, it unloads hidden programs, commands, scripts, or any number of commands with or without the user’s knowledge or consent.

Trojan

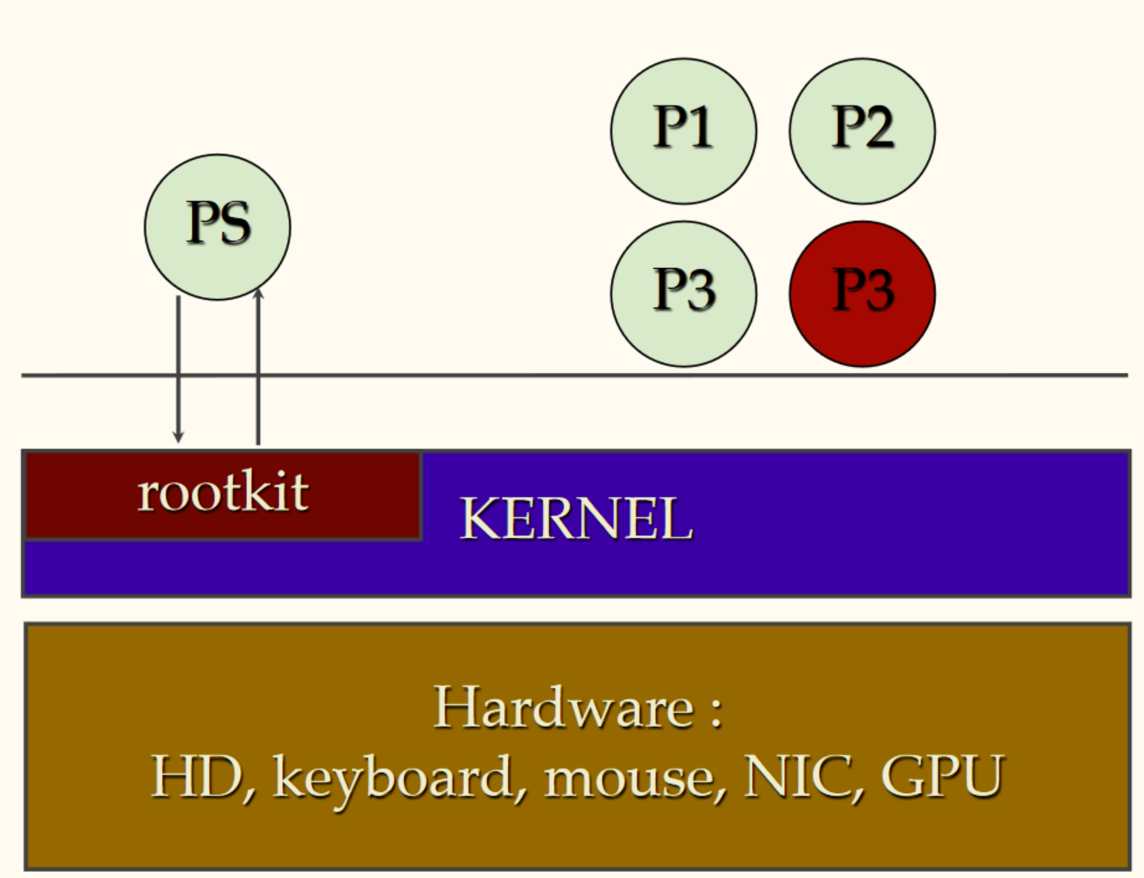
- *To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust: the people who wrote the software.*
  - Ken Thomson (Turing Award acceptance lecture, 1983)

Rootkit

- Any software that acquires and maintains privileged access to the operating system while hiding its presence by subverting normal OS behavior.
  - Symantec Report

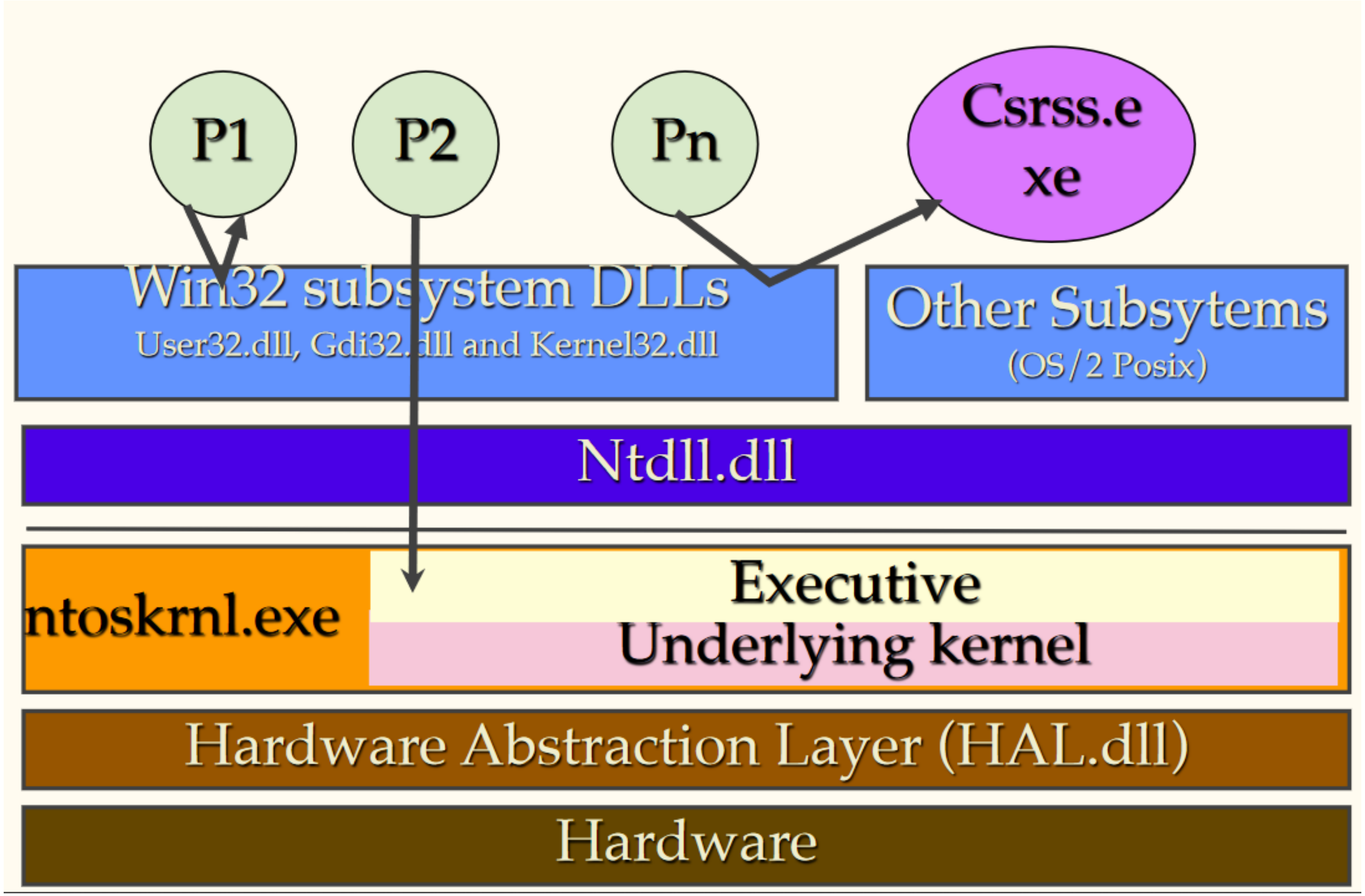
Rootkit

- Kernel Rootkit



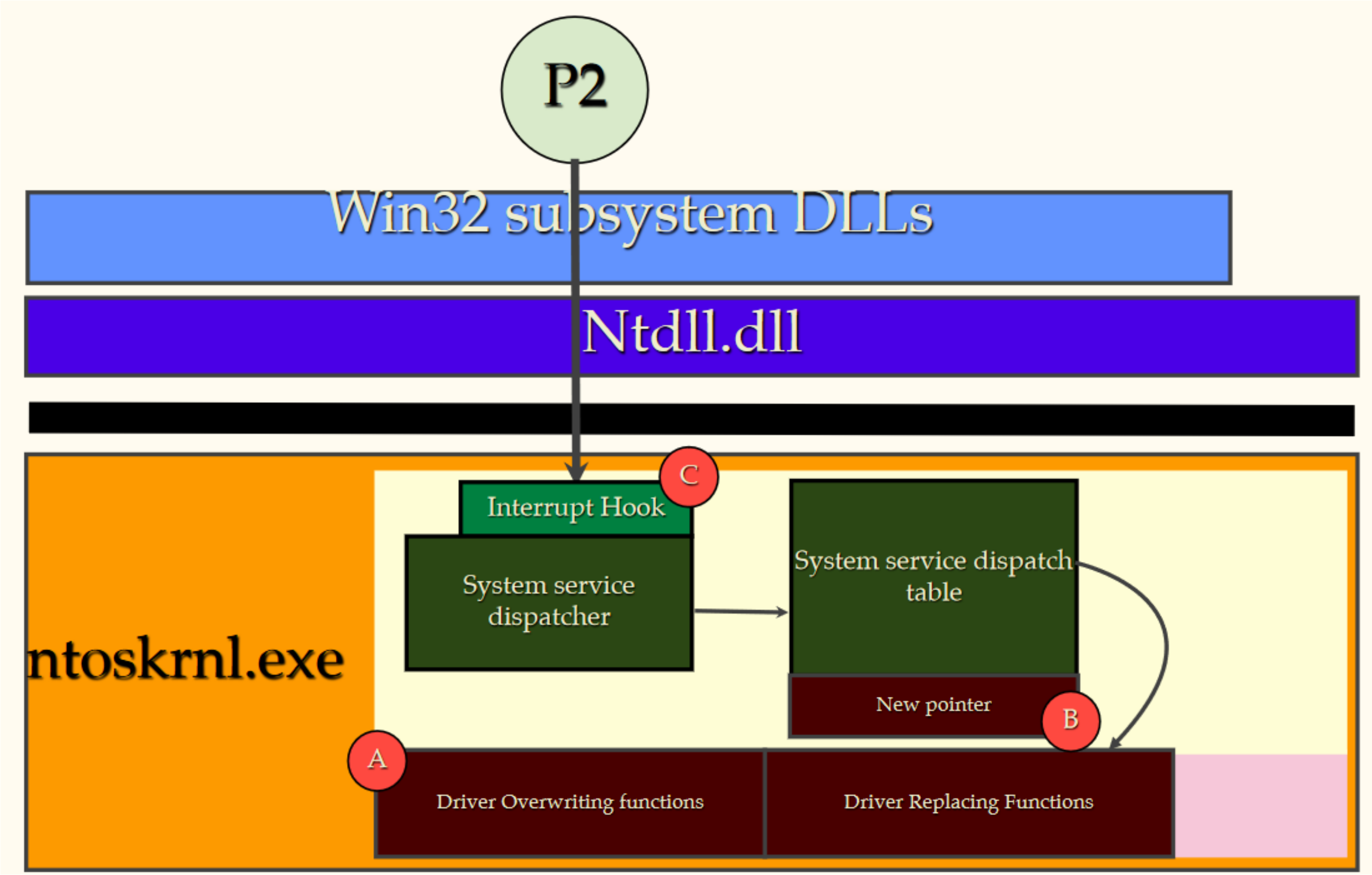
Rootkit

- Windows Kernel



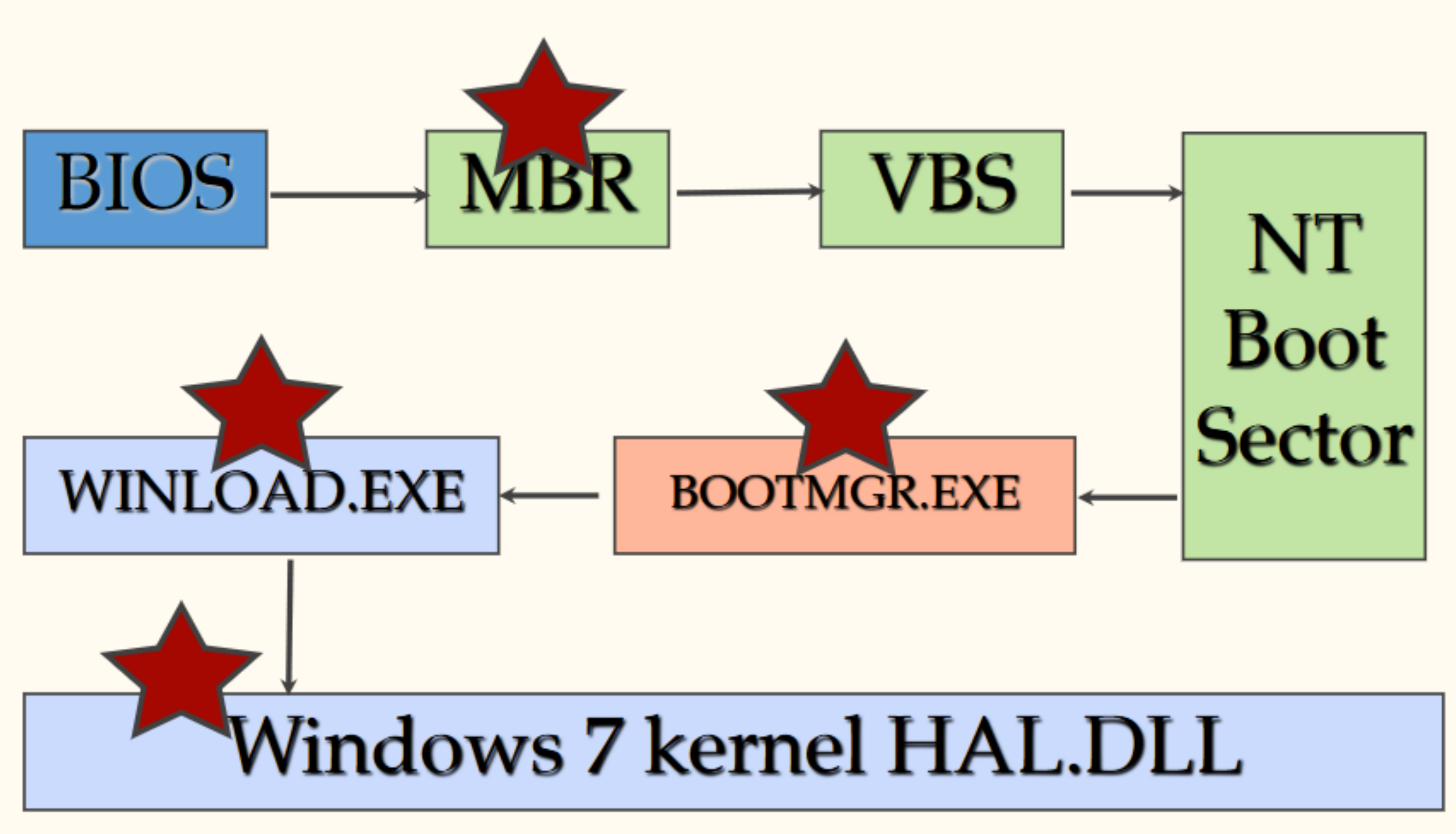
Rootkit

- Kernel Device Driver


P2
Win32 subsystem DLLs
Ntdll.dll
ntoskrnl.exe
Interrupt Hook
C
System service dispatcher
System service dispatch table
New pointer
B
A
Driver Overwriting functions
Driver Replacing Functions

Rootkit

- Bootkit
  - infects the master boot record, volume boot record or boot section during computer startup.
  - can be used to avoid all protections of an OS, because OS consider that the system was in trusted stated at the moment the OS boot loader took control.


BIOS
MBR
VBS
NT Boot Sector
BOOTMGR.EXE
WINLOAD.EXE
Windows 7 kernel HAL.DLL

Worm

- Self-replicating program that uses a *network* to send copies of itself to other nodes and do so without any user intervention.

- Typically exploit security flaws in widely used services, such as buffer overflow vulnerabilities in a network service.

Worm

- Morris worm (1988)
  - Infected approximately 6,000 machines
    - 10% of the entire internet
  - Cost ~$10 million

Solution

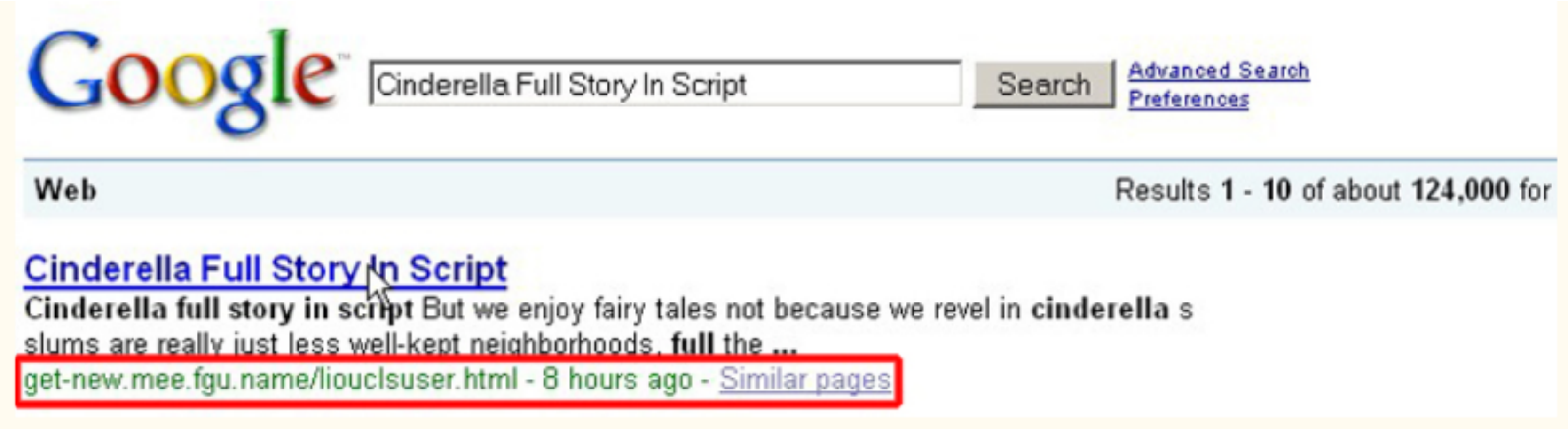
Worm

- Code Red worm (2001)
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
    - Programmed to go into infinite sleep mode (July 28)
  - ~2.6 billion in damage
- Love Bug worm
  - Email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs"
  - ~8.75 billion

Virus vs Trojan vs Worm

- Virus: code embedded in a file or program
- Virus and Trojan horses rely on human intervention
- Worms are self-contained and may spread autonomously

Browser hijacking



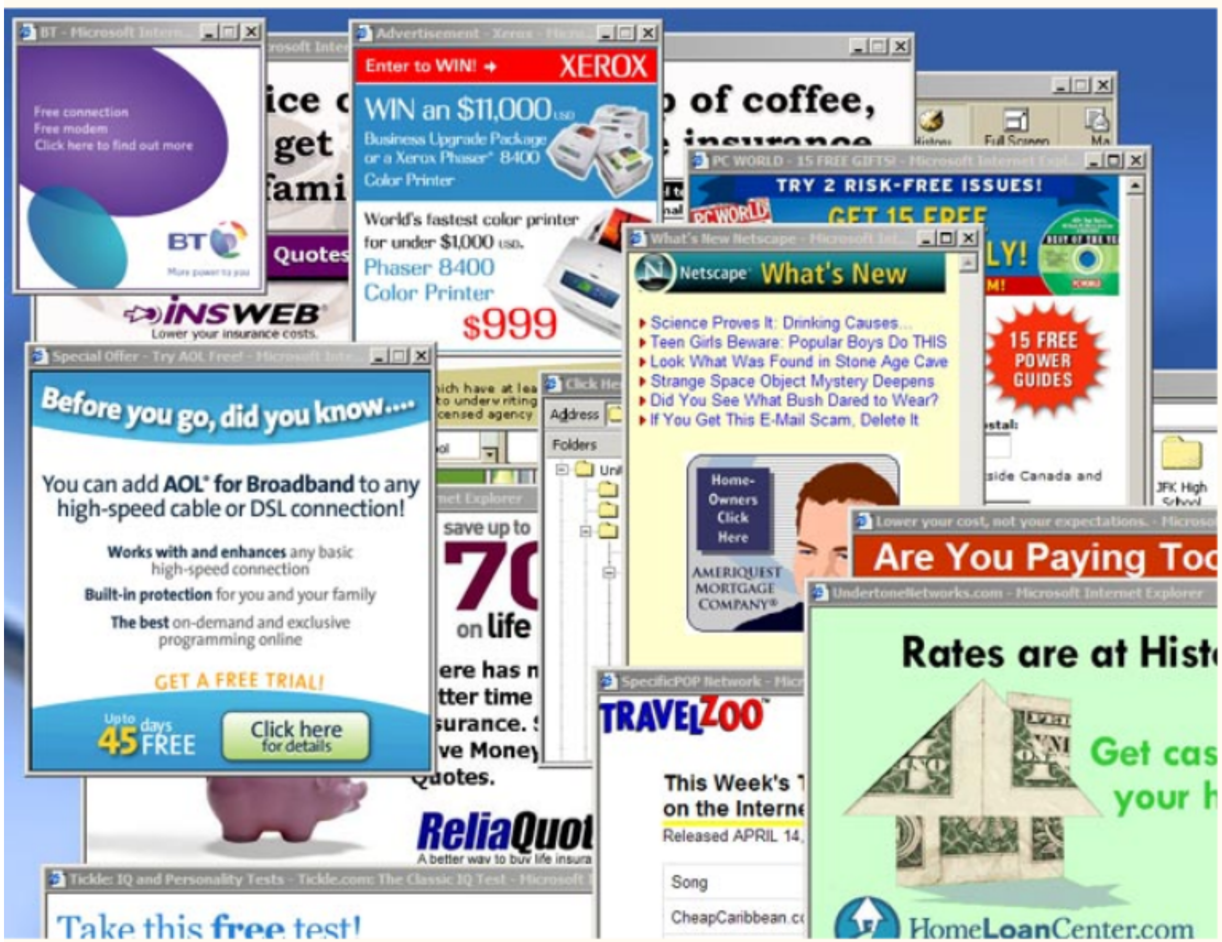
Results 1 - 10 of about 124,000 for

Cinderella Full Story In Script

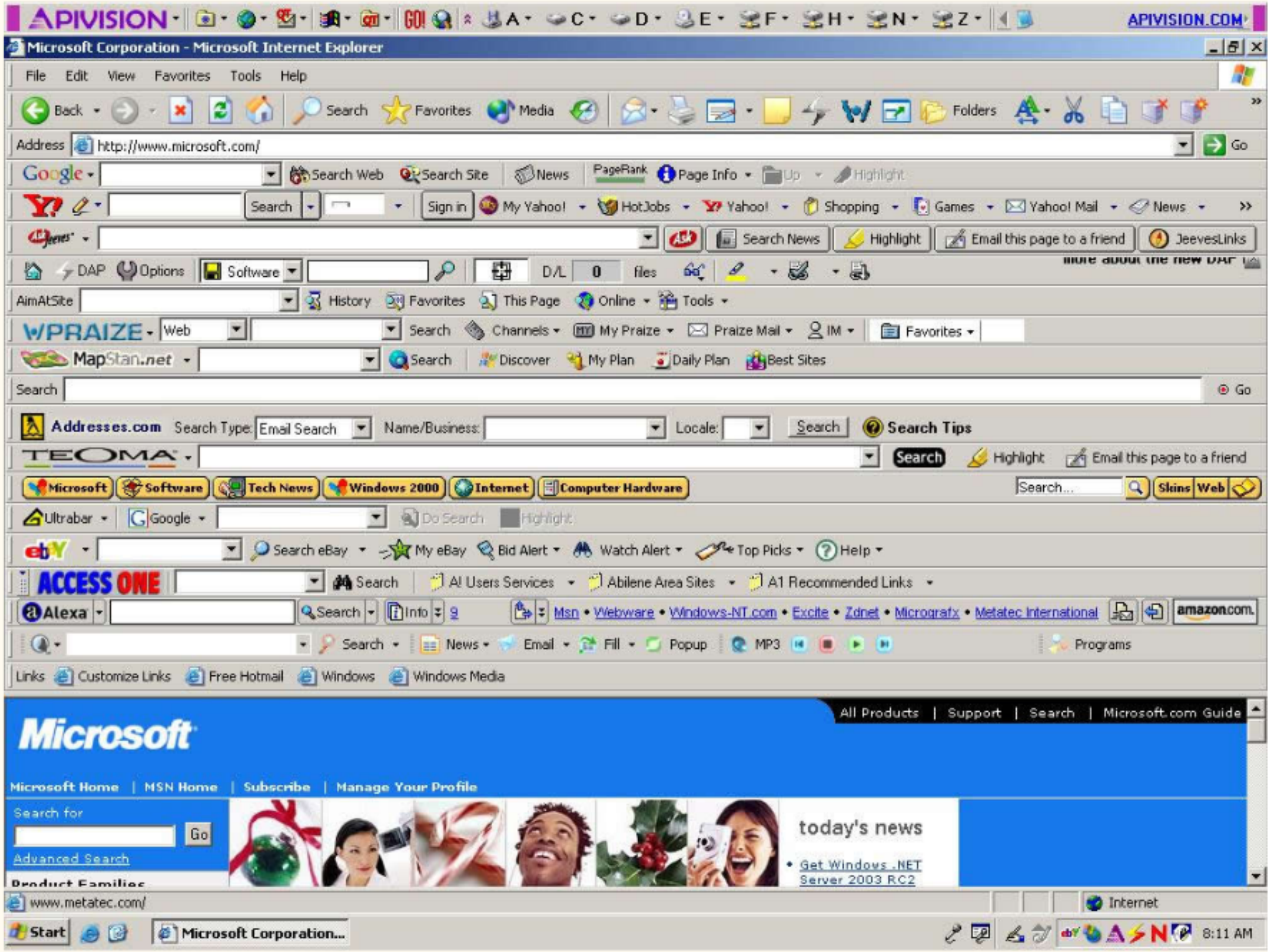
Cinderella full story in script But we enjoy fairy tales not because we revel in **cinderella** s slums are really just less well-kept neighborhoods, **full** the ...

get-new.mee.fgu.name/liouclsuser.html - 8 hours ago - Similar pages

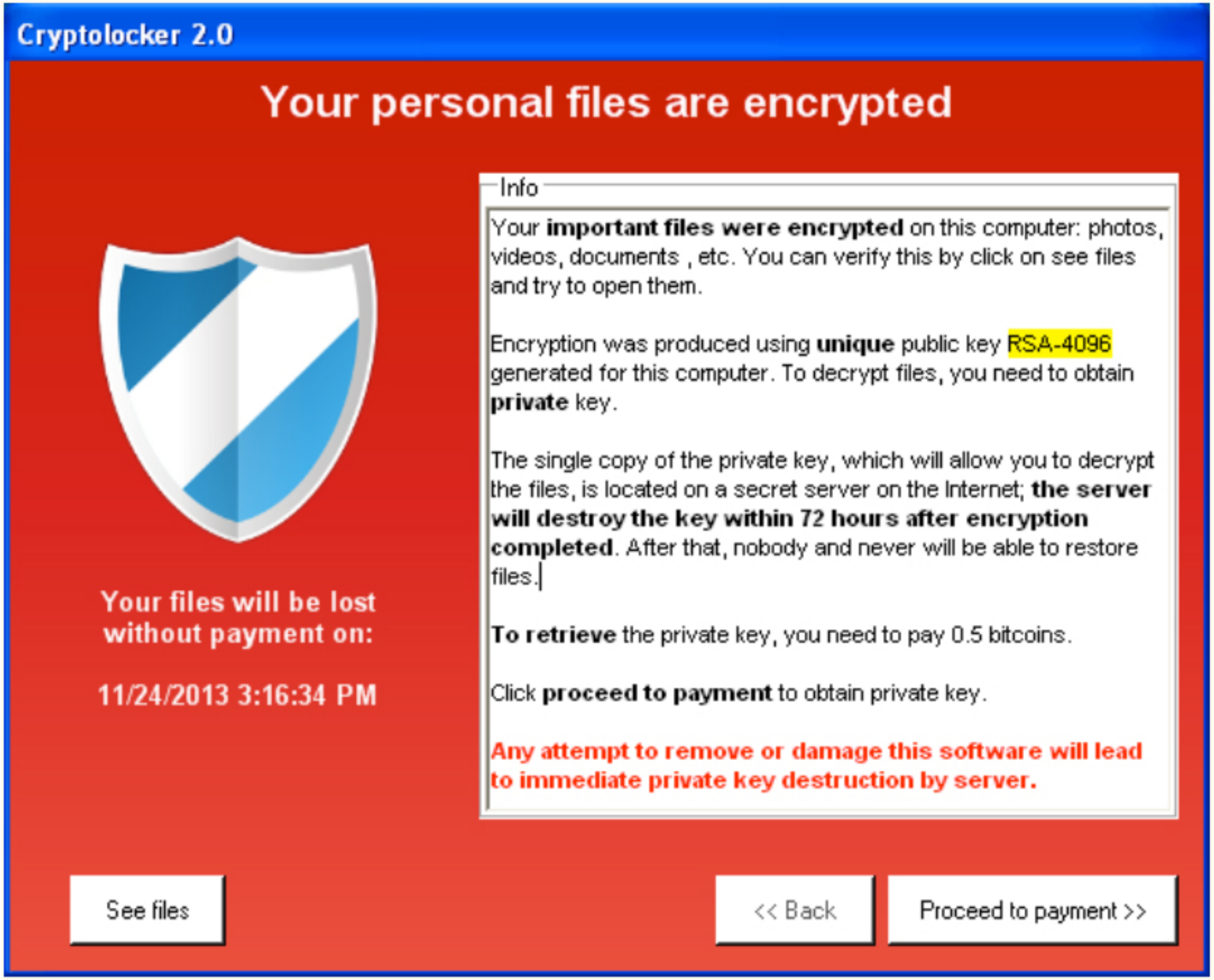
Adware


BT - Microsoft Intern...
Free connection
Free modem
Click here to find out more
BT
More power to you
iNSWEB
Lower your insurance costs
Quotes
Advertisement - Xerox - Micro...
Enter to WIN!
XEROX
WIN an $11,000 USD
Business Upgrade Package or a Xerox Phaser 8400 Color Printer
World's fastest color printer for under $1,000 USD.
Phaser 8400 Color Printer
$999
of coffee,
PC WORLD - 15 FREE GIFTS! - Microsoft Internet Expl...
TRY 2 RISK-FREE ISSUES!
PC WORLD
GET 15 FREE
15 FREE POWER GUIDES
What's New Netscape - Microsoft Int...
Netscape What's New
Science Proves It: Drinking Causes...
Teen Girls Beware: Popular Boys Do THIS
Look What Was Found in Stone Age Cave
Strange Space Object Mystery Deepens
Did You See What Bush Dared to Wear?
If You Get This E-Mail Scam, Delete It
Home-Owners Click Here
AMERIQUEST MORTGAGE COMPANY
Special Offer - Try AOL Free! - Microsoft Inte...
Before you go, did you know....
You can add AOL for Broadband to any high-speed cable or DSL connection!
Works with and enhances any basic high-speed connection
Built-in protection for you and your family
The best on-demand and exclusive programming online
GET A FREE TRIAL!
Up to 45 days FREE
Click here for details
save up to
70
on life
ere has n
tter time
surance.
ve Money
Quotes.
ReliaQuot
A better way to buy life insura
Address
Folders
Lower your cost, not your expectations. - Microso
Are You Paying Too
Undertonenetworks.com - Microsoft Internet Explorer
Rates are at Hist
Get cas
your h
HomeLoanCenter.com
SpecificPOP Network - Micr
TRAVELZOO
This Week's T
on the Interne
Released APRIL 14,
Song
CheapCaribbean.co
Tickle: IQ and Personality Tests - Tickle.com: The Classic IQ Test - Microsoft
Take this free test!

Browser Toolbar


APIVISION
A C D E F H N Z
APIVISION.COM
Microsoft Corporation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Folders
Address http://www.microsoft.com/ Go
Google Search Web Search Site News PageRank Page Info Up Highlight
Y! Search Sign in My Yahoo! HotJobs Yahoo! Shopping Games Yahoo! Mail News
Jeeves Search News Highlight Email this page to a friend JeevesLinks
DAP Options Software D/L 0 files
more about the new DAP
AimAtSite History Favorites This Page Online Tools
WPRAIZE Web Search Channels My Praize Praize Mail IM Favorites
MapStan.net Search Discover My Plan Daily Plan Best Sites
Search Go
Addresses.com Search Type: Email Search Name/Business: Locale: Search Search Tips
TEOMA Search Highlight Email this page to a friend
Microsoft Software Tech News Windows 2000 Internet Computer Hardware Search... Skins Web
Ultrabar Google Do Search Highlight
ebY Search eBay My eBay Bid Alert Watch Alert Top Picks Help
ACCESS ONE Search AI Users Services Abilene Area Sites A1 Recommended Links
Alexa Search Info 9 Msn • Webware • Windows-NT.com • Excite • Zdnet • Micrografx • Metatec International amazon.com
Search News Email Fill Popup MP3 Programs
Links Customize Links Free Hotmail Windows Windows Media
All Products | Support | Search | Microsoft.com Guide
Microsoft
Microsoft Home | MSN Home | Subscribe | Manage Your Profile
Search for Go
Advanced Search
Product Families
today's news
Get Windows .NET Server 2003 RC2
www.metatec.com/ Internet
Start Microsoft Corporation... 8:11 AM

Ransomware



Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

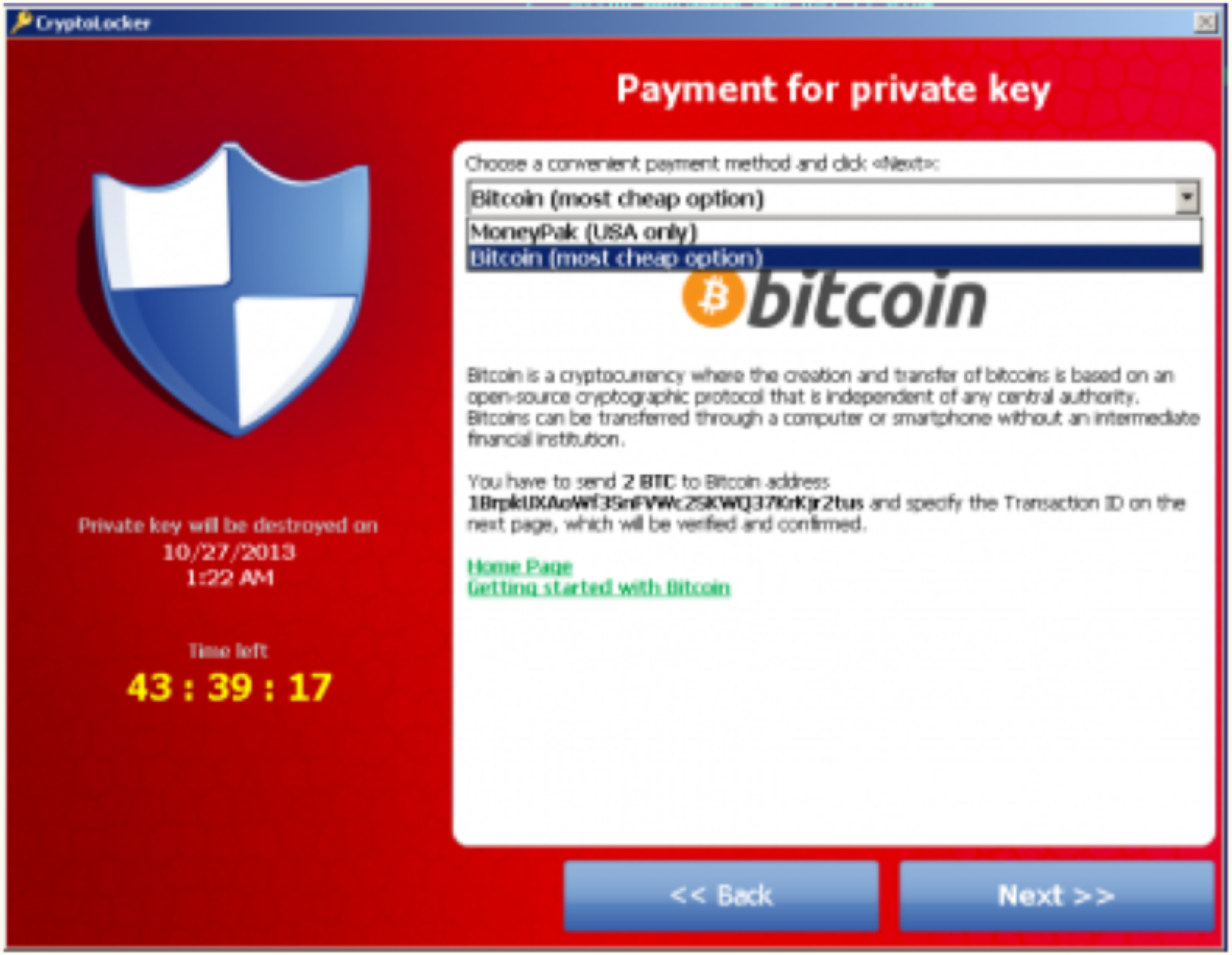
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Ransomware



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

MoneyPak (USA only)

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

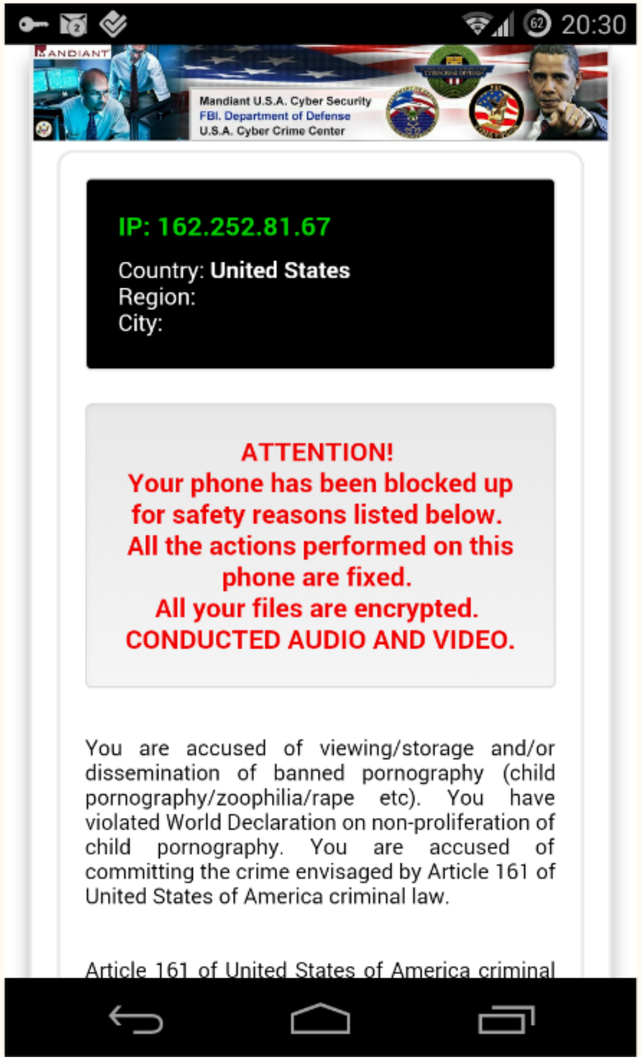
You have to send **2 BTC** to Bitcoin address **1BrpkUXAoWf3SnFVWc2SKWQ37KrKjr2tus** and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 39 : 17

Mobile Ransomware


20:30
MANDIANT
Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

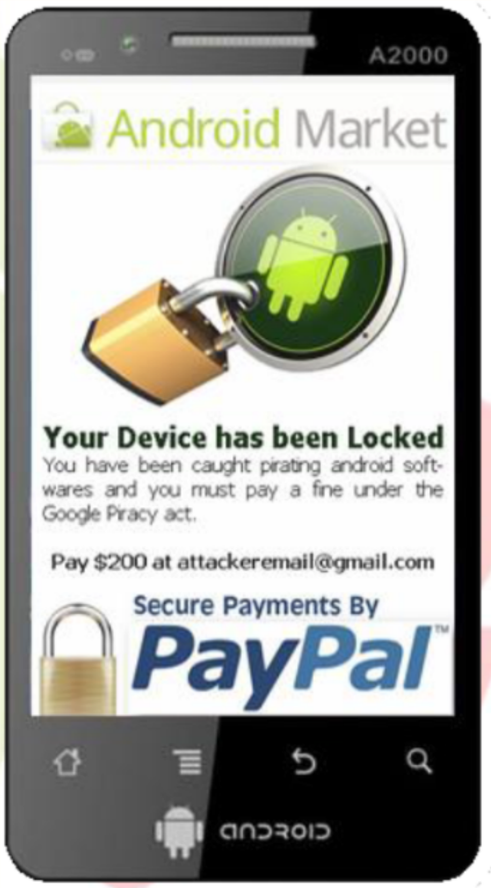
IP: 162.252.81.67

Country: United States
Region:
City:

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal

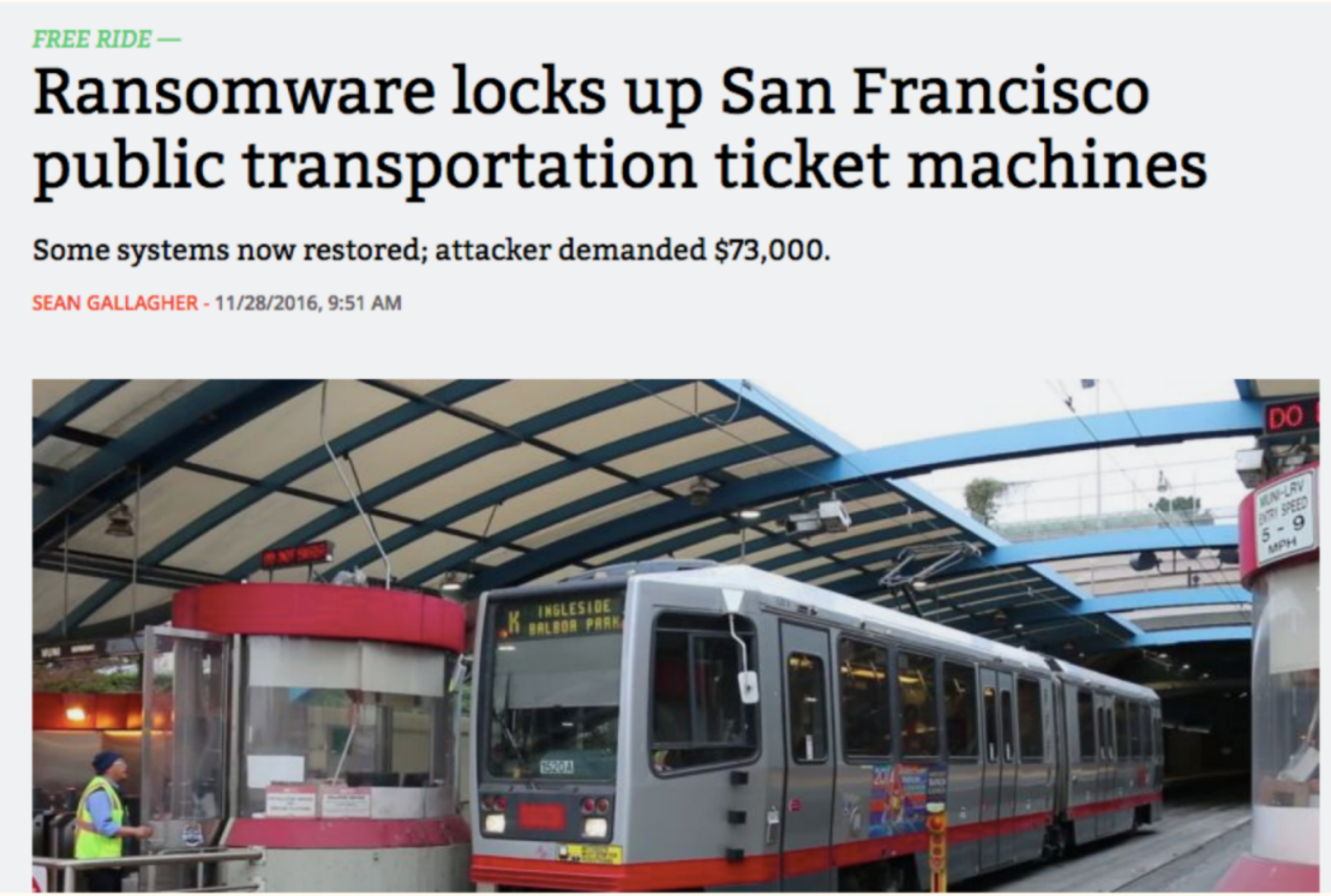


Your Device has been Locked

You have been caught pirating android softwares and you must pay a fine under the Google Piracy act.

Pay $200 at attackeremail@gmail.com

Secure Payments By PayPal

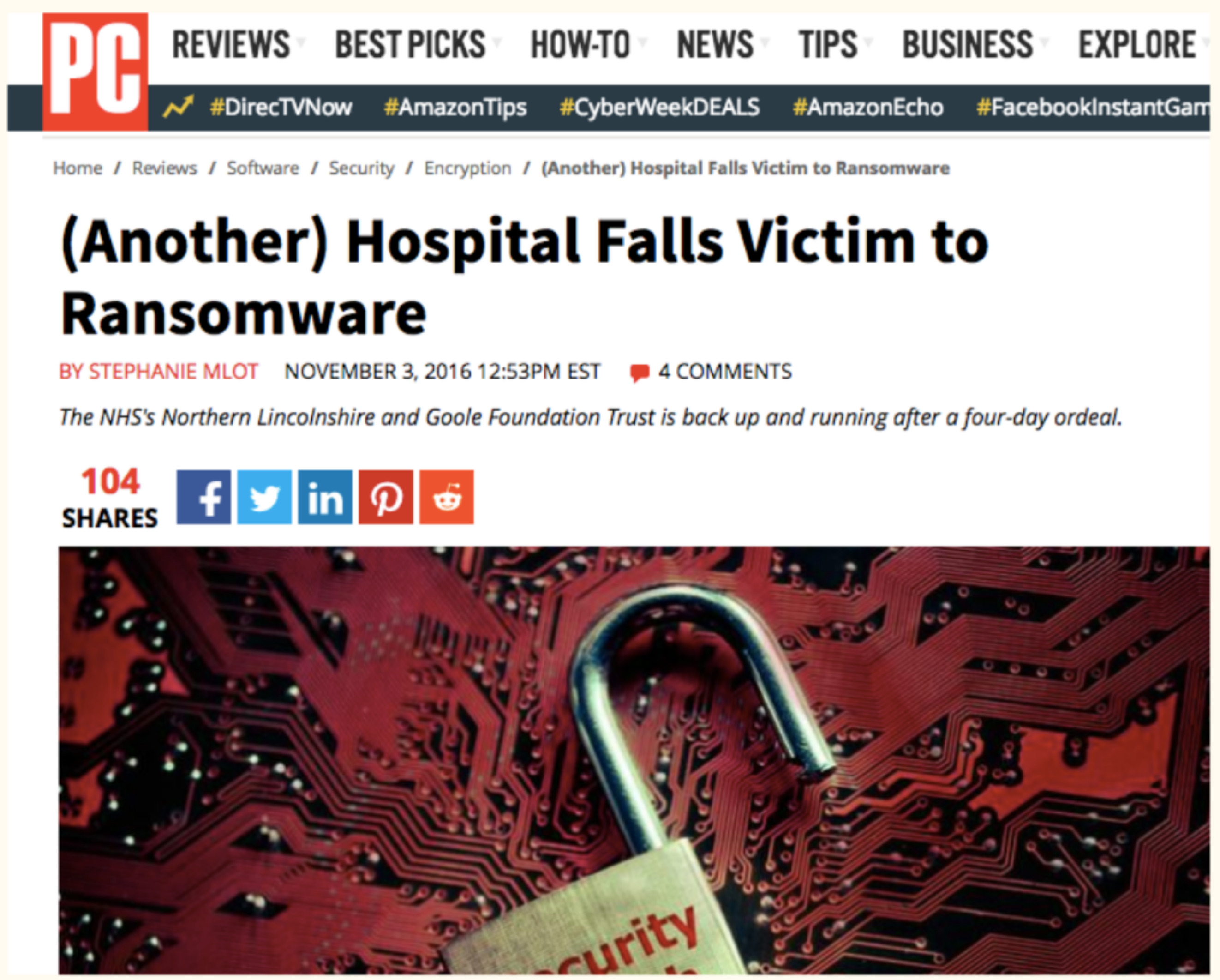


FREE RIDE —

Ransomware locks up San Francisco public transportation ticket machines

Some systems now restored; attacker demanded $73,000.

SEAN GALLAGHER - 11/28/2016, 9:51 AM



Home / Reviews / Software / Security / Encryption / **(Another) Hospital Falls Victim to Ransomware**

(Another) Hospital Falls Victim to Ransomware

BY STEPHANIE MLOT NOVEMBER 3, 2016 12:53PM EST 4 COMMENTS

The NHS's Northern Lincolnshire and Goole Foundation Trust is back up and running after a four-day ordeal.

Botnet

- Collection of compromised hosts
  - Network of ‘bots’ (or ‘zombies’)
  - Spread like worm and virus
  - Respond to remote commands

Botnet

- One of the major threats:
  - Consist of a large pool (millions) of compromised computers (a.k.a., Zombie Armies)
  - Carry out sophisticated attacks to disrupt, gather sensitive data, or increase the armies
    - Spam forwarding (~70% of all spam)
    - Key logging
    - DDoS
  - Vint Cerf: 25% of hosts connected to the Internet

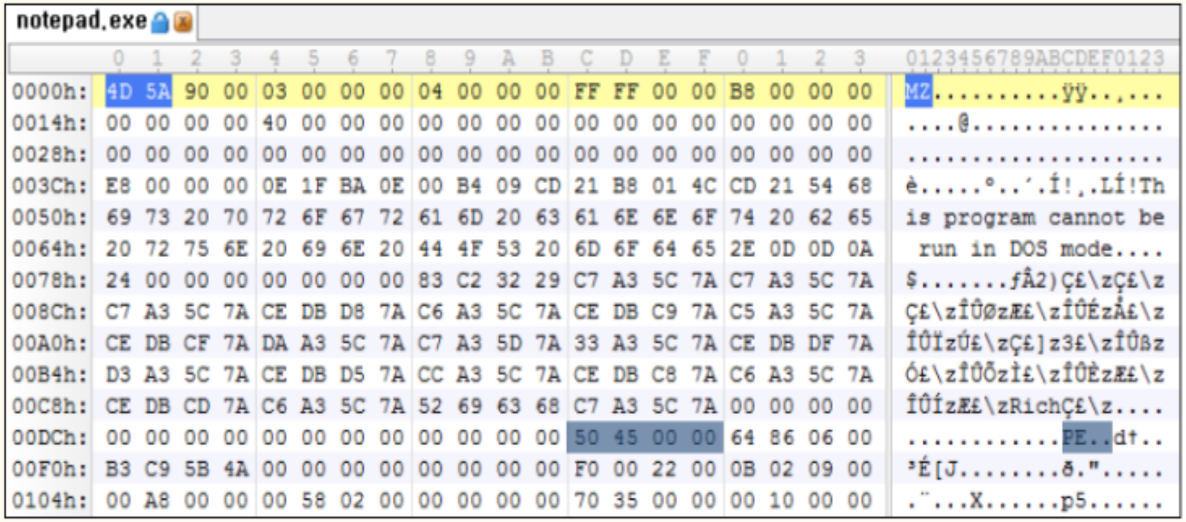
Malware Analysis

- A malware sample is executed in a controlled environment, which makes it possible to observe the traffic that is exchanged between the bot and its command and control (C&C) server(s).
- Involves reverse engineering
- Researchers join a botnet to perform analysis from the inside.

Windows PE format

- PE classification
  - Portable executable (PE) classification based on common object *file format (COFF) for Windows 3.1 and later*
  - *EXE*
  - *DLL*
  - *SYS/VXD*
  - *SCR*
  - *OCX*

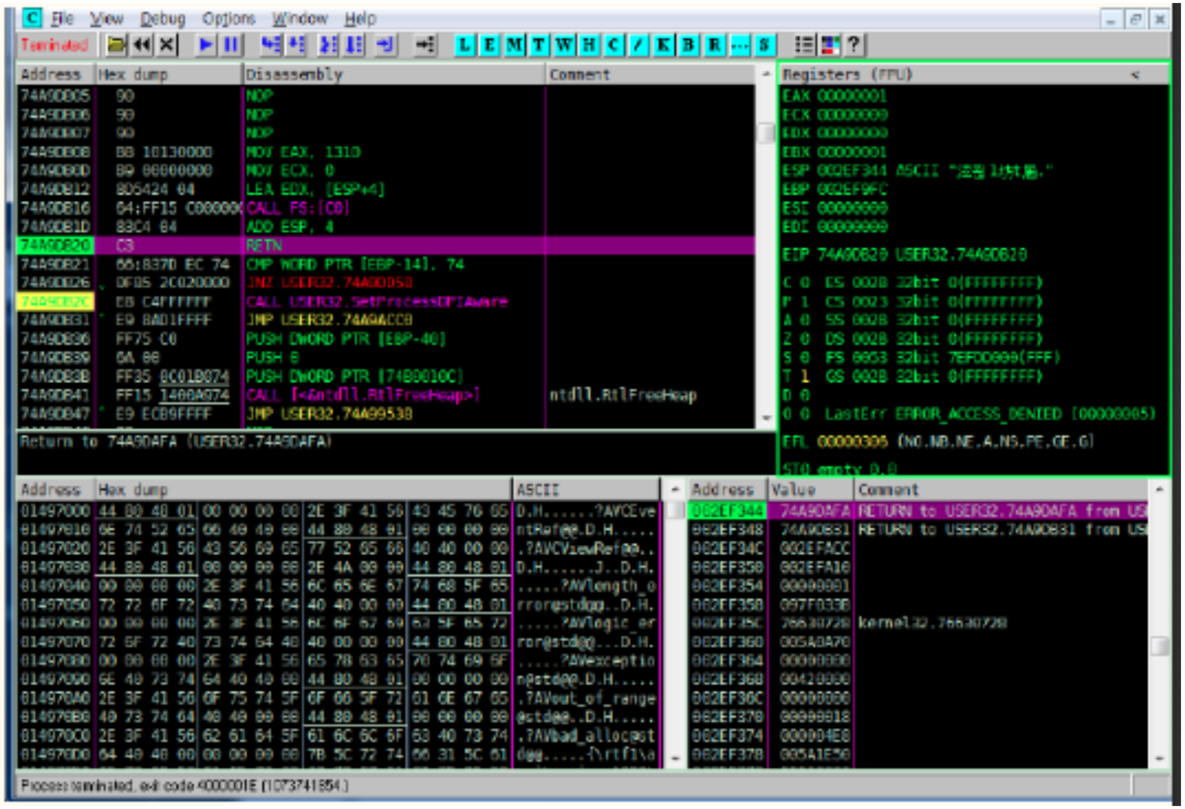
PE signature



```
notepad.exe
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0  1  2  3   0123456789ABCDEF0123
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00   MZ..........ÿÿ..,...
0014h: 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....@...............
0028h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....................
003Ch: E8 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   è.....°..´.Í!,.LÍ!Th
0050h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65   is program cannot be
0064h: 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A    run in DOS mode....
0078h: 24 00 00 00 00 00 00 00 83 C2 32 29 C7 A3 5C 7A C7 A3 5C 7A   $.......ƒÂ2)Ç£\zÇ£\z
008Ch: C7 A3 5C 7A CE DB D8 7A C6 A3 5C 7A CE DB C9 7A C5 A3 5C 7A   Ç£\zÎÛØzÆ£\zÎÛÉzÅ£\z
00A0h: CE DB CF 7A DA A3 5C 7A C7 A3 5D 7A 33 A3 5C 7A CE DB DF 7A   ÎÛÏzÚ£\zÇ£]z3£\zÎÛßz
00B4h: D3 A3 5C 7A CE DB D5 7A CC A3 5C 7A CE DB C8 7A C6 A3 5C 7A   Ó£\zÎÛÕzÌ£\zÎÛÈzÆ£\z
00C8h: CE DB CD 7A C6 A3 5C 7A 52 69 63 68 C7 A3 5C 7A 00 00 00 00   ÎÛÍzÆ£\zRichÇ£\z....
00DCh: 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00   ............PE..d†..
00F0h: B3 C9 5B 4A 00 00 00 00 00 00 00 00 F0 00 22 00 0B 02 09 00   ³É[J........ð.".....
0104h: 00 A8 00 00 00 58 02 00 00 00 00 00 70 35 00 00 00 10 00 00   .¨...X......p5......
```

Static Analysis

- Manual investigation
  - Debugging: OllyDbg, IDA pro
  - VM-based memory analysis


C File View Debug Options Window Help
Terminated
L E M T W H C / K B R ... S
?

```
Address   Hex dump            Disassembly                       Comment
74A9D805    90                NOP
74A9D806    90                NOP
74A9D807    90                NOP
74A9D808    B8 10130000       MOV EAX, 1310
74A9D80D    B9 00000000       MOV ECX, 0
74A9D812    8D5424 04         LEA EDX, [ESP+4]
74A9D816    64:FF15 C000000   CALL FS:[C0]
74A9D81D    83C4 04           ADD ESP, 4
74A9D820    C3                RETN
74A9D821    66:837D EC 74     CMP WORD PTR [EBP-14], 74
74A9D826  . 0F85 2C020000     JNZ USER32.74A9D058
74A9D82C    E8 C4FFFFFF       CALL USER32.SetProcessDPIAware
74A9D831  ' E9 BAD1FFFF       JMP USER32.74A9ACC8
74A9D836    FF75 C0           PUSH DWORD PTR [EBP-40]
74A9D839    6A 00             PUSH 0
74A9D83B    FF35 0C01B074     PUSH DWORD PTR [74B0010C]
74A9D841    FF15 1400A974     CALL [<&ntdll.RtlFreeHeap>]       ntdll.RtlFreeHeap
74A9D847  ' E9 ECB9FFFF       JMP USER32.74A99538
Return to 74A9DAFA (USER32.74A9DAFA)
```

```
Registers (FPU)
EAX 00000001
ECX 00000000
EDX 00000000
EBX 00000001
ESP 002EF344 ASCII "[illegible]."
EBP 002EF9FC
ESI 00000000
EDI 00000000

EIP 74A9D820 USER32.74A9D820

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7EFDD000(FFF)
T 1  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_ACCESS_DENIED (00000005)

EFL 00000306 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty 0.0
```

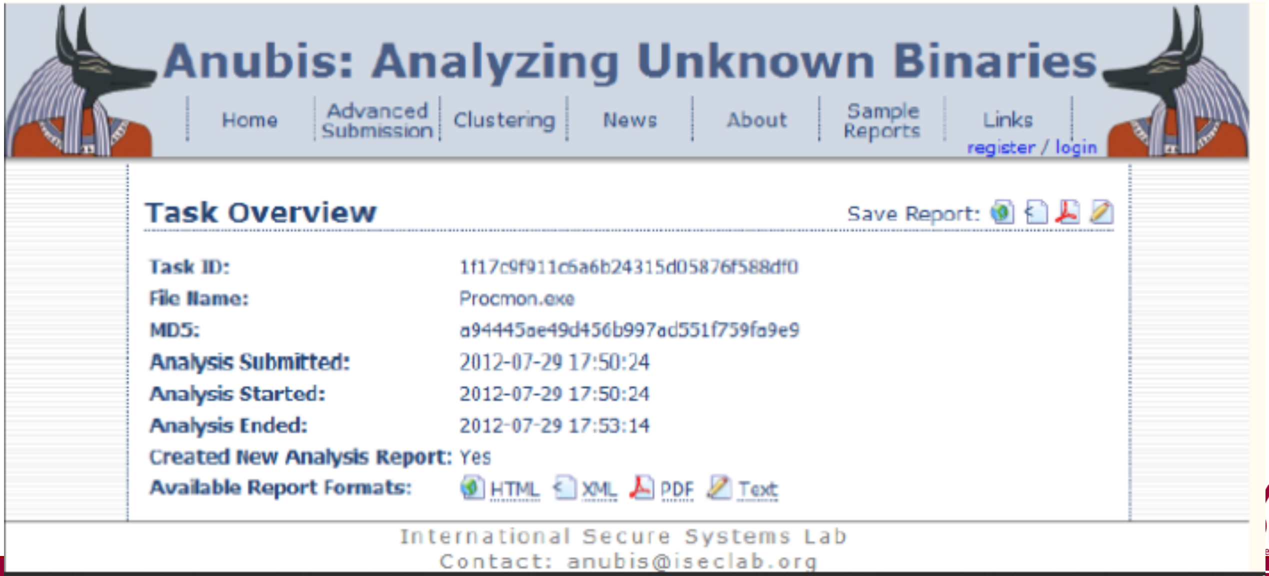
```
Address   Hex dump                                         ASCII
01497000  44 00 48 01 00 00 00 00 2E 3F 41 56 43 45 76 65  D.H......?AVCEve
01497010  6E 74 52 65 66 40 40 00 44 00 48 01 00 00 00 00  ntRef@@.D.H.....
01497020  2E 3F 41 56 43 56 69 65 77 52 65 66 40 40 00 00  .?AVCViewRef@@..
01497030  44 00 48 01 00 00 00 00 2E 4A 00 00 44 00 48 01  D.H......J..D.H.
01497040  00 00 00 00 2E 3F 41 56 6C 65 6E 67 74 68 5F 65  .....?AVlength_e
01497050  72 72 6F 72 40 73 74 64 40 40 00 00 44 00 48 01  rror@std@@..D.H.
01497060  00 00 00 00 2E 3F 41 56 6C 6F 67 69 63 5F 65 72  .....?AVlogic_er
01497070  72 6F 72 40 73 74 64 40 40 00 00 00 44 00 48 01  ror@std@@...D.H.
01497080  00 00 00 00 2E 3F 41 56 65 78 63 65 70 74 69 6F  .....?AVexceptio
01497090  6E 40 73 74 64 40 40 00 44 00 48 01 00 00 00 00  n@std@@.D.H.....
014970A0  2E 3F 41 56 6F 75 74 5F 6F 66 5F 72 61 6E 67 65  .?AVout_of_range
014970B0  40 73 74 64 40 40 00 00 44 00 48 01 00 00 00 00  @std@@..D.H.....
014970C0  2E 3F 41 56 62 61 64 5F 61 6C 6C 6F 63 40 73 74  .?AVbad_alloc@st
014970D0  64 40 40 00 00 00 00 00 7B 5C 72 74 66 31 5C 61  d@@.....{\rtf1\a
```

```
Address   Value     Comment
002EF344  74A9DAFA  RETURN to USER32.74A9DAFA from US
002EF348  74A9D831  RETURN to USER32.74A9D831 from US
002EF34C  002EFACC
002EF350  002EFA10
002EF354  00000001
002EF358  097F033B
002EF35C  76630728  kernel32.76630728
002EF360  005A0A70
002EF364  00000000
002EF368  00420000
002EF36C  00000000
002EF370  00000018
002EF374  000004E8
002EF378  005A1E50
```

```
Process terminated, exit code 4000001E (1073741854.)
```

Dynamic Analysis

- Monitors process, file access, DLL, registry, network connection, etc.
- Tools:
  - Anubis
  - CW Sandbox
  - Norman Sandbox
  - Joebox
  - VirusTotal



Task Overview

Task ID:	1f17c9f911c6a6b24315d05876f588df0
File Name:	Procmon.exe
MD5:	a94445ae49d456b997ad551f759fa9e9
Analysis Submitted:	2012-07-29 17:50:24
Analysis Started:	2012-07-29 17:50:24
Analysis Ended:	2012-07-29 17:53:14
Created New Analysis Report:	Yes
Available Report Formats:	HTML XML PDF Text

International Secure Systems Lab
Contact: anubis@iseclab.org

Demo