Lecture 11 – Malware

Stephen Checkoway

University of Illinois at Chicago

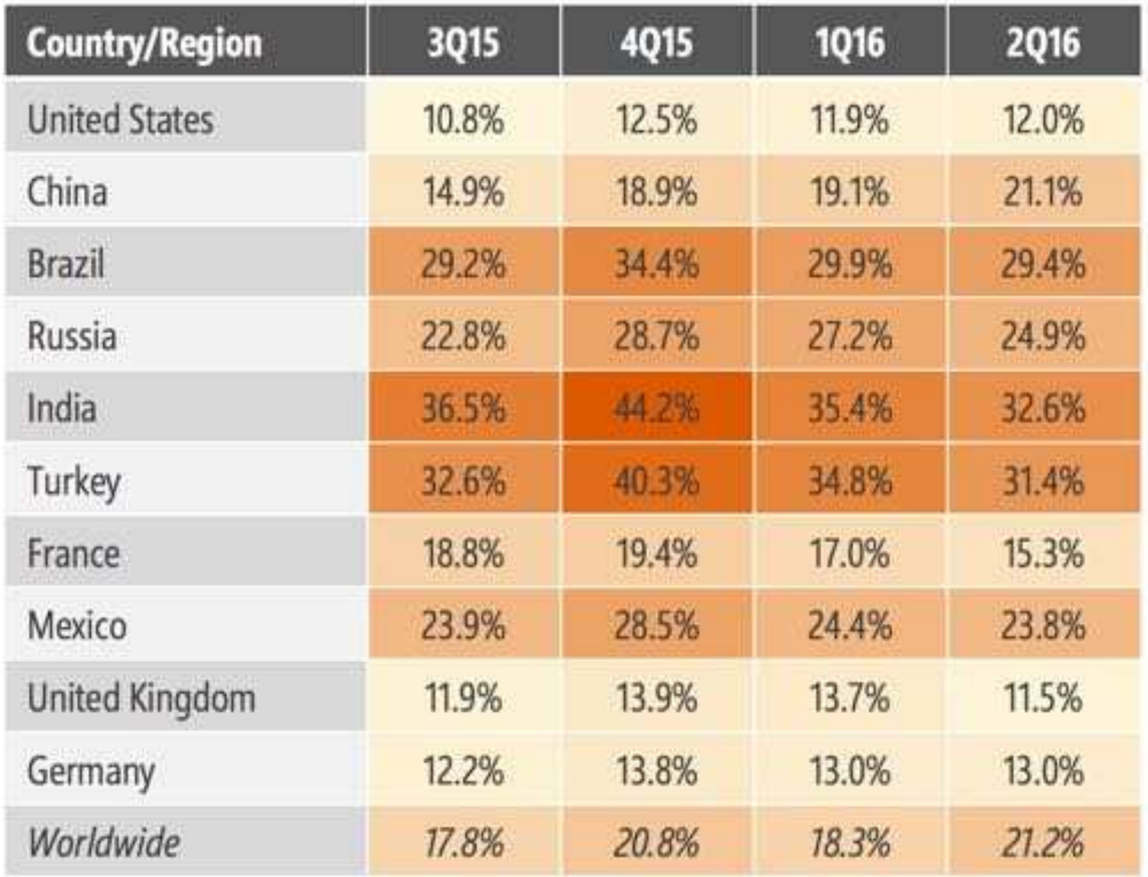
CS 487 – Fall 2017

Slides adapted from Michael Bailey

Malware definition and goals

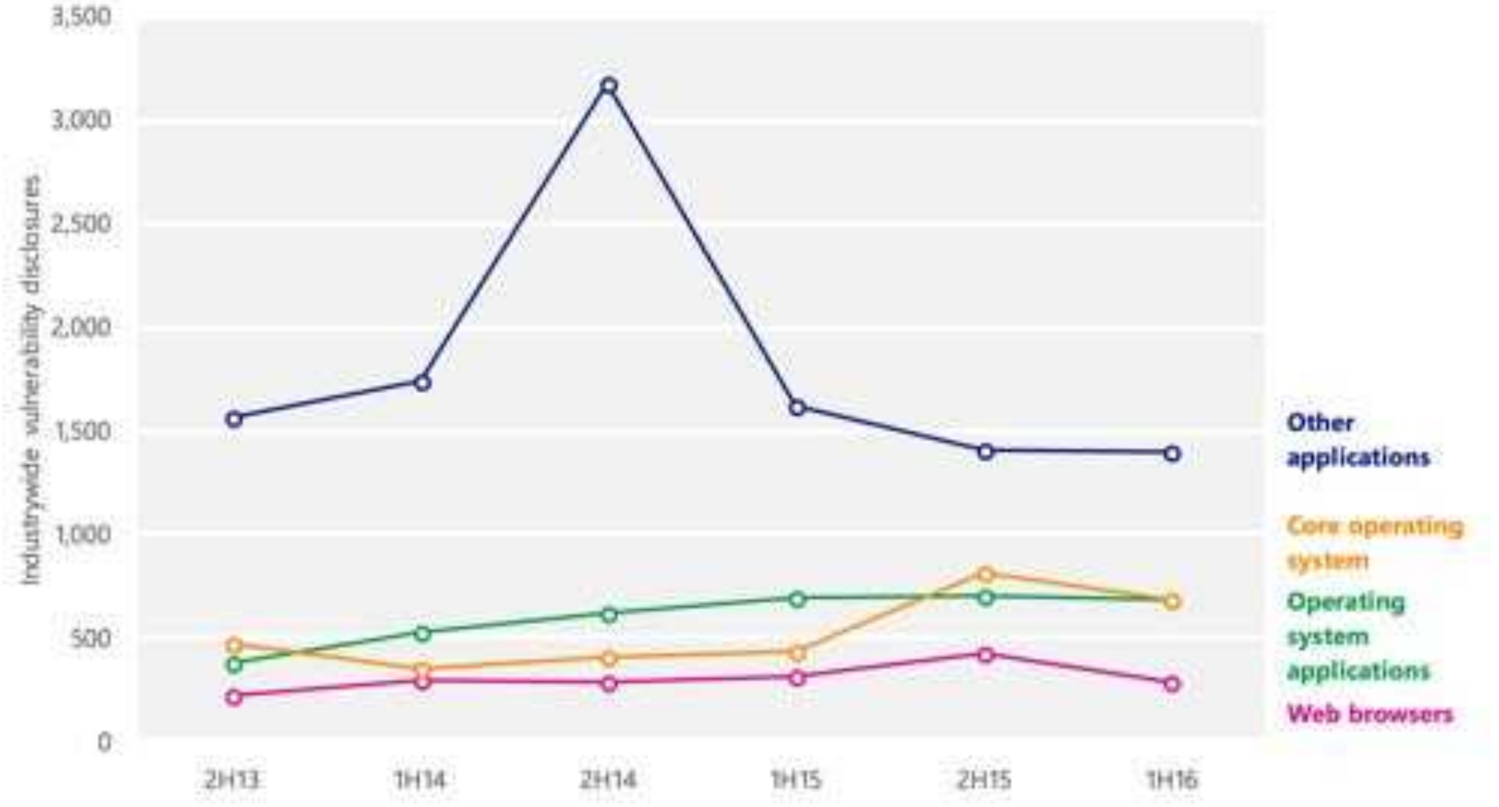
- What is malware?
  - Set of instructions that run on your computer and do something an attacker wants it to do.
- Muddled Taxonomy, but difference primarily
  - How they get on your machine
  - What do they do

Encounter rate trends for the locations with the most (Windows) computers reporting malicious and unwanted software encounters, by number of computers reporting Country/Region



Country/Region	3Q15	4Q15	1Q16	2Q16
United States	10.8%	12.5%	11.9%	12.0%
China	14.9%	18.9%	19.1%	21.1%
Brazil	29.2%	34.4%	29.9%	29.4%
Russia	22.8%	28.7%	27.2%	24.9%
India	36.5%	44.2%	35.4%	32.6%
Turkey	32.6%	40.3%	34.8%	31.4%
France	18.8%	19.4%	17.0%	15.3%
Mexico	23.9%	28.5%	24.4%	23.8%
United Kingdom	11.9%	13.9%	13.7%	11.5%
Germany	12.2%	13.8%	13.0%	13.0%
Worldwide	*17.8%*	*20.8%*	*18.3%*	*21.2%*

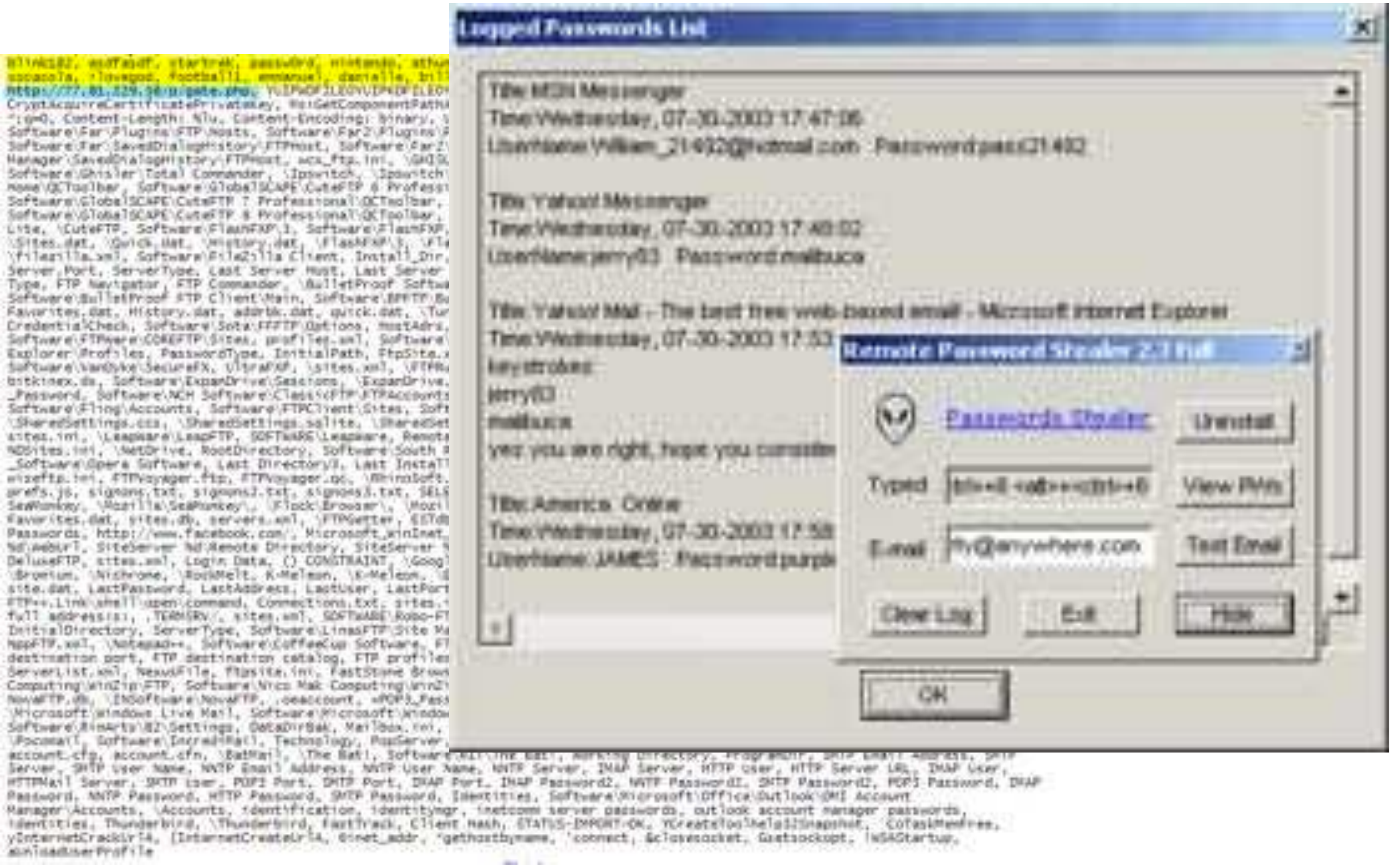
Industry-wide operating system, browser, and application vulnerabilities, 2H13–1H16



What Can Malware Do?

- Pretty much *anything*
  - Payload generally decoupled from how manages to run
  - Only subject to permissions under which it runs
- Examples:
  - Brag or exhort or extort (pop up a message/display)
  - Trash files (just to be nasty)
  - Damage hardware (Stuxnet)
  - Launch external activity (spam, *click fraud*, DoS)
  - Steal information (*exfiltrate*)
  - Keylogging; screen / audio / camera capture
    - ***Robbins v. Lower Merion School District***
  - Encrypt files (*ransomware*)
- Possibly delayed until condition occurs
  - “time bomb” / “logic bomb”

Key logging and Password Stealing



```
blink182, asdfasdf, startrek, password, nintendo, athu
cocacola, iloveqod, football1, emmanuel, danielle, bri
http://77.81.129.56/p/gate.php, YUIPWDFILE0YUIPKDFILE0
CryptAcquireCertificatePrivateKey, MsiGetComponentPath
*;q=0, Content-Length: %lu, Content-Encoding: binary, \
Software\Far\Plugins\FTP\Hosts, Software\Far2\Plugins\F
Software\Far\SavedDialogHistory\FTPHost, Software\Far2\
Manager\SavedDialogHistory\FTPHost, wcx_ftp.ini, \GHISL
Software\Ghisler\Total Commander, \Ipswitch, \Ipswitch\
Home\QCToolbar, Software\GlobalSCAPE\CuteFTP 6 Professi
Software\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar,
Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar,
Lite, \CuteFTP, Software\FlashFXP\3, Software\FlashFXP,
\Sites.dat, \Quick.dat, \History.dat, \FlashFXP\3, \Fl
\filezilla.xml, Software\FileZilla Client, Install_Dir,
Server.Port, ServerType, Last Server Host, Last Server
Type, FTP Navigator, FTP Commander, \BulletProof Softwa
Software\BulletProof FTP Client\Main, Software\BPFTP\Bu
Favorites.dat, History.dat, addrbk.dat, quick.dat, \Tur
CredentialCheck, Software\Sota\FFFTP\Options, HostAdrs,
Software\FTPWare\COREFTP\Sites, profiles.xml, Software\
Explorer\Profiles, PasswordType, InitialPath, FtpSite.x
Software\VanDyke\SecureFX, UltraFXP, \sites.xml, \FTPRu
bitkinex.ds, Software\ExpanDrive\Sessions, \ExpanDrive,
_Password, Software\NCH Software\Classic\FTP\FTPAccounts
Software\Fling\Accounts, Software\FTPClient\Sites, Soft
\SharedSettings.ccs, \SharedSettings.sqlite, \SharedSet
sites.ini, \Leapware\LeapFTP, SOFTWARE\Leapware, Remote
NDSites.ini, \NetDrive, RootDirectory, Software\South R
_Software\Opera Software, Last Directory3, Last Install
wiseftp.ini, FTPVoyager.ftp, FTPVoyager.qc, \RhinoSoft.
prefs.js, signons.txt, signons2.txt, signons3.txt, SELE
SeaMonkey, \Mozilla\SeaMonkey\, \Flock\Browser\, \Mozil
Favorites.dat, sites.db, servers.xml, \FTPGetter, ESTdb
Passwords, http://www.facebook.com/, Microsoft_WinInet_
%d\WebUrl, SiteServer %d\Remote Directory, SiteServer %
DeluxeFTP, sites.xml, Login Data, () CONSTRAINT, \Goog
\Bromium, \Nichrome, \RockMelt, K-Meleon, \K-Meleon, \
site.dat, LastPassword, LastAddress, LastUser, LastPort
FTP++.Link\shell\open\command, Connections.txt, sites.
full address:s:, .TERMSRV\, sites.xml, SOFTWARE\Robo-FT
InitialDirectory, ServerType, Software\LinasFTP\Site Ma
NppFTP.xml, \Notepad++, Software\CoffeeCup Software, FT
destination port, FTP destination catalog, FTP profiles
Serverlist.xml, NexusFile, ftpsite.ini, FastStone Brows
Computing\WinZip\FTP, Software\Nico Mak Computing\WinZi
NovaFTP.db, \INSoftware\NovaFTP, .oeaccount, *POP3_Pass
\Microsoft\Windows Live Mail, Software\Microsoft\Window
Software\RimArts\B2\Settings, DataDirBak, MailBox.ini,
\Pocomail, Software\IncrediMail, Technology, PopServer,
account.cfg, account.cfn, \BatMail, \The Bat!, Software\RIT\The Bat!, Working Directory, ProgramDir, SMTP Email Address, SMTP
Server, SMTP User Name, NNTP Email Address, NNTP User Name, NNTP Server, IMAP Server, HTTP User, HTTP Server URL, IMAP User,
HTTPMail Server, SMTP User, POP3 Port, SMTP Port, IMAP Port, IMAP Password2, NNTP Password2, SMTP Password2, POP3 Password, IMAP
Password, NNTP Password, HTTP Password, SMTP Password, Identities, Software\Microsoft\Office\Outlook\OMI Account
Manager\Accounts, \Accounts, identification, identitymgr, inetcomm server passwords, outlook account manager passwords,
identities, Thunderbird, \Thunderbird, FastTrack, Client Hash, STATUS-IMPORT-OK, YCreateToolhelp32Snapshot, CoTaskMemFree,
yInternetCrackUrlA, [InternetCreateUrlA, 6inet_addr, *gethostbyname, 'connect, &closesocket, Ggetsockopt, !WSAStartup,
aUnloadUserProfile
```

Logged Passwords List

```
Title:MSN Messenger
Time:Wednesday, 07-30-2003 17:47:06
UserName:William_21402@hotmail.com  Password:pass21402

Title:Yahoo! Messenger
Time:Wednesday, 07-30-2003 17:49:02
UserName:jerry03  Password:malbuca

Title:Yahoo! Mail - The best free web-based email - Microsoft Internet Explorer
Time:Wednesday, 07-30-2003 17:53
keystrokes:
jerry03
malbuca
yes you are right, hope you conside

Title:America  Online
Time:Wednesday, 07-30-2003 17:58
UserName: JAMES  Password:purple
```

Remote Password Stealer 2.7 Full

Passwords Stealer

Typed: ctrl>+d <alt>+<ctrl>+6

E-mail: fly@anywhere.com

Logic Bombs

- A **logic bomb** is a program that performs a malicious action as a result of a certain logic condition.
- The classic example of a logic bomb is a programmer coding up the software for the payroll system who puts in code that makes the program crash should it ever process two consecutive payrolls without paying him.
- Another classic example combines a logic bomb with a backdoor, where a programmer puts in a logic bomb that will crash the program on a certain date.

The Omega Engineering Logic Bomb

IDG

FEBRUARY 23, 1998 VOLUME 15, NUMBER 8

NetworkWorld

THE NEWSWEEKLY OF ENTERPRISE NETWORK COMPUTING

Going with Gigabit Ethernet [illegible] Page 6

- An example of a logic bomb that was actually triggered and caused damage is one that programmer Tim Lloyd was convicted of using on his former employer, Omega Engineering Corporation.
- On July 31, 1996, a logic bomb was triggered on the server for Omega Engineering's manufacturing operations, which ultimately cost the company millions of dollars in damages and led to it laying off many of its employees.

A view into a network attack

Net administrator charged in $10M "logic bomb" case.

By Ellen Messmer

Bridgeport, Conn.

In one of the costliest reported acts of computer sabotage, an engineering company [illegible] will prosecute its former network administrator for electronically destroying computer files that the company claims cost it about $10 million in sales.

Omega Engineering, Inc. is set to go to trial against Timothy Lloyd, the chief network program designer, who the company said planted a LAN-based logic bomb that went off after his job was terminated. The logic bomb wiped out all the files on the company's Novell, Inc. network-based servers.

What detonated the Omega bomb was not immediately clear.

Security experts said a logic bomb usually is a software program that, once activated by a specific date for example, can through files or reformats hard drives. The bomber's intent is to hopelessly damage and erase data.

"[Logic bombs] can be as simple as a script that runs a bunch of delete commands," said Chris Byrnes, vice president for servers and systems management strategy

See Bomb, page 16

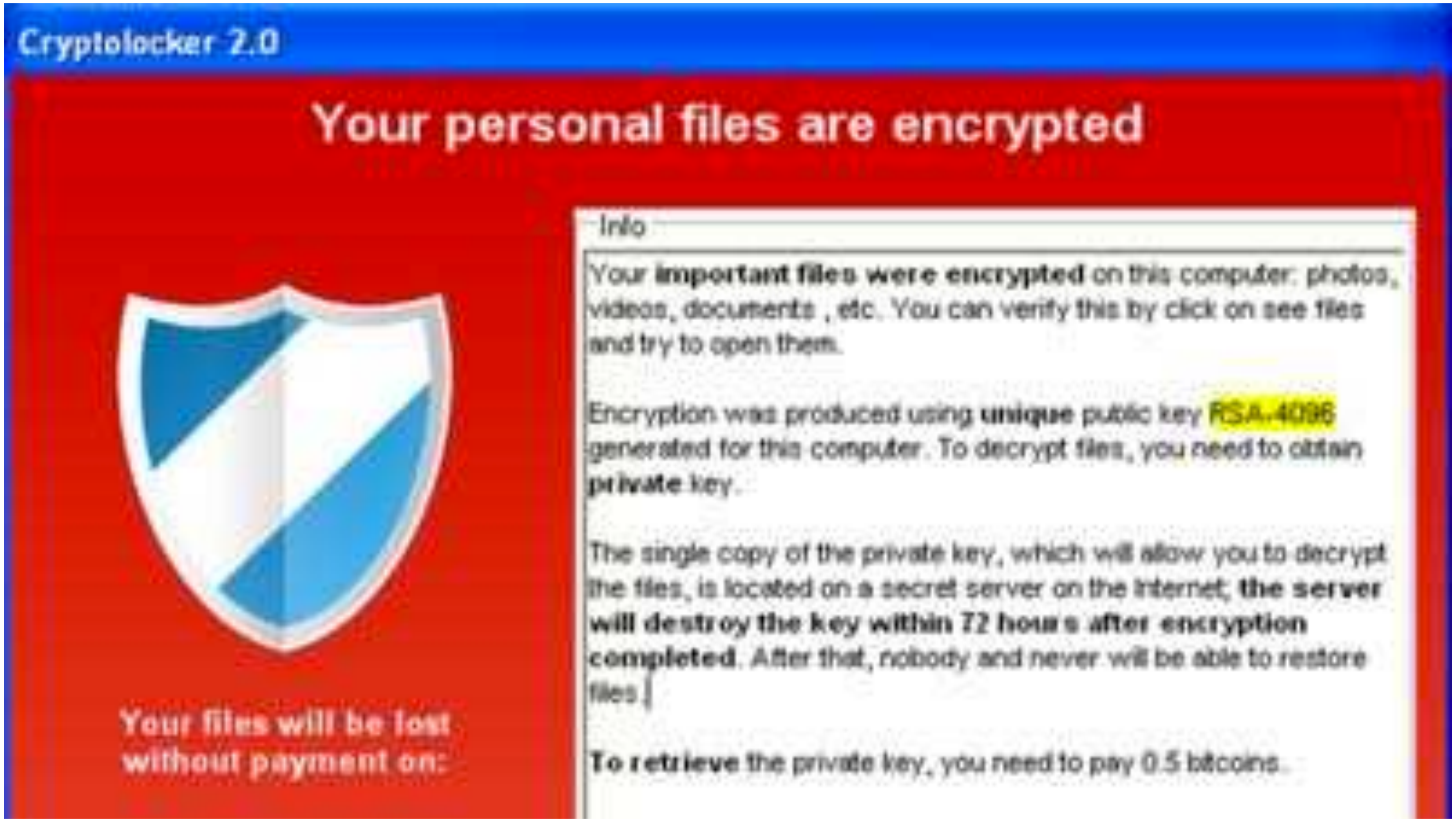
The Omega Bomb Code

- The Logic Behind the Omega Engineering Time Bomb included the following strings:
  - 7/30/96
    - Event that triggered the bomb
  - F:
    - Focused attention to volume F, which had critical files
  - F:\LOGIN\LOGIN 12345
    - Login a fictitious user, 12345 (the back door)
  - CD \PUBLIC
    - Moves to the public folder of programs
  - FIX.EXE /Y F:\*.*
    - Run a program, called FIX, which actually deletes everything
  - PURGE F:\/ALL
    - Prevent recovery of the deleted files

LOGIC BOMB SET OFF SOUTH KOREA CYBERATTACK

A disconnected computer monitor is seen at a newsroom of Korean Broadcasting System (KBS) at its headquarter in Seoul, South Korea, Wednesday, March 20, 2013. Computers networks at two major South Korean banks and three top TV broadcasters went into shutdown mode en masse Wednesday, paralyzing bank machines across the country. *Photo: AP/Kim Ju-sung, Yonhap*

Ransomware



Your personal files are encrypted

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.

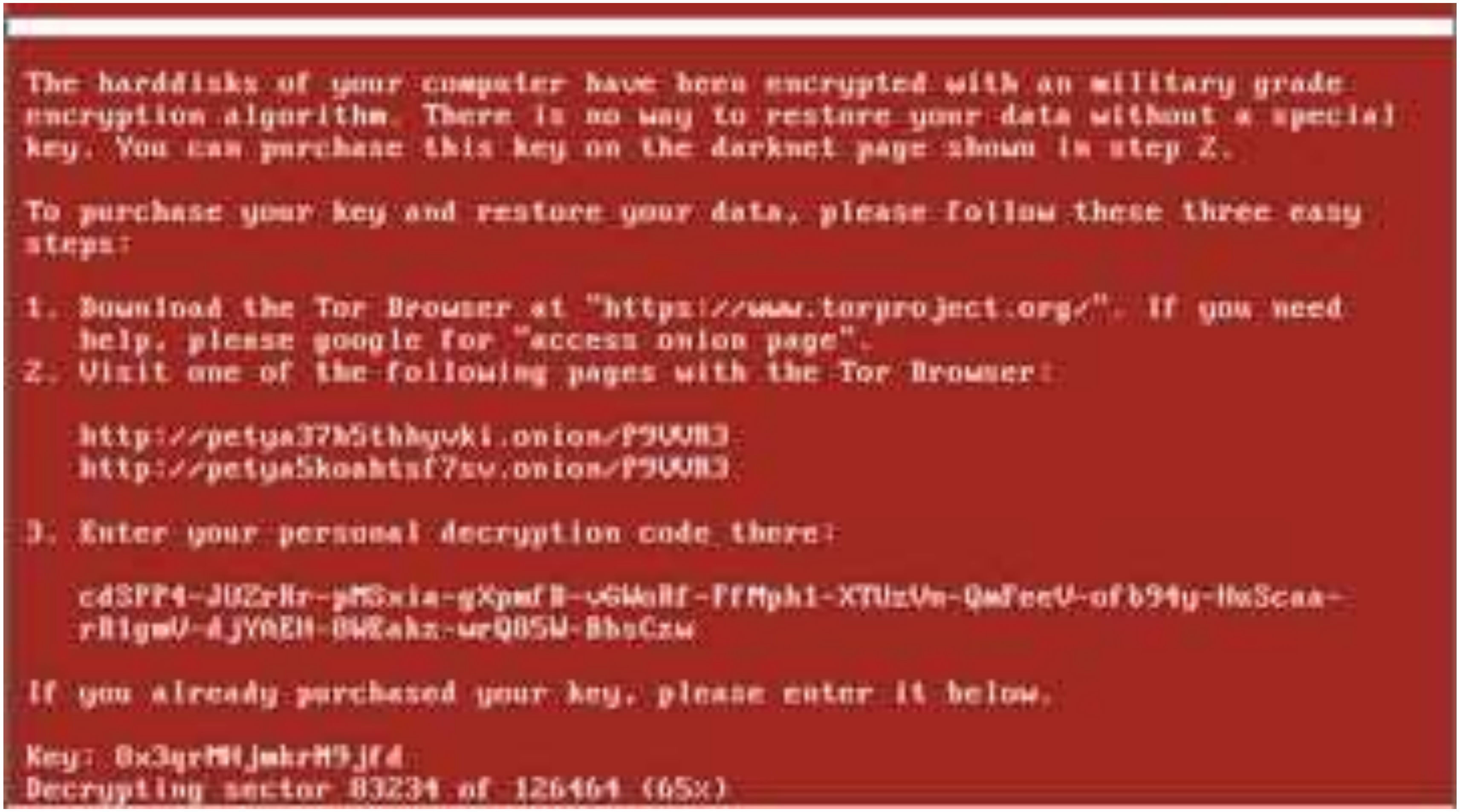
Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

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.

Your files will be lost without payment on:

Petya Ransomware

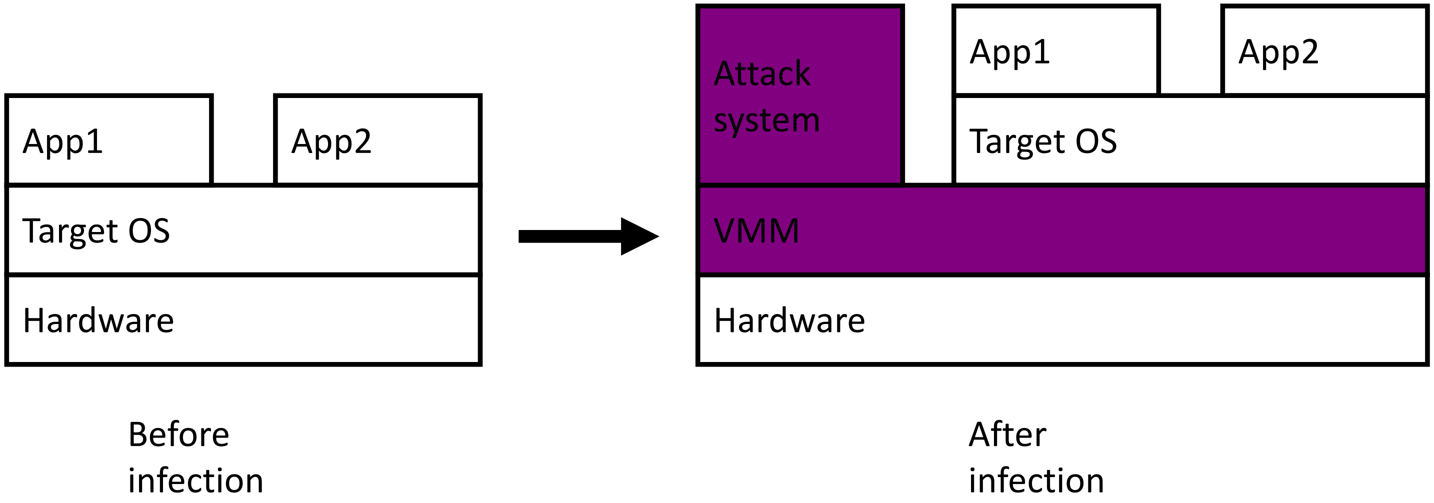


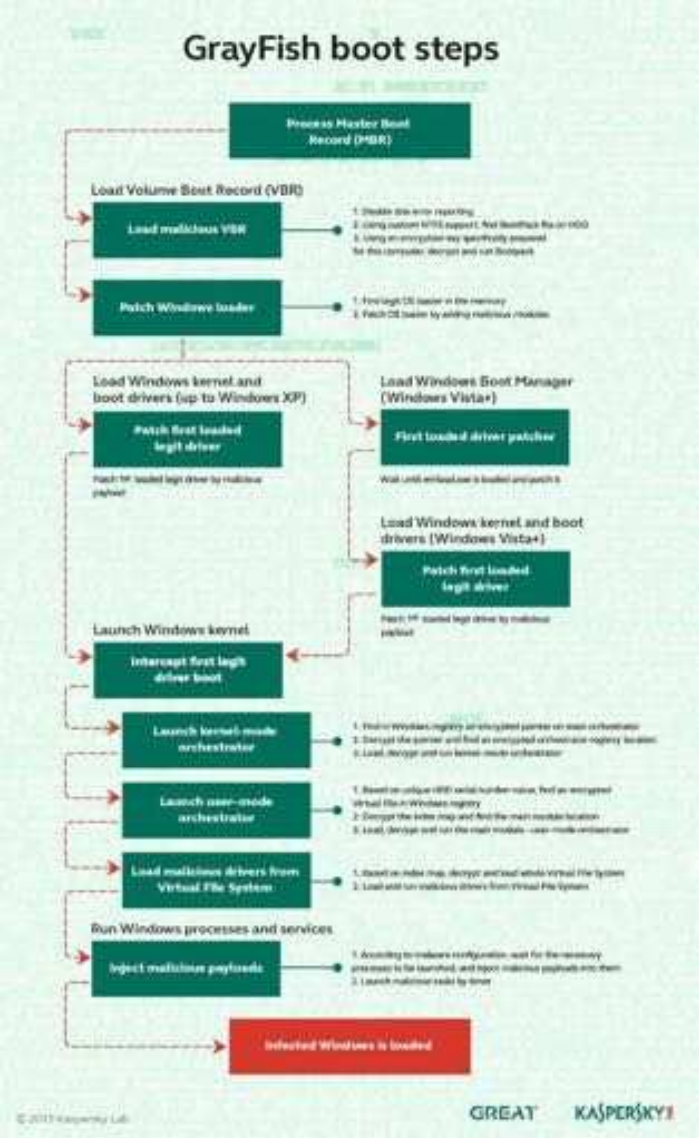
```
The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/P9VV83
   http://petya5koahtsf7sv.onion/P9VV83

3. Enter your personal decryption code there:

   cdSPF4-J2ZrHr-yM5xia-gXpmfB-v6WoRf-FfMph1-XTUzVm-QmFeeV-ofb94y-HxScaa-
   rB1gmV-dJYAEH-8WEahz-wrQ85W-BbsCzw

If you already purchased your key, please enter it below.

Key: 8x3qrMNjmkrM9jfd
Decrypting sector 83234 of 126464 (65%)
```

Rootkits

- A rootkit modifies the operating system to hide its existence
  - E.g., modifies file system exploration utilities
  - Hard to detect using software that relies on the OS itself
- Operation:
  - Intercept system calls for listing files, processes, etc.
  - Filter out malware's files and processes
  - Example: Magic prefix -- $sys$filename
  - Diagram:
  - Applications --> System Call ---> (Rootkit) --> Kernel
  - <-- Results --- If call is from rootkit application (e.g. $sys$rootkit.exe), don't filter!

Virtual-machine based rootkits (VMBRs)

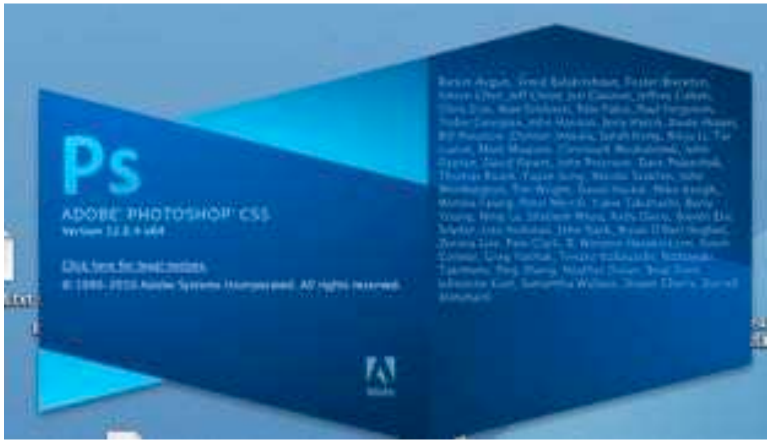



GrayFish boot steps
Process Master Boot Record (MBR)
Load Volume Boot Record (VBR)
Load malicious VBR
1. Disable disk error reporting
2. Using custom NTFS support, find BootPack file on HDD
3. Using an encryption key specifically prepared for this computer, decrypt and run Bootpack
Patch Windows loader
1. Find legit OS loader in the memory
2. Patch OS loader by adding malicious modules
Load Windows kernel and boot drivers (up to Windows XP)
Patch first loaded legit driver
Patch 1st loaded legit driver by malicious payload
Load Windows Boot Manager (Windows Vista+)
First loaded driver patcher
Wait until winload.exe is loaded and patch it
Load Windows kernel and boot drivers (Windows Vista+)
Patch first loaded legit driver
Patch 1st loaded legit driver by malicious payload
Launch Windows kernel
Intercept first legit driver boot
Launch kernel-mode orchestrator
1. Find in Windows registry an encrypted pointer on main orchestrator
2. Decrypt the pointer and find an encrypted orchestrator registry location
3. Load, decrypt and run kernel-mode orchestrator
Launch user-mode orchestrator
1. Based on unique HDD serial number value, find an encrypted Virtual File in Windows registry
2. Decrypt the index map and find the main module location
3. Load, decrypt and run the main module - user-mode orchestrator
Load malicious drivers from Virtual File System
1. Based on index map, decrypt and load whole Virtual File System
2. Load and run malicious drivers from Virtual File System
Run Windows processes and services
Inject malicious payloads
1. According to malware configuration, wait for the necessary processes to be launched, and inject malicious payloads into them
2. Launch malicious tasks by timer
Infected Windows is loaded
© 2015 Kaspersky Lab
GREAT
KASPERSKY

Backdoors

- A **backdoor,** which is also sometimes called a **trapdoor,** is a hidden feature or command in a program that allows a user to perform actions he or she would not normally be allowed to do.
- When used in a normal way, this program performs completely as expected and advertised.
- But if the hidden feature is activated, the program does something unexpected, often in violation of security policies, such as performing a privilege escalation.
- Usually enable remote access to the attacker
- Benign example: **Easter Eggs** in DVDs and software

Easter Eggs



Ps

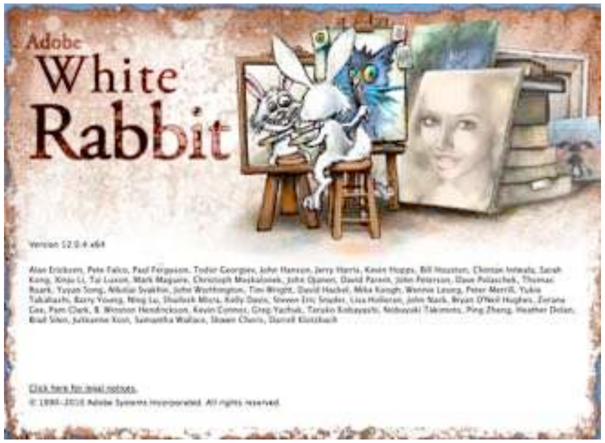
ADOBE® PHOTOSHOP® CS5

Version 12.0.4 x64

Click here for legal notices.

© 1990-2010 Adobe Systems Incorporated. All rights reserved.

Barkin Aygun, Vinod Balakrishnan, Foster Brereton, Simon Chen, Jeff Chien, Jon Clauson, Jeffrey Cohen, Chris Cox, Alan Erickson, Pete Falco, Paul Ferguson, Todor Georgiev, John Hanson, Jerry Harris, Kevin Hopps, Bill Houston, Chintan Intwala, Sarah Kong, Xinju Li, Tai Luxon, Mark Maguire, Christoph Moskalonek, John Ojanen, David Parent, John Peterson, Dave Polaschek, Thomas Ruark, Yuyan Song, Nikolai Svakhin, John Worthington, Tim Wright, David Hackel, Mike Keogh, Wennie Leung, Peter Merrill, Yukie Takahashi, Barry Young, Ning Lu, Shailesh Misra, Kelly Davis, Steven Eric Snyder, Lisa Holleran, John Nack, Bryan O'Neil Hughes, Zorana Gee, Pam Clark, B. Winston Hendrickson, Kevin Connor, Greg Yachuk, Tatsuo Kobayashi, Nobuyuki Takimoto, Ping Zhang, Heather Dolan, Brad Silen, Julieanne Kost, Samantha Wallace, Shawn Cheris, Darrell Klotzbach



Adobe White Rabbit

Version 12.0.4 x64

Alan Erickson, Pete Falco, Paul Ferguson, Todor Georgiev, John Hanson, Jerry Harris, Kevin Hopps, Bill Houston, Chintan Intwala, Sarah Kong, Xinju Li, Tai Luxon, Mark Maguire, Christoph Moskalonek, John Ojanen, David Parent, John Peterson, Dave Polaschek, Thomas Ruark, Yuyan Song, Nikolai Svakhin, John Worthington, Tim Wright, David Hackel, Mike Keogh, Wennie Leung, Peter Merrill, Yukie Takahashi, Barry Young, Ning Lu, Shailesh Misra, Kelly Davis, Steven Eric Snyder, Lisa Holleran, John Nack, Bryan O'Neil Hughes, Zorana Gee, Pam Clark, B. Winston Hendrickson, Kevin Connor, Greg Yachuk, Tatsuo Kobayashi, Nobuyuki Takimoto, Ping Zhang, Heather Dolan, Brad Silen, Julieanne Kost, Samantha Wallace, Shawn Cheris, Darrell Klotzbach

Click here for legal notices.

© 1990-2010 Adobe Systems Incorporated. All rights reserved.

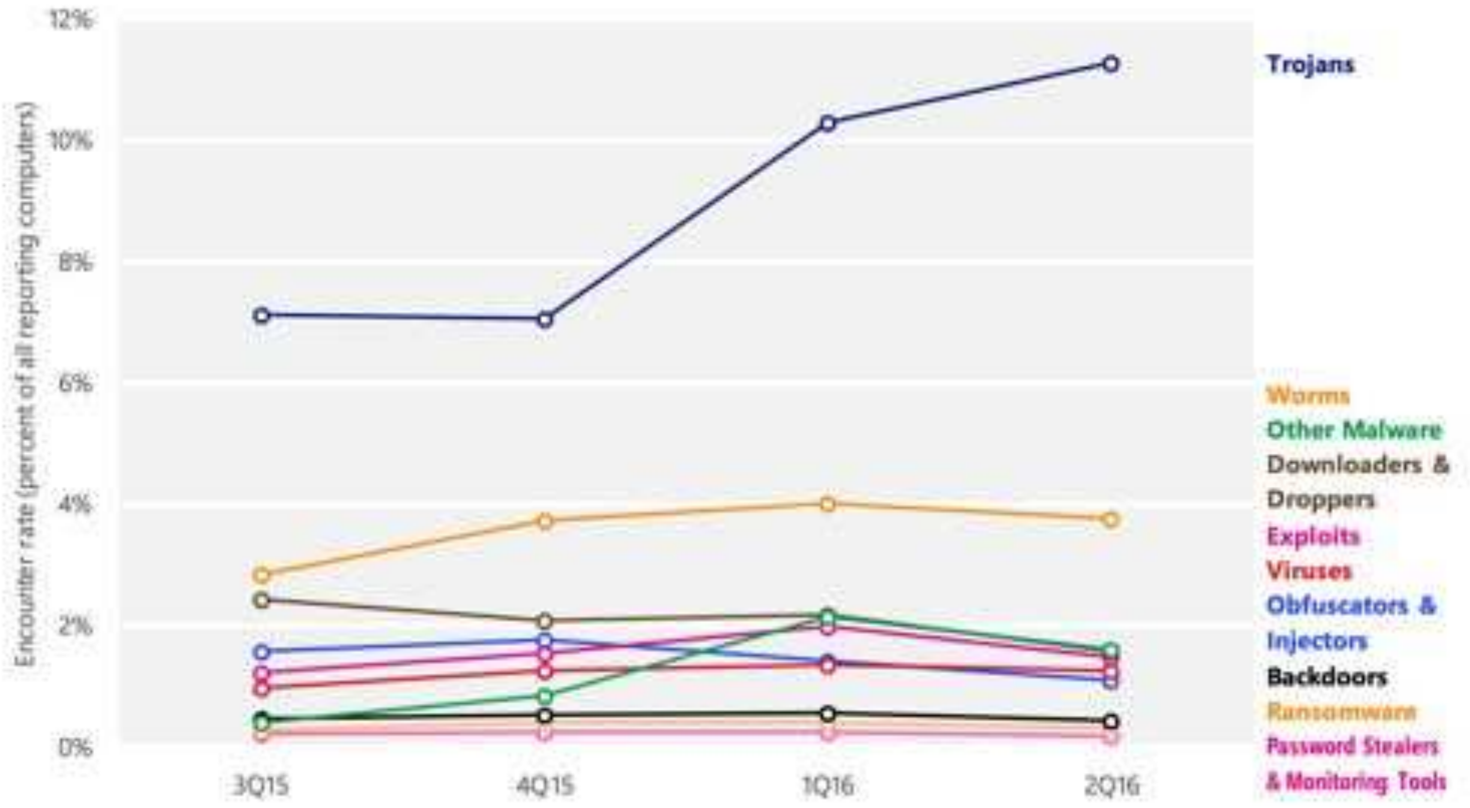
How does malware manage to run?

- Buffer overflow in network-accessible vulnerable service
- Vulnerable client (e.g. browser) connects to remote system that sends over an attack (a driveby)
- Social engineering: trick user into running/installing
- “Autorun” functionality (esp. from plugging in USB device)
- Slipped into a system component (at manufacture; compromise of software provider; substituted via MITM)
- Attacker with local access downloads/runs it directly
  - Might include using a “local root” exploit for privileged access

Insider Attacks

- An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.
- In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.

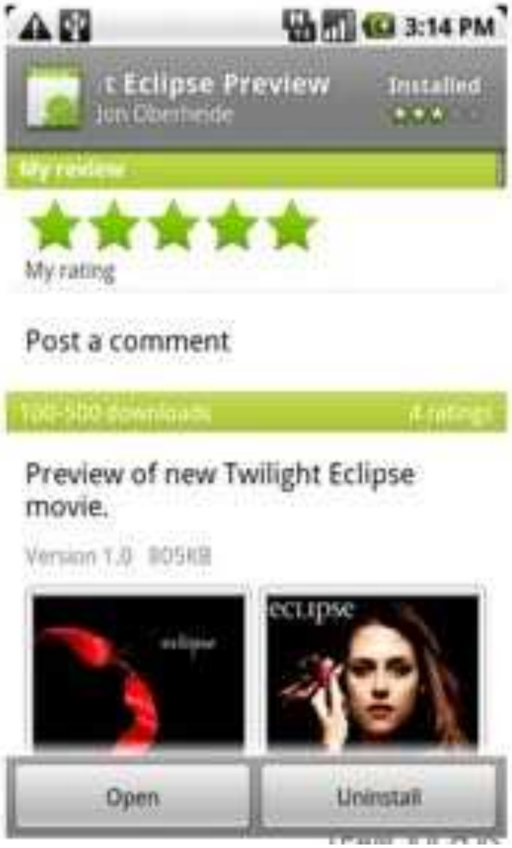
Encounter rates for significant malicious software categories, 3Q15–2Q16



Trojan horse

- Software that appears to perform a desirable function but is actually designed to perform undisclosed malicious functions
  - Spyware: installed by legitimate looking programs, then provides remote access to the computer, such as logging keys or sending back documents
  - Adware: shows popup ads
  - Ransomware: encrypts data and requires payment to decrypt

Android Example



3:14 PM

t Eclipse Preview

Jon Oberheide

Installed

My review

★★★★★

My rating

Post a comment

100-500 downloads

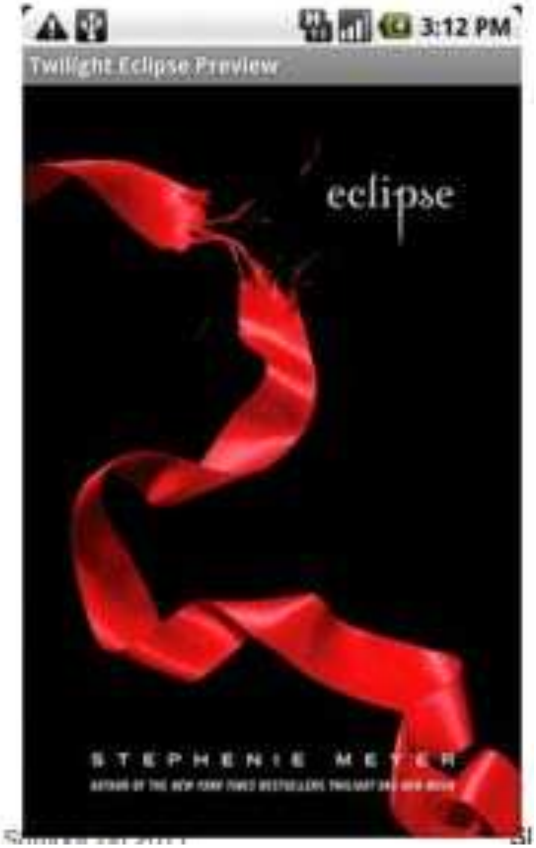
4 ratings

Preview of new Twilight Eclipse movie.

Version 1.0 805KB

Open

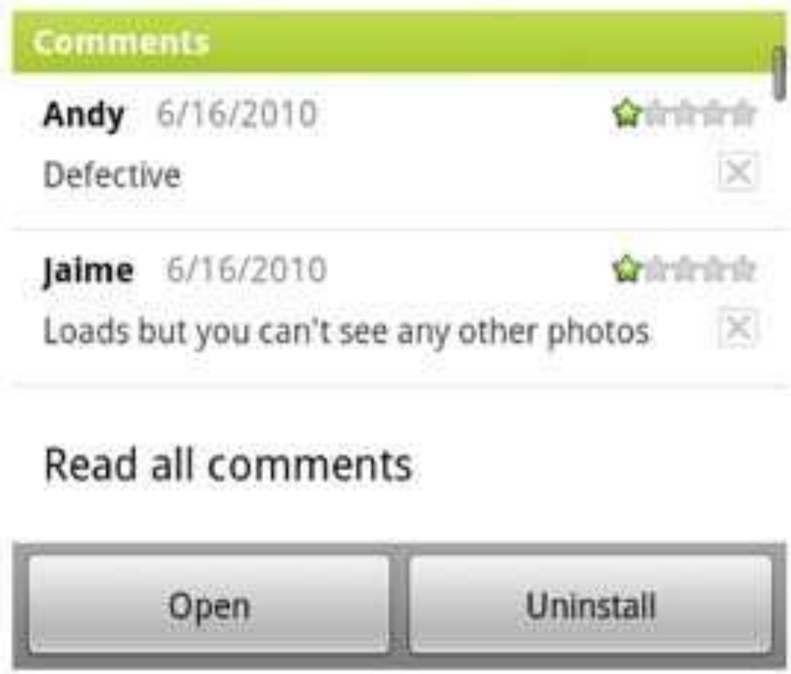
Uninstall



3:12 PM

Twilight Eclipse Preview

Example (cont.)



Comments

Andy 6/16/2010

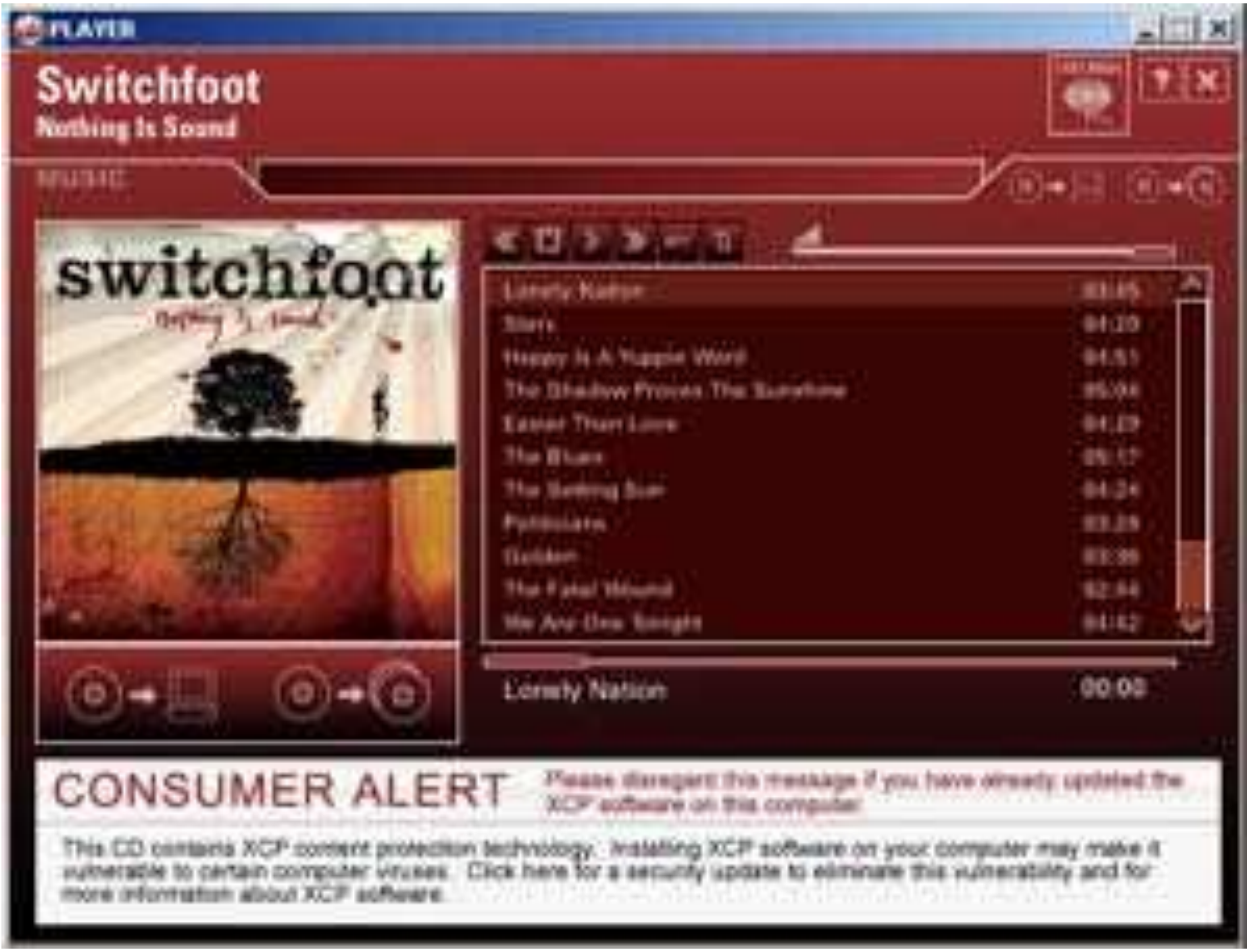
Defective

Jaime 6/16/2010

Loads but you can't see any other photos

Read all comments

- Still, 200+ downloads in under 24 hours
- With a legit-looking app/game, you could collect quite an install base for RootStrap



Switchfoot
Nothing Is Sound

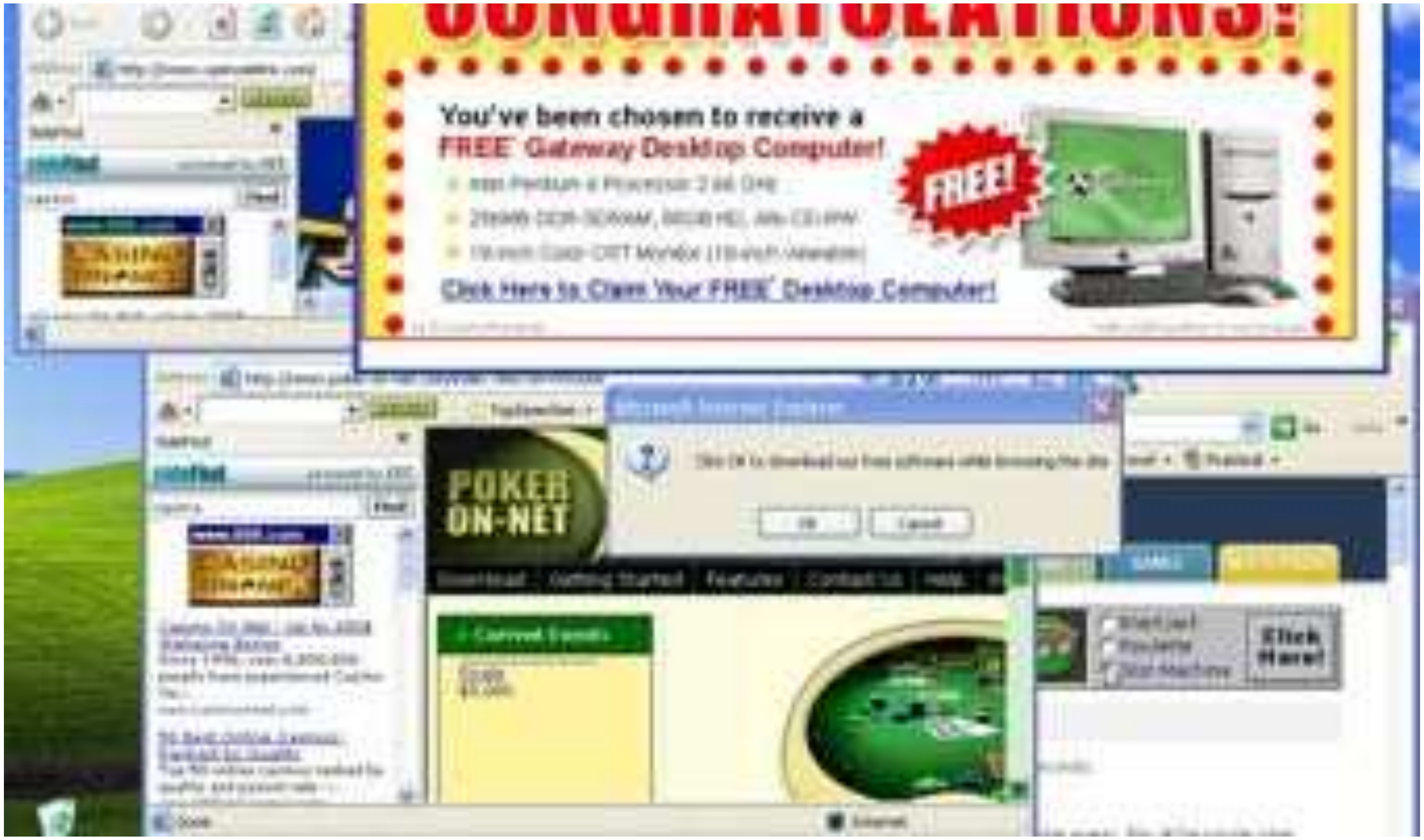
Lonely Nation	03:45
Stars	04:20
Happy Is A Yuppie Word	04:51
The Shadow Proves The Sunshine	05:04
Easier Than Love	04:29
The Blues	05:17
The Setting Sun	04:24
Politicians	03:29
Golden	03:39
The Fatal Wound	02:44
We Are One Tonight	04:42

Lonely Nation 00:00

CONSUMER ALERT Please disregard this message if you have already updated the XCP software on this computer.

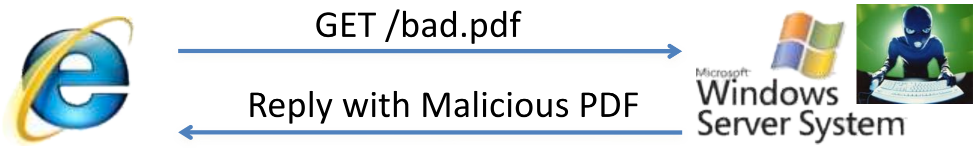
This CD contains XCP content protection technology. Installing XCP software on your computer may make it vulnerable to certain computer viruses. Click here for a security update to eliminate this vulnerability and for more information about XCP software.

Adware


CONGRATULATIONS!
You've been chosen to receive a
FREE* Gateway Desktop Computer!
FREE!
Click Here to Claim Your FREE* Desktop Computer!
POKER ON-NET
Download
Getting Started
Features
Contact Us
Help
Current Events
OK
Cancel
Click Here!

Code Injection Exploits

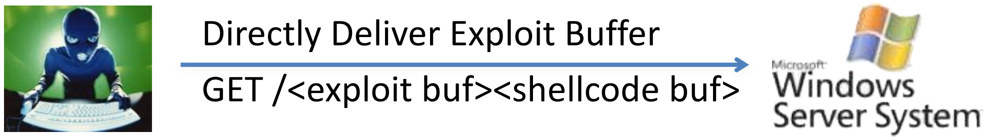
- Client software exploit (e.g. PDF, Flash, MSWord, etc.)



GET /bad.pdf

Reply with Malicious PDF

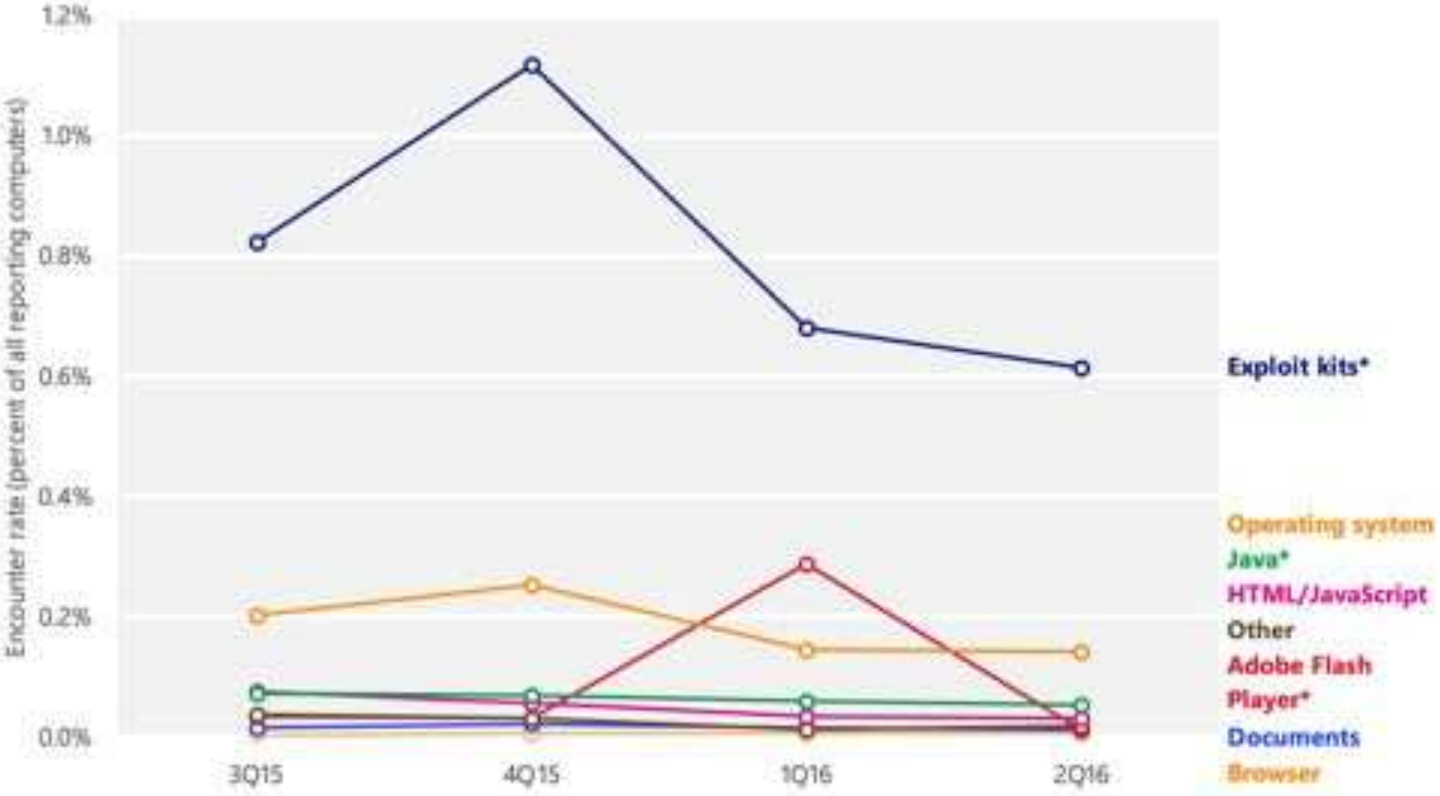
- Network-based exploit (HTTP, File, RPC servers, etc.)



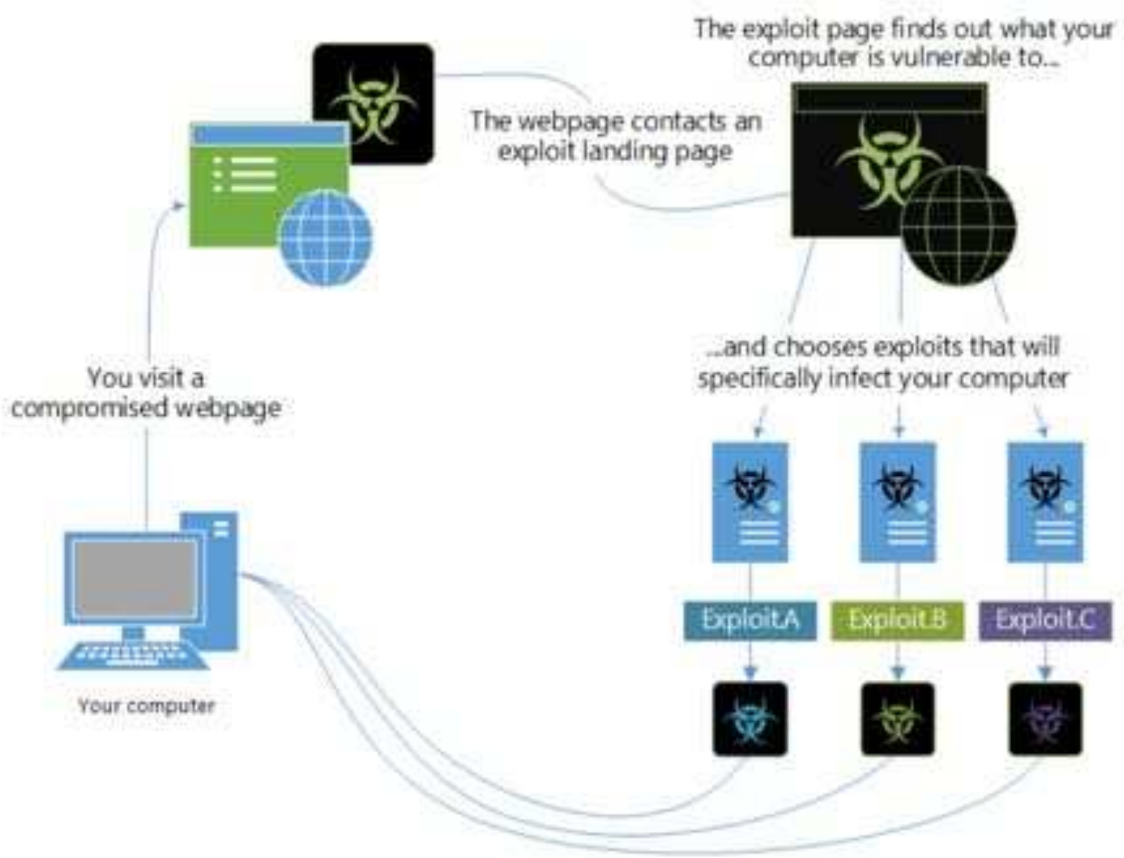
Directly Deliver Exploit Buffer

GET /<exploit buf><shellcode buf>

Encounter rates for different types of exploit attempts on the Internet, 3Q15–2Q16



How a typical exploit kit works


The exploit page finds out what your computer is vulnerable to...
The webpage contacts an exploit landing page
You visit a compromised webpage
...and chooses exploits that will specifically infect your computer
Exploit.A
Exploit.B
Exploit.C
Your computer

Malware That Automatically Propagates

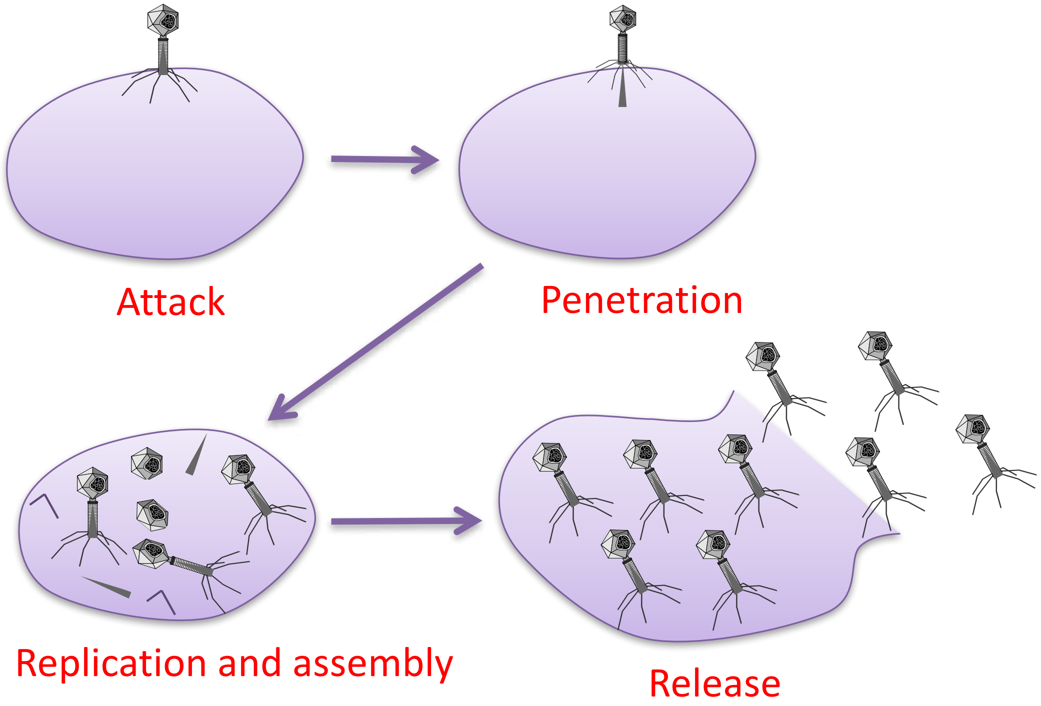
- Virus = code that propagates (**replicates**) across systems by arranging to have itself *eventually executed,* creating additional, new instances of itself
  - Generally infects by altering stored code
  - Typically with the help of a user
- Worm = code that self-propagates/replicates across systems by arranging to have itself *immediately executed,* creating additional, new instances of itself
  - Generally infects by altering running code
  - No user intervention required
- (Note: line between these isn't always so crisp; plus some malware incorporates both styles)

Computer Viruses

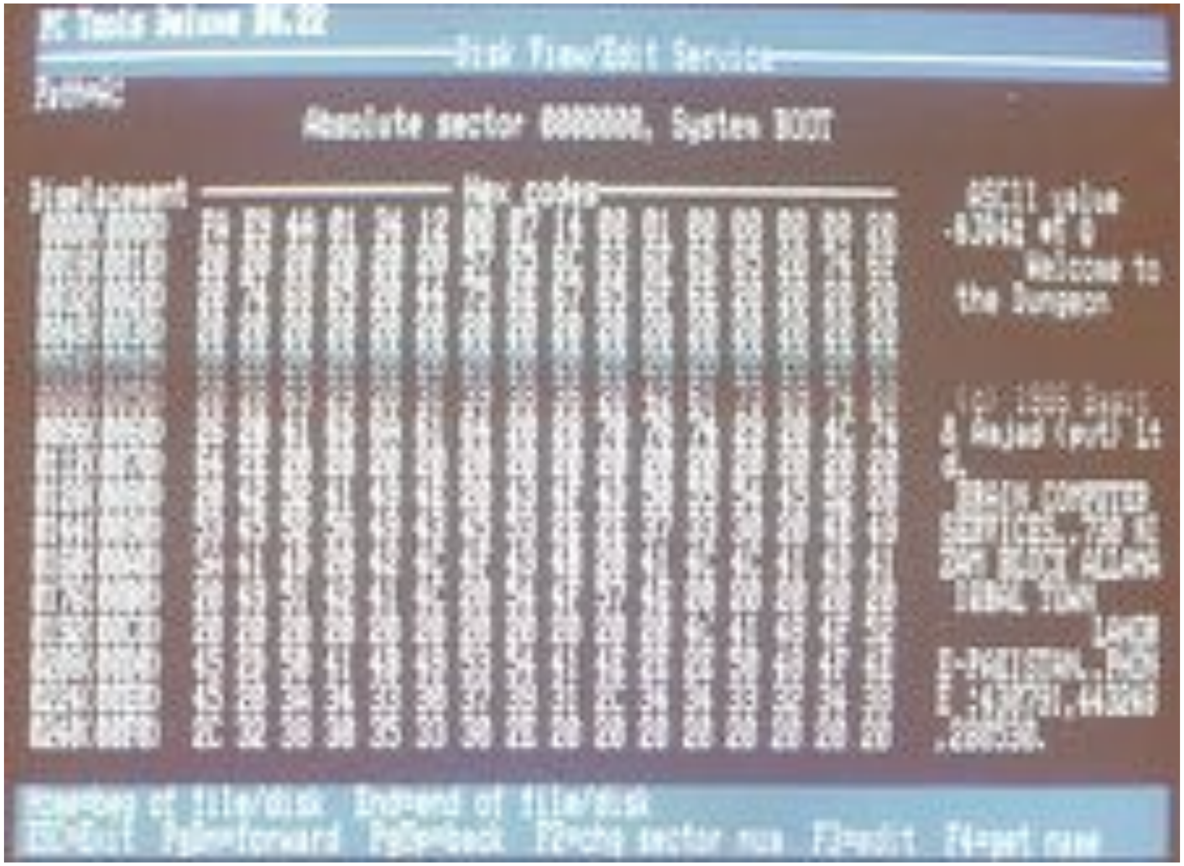
- A **computer virus** is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication.
- This self-replication property is what distinguishes computer viruses from other kinds of malware, such as logic bombs.
- Another distinguishing property of a virus is that replication requires some type of **user assistance,** such as clicking on an email attachment or sharing a USB drive.

Biological Analogy

- Computer viruses share some properties with Biological viruses



Brain



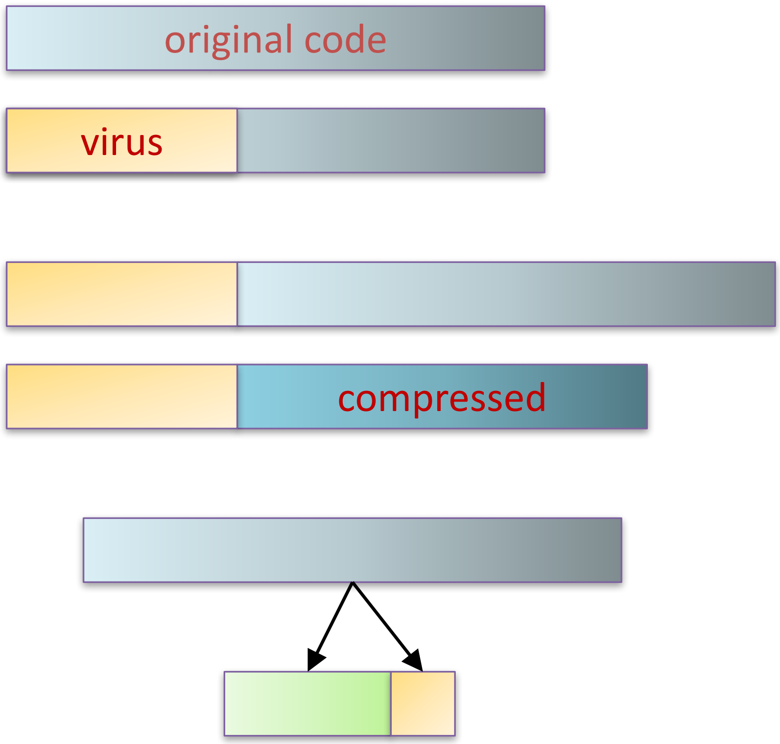
```
PC Tools Deluxe R4.22
                         Disk View/Edit Service
Path=A:\
              Absolute sector 0000000, System BOOT

Displacement  ————————— Hex codes ——————————————    ASCII value
[illegible]                                          .4J4 ...
                                                         Welcome to
                                                     the Dungeon

                                                     (c) 1986 Basit
                                                     & Amjad (pvt) Lt
                                                     d.
                                                      BRAIN COMPUTER
                                                     SERVICES..730 N
                                                     IZAM BLOCK ALLAMA
                                                      IQBAL TOWN
                                                                 LAHOR
                                                     E-PAKISTAN..PHON
                                                     E :430791,443248
                                                     ,280530.

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Virus Phases

- **Dormant phase.** During this phase, the virus just exists—the virus is laying low and avoiding detection.
- **Propagation phase.** During this phase, the virus is replicating itself, infecting new files on new systems.
- **Triggering phase.** In this phase, some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
- **Action phase.** In this phase, the virus performs the malicious action that it was designed to perform, called its **payload.**
  - This action could include something seemingly innocent, like displaying a silly picture on a computer’s screen, or something quite malicious, such as deleting all essential files on the hard drive.

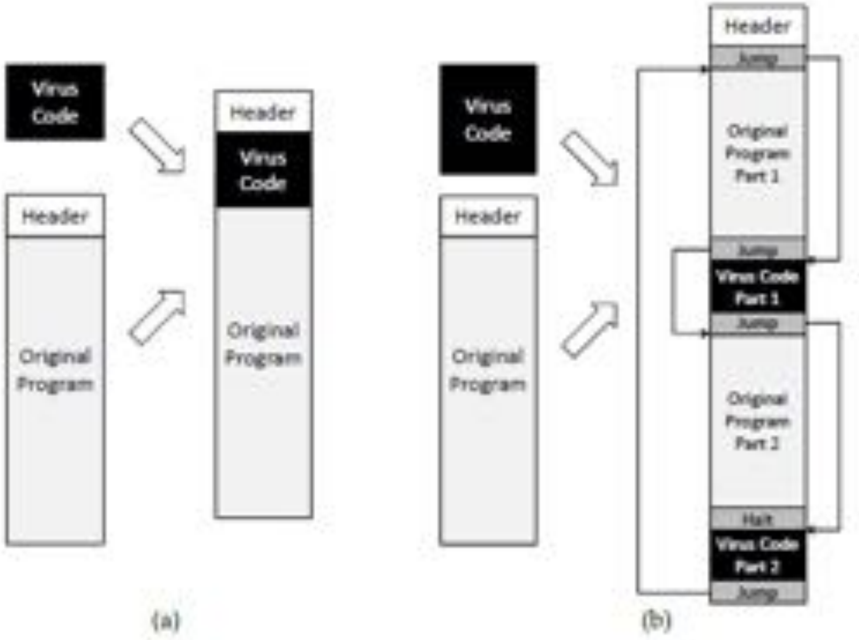
Infection Types

- Overwriting
  - Destroys original code
- Pre-pending
  - Keeps original code, possibly compressed
- Infection of libraries
  - Allows virus to be memory resident
  - E.g., kernel32.dll
- Macro viruses
  - Infects MS Office documents
  - Often installs in main document template
  - LaTeX typesetting system viruses



Degrees of Complication

- Viruses have various degrees of complication in how they can insert themselves in computer code.



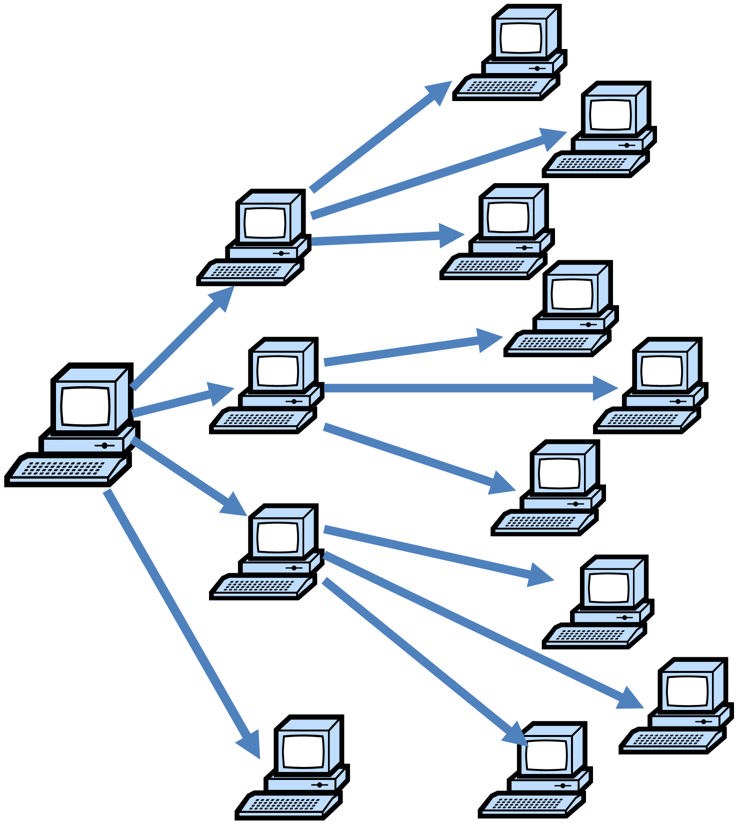
Worm

- Worm = code that self-propagates/replicates across systems by arranging to have itself immediately executed
  - Generally infects machines by altering running code
  - No user intervention required

Rapid Propagation

Worms can potentially spread quickly because they parallelize the process of propagating/ replicating.

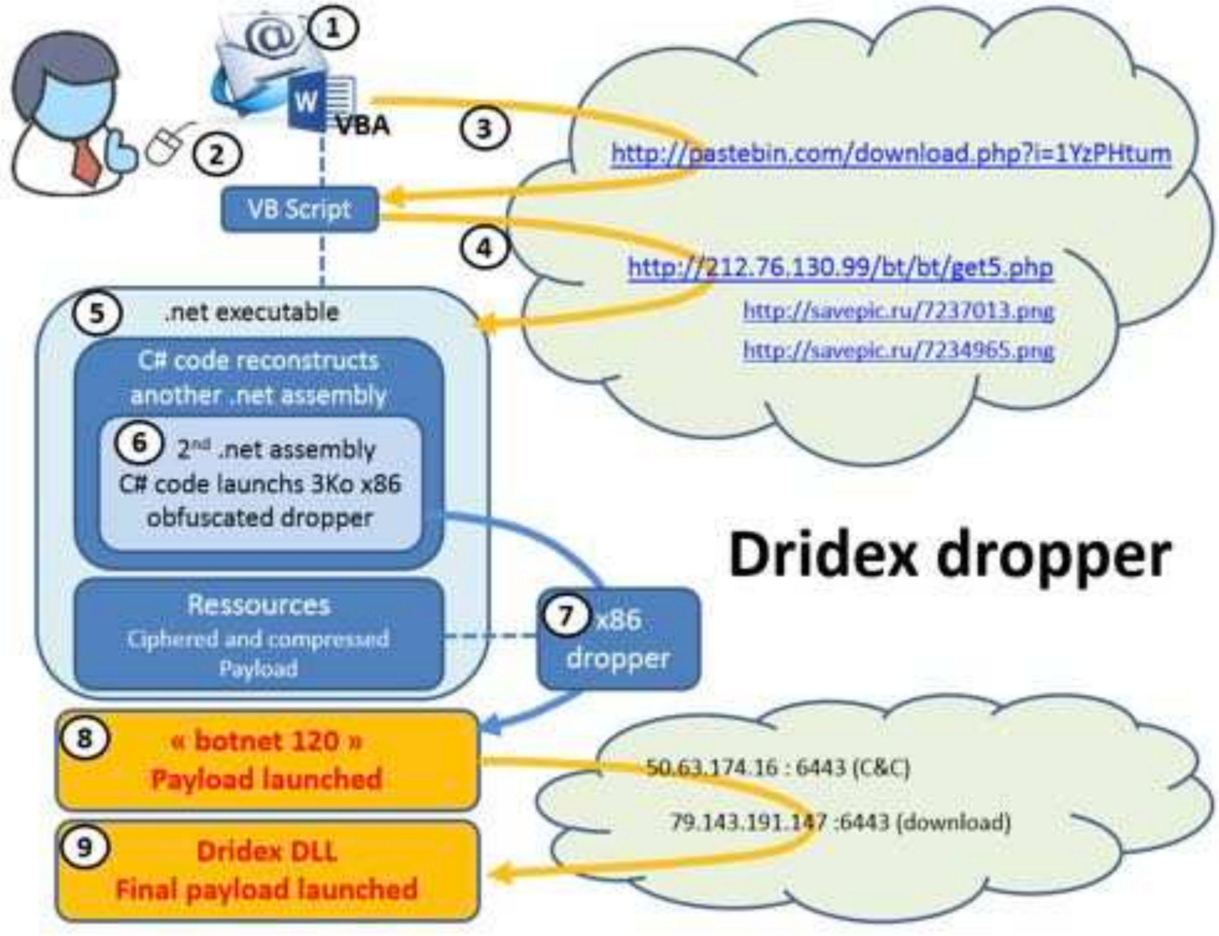
Same holds for viruses, but they often spread more slowly since they require some sort of user action to trigger each propagation.



The Arrival of Internet Worms

- Worms date to Nov 2, 1988 - the *Morris Worm*
- ***Way*** ahead of its time
- Employed a whole suite of tricks to infect systems …
  - *Multiple* buffer overflows (“gets” function in finger server)
  - Guessable passwords
  - “Debug” configuration option in sendmail that provided shell access
  - Common user accounts across multiple machines
- … and of tricks to find victims
  - Scan local subnet
  - Machines listed in system’s network config, e.g., /etc/hosts.equiv, /.rhosts
  - Look through user files for mention of remote hosts, e.g., .forward, .rhosts

Droppers


1
VBA
2
3
http://pastebin.com/download.php?i=1YzPHtum
VB Script
4
http://212.76.130.99/bt/bt/get5.php
http://savepic.ru/7237013.png
http://savepic.ru/7234965.png
5 .net executable
C# code reconstructs another .net assembly
6 2nd .net assembly C# code launchs 3Ko x86 obfuscated dropper
Ressources
Ciphered and compressed Payload
7 x86 dropper
Dridex dropper
8 « botnet 120 » Payload launched
50.63.174.16 : 6443 (C&C)
79.143.191.147 :6443 (download)
9 Dridex DLL Final payload launched

Bridging the how and what of malware: Botnets

- Collection of compromised machines (bots) under (unified) control of an attacker (botmaster)
- Method of compromise decoupled from method of control
  - Launch a worm / virus / drive-by infection / etc.
- Upon infection, new bot "*phones home*" to rendezvous w/ botnet *command-and-control* (**C&C**)
- Lots of ways to architect C&C:
  - Star topology; hierarchical; peer-to-peer
  - Encrypted/stealthy communication
- Botmaster uses C&C to push out commands and updates

Example of C&C Messages

1. Activation (report from bot to botmaster)
2. Email address harvests
3. Spamming instructions
4. Delivery reports
5. DDoS instructions
6. *FastFlux* instructions (rapidly changing DNS)
7. HTTP proxy instructions
8. Sniffed passwords report
9. IFRAME injection/report

From the “Storm” botnet circa 2008