

Lecture 17 – Malware

Stephen Checkoway

Oberlin College

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

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*)**
 - Coruna iOS exploit kit (2026) steals financial information, cryptocurrency
 - 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, passw0rd, nintendo, athur
cocacola, ilovegod, football1, emmanuel, danielle, bill
http://77.81.229.38/p/gate.php, YUIPWDFILEDYUIPKDFILEDY
CryptAcquireCertificatePrivateKey, MsiGetComponentPathA
;q=0, Content-Length: %lu, Content-Encoding: binary, U
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 Profession
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\ExpandDrive\Sessions, \ExpandDrive,
_Password, Software\NCH Software\ClassicFTP\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 F
_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, \Googl
\Bromium, \Nichrome, \RockMelt, K-Meleon, \K-Meleon, \E
site.dat, LastPassword, LastAddress, LastUser, LastPort
FTP++.Link\shell\open\command, Connections.txt, sites.i
full address:s:, .TERMSRV/, sites.xml, SOFTWARE\Robo-FT
InitialDirectory, ServerType, Software\LinusFTP\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, \INSSoftware\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\RLI\The Bat!, WORKING Directory, ProgramDir, SMTP Email Address, SMTP
Server, SMTP User Name, NNTP Email Address, NNTP User Name, IMAP 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, YCreateTooThep32Snapshot, 'CoTaskMemFree,
yInternetCrackUrIA, {InternetCreateUrIA, 6inet_addr, *gethostbyname, 'connect, &closesocket, Gsetsockopt, IWSASStartup,
aUnloadUserProfile

Logged Passwords List

Title: MSN Messenger
Time: Wednesday, 07-30-2003 17:47:06
UserName: William_21492@hotmail.com Password: pass21492

Title: Yahoo! Messenger
Time: Wednesday, 07-30-2003 17:48:02
UserName: jerry83 Password: malibuca

Title: Yahoo! Mail - The best free web-based email! - Microsoft Internet Explorer
Time: Wednesday, 07-30-2003 17:53:
keystrokes:
jerry83
malibuca
yes you are right, hope you consider

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

Remote Password Stealer 2.7 Full

 [Passwords Stealer](#)

Typed: <trl>+8 <alt>+<ctrl>+8

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



- 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 next month 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, eats 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*

Siemens logic bomb

- David Tinley, a Siemens contractor inserted logic bombs which caused malfunctions after certain dates
- Siemens was paying Tinley to fix the issues he had caused
- Eventually, he was caught and pleaded guilty

Ransomware

Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost
without payment on:

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.

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/P9UUR3>
<http://petya5koahsf7sv.onion/P9UUR3>

3. Enter your personal decryption code there:

cdSPP4-JUZrRr-pMSxia-gXpmfB-vGworf-FfMph1-XTUzUn-QmFeeU-ofb94y-HuScaa-rB1gmU-djYAEH-8WEakz-wrQ85W-BbsCzw

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

Key: 8x3qrMHjmkRN9jfd
Decrypting sector 83234 of 126464 (65%)

University of Mississippi Medical Center

Feb, 2026 ransomware takes down University of Mississippi Medical Center

Ransomware targeting hospitals is on the rise

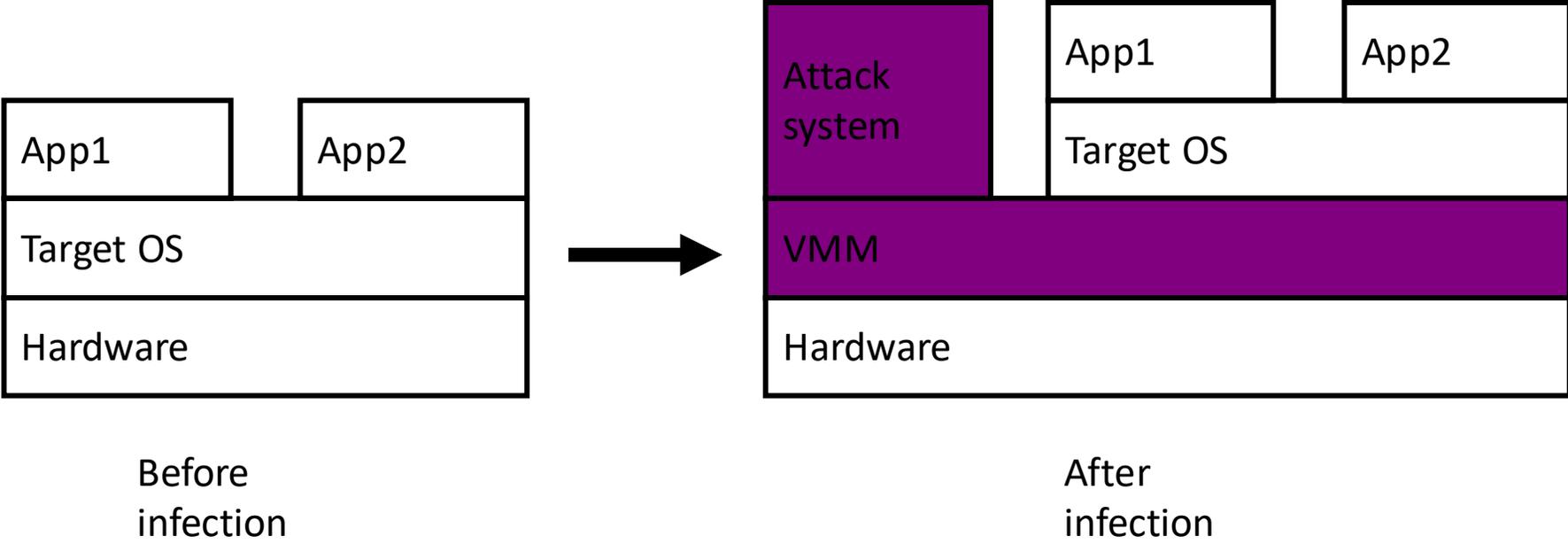


Eric Shelton/Mississippi Today

Rootkits

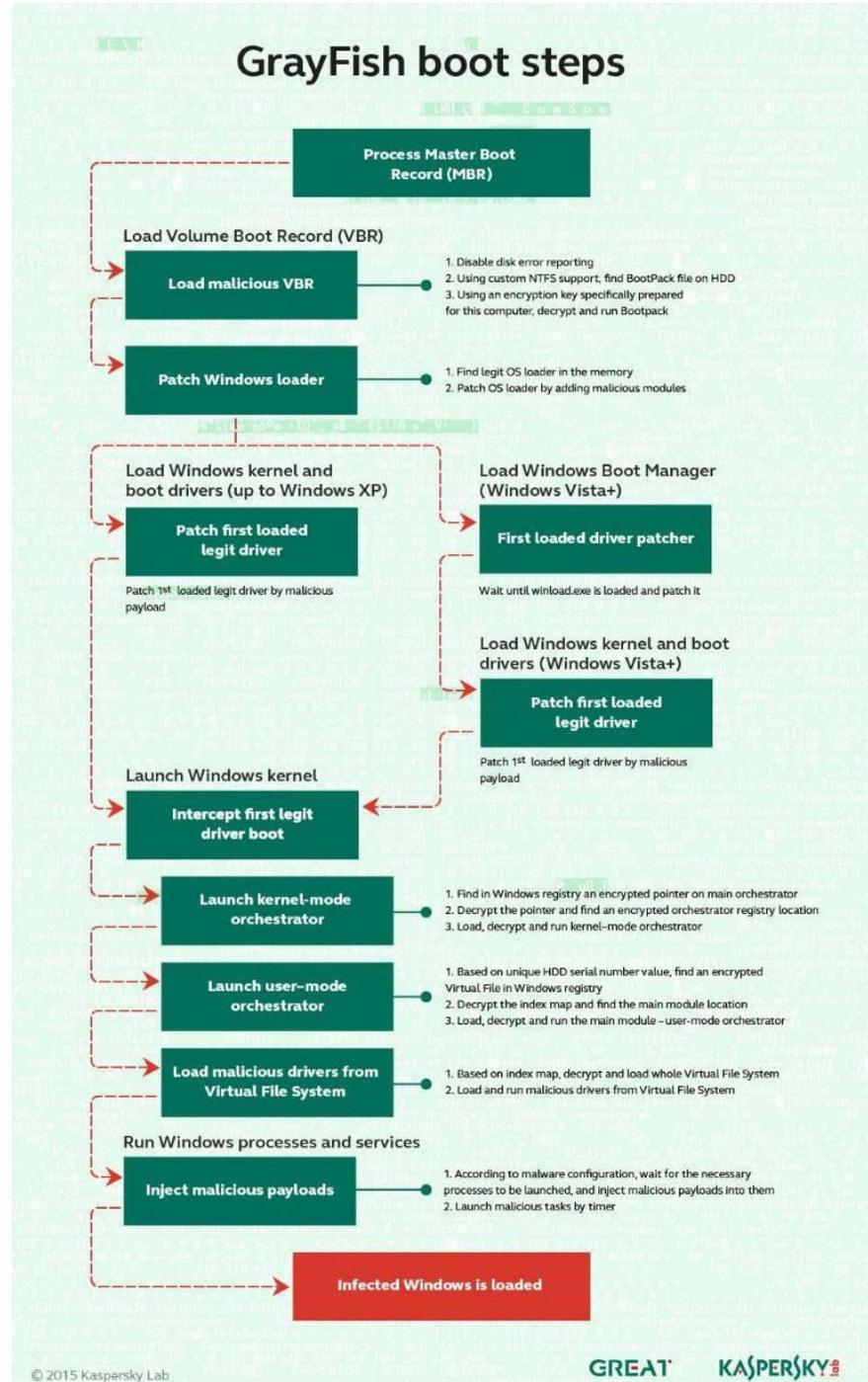
- A rootkit modifies the operating system to hide its existence
 - E.g., modifies file system exploration utilities
 - Hard to detect using software that relies on the OS itself
- Operation:
 - Intercept system calls for listing files, processes, etc.
 - Filter out malware's files and processes
 - Example: 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)





- Probably NSA malware
- Infects MBR on hard drive
- Patches Windows at boot
- Injects code into specific processes



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

Juniper ScreenOS Backdoor

```
ROM:0013DC4C STR R12, [SP,#0x30+var_24]
ROM:0013DC50 LDR R0, =aScTUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC54 LDR R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC58 BL sub_558F74
ROM:0013DC5C ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC5C loc_13DC5C ADD R0, R5, #0x44
ROM:0013DC60 LDR R1, =aSunSU ; "<<<< %s(un='%s') = %u"
ROM:0013DC64 BL strcmp
ROM:0013DC68 CMP R0, #0
ROM:0013DC6C BNE loc_13DC78
ROM:0013DC70 MOV R0, #0xFFFFFFFF
ROM:0013DC74 LDMDB R11, {R4-R8,R11,SP,PC}
ROM:0013DC78
```

```
ROM:0013DC44 STR R12, [SP,#0x30+var_24]
ROM:0013DC48 LDR R0, =aScTUUnSSipSDip ; ">>> %s(ct=%u, un='%s',
ROM:0013DC4C LDR R1, =aAuth_admin_int ; "auth_admin_internal"
ROM:0013DC50 BL sub_558810
ROM:0013DC54 ; CODE XREF: auth_admin_internal+2C↑j
ROM:0013DC54 loc_13DC54 ADD R0, R5, #0x6C
ROM:0013DC58 BL sub_147224
ROM:0013DC5C MOVUS R0, R0,LSL#16
ROM:0013DC60 MOVNE R7, #1
ROM:0013DC64 BNE loc_13DD08
ROM:0013DC68 LDRH R12, [R5,#0x68]
ROM:0013DC6C ADD R12, R12, #0xFF00
ROM:0013DC70 AND R12, R12, #0xFF
```

- Dec. 2015 Juniper issued an advisory that unauthorized code had been introduced into some of their firewall devices
- One of the pieces of code is a backdoor with a hard coded password: "<<<< %s(un='%s') = %u"
- Designed to look like a printf format string
- On the left, the modified disassembled firmware is passing that string to strcmp
- (There was a separate backdoor involving random number generators which was more complicated to exploit)

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.

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



CrashFix (2026)

- Fake ad blocker impersonates uBlock Origin Lite
- Displays a fake security warning
- Tricks users into running PowerShell commands
- Installs a remote access trojan



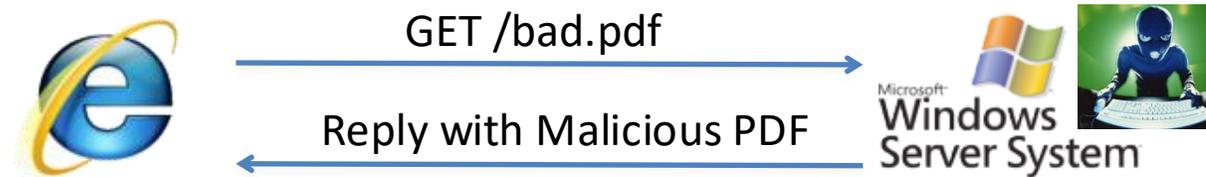
Adware

The image shows a screenshot of a web browser with several elements:

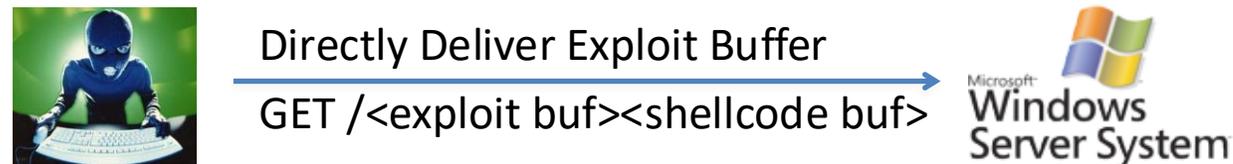
- Browser Address Bar:** Shows the URL `http://www.casinonet.com/`.
- Search Bar:** Labeled "SideFind powered by IST" with the search term "casino".
- Search Results:** A result for "www.888.com" with a "CASINO ON NET" logo and a "Click" button.
- Pop-up Advertisement:** A large yellow and red banner with the text "CONGRATULATIONS!" and "You've been chosen to receive a FREE Gateway Desktop Computer!". It lists specifications: Intel Pentium 4 Processor 2.66 GHz, 256MB DDR-SDRAM, 80GB HD, 48x CD-RW, and a 19-inch Color CRT Monitor. A "FREE!" starburst is next to the computer image. A link says "Click Here to Claim Your FREE Desktop Computer!".
- Microsoft Internet Explorer Dialog Box:** A small window with a question mark icon and the text "Click OK to download our free software while browsing the site". It has "OK" and "Cancel" buttons.
- Background Page:** A page for "POKER ON-NET" with a navigation menu (Download, Getting Started, Features, Contact Us, Help) and a "Current Events" section listing a "Finale \$5,000".

Code Injection Exploits

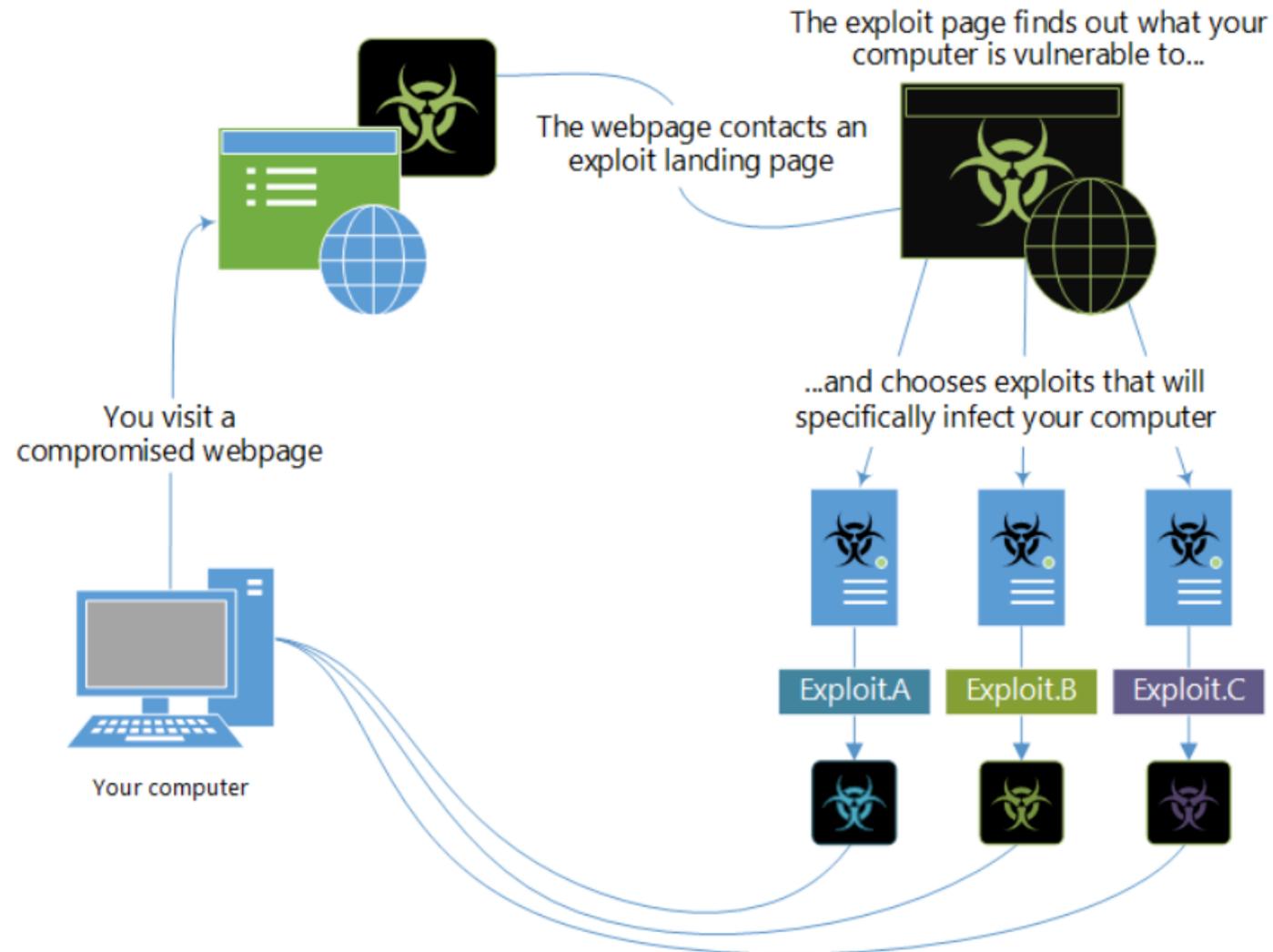
- Client software exploit (e.g. PDF, Flash, MSWord, etc.)



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



How a typical exploit kit works



Coruna iOS Exploit Kit (2026)

- JavaScript framework identifies model of iPhone and version of iOS
- Based on that, loads a WebKit remote code execution exploit
- Bypasses pointer authentication code mitigations designed to stop ROP and other control-flow hijacking attacks
- Chain of exploits ends with payload that steals financial information and can download and run additional code

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.

First PC virus: Brain

```
PC Tools Deluxe V4.22
Disk View/Edit Service
Path=A:
Absolute sector 0000000, System BOOT

Displacement Hex codes ASCII value
0000(0000) FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20 .9J04t 0f 0
0016(0010) 20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F Welcome to
0032(0020) 20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20 the Dungeon
0048(0030) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0064(0040) 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0080(0050) 20 20 63 23 20 31 39 38 36 20 42 61 73 69 74 20
0096(0060) 26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74 (c) 1986 Basit
0112(0070) 64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20 & Amjad (pvt) Lt
0128(0080) 20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20 d.
0144(0090) 53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49 BRAIN COMPUTER
0160(00A0) 5A 41 4D 20 42 4C 4F 43 48 20 41 4C 4C 41 4D 41 SERVICES..730 NI
0176(00B0) 20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20 ZAM BLOCI ALLAMA
0192(00C0) 20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52 IQBAL TOWN
0208(00D0) 45 2D 50 41 48 49 53 54 41 4E 2E 2E 50 48 4F 4E LAHOB
0224(00E0) 45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38 E-PAKISTAN..PHON
0240(00F0) 2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20 E :430791,443248
,280530.

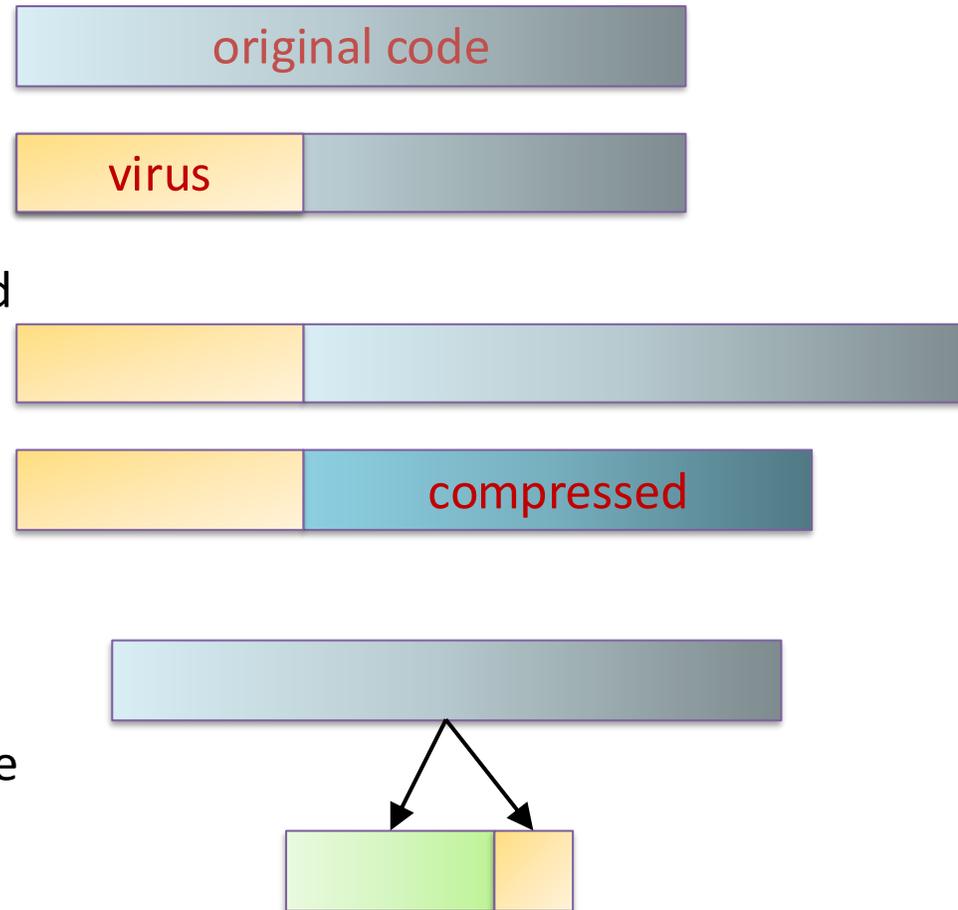
Home=begin of file/disk End=end of file/disk
ESC=Exit PgDn=forward PgUp=back F2=chg sector num F3=edit F4=get name
```

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.

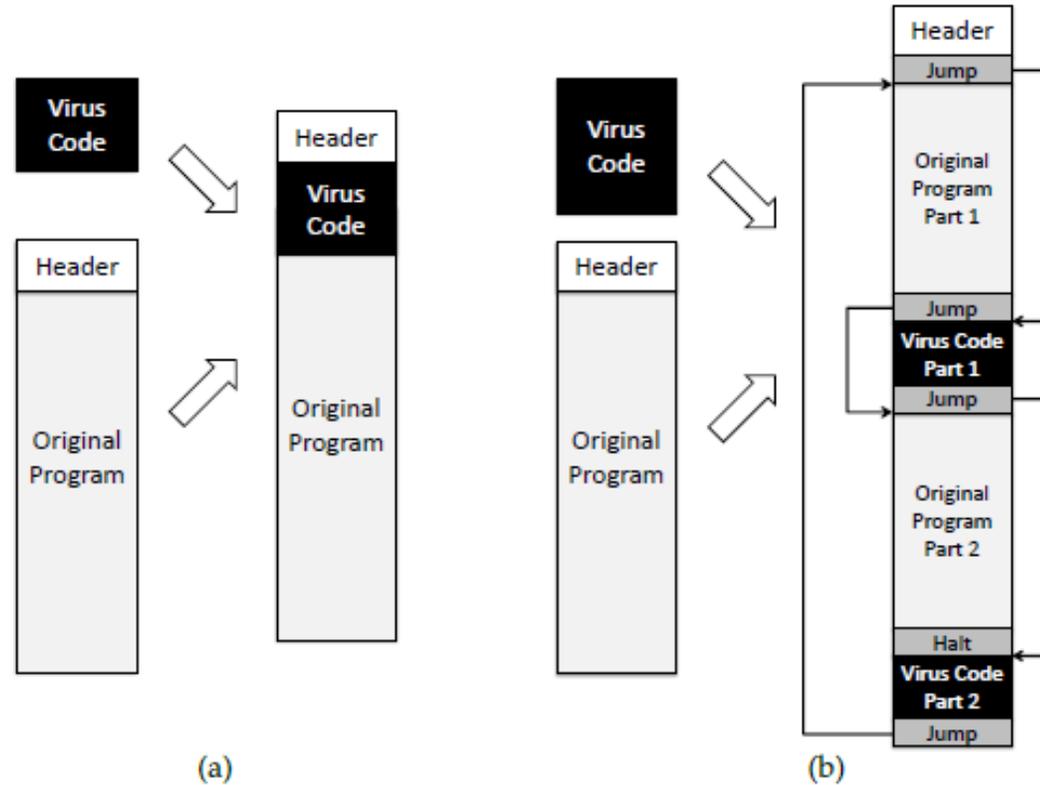
Infection Types

- 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.

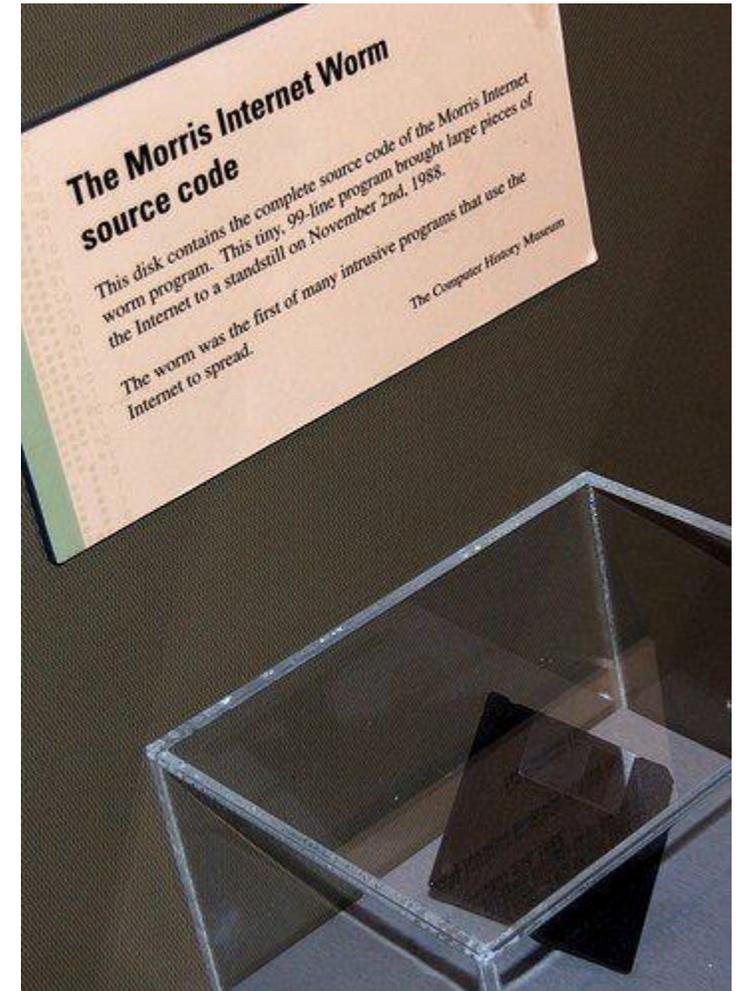


Worm

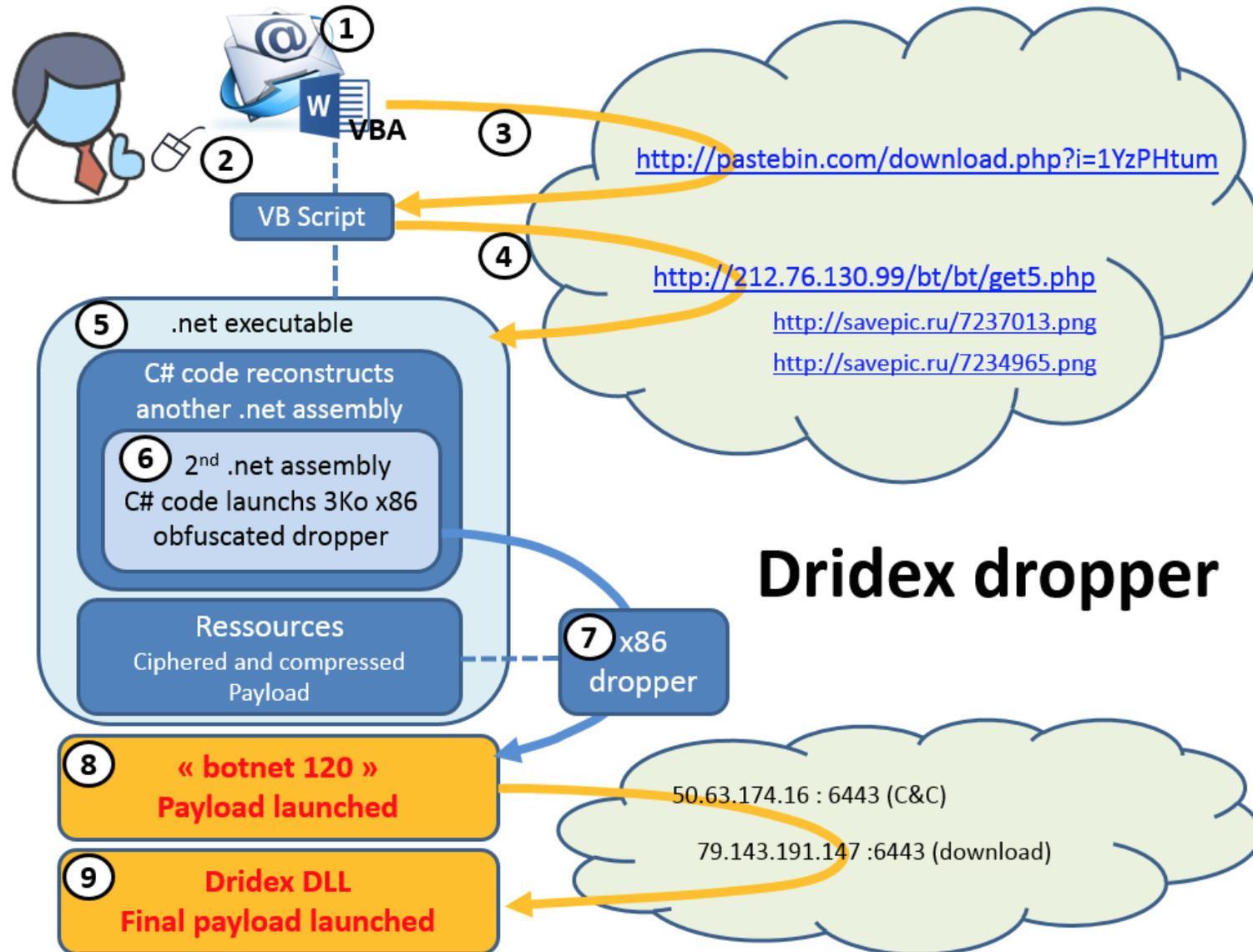
- Worm = code that self-propagates/replicates across systems by arranging to have itself immediately executed
 - Generally infects machines by altering running code
 - No user intervention required

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



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 or C2)*
- 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