Lecture 14 –Malware Part 1

Ryan Cunningham

University of Illinois

ECE 422/CS 461 – Fall 2017

Announcement

- Midterm moved:
  - Monday, Oct. 16th 7-9pm
  - ECEB 1002 (here)

Security News

- SEC breached, leaked preliminary filing data
- Sonic breached, leaked cc data
- Whole Foods breached, leaked cc data
- “Illusion Gap” bypass for Windows Defender
- DEA arrests French national Gal Vallerius

Malware

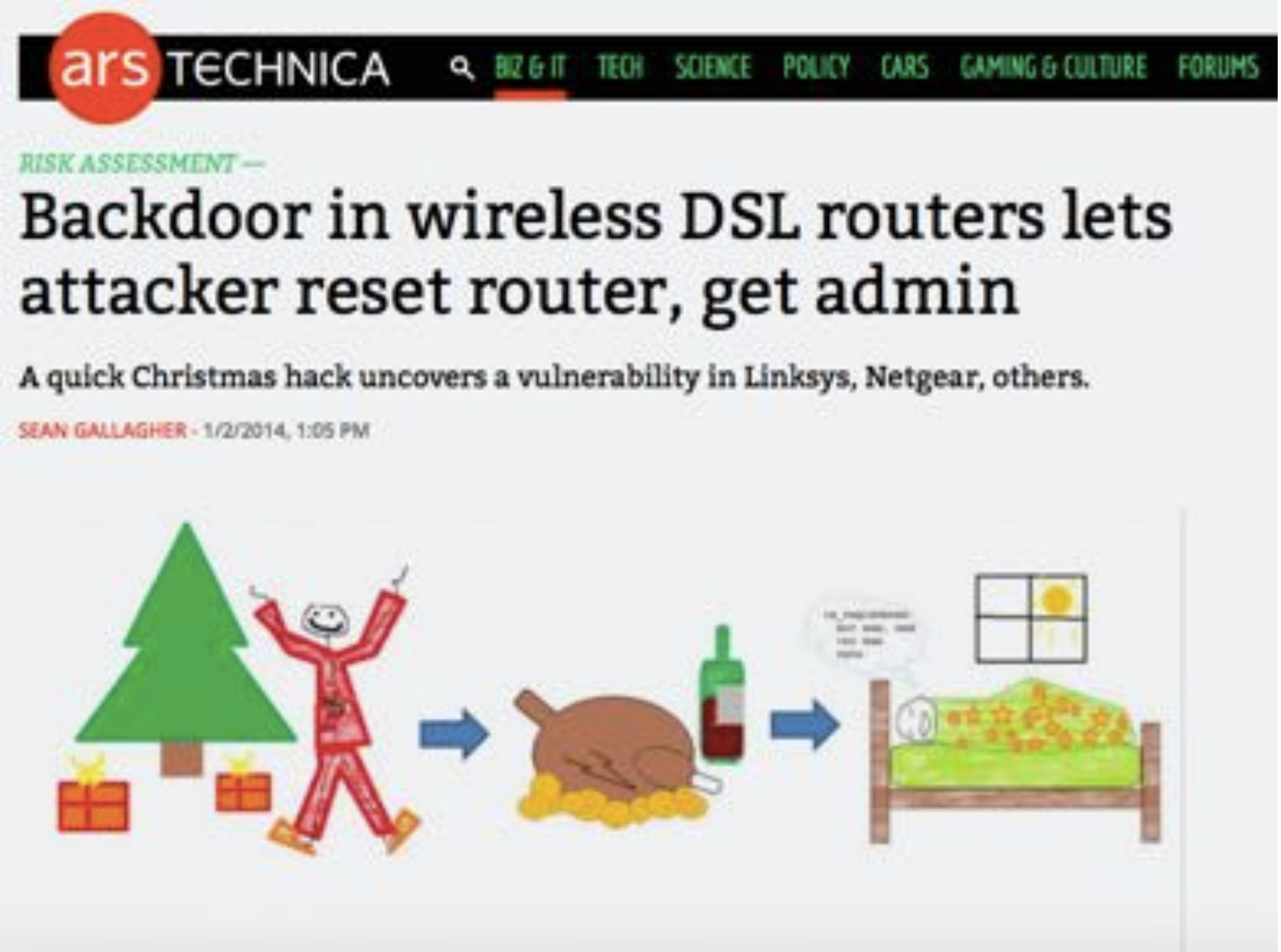
- We understand principles of software exploitation
- Time to learn what can be done with them
- malware - *a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim*
- Classified mostly by:
  - propagation method
  - payload type

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.

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.
- Benign example: **Easter Eggs** in DVDs and software



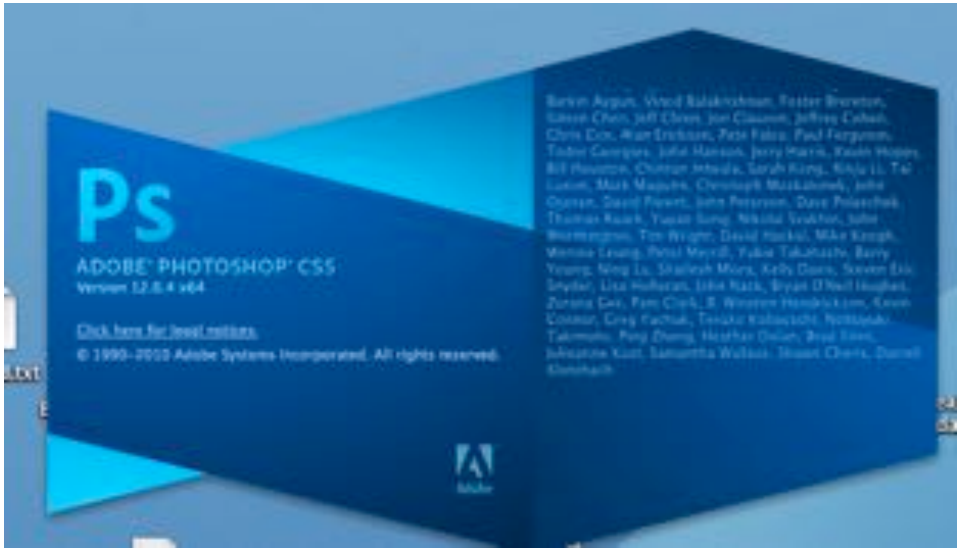
RISK ASSESSMENT —

Backdoor in wireless DSL routers lets attacker reset router, get admin

A quick Christmas hack uncovers a vulnerability in Linksys, Netgear, others.

SEAN GALLAGHER - 1/2/2014, 1:05 PM

Easter Eggs



Ps

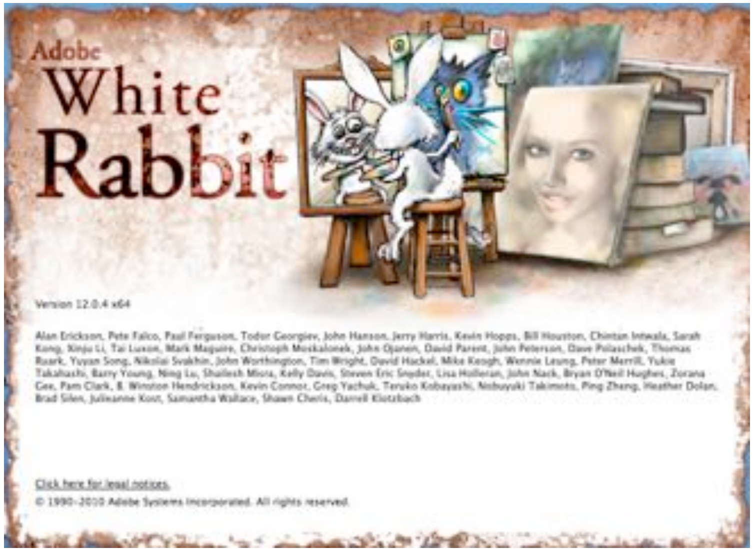
ADOBE® PHOTOSHOP® CS5

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, Teruko Kobayashi, Nobuyuki Takimoto, Ping Zheng, 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, Teruko Kobayashi, Nobuyuki Takimoto, Ping Zheng, 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.

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

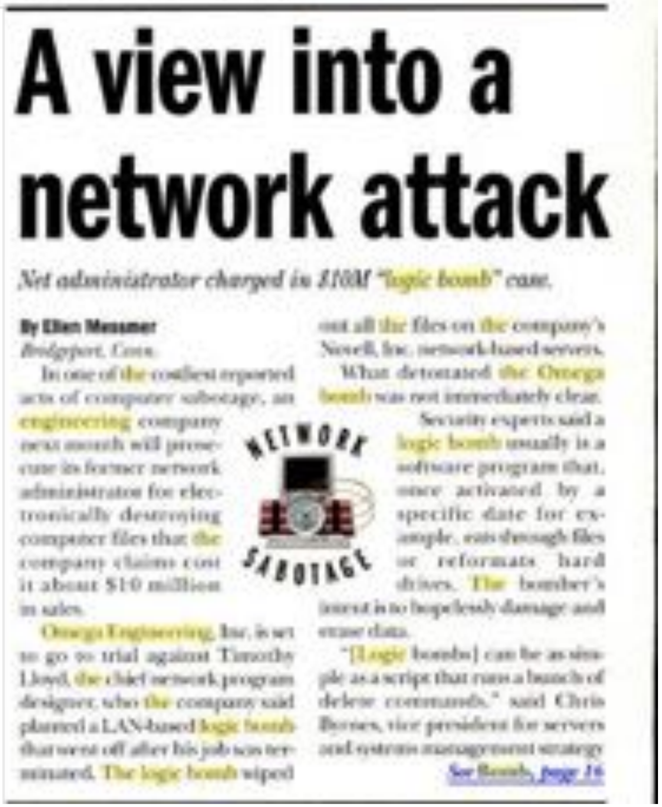
NetworkWorld

THE NEWSWEEKLY OF ENTERPRISE NETWORK COMPUTING

Going with Gigabit Ethernet

[illegible] technology. Page 8

- 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.



NETWORK
SABOTAGE

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 Bernes, vice president for servers and systems management strategy

See Bomb, page 16

The Omega Bomb Code

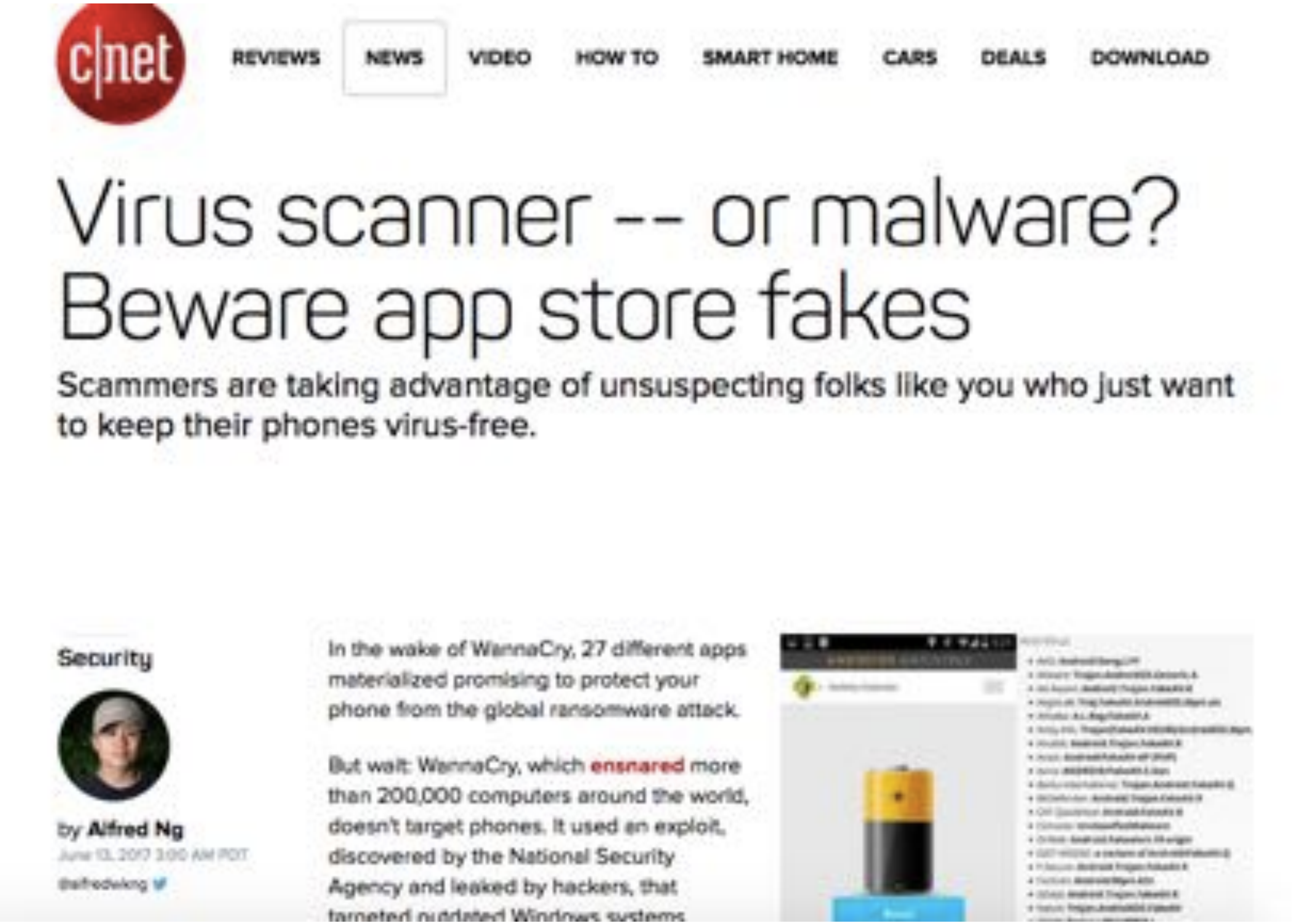
- The Logic Behind the Omega Engineering Time Bomb included the following strings:
- 7/30/96
  - Event that triggered the bomb
- F:
  - Focused attention to volume F, which had critical files
- F:\LOGIN\LOGIN 12345
  - Login a fictitious user, 12345 (the back door)
- CD \PUBLIC
  - Moves to the public 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

Defenses against Insider Attacks

- Avoid single points of failure.
- Use code walk-throughs.
- Use archiving and reporting tools.
- Limit authority and permissions.
- Physically secure critical systems.
- Monitor employee behavior.
- Control software installations.

Trojan horses

- 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



Virus scanner -- or malware? Beware app store fakes

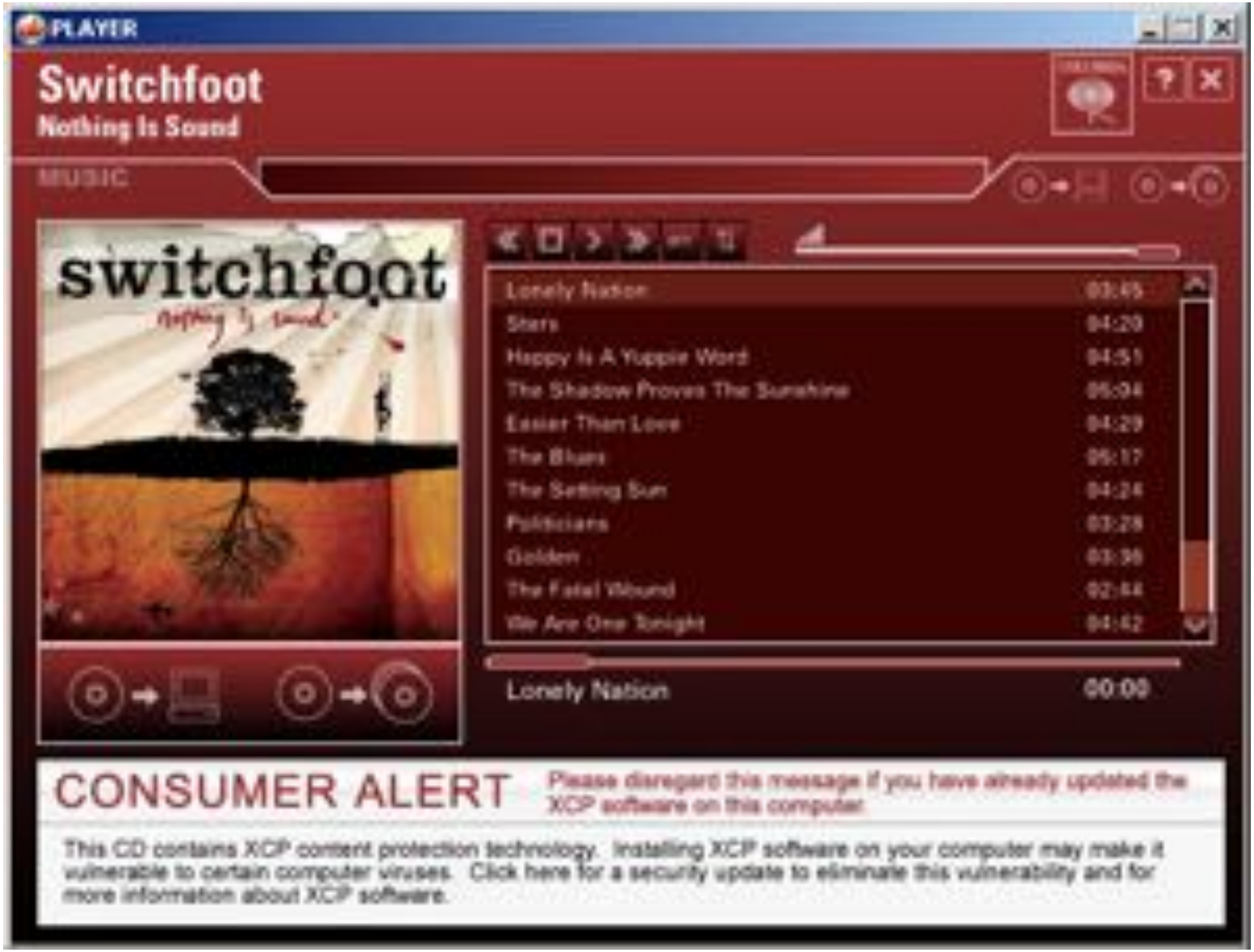
Scammers are taking advantage of unsuspecting folks like you who just want to keep their phones virus-free.

Security

by Alfred Ng
June 13, 2017 3:00 AM PDT
@alfredwkng

In the wake of WannaCry, 27 different apps materialized promising to protect your phone from the global ransomware attack.

But wait: WannaCry, which ensnared more than 200,000 computers around the world, doesn't target phones. It used an exploit, discovered by the National Security Agency and leaked by hackers, that targeted outdated Windows systems



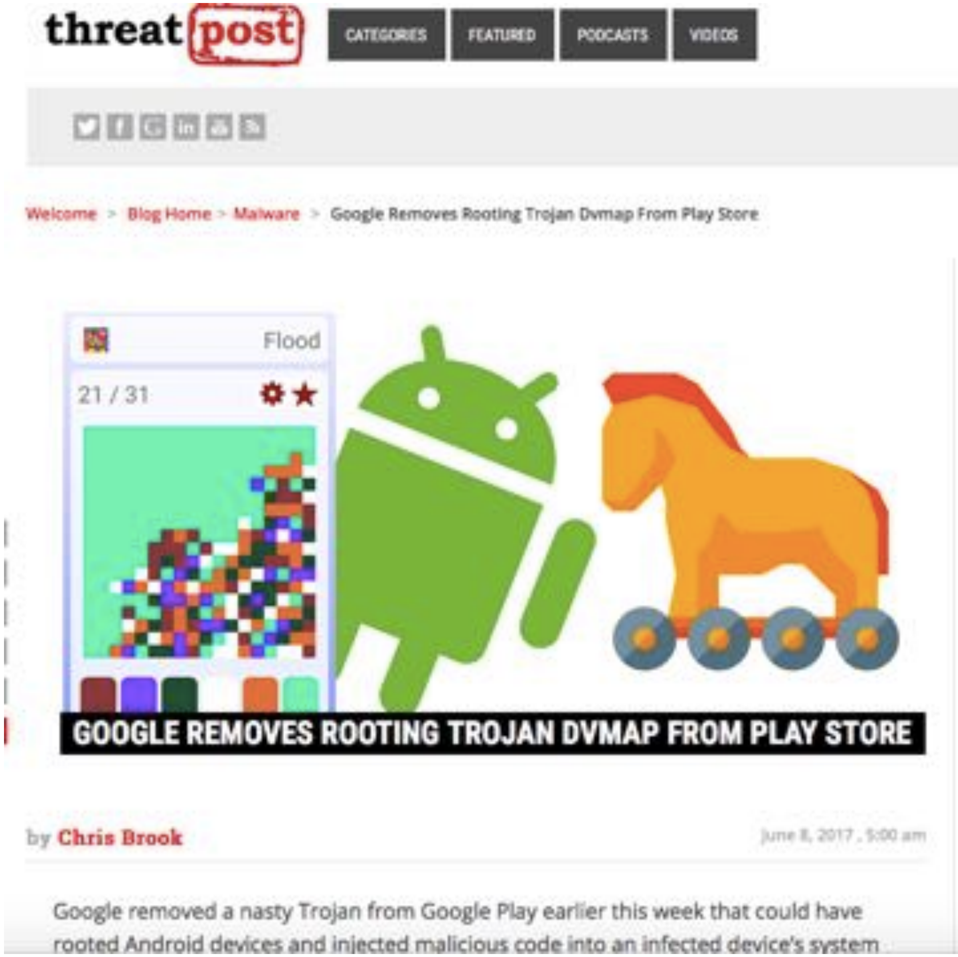
Lonely Nation	03:45
Stars	04:29
Happy Is A Yuppie Word	04:51
The Shadow Proves The Sunshine	05:04
Easier Than Love	04:29
The Blues	05:17
The Setting Sun	04:24
Politicians	03:28
Golden	03:38
The Fatal Wound	02:44
We Are One Tonight	04:42

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.



Welcome > Blog Home > Malware > Google Removes Rooting Trojan Dvmap From Play Store

GOOGLE REMOVES ROOTING TROJAN DVMAP FROM PLAY STORE

by Chris Brook

June 8, 2017 , 5:00 am

Google removed a nasty Trojan from Google Play earlier this week that could have rooted Android devices and injected malicious code into an infected device's system

usenix

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Jekyll on iOS: When Benign Apps Become Evil

Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee,
Georgia Institute of Technology

Evergreen Infosec Advice

ATTACKS

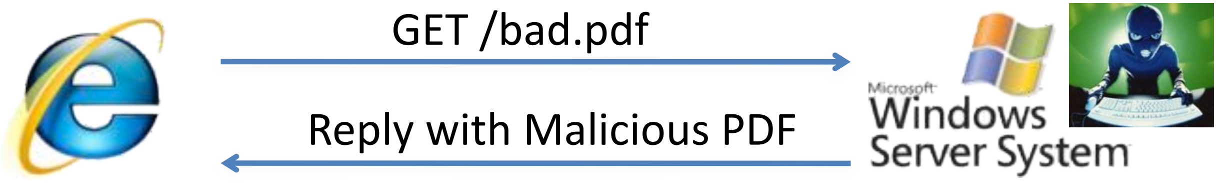
NEVER

GO

AWAY!

Code Injection Exploits

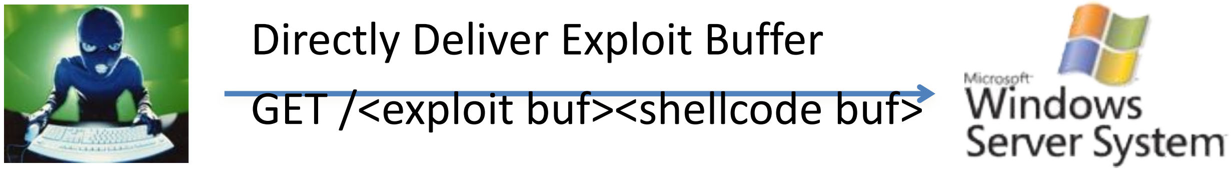
- Client software exploit (e.g. PDF, Flash, MSWord, etc.)



GET /bad.pdf

Reply with Malicious PDF

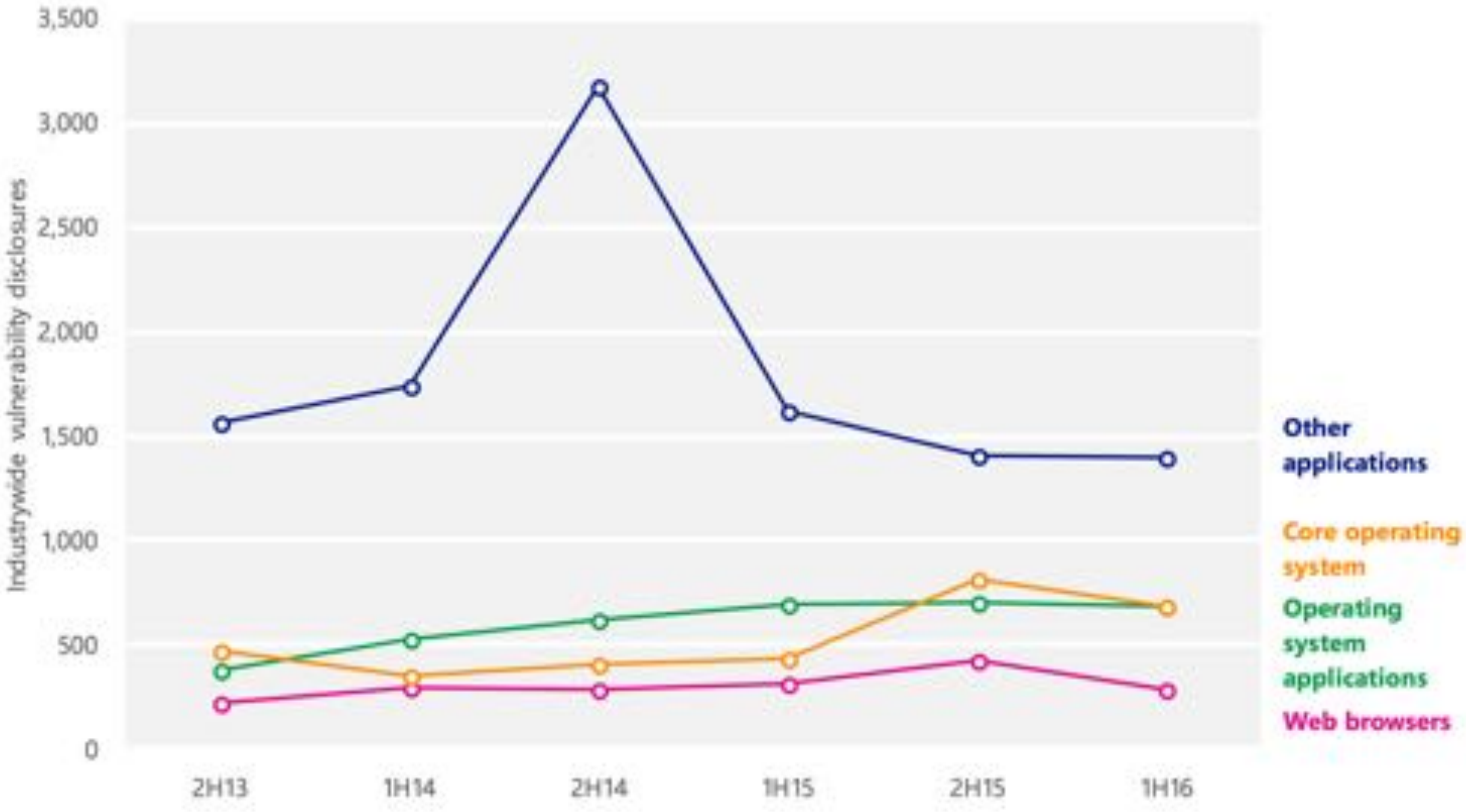
- Network-based exploit (HTTP, File, RPC servers, etc.)



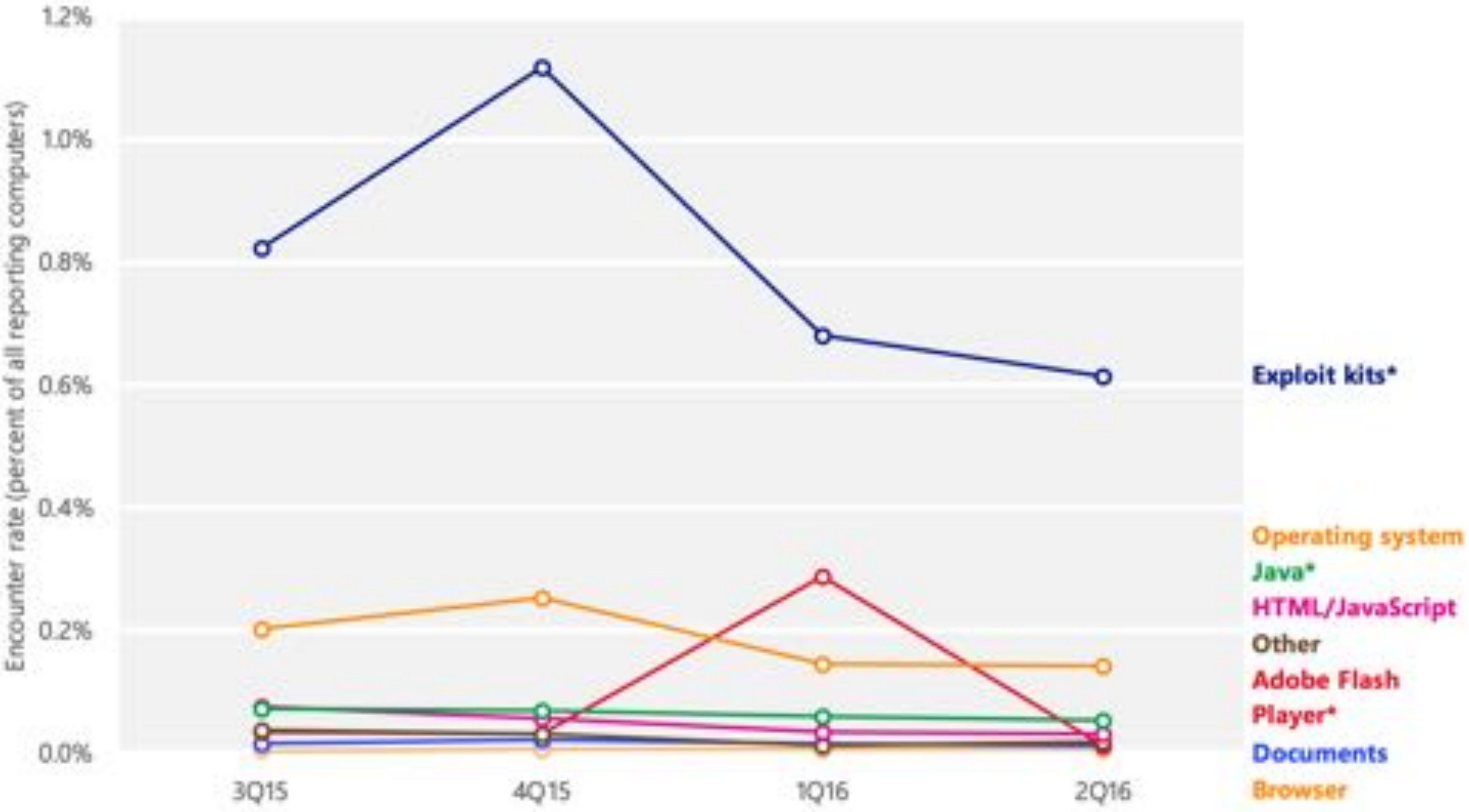
Directly Deliver Exploit Buffer

GET /<exploit buf><shellcode buf>

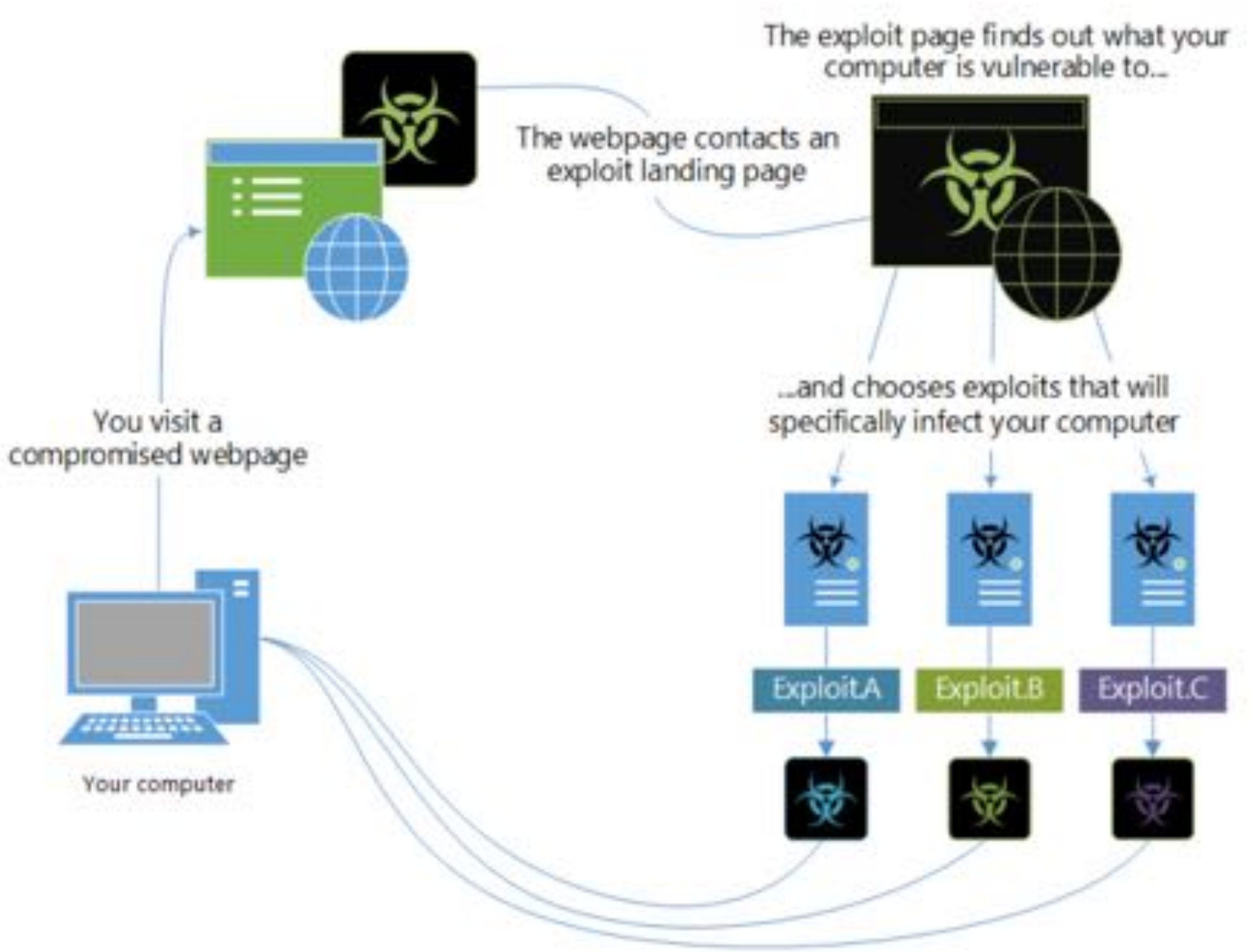
Industry-wide operating system, browser, and application vulnerabilities, 2H13–1H16



Encounter rates for different types of exploit attempts, 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

...and chooses exploits that will specifically infect your computer

You visit a compromised webpage

Malware That Automatically Propagates

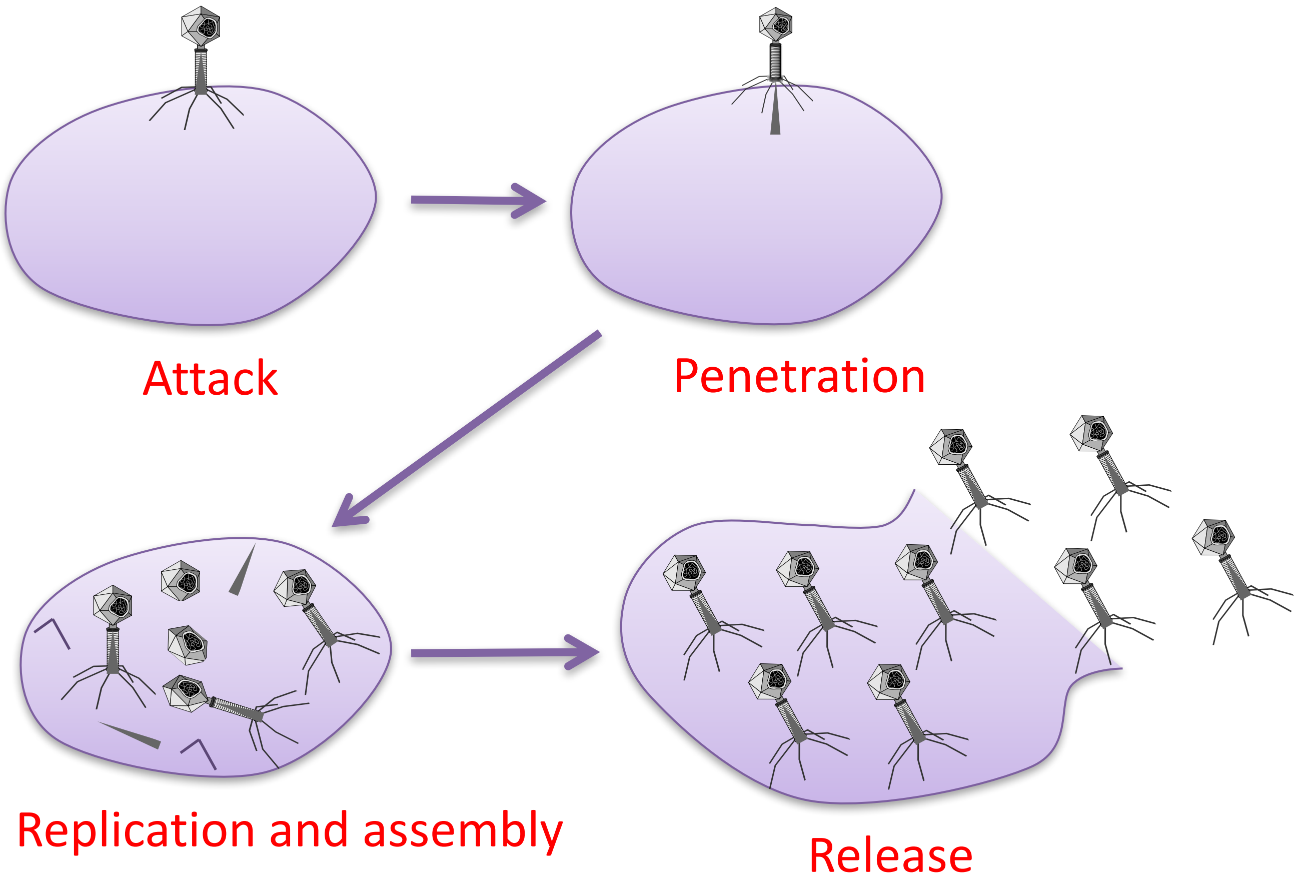
- Virus = code that propagates (**replicates**) across systems by arranging to have itself *eventually executed,* creating anew additional instance
  - Generally infects by altering stored code
  - Typically with the help of a user
- Worm = code that self-propagates/replicates across systems by arranging to have itself *immediately executed* (creating new addl. instance)
  - 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



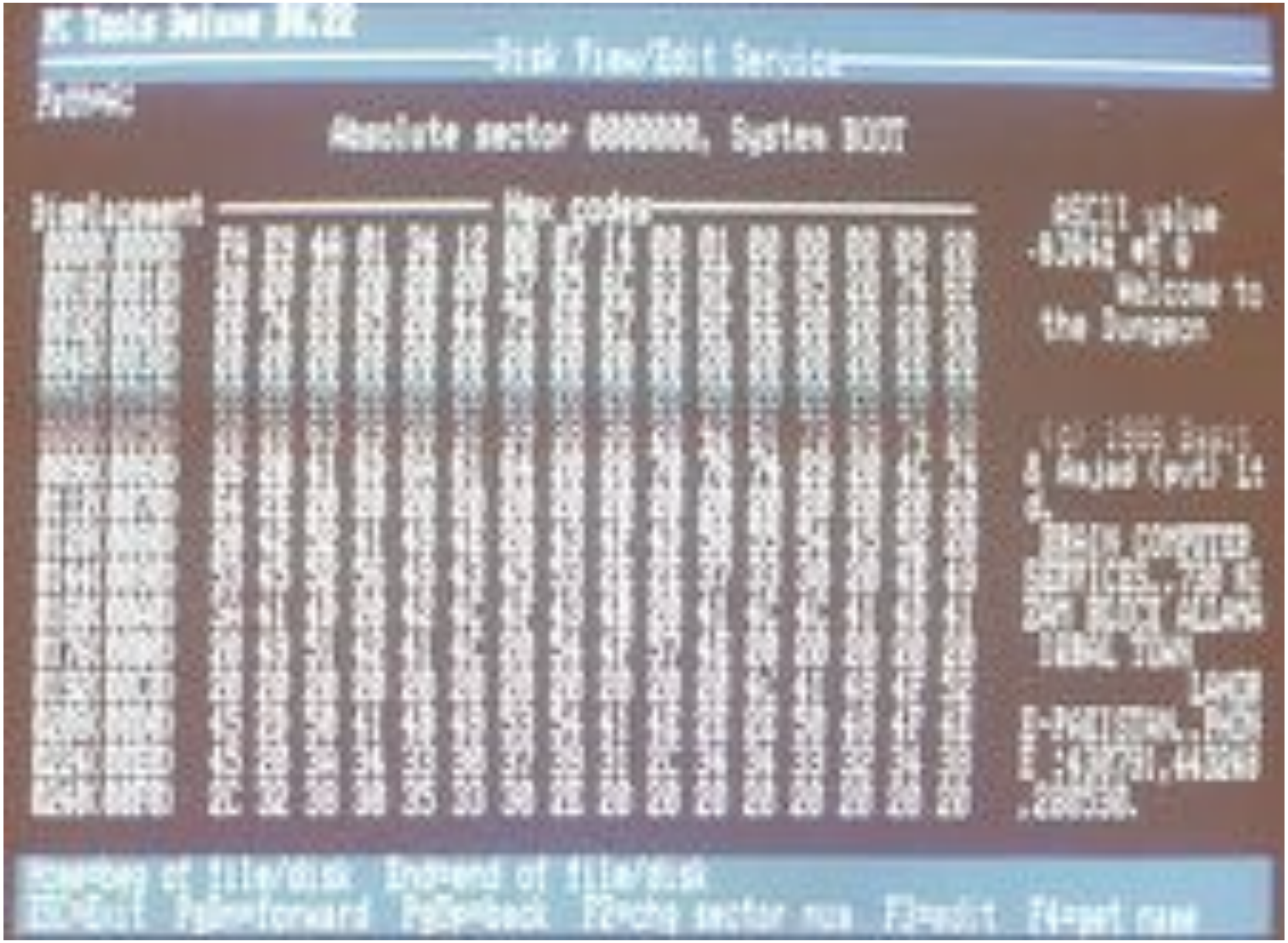
Propagation - Viruses

- Malware that infects other programs
- Three parts:
  - infection vector
  - trigger
  - payload
- Four phases:
  - Dormant
  - Propagation
  - Trigger
  - Execution

Propagation - Viruses

- Can target many locations
  - Boot sector
  - Files
  - Macros
  - Multipartite
- Can conceal itself many ways:
  - Encryption
  - Stealth
  - Polymorphic
  - Metamorphic

Brain



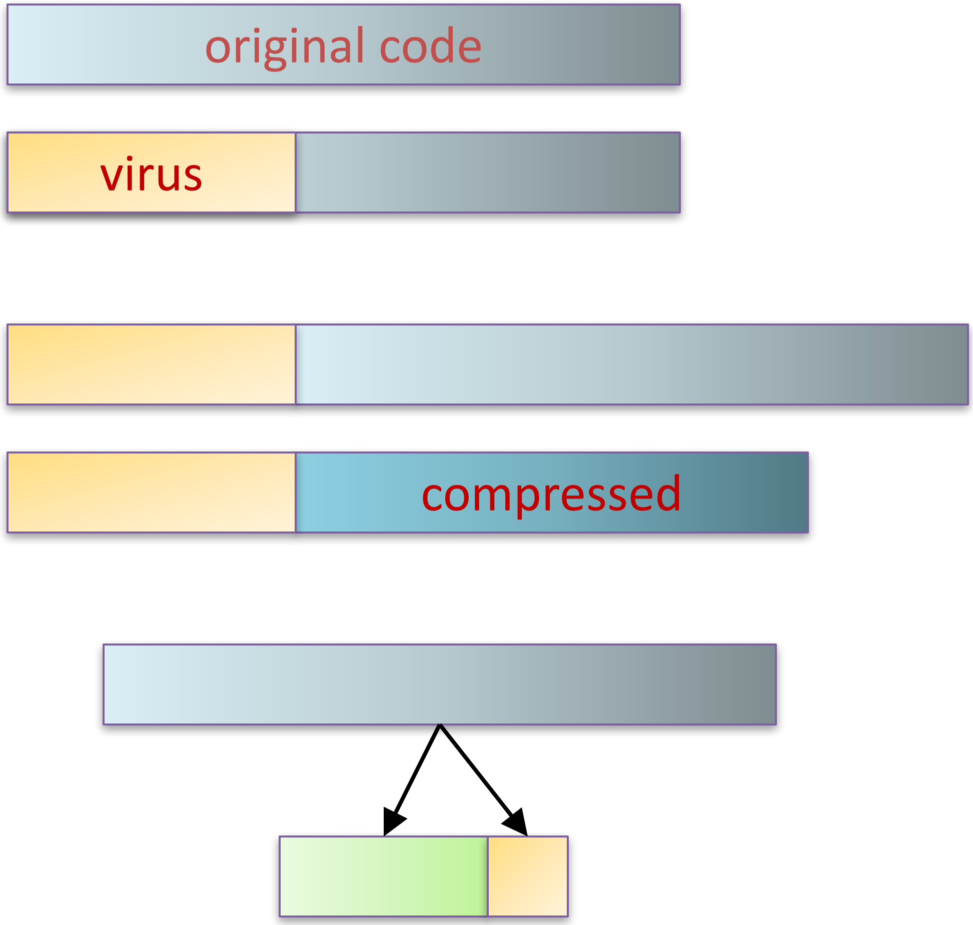
```
PC Tools Deluxe R4.22
─────────────────Disk View/Edit Service──────────────────
Path=A:
              Absolute sector 0000000, System BOOT

Displacement ──────────── Hex codes ─────────────────      ASCII value
0000(0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 20 20   [illegible]
[illegible]                                                      Welcome to
                                                          the Dungeon

                                                          (c) 1986 Basit
                                                          & Amjad (pvt) Lt
                                                          d.
                                                           BRAIN COMPUTER
                                                          SERVICES..730 NI
                                                          ZAM BLOCK ALLAMA
                                                           IQBAL TOWN
                                                                     LAHOR
                                                          E-PAKISTAN..PHON
                                                          E :430791,443248
0496(01F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,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 **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.

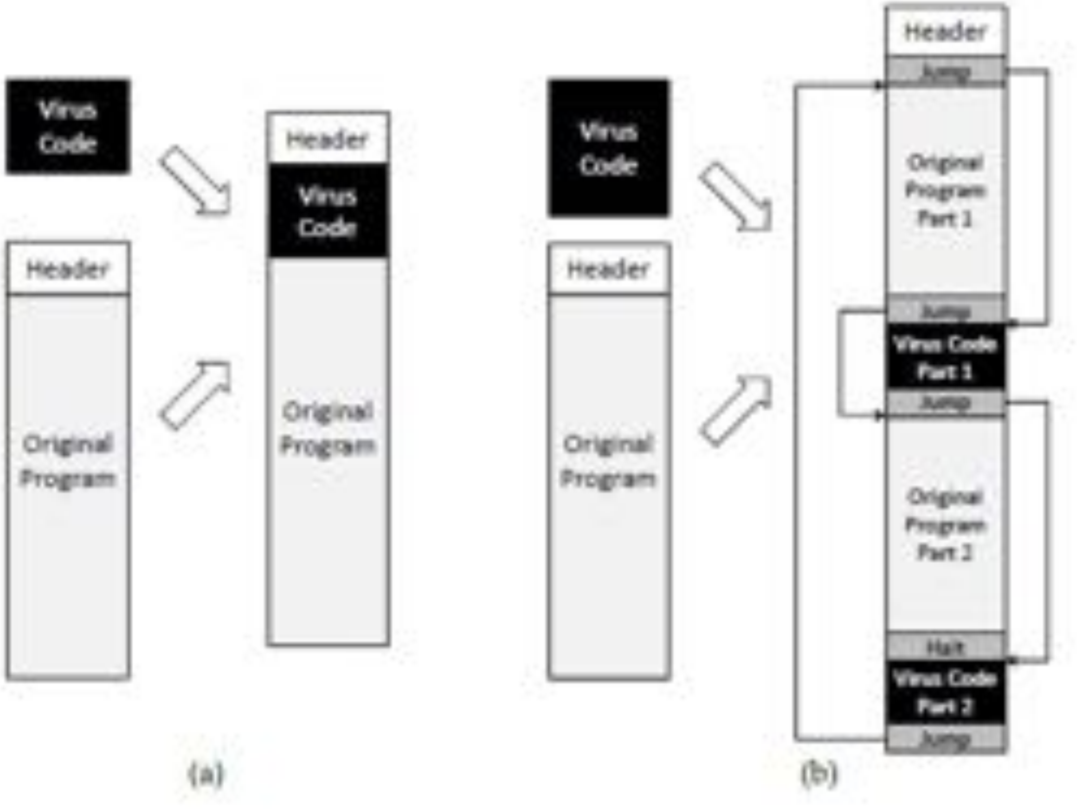
Infection Types

- 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



Degrees of Complication

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



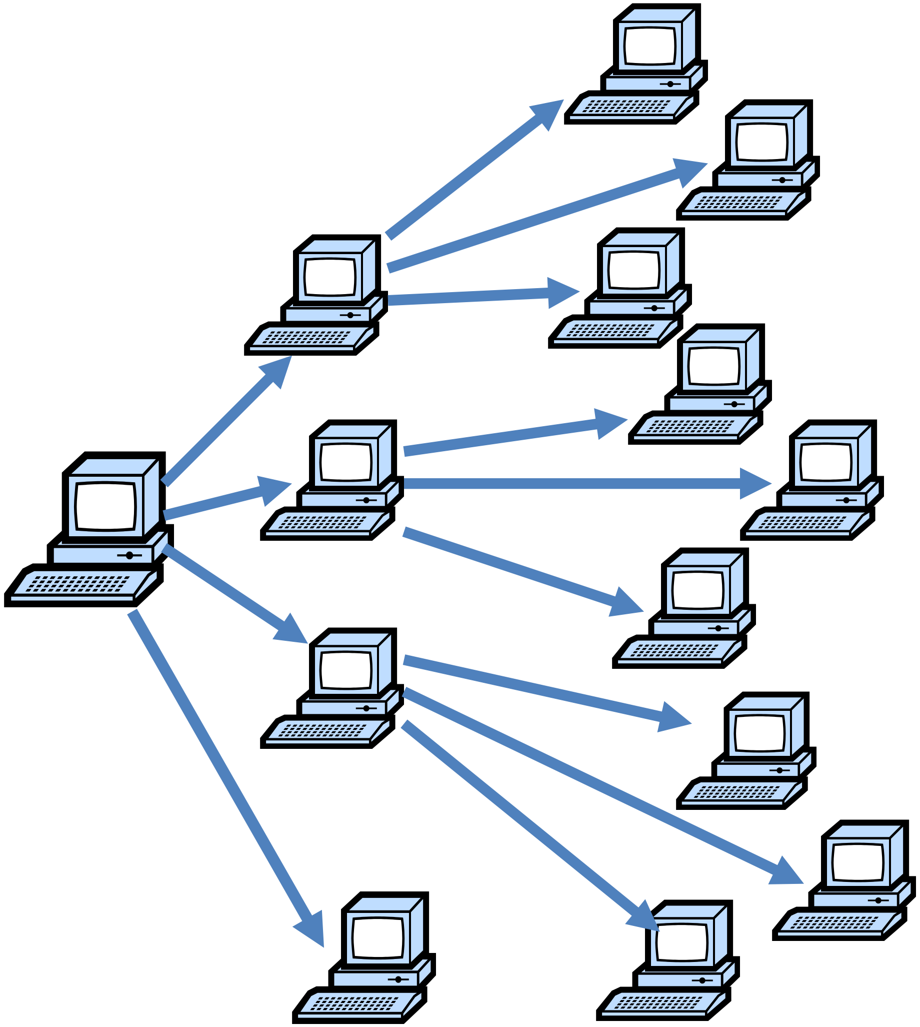
Worm

- 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

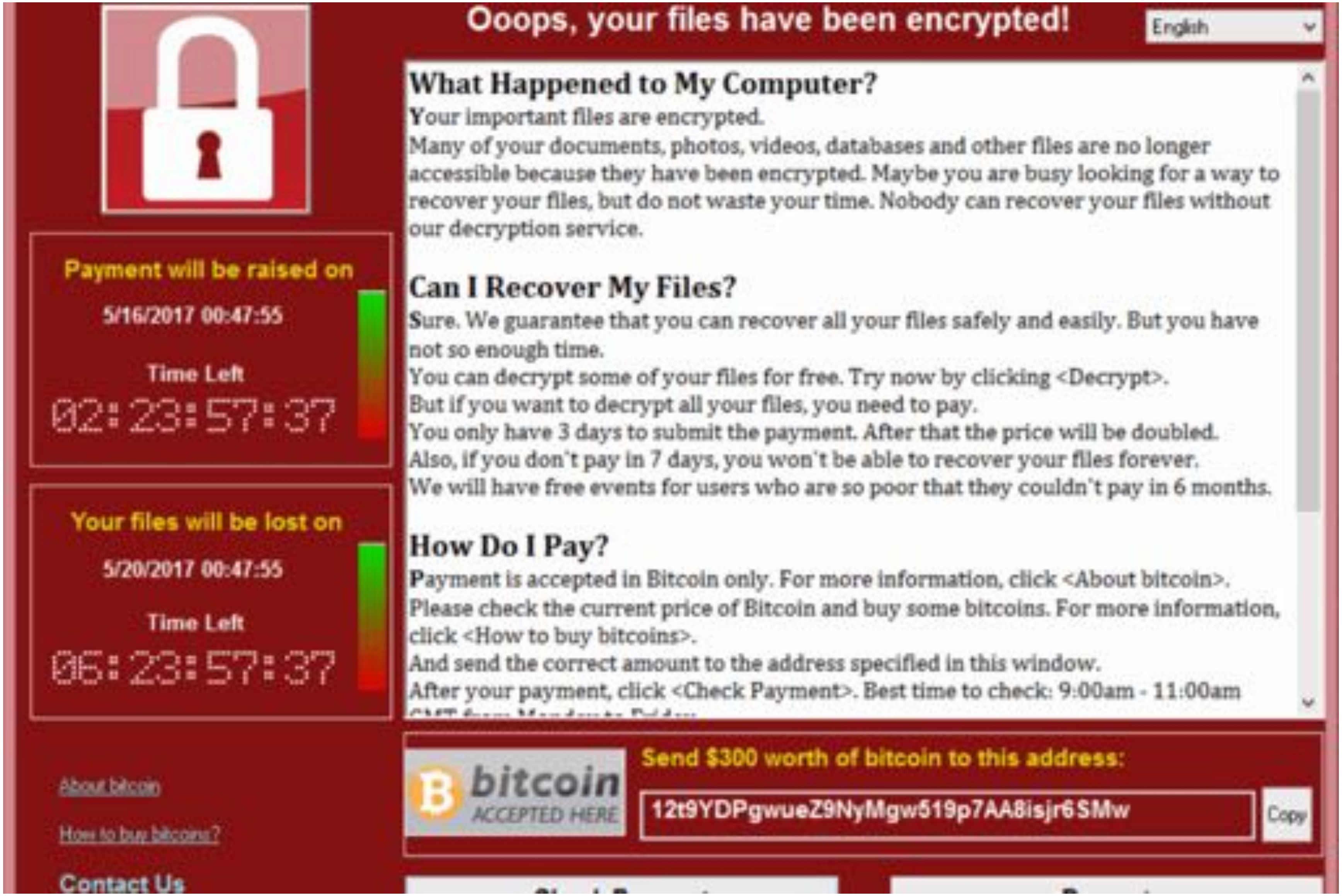
Worms can potentially spread quickly because they parallelize the process of propagating/ replicating.

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



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Evergreen Infosec Advice

NEVER

GET

COMPLACENT!

PAYLOADS

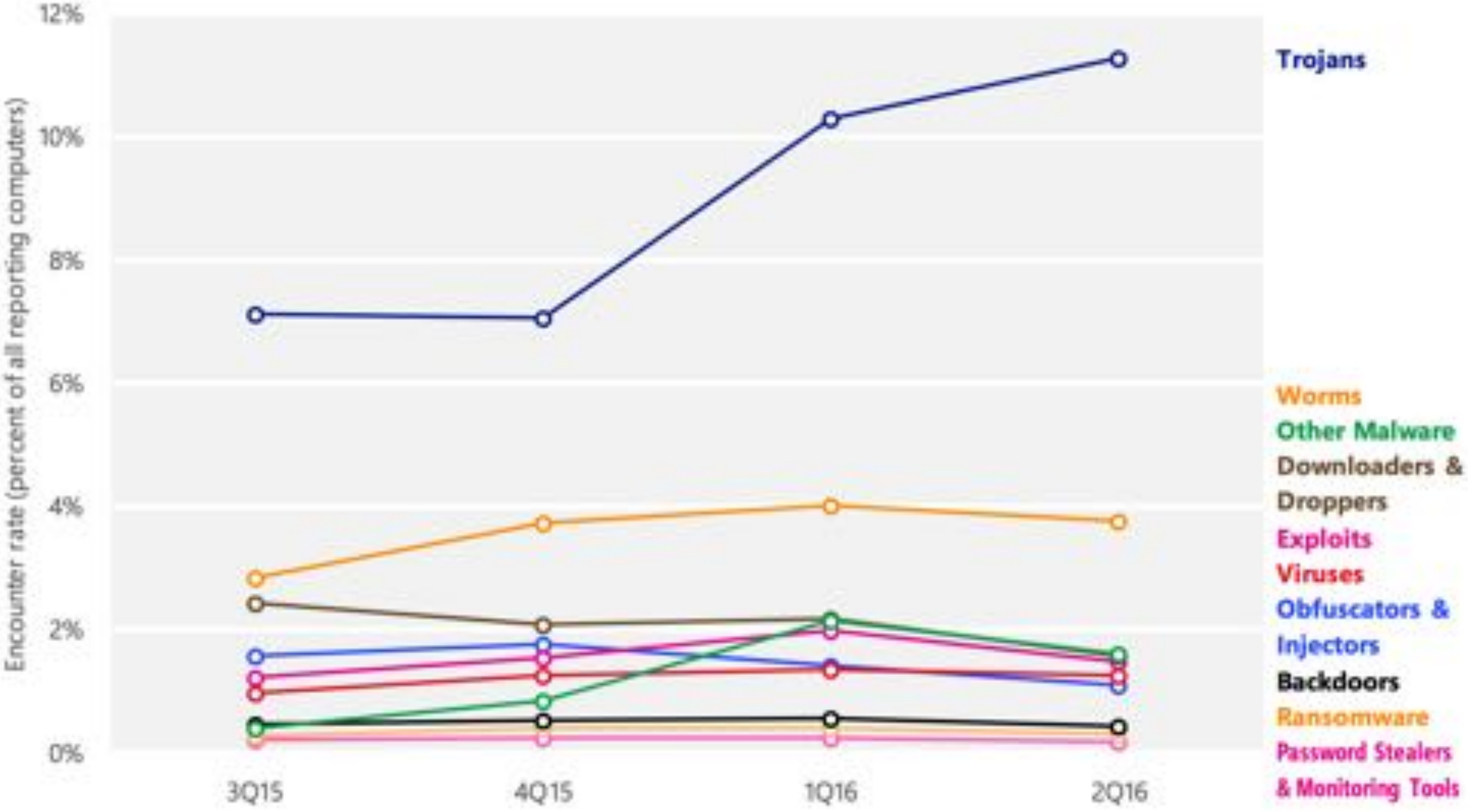
What Can Malware Do?

- 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”

Payload - Information theft

- Payload can allow for remote monitoring of user
- This can be used to steal login credentials (e.g. passwords)
- Keyloggers - programs to record keystrokes and report them to the attacker
- Spyware - programs that monitor browsing history, cameras (term originated with Steve Gibson)
- Phishing - direct users to fake websites to enter login credentials
- Spear-phishing - specific user targeted by phishing attack

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



Payload - Stealthing

- A user can gain access and hide on a system
- Maintain a *backdoor* - secret remote login
- rootkits allow the user to maintain *root access* while hiding existence
  - backdoor + stealthing + root access
- Rootkits modify call table (hooking)
  - How can you find something when you can’t trust *any* system calls?!

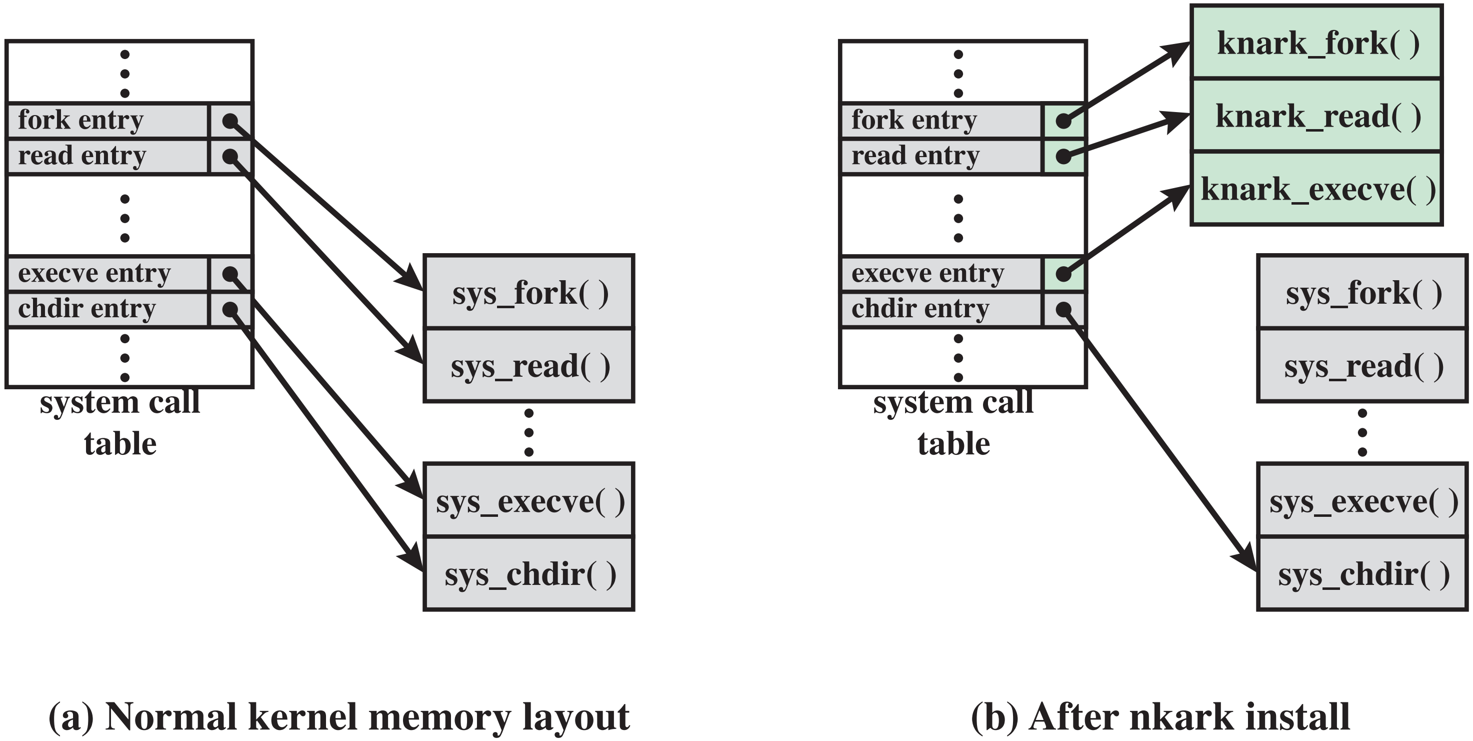
Rootkits

- 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:

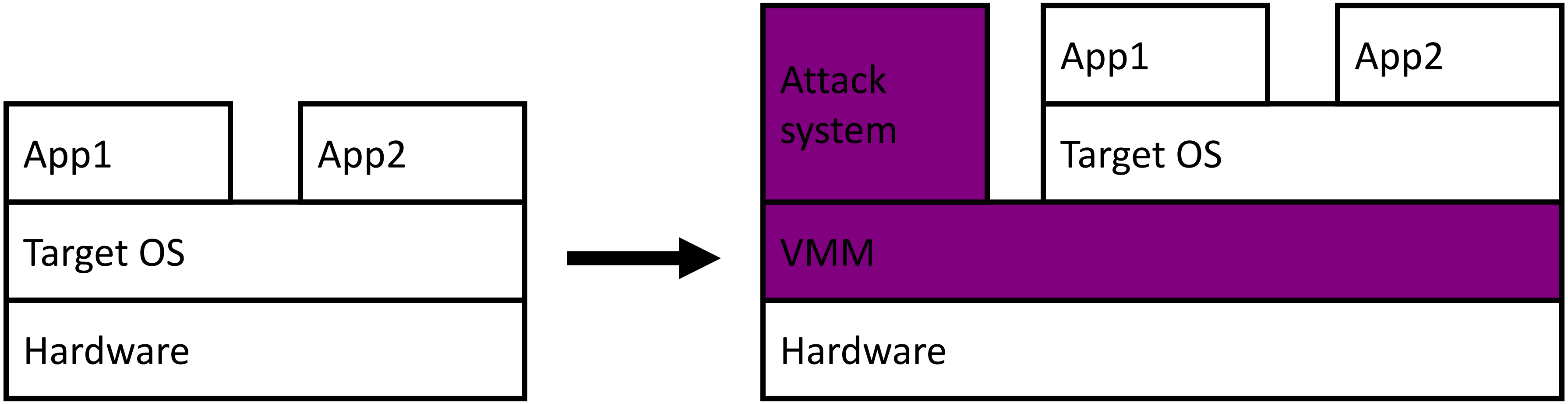
    Applications --> System Call ---> (Rootkit) --> Kernel

    <-- Results --- If call is from rootkit application (e.g. $sys$rootkit.exe), don't filter!
- RootkitRevealer
  - By Bryce Cogswell and Mark Russinovich (Sysinternals)
  - Two scans of file system
  - High-level scan using the Windows API
  - Raw scan using disk access methods
  - Discrepancy reveals presence of rootkit
  - Could be defeated by rootkit that intercepts and modifies results of raw scan operations

Hooking


fork entry
read entry
execve entry
chdir entry
system call table
sys_fork( )
sys_read( )
sys_execve( )
sys_chdir( )
(a) Normal kernel memory layout
knark_fork( )
knark_read( )
knark_execve( )
fork entry
read entry
execve entry
chdir entry
system call table
sys_fork( )
sys_read( )
sys_execve( )
sys_chdir( )
(b) After nkark install

Virtual-machine based rootkits (VMBRs)



App1

App2

Target OS

Hardware

Attack system

App1

App2

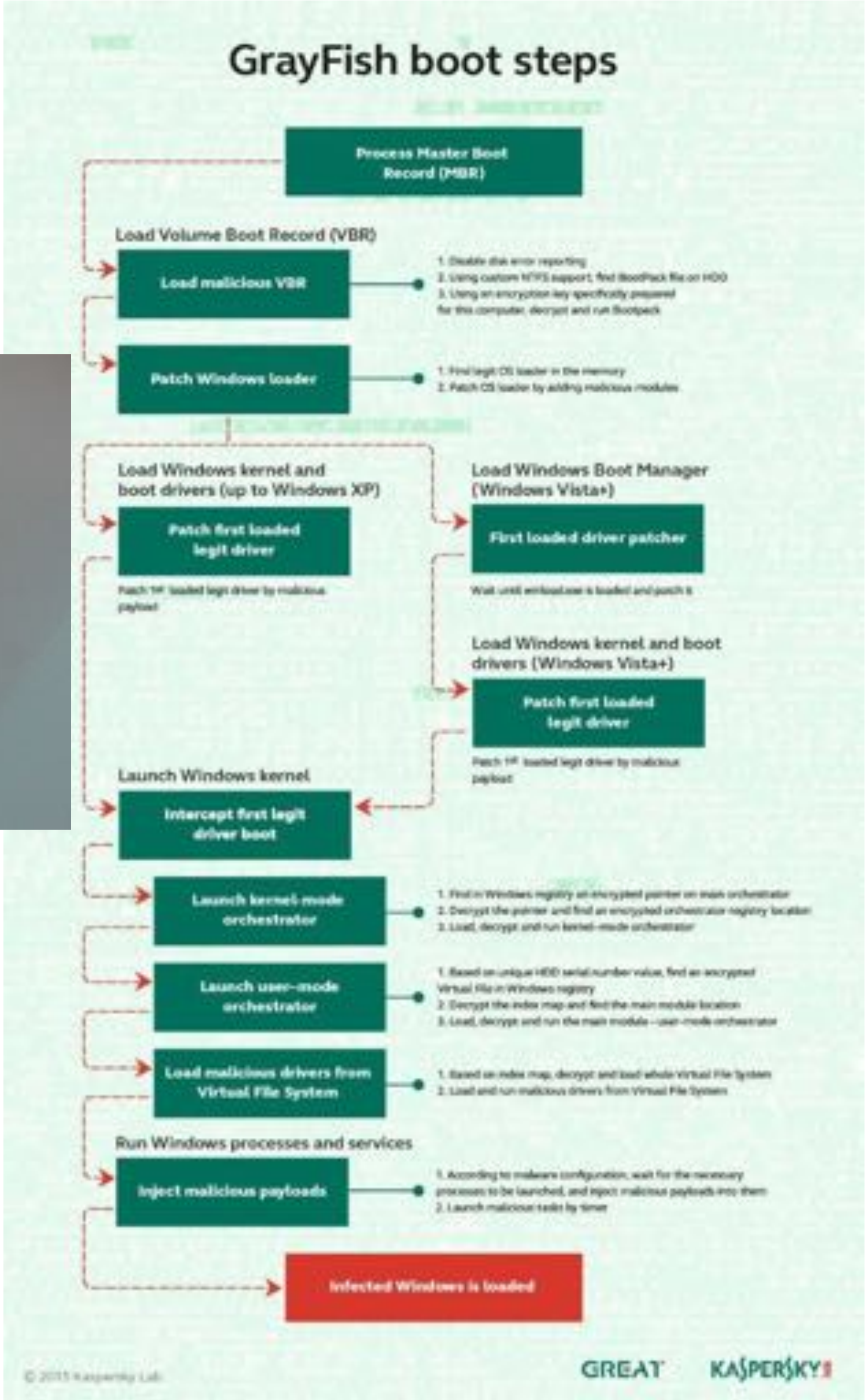
Target OS

VMM

Hardware

Before infection

After infection



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

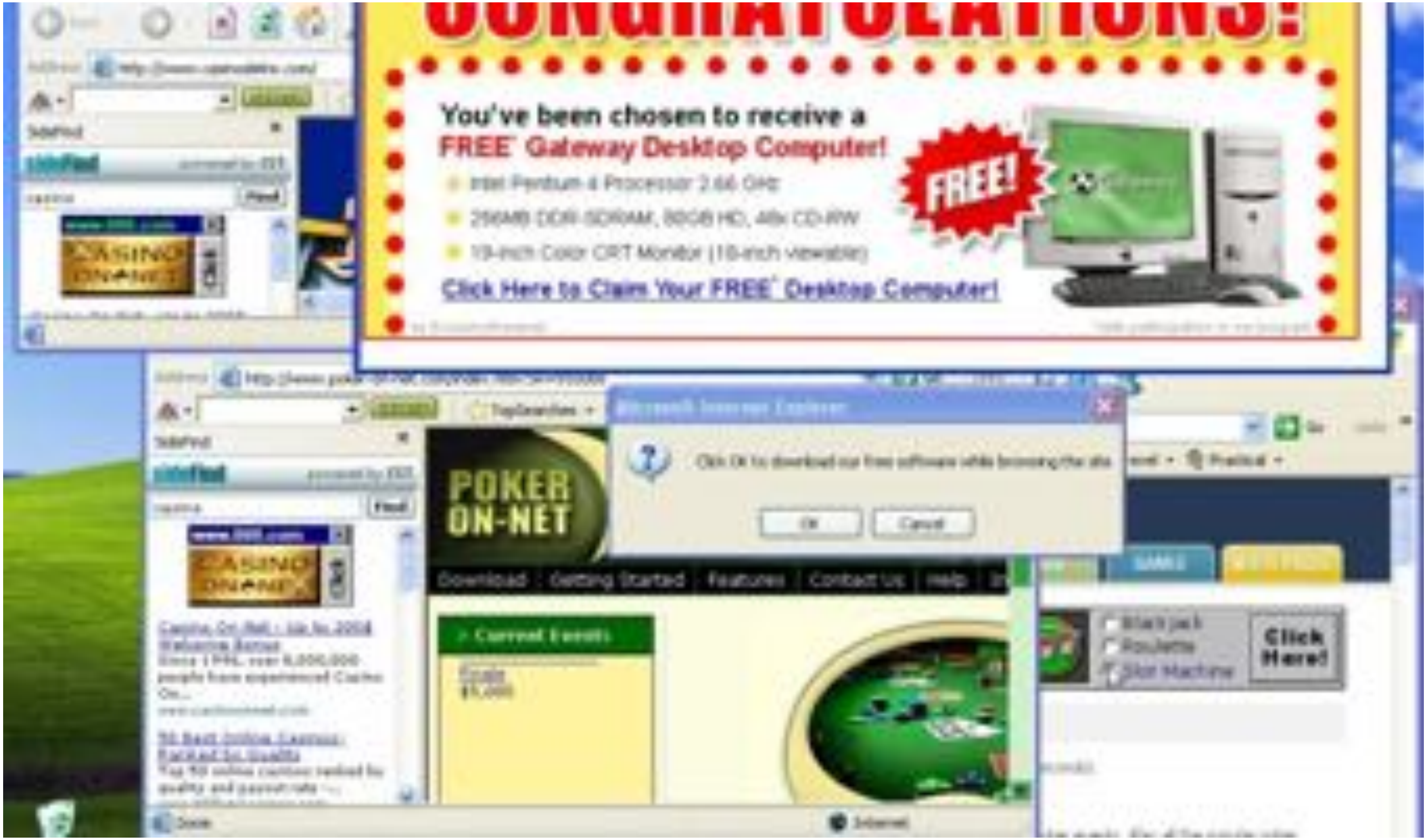
Run Windows processes and services

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

Adware



CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

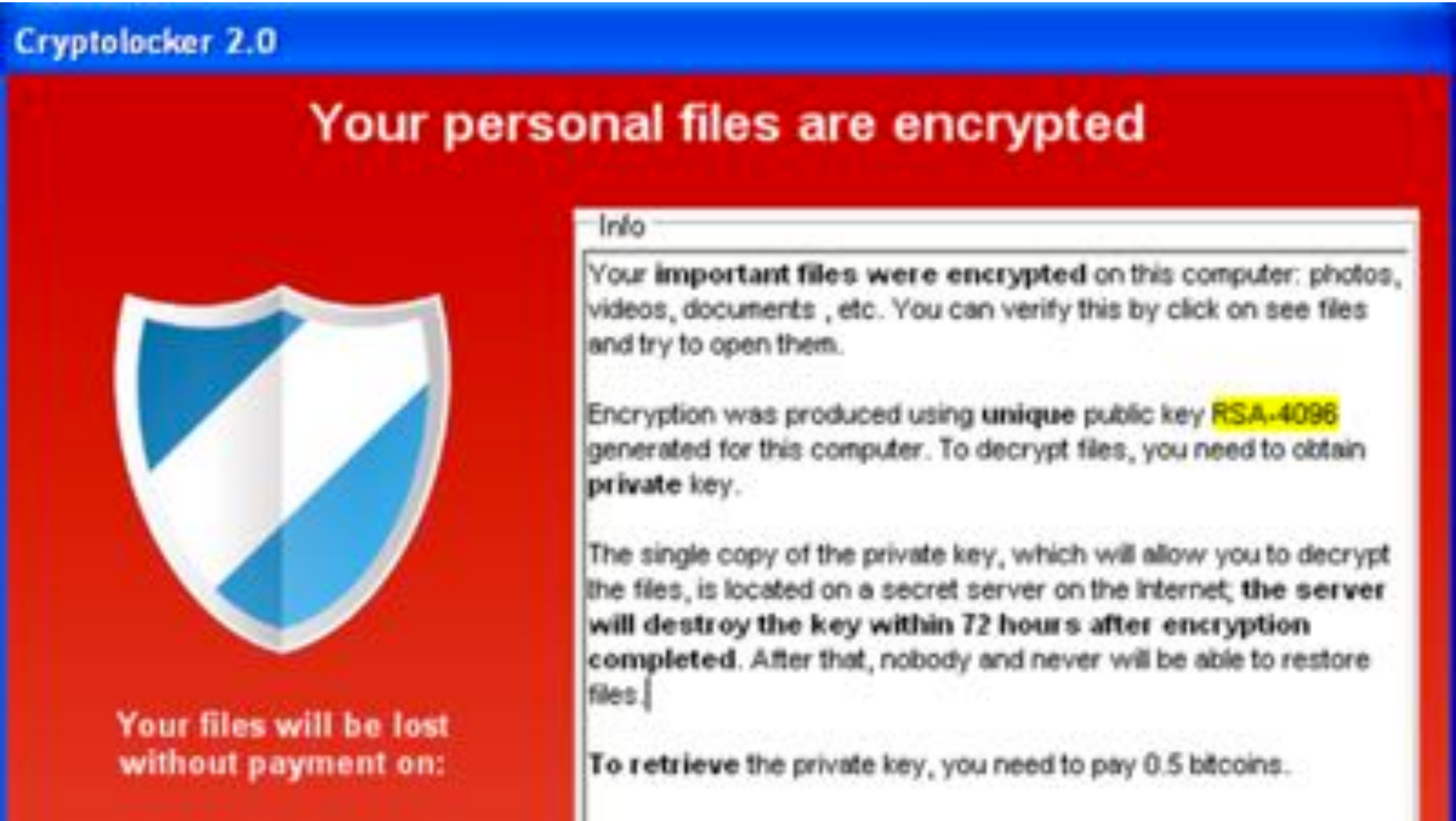
- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

Ransomware



Your personal files are encrypted

Your files will be lost without payment on:

Info

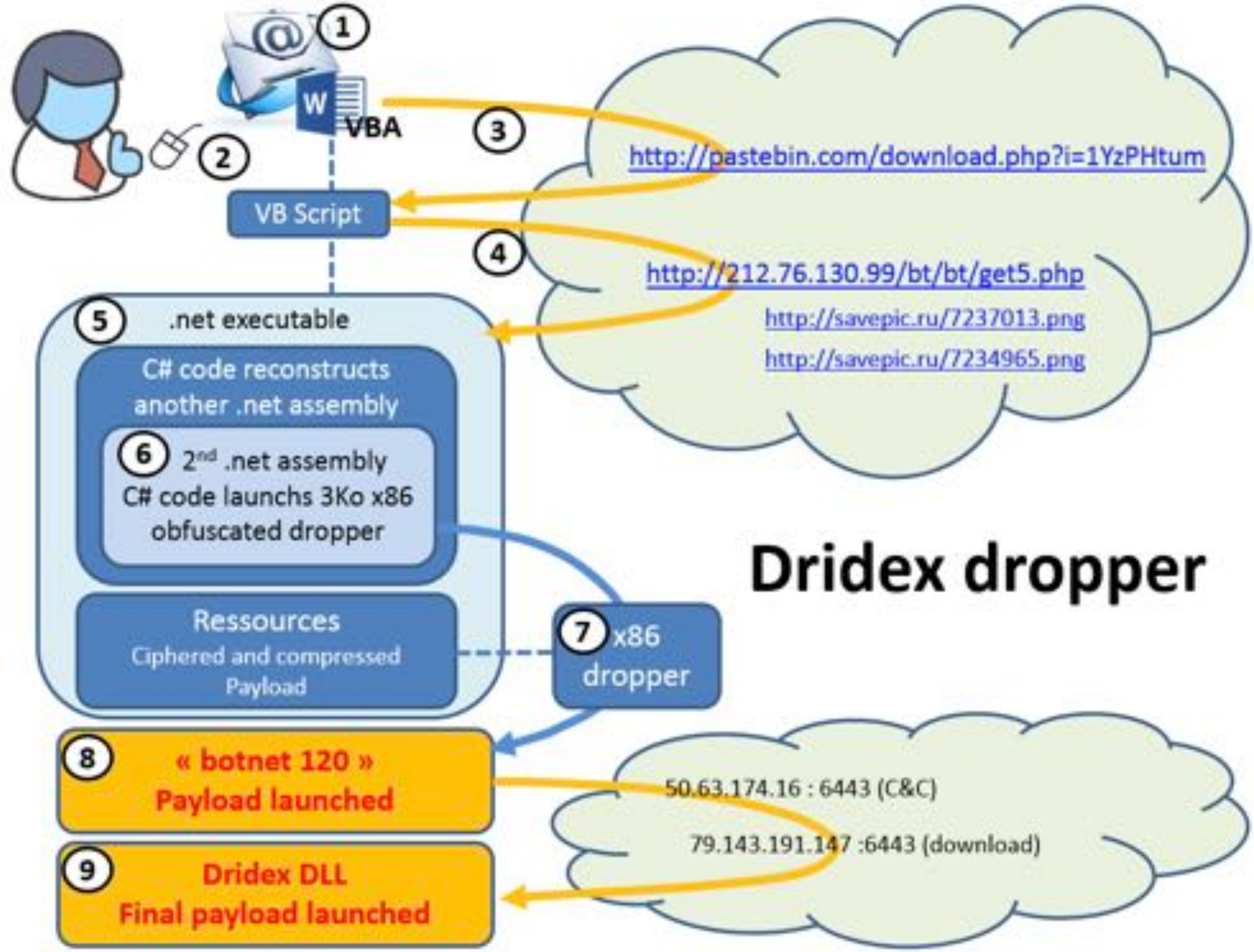
Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

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.

Droppers



1

2

VBA

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

8 « botnet 120 » Payload launched

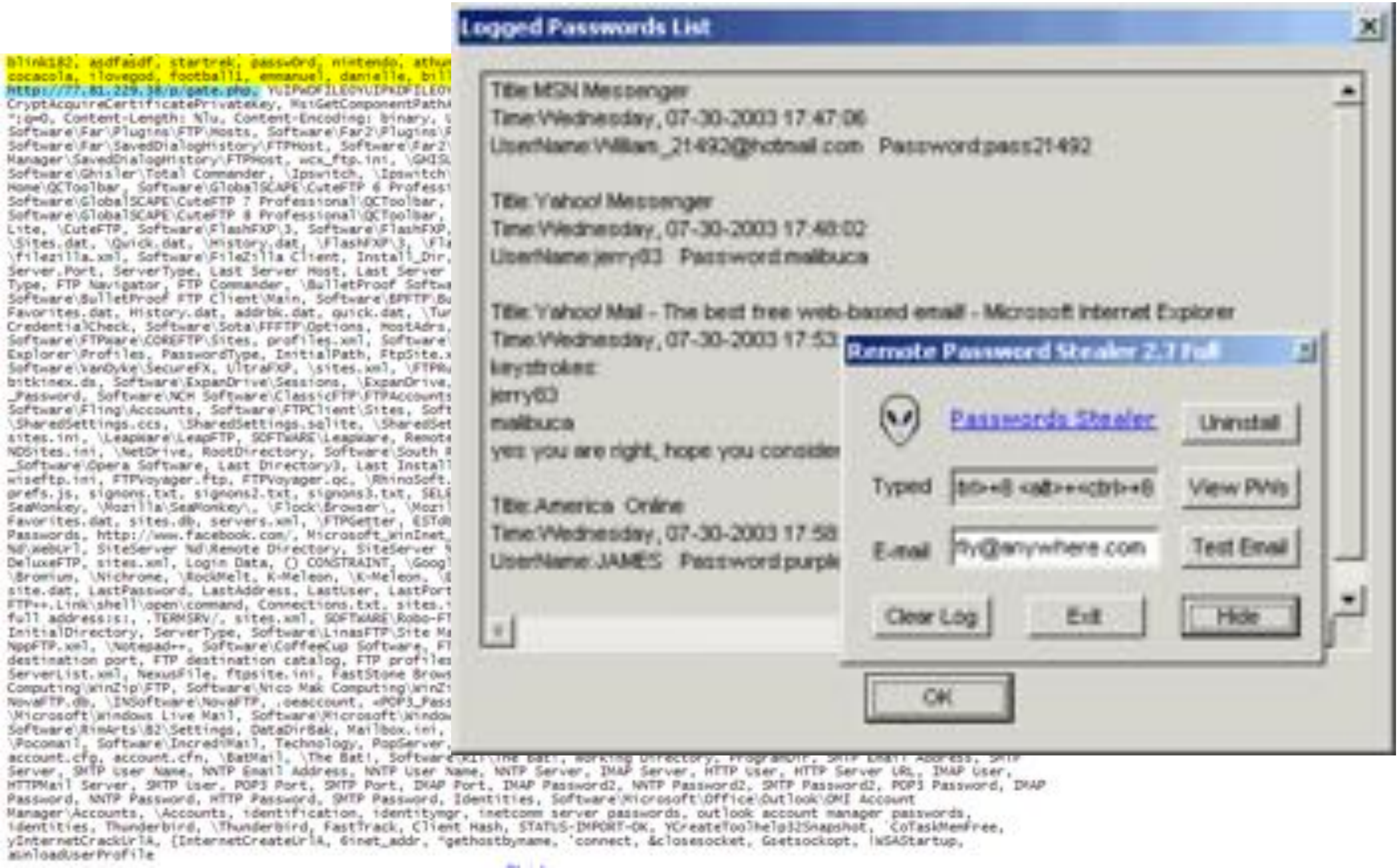
50.63.174.16 : 6443 (C&C)

79.143.191.147 :6443 (download)

9 Dridex DLL Final payload launched

Dridex dropper

Key logging and Password Stealing



```
blink182, asdfasdf, startrek, passw0rd, nintendo, athu
cocacola, ilovegod, football1, emmanuel, danielle, bil
http://77.81.229.38/p/gate.php, YUIPWDFILE0YUIPKDFILE0Y
CryptAcquireCertificatePrivateKey, MsiGetComponentPathA
";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, \Fla
\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\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 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\, \Mozi
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\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, Gsetsockopt, !WSAStartup,
aUnloadUserProfile
```

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

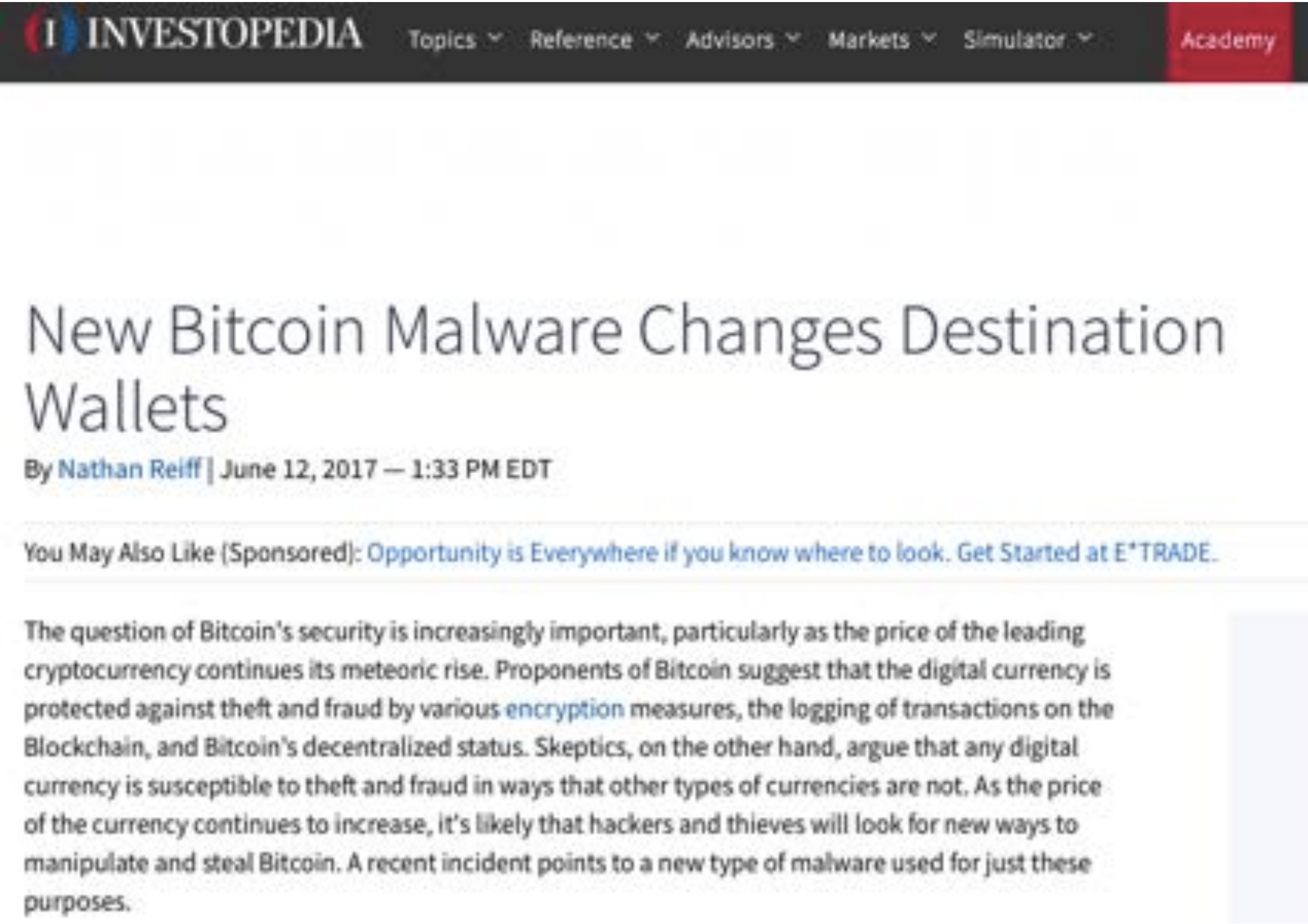
Title:Yahoo! Messenger
Time:Wednesday, 07-30-2003 17:48:02
UserName:jerry03 Password:malibuca

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

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

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

E-mail fly@anywhere.com



New Bitcoin Malware Changes Destination Wallets

By Nathan Reiff | June 12, 2017 — 1:33 PM EDT

The question of Bitcoin's security is increasingly important, particularly as the price of the leading cryptocurrency continues its meteoric rise. Proponents of Bitcoin suggest that the digital currency is protected against theft and fraud by various encryption measures, the logging of transactions on the Blockchain, and Bitcoin's decentralized status. Skeptics, on the other hand, argue that any digital currency is susceptible to theft and fraud in ways that other types of currencies are not. As the price of the currency continues to increase, it's likely that hackers and thieves will look for new ways to manipulate and steal Bitcoin. A recent incident points to a new type of malware used for just these purposes.

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

Advanced Persistent Threats (APT)

- Not a new form of malware
- Advanced
  - variety of intrusion methods
  - custom malware (0-days)
  - tailored to attack target
- Persistent
  - attacks target over extended period of time
  - takes down layers of defense with stealth
- Threat

Advanced Persistent Threats (APT)

- Goals
  - Steal IP
  - Compromise security infrastructure
  - Damage physical assets
- Techniques
  - social engineering
  - spear phishing
  - drive by downloads (website that exploits browser)
- Source
  - Usually state sponsored

Stuxnet

- Initially spread by infected USB flash drives
- Worm spreads quickly through Windows networks
- From Windows machine, attacked specific microcontrollers
- Incorporated 4 0-day exploits!
- Speculation: a US/Israel collaboration to target Iran
  - Reportedly ruined 1/5 of Iran’s nuclear centrifuges
- Read more here: http://en.wikipedia.org/wiki/Stuxnet