



Malware

Spring 2017

Trojans Programs. Worms

Sergii Lysenko, PhD



Co-funded by the
Tempus Programme
of the European Union



Your computer could be watching your every move!



Introduction

Overview

- Introduction to Spyware / Trojan Horses
- Spyware – Examples, Mechanics, Effects, Solutions
- Tracking Cookies – Mechanics, Effects, Solutions
- Trojan Horses – Mechanics, Effects, More Examples
- Solutions to the problems posed
- Human Factors – Human interaction with Spyware
- “System X” – Having suitable avoidance mechanisms

Definitions

A general term for a program that surreptitiously monitors your actions. While they are sometimes sniffer, like a remote control program used by a hacker, software companies have been known to use Spyware to gather data about customers. The practice is generally frowned upon.

Definition from: BlackICE Internet Security Systems - <http://blackice.iss.net/glossary.php>

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.

Definition from: Texas State Library and Archives Commission - <http://www.tsl.state.tx.us/d/pubs/compsecurity/glossary.html>

Symptoms

- Targeted Pop-ups
- Slow Connection
- Targeted E-Mail (Spam)
- Unauthorized Access
- Spam Relaying
- System Crash
- Program Customisation

SPYWARE

SPYWARE / TROJAN

SPYWARE

TROJAN HORSE

TROJAN HORSE

SPYWARE / TROJAN

SPYWARE

Summary of Effects

- Collection of data from your computer without consent
- Execution of code without consent
- Assignment of a unique code to identify you
- Collection of data pertaining to your habitual use
- Installation on your computer without your consent
- Inability to remove the software
- Performing other undesirable tasks without consent

Similarities / Differences

Spyware	Trojan Horses
Commercially Motivated	Malicious
Internet connection required	Any network connection required
Initiates remote connection	Receives incoming connection
Purpose: To monitor activity	Purpose: To control activity
Collects data and displays pop-ups	Unauthorized access and control
Legal	Illegal
Not Detectable with Virus Checker	Detectable with Virus Checker
Age: Relatively New (< 5 Years)	Age: Relatively Old (> 20 Years)
Memory Resident Processes	
Surreptitiously installed without user's consent or understanding	
Creates a security vulnerability	

Spyware

Software Examples

- GAIN / Gator
- Gator E-Wallet
- Cydoor
- BonziBuddy
- MySearch Toolbar
- DownloadWare
- BrowserAid
- Dogpile Toolbar



Image Sources...

GAIN Logo – The Gator Corporation – <http://www.gator.com>

BonziBuddy Logo – Bonzi.com – <http://images.bonzi.com/images/gorillatalk.gif>

DownloadWare Logo – DownloadWare – <http://www.downloadware.net>

Advantages

- Precision Marketing
 - Relevant pop-ups are better than all of them!
 - You may get some useful adverts!
- Useful Software
 - DivX Pro, IMesh, KaZaA, Winamp Pro
 - (Experienced) people understand what they are installing.
- Enhanced Website Interaction
 - Targeted banner adverts
 - Website customisation

User Perspective - I

Disadvantages

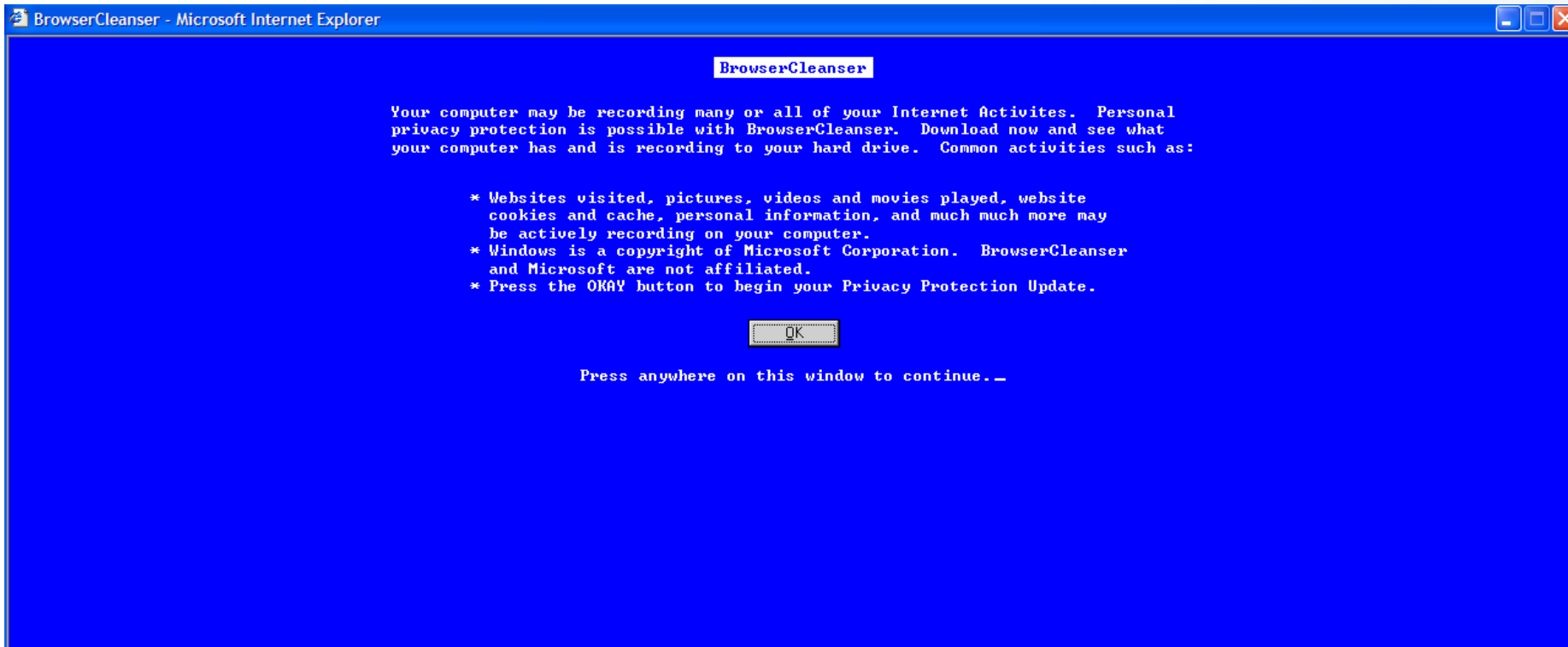
- Browsing profiles created for users without consent
 - Used for target marketing and statistical analysis
- Unable to remove Spyware programs or disable them
- Increased number of misleading / inappropriate pop-ups
- Invasion of user privacy (hidden from user)
- Often badly written programs corrupt user system
- Automatically provides unwanted “helpful” tools
- “80 million+ people have Spyware on their machines.”

Source - Dec '16 GartnerG2 Report

User Perspective - II

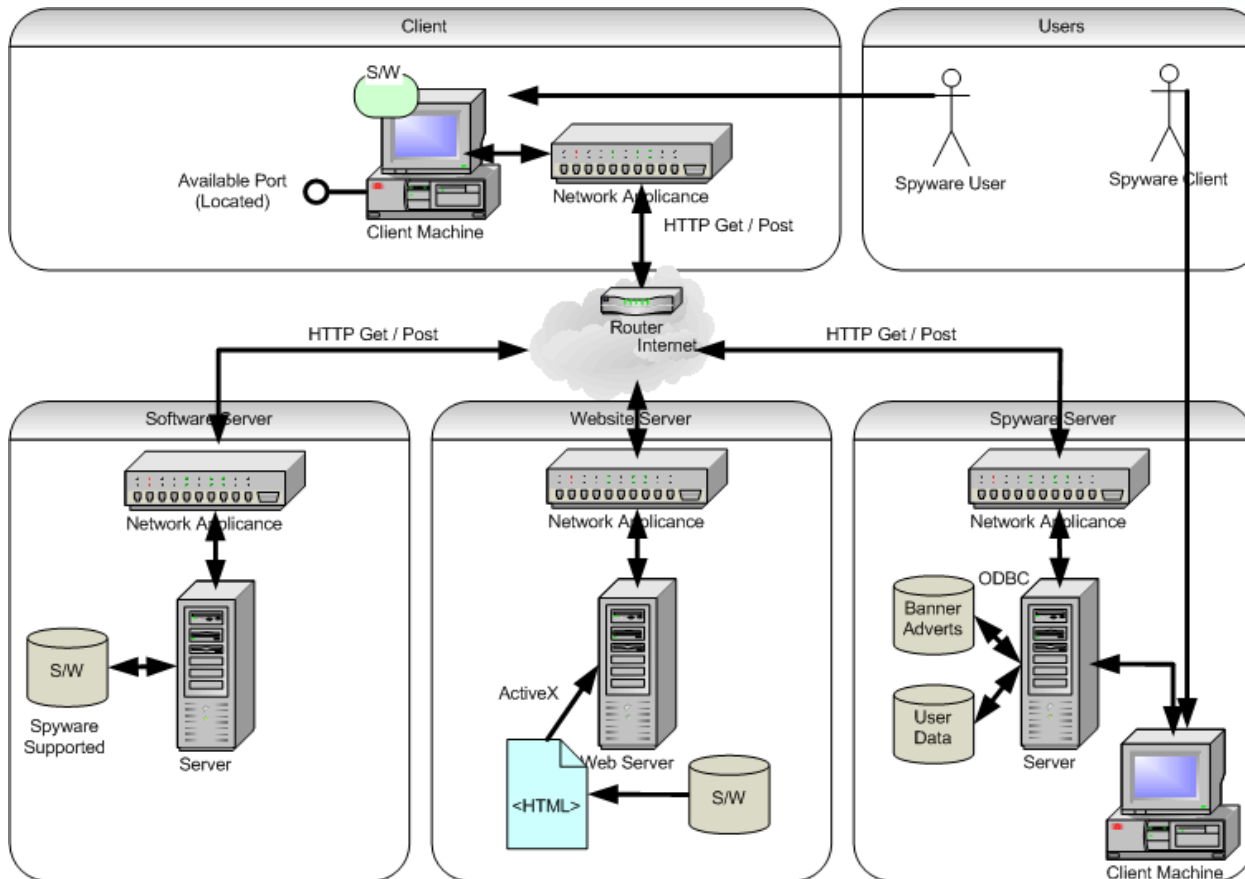
Example Pop-up

Misleading Pop-up



User Perspective - III

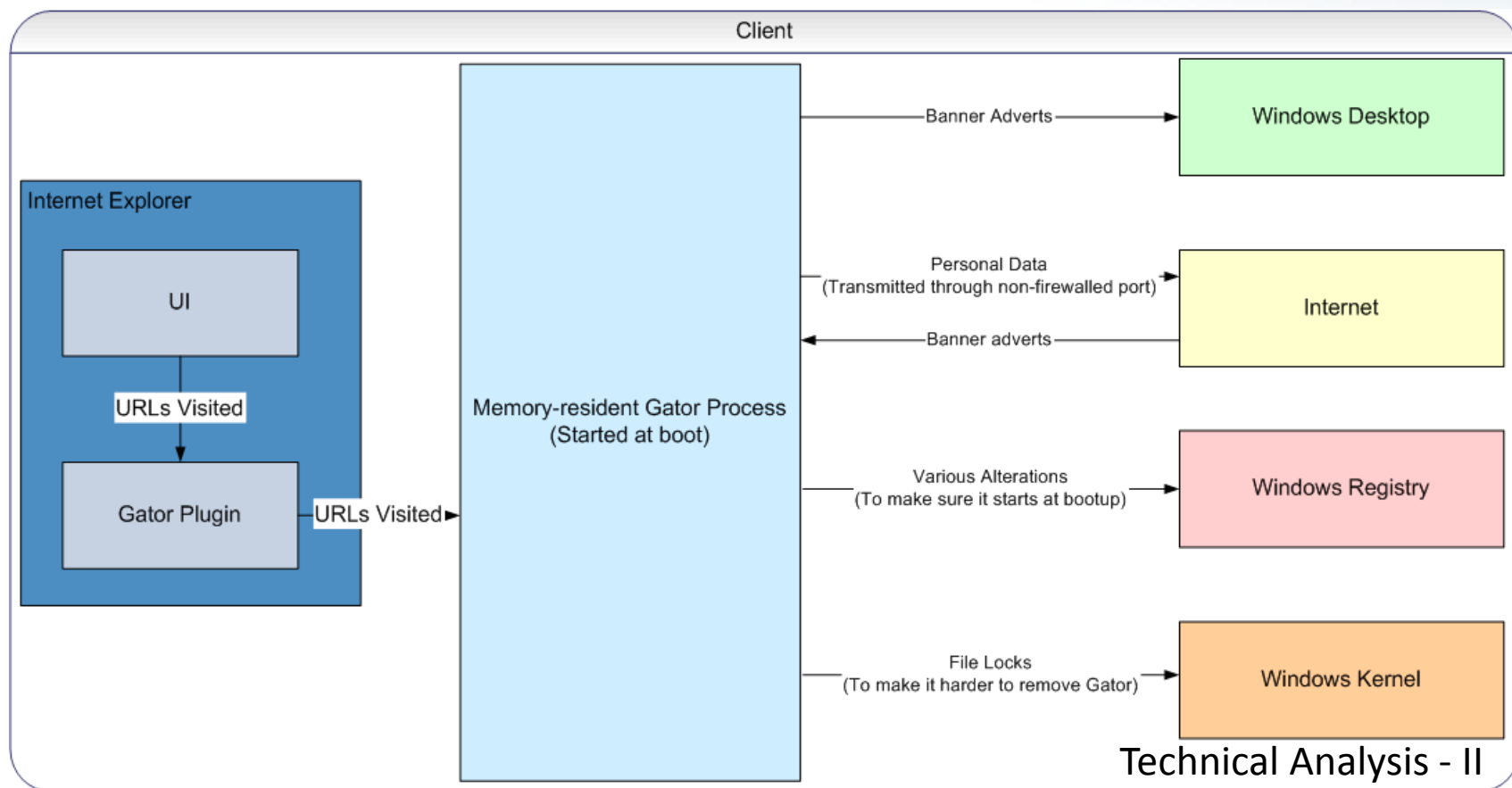
Network Overview



- Push
 - Advertising
- Pull
 - Tracking
 - Personal data

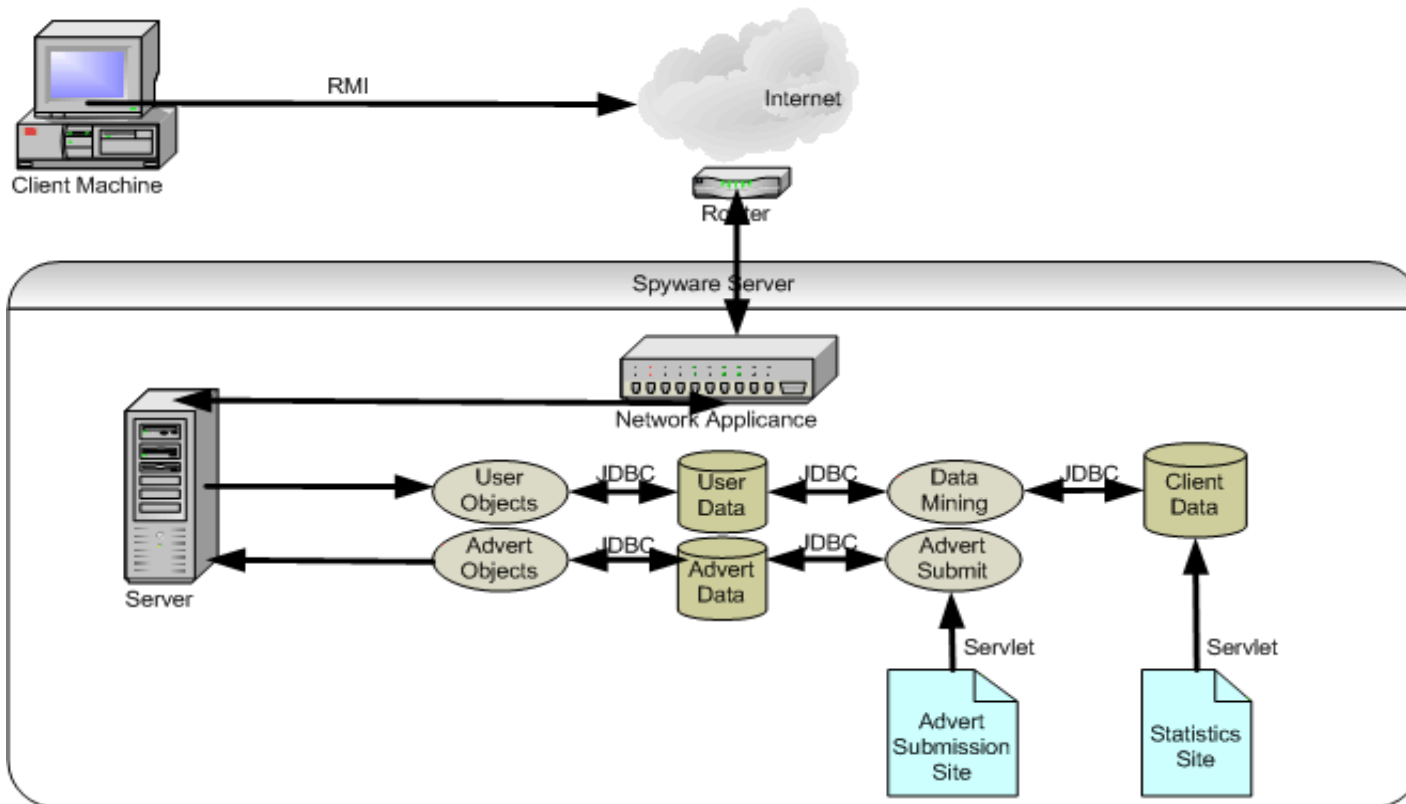
Technical Analysis - I

Client-Side Operation



Server-Side Operation

- Server-side operation is relatively unknown. However, if we were to develop such a system, it would contain...



Technical
Analysis - III

Spyware Defence

User Initiatives...

- **Issue Awareness**
- **Use Legitimate S/W Sources**
- **Improved Technical Ability**
- **Choice of Browser**
- **Choice of OS**
- **Legal action taken against breaches of privacy**
 - **Oct '16 Doubleclick**

Technical Initiatives...

- **Spyware Removal Programs**
- **Pop-up Blockers**
- **Firewall Technology**
- **Disable ActiveX Controls**
 - **Not Sandboxed**
- **E-Mail Filters**
- **Download Patches**

GAIN Case Study

- Installed IMesh, which includes Gator Installation
 - We accessed multiple internet sites
 - We simultaneously analyzed network traffic (using IRIS)
 - We found the packets of data being sent to GAIN
 - Packets were encrypted and we could not decrypt them
-
- See Example ->

IRIS v3.7

File View Capture Decode Filters Tools Help

Inis

- Capture
- Decode
- Guard
- Filters
- Logs

Decode

Hosts activity

- di.tnib.de (192.168.0.65)
 - TCP->CERT-RESPONDER (1640) (192.168.0.117)
 - TCP->HTTP (80)

No.	Date/Time (M:D:Y/h:m:s:ms)	Client	Server	Client port	Server port	MAC client	Bytes in	Bytes out	Total bytes
0	2:9:2004/11:29:2:093	19...	www.msn.com (207.68.173.254)	1806	80	00:03:F...	271	33133	33404
1	2:9:2004/11:29:6:265	19...	c.msn.com (65.54.140.158)	1808	80	00:03:F...	376	448	824
2	2:9:2004/11:29:6:421	19...	c.msn.com (65.54.140.158)	1809	80	00:03:F...	352	448	800
3	2:9:2004/11:29:6:531	19...	a.sc.msn.com (193.108.153.25)	1811	80	00:03:F...	992	16863	17855
4	2:9:2004/11:29:6:671	19...	a.sc.msn.com (193.108.153.25)	1812	80	00:03:F...	982	9213	10195
5	2:9:2004/11:29:7:750	19...	global.msads.net (212.187.162.158)	1815	80	00:03:F...	278	11946	12224
6	2:9:2004/11:29:7:796	19...	view.atdmt.com (64.14.128.201)	1816	80	00:03:F...	331	244	575
7	2:9:2004/11:29:8:562	19...	spe.atdmt.com (80.15.238.67)	1818	80	00:03:F...	322	5036	5358
8	2:9:2004/11:29:12:593	19...	ss.gator.com (64.157.165.173)	1820	80	00:03:F...	400	295	695
9	2:9:2004/11:29:20:015	19...	gbs.gator.com (66.35.229.217)	1822	80	00:03:F...	3592	448	4040

Find

```

POST /gbs/gbs.dll?GBL HTTP/1.1
Accept: */*
Content-Type: application/octet-stream
X-UA: WinInet 5.0.2614.3500, 1.1, 1.0
User-Agent: Gator/5.0
Host: gbs.gator.com
Content-Length: 3376
Connection: Keep-Alive

CB'' (
Éäv
L"i0*éu00/00] 4ÉÈxü0p'ÉšY"1sšKrlnfÄ0u0+*x0 =P-EO_>šF-NXpe1=ptÄ+8x0Eg'°šéäÖü+èèÈG.° [! [0È>Ri+u00' uáÉ0"0;<È
L"i0šcdZýcù0š
0v.ÈÈ{4
40+)Ä0n#YL0ÁŽ (N'Suf"zý0"òžOR.ž)Az#Èš0šZiq; 6ž0M(00'if{; äM0; JÈ0 (0{ie0"<é0)000"d"Ev, "š0e (yc%Á~; I00-Ñ"=i87
AÈK'L)Cy*0>yKLO0
0\ÄW: 'eu"É, iÁA) µ00
^@è iÜ0è*000.Xi0s.*š00] :0š0KIF#°'À"0«YÜm#ÈÈ00«av; p'šqÁš0s7È%!*RmR; 0"3Pfy69Á, ežiažp00/Ü±IIÄ0xU0 (^dueÈ0iÈ
uLYš0; (e0Y'; QšÈYya?"00x"i7; œ1"0b, °00È"±000žYcY-<'±'š500š0[>^000èš0Iq0?Y»Á"0-i.Yv.M:0hÈ70NSè]Èš"t %
Nžµ:000<0VYV; 0µ0'š0èñýBcI"b00Rq-0: 3.µ00ÄèZünž*µ'Iyb<0vNğr0, Lwt ÁG0-j0<{''; 000r+pl*Đj@šE; ái"0š"0; #ÜÈ0°
0, Ū,+6034-fHÈIuk"i/000è0-Á;-lñ*400%+Q00ÁB*X
0xN"šd, i ÈÜ=0ADz>ÜP#»Lz08W*ž"ÉšI: ^I00>0š%-š0=Yz| 0q00/nQè6FÜ'>0'<@:v0ÈÁ00'0n0Áÿ†È00«#X0|EHBšWÈš00 J0-<=
w0š0rB0µ0V; 6hššš0š00x <00zi-'i^ *P0iÄ0èVÈèfèš0; py.01š1Sy; 007-ÄEPqY»0H0he#010'FY0Fm=Á, ç"0°=?{K6Y#š6
Server: Microsoft-IIS/5.0
Date: Mon, 09 Feb 2004 11:29:21 GMT
  
```

Statistics

Links

Help

Did you know...
 You can set a default filter which to be loaded and applied upon IRIS's loading. To do that, go to Tools|Settings|Capture.

Spyware Removers

Ad-aware (by Lavasoft)

- Reverse Engineer Spyware
- Scans Memory, Registry and Hard Drive for...
 - Data Mining components
 - Aggressive advertising components
 - Tracking components
- Updates from Lavasoft
- Plug-ins available
 - Extra file information
 - Disable Windows Messenger Service



Vulnerable Systems

- Those with an internet connection!
- Microsoft Windows NT/2000/XP/Win7/8/10
- Android
- Less iOS
- Does not affect Open Source OSs
- Non - fire-walled systems
- Internet Explorer and other browsers not affected



Tracking Cookies

Cookies

- A Cookie is a small text file sent to the user from a website
 - **Contains Website visited**
 - **Provides client-side personalisation**
 - **Supports easy Login**
- Cookies are controlled by...
 - **Website's Application Server**
 - **Client-side Java Script**
- The website is effectively able to 'remember' the user and their activity on previous visits
- Spyware companies working with websites are able to use this relatively innocent technology to deliver targeted REAL TIME marketing, based on cookies and profiles

Case Study - DoubleClick

- Most regular web users will have a “doubleclick.net” cookie.
- Affiliated sites request the DoubleClick cookie on the users computer.
- The site then sends...
 - Who you are
 - All other information in your cookie file
- In return for...
 - All available marketing information on you - collected from other affiliated sites which the you have hit.

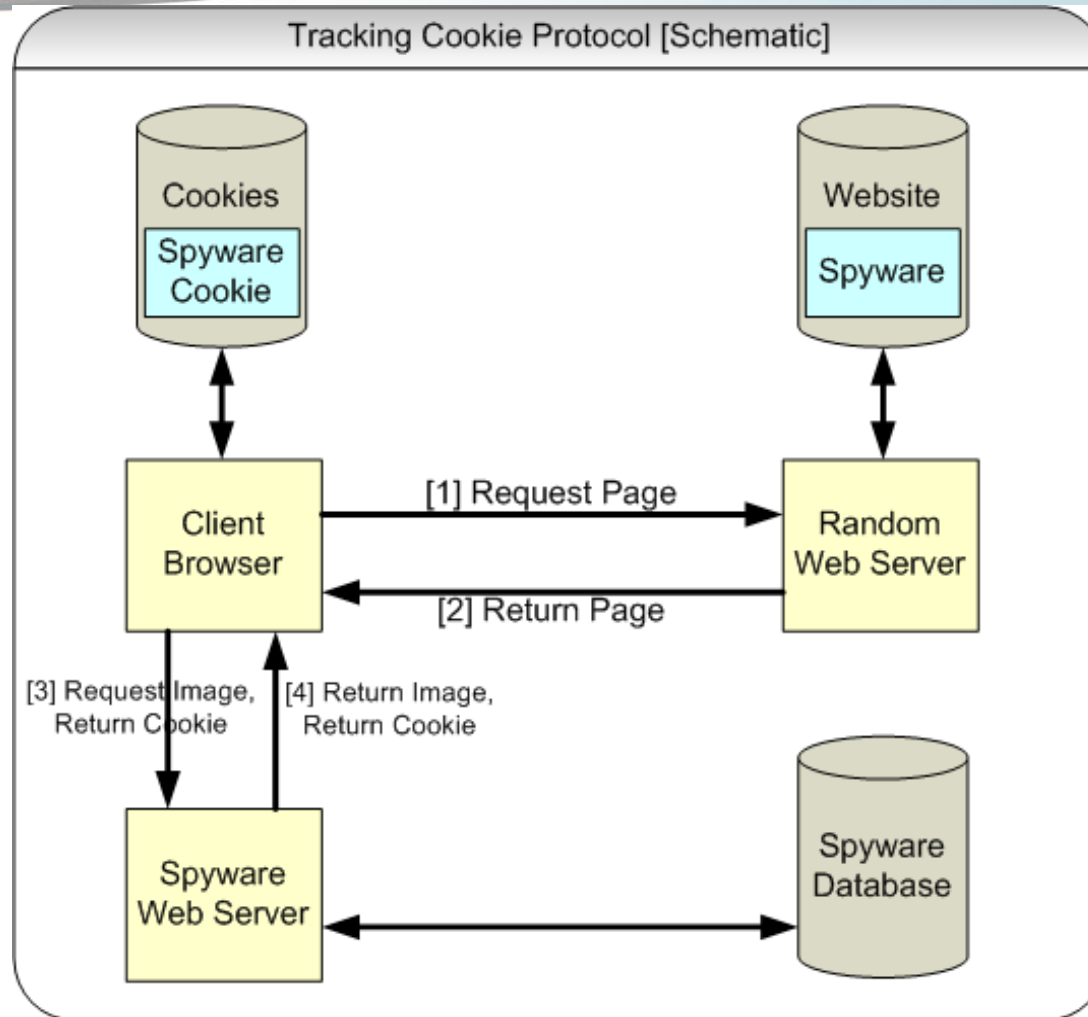
Case Study – DoubleClick

- Site targets banner adverts, e-mails and pop-ups to the user.
- If the user visits an affiliated site without a DoubleClick cookie, then one is sent to the user.
- The whole process is ‘opaque’ to the user and occurs without their consent.

Tracking Cookie Implementation

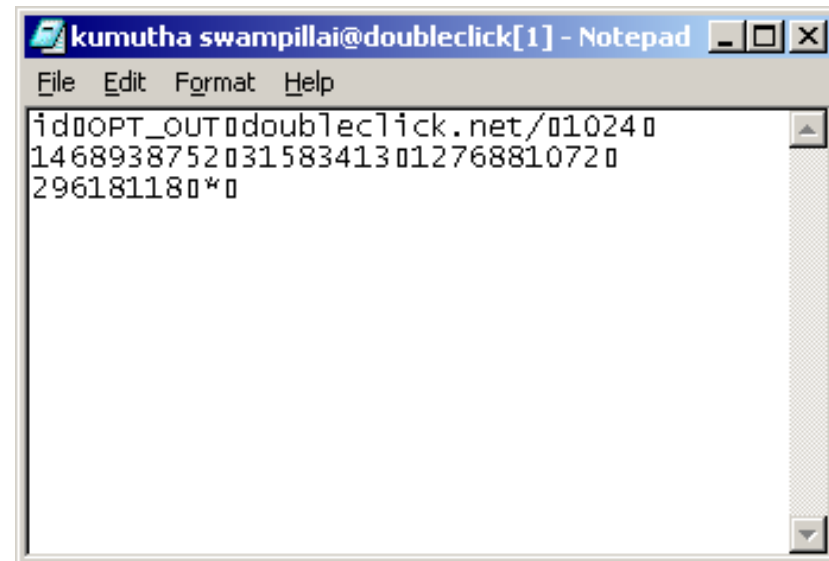
- Protocol designed to only allow the domain who created a cookie to access it.
- IE had a number of security holes...
 - Up to IE 5, domain names specified incorrectly.
 - Up to IE 6, able to fool IE into believing it is in another domain.
- Patches and IE solved a number of problems
- Since then, tracking cookies are still proving a large problem, there are still a number of holes still open.

Tracking Cookie Implementation



Tracking Cookie Defence

- Replace tracking cookies with write protected zero length files of the same name.
- DoubleClick offer an opt-out cookie, which can be obtained from their website.
- Disable cookies
 - Makes many websites unusable
- Delete cookies after session
- Spyware remover (Ad-aware)

A screenshot of a Notepad window titled "kumutha swampillai@doubleclick[1] - Notepad". The window contains the following text: "idOPT_OUTdoubleclick.net/102414689387520315834130127688107229618118*".

```
kumutha swampillai@doubleclick[1] - Notepad
File Edit Format Help
idOPT_OUTdoubleclick.net/1024
146893875203158341301276881072
29618118*
```



Trojan Horses

Installation

- Secretly installed when an infected executable is run
 - Much like a virus
 - Executables typically come from P2P networks or unscrupulous websites
- ActiveX controls on websites
 - ActiveX allows automatic installation of software from websites
 - User probably does not know what they are running
 - Misleading descriptions often given
 - Not sandboxed!
 - Digital signatures used, signing not necessary

Installation



- **Certificate Authority**
- **Misleading Certificate Description**
- **Who is trusted?**

Image Source – Screenshot of Microsoft Internet Explorer 6 security warning, prior to the installation of an ActiveX Control from "Roings".

Effects

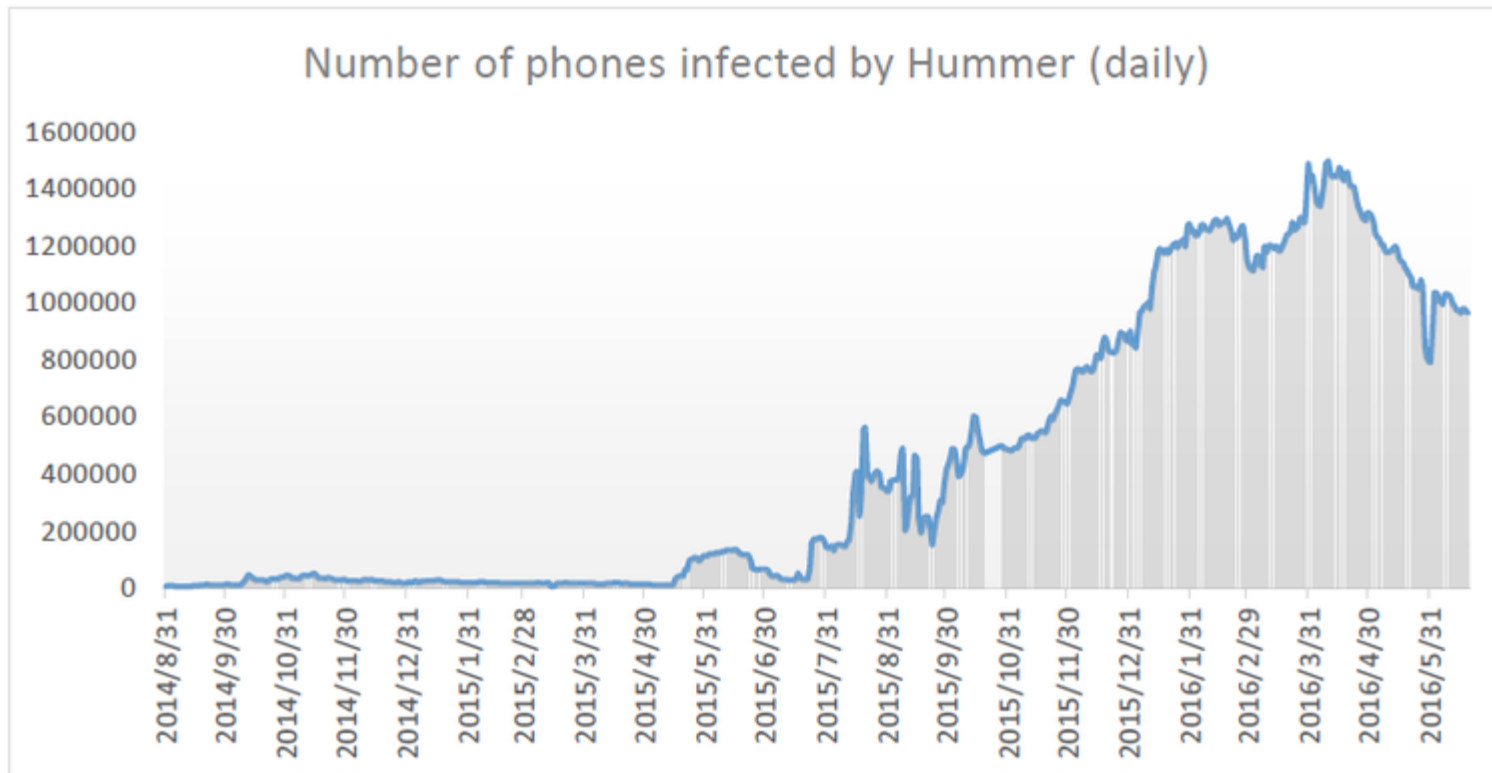
- Allows remote access
 - To spy
 - To disrupt
 - To relay a malicious connection, so as to disguise the attacker's location (spam, hacking)
 - To access resources (i.e. bandwidth, files)
 - To launch a DDoS attack

Operation

- Listen for connections
- Memory resident
- Start at boot-up
- Disguise presence
- Rootkits integrate with kernel
- Password Protected

Examples: Hummer

- based on an email address linked to the domains
- in several hours, the trojan accessed the network over 10,000 times and downloaded over 200 APKs, consuming 2 GB of network traffic



Examples: PluginPhantom

- steals many types of user information including: files, location data, contacts and Wi-Fi information.
- takes pictures, captures screenshots, records audios, intercepts and sends SMS messages
- can log the keyboard input by the Android accessibility service, acting as a keylogger.

- it is the first to use updating and to evade static detection
- abuses the legitimate and popular open source framework “DroidPlugin”, which allows an app to dynamically launch any apps as plugins without installing them in the system. PluginPhantom implements each element

Examples: Android's

CYBER.POLICE

- install malicious apps on a mobile device without any user interaction on the part of the victim

SpyNote

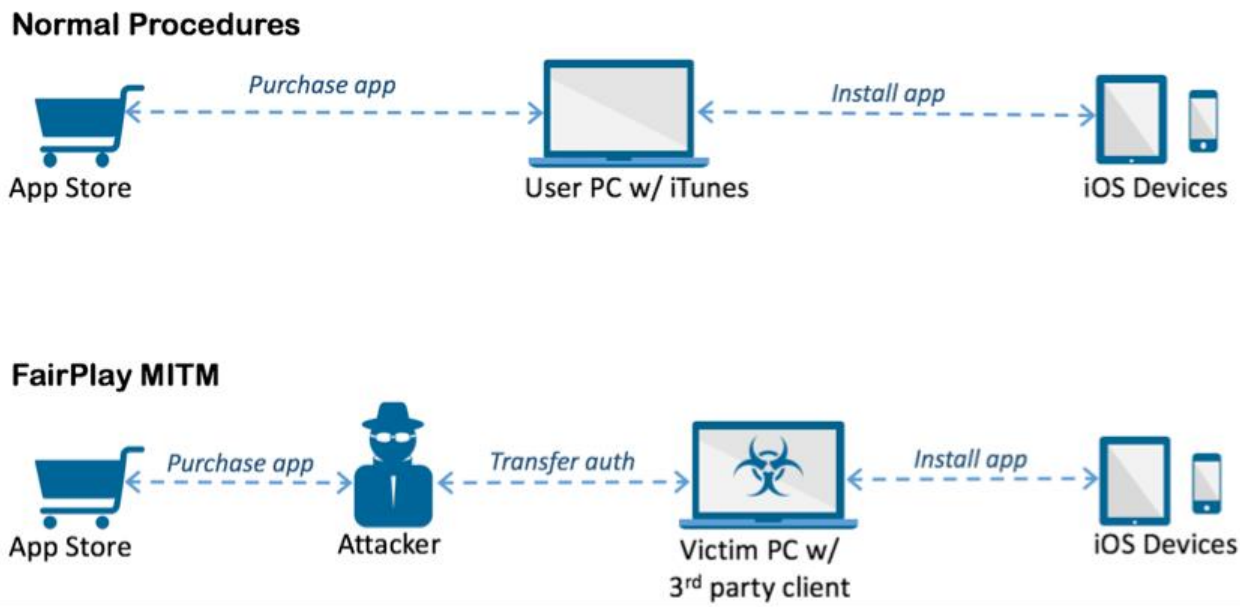
the ability to view all messages on a device, eavesdrop on phone calls, activate the phone's camera or microphone remotely or track the phone's GPS location. The APK (Android application package file) containing the remote access tool (RAT) SpyNote, gives an attacker complete access to a victim's phone



Examples: iOS

AceDeceiver

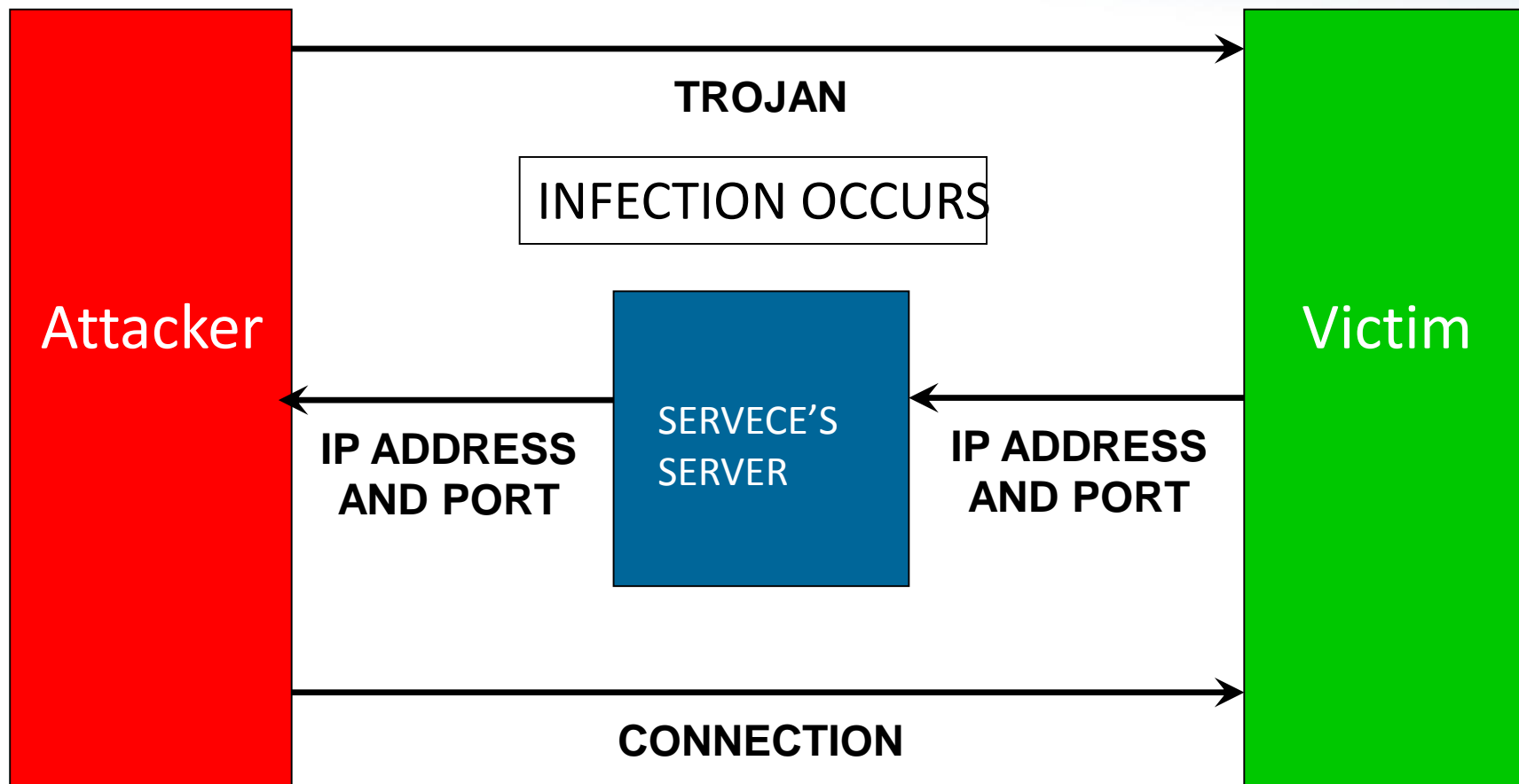
First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device



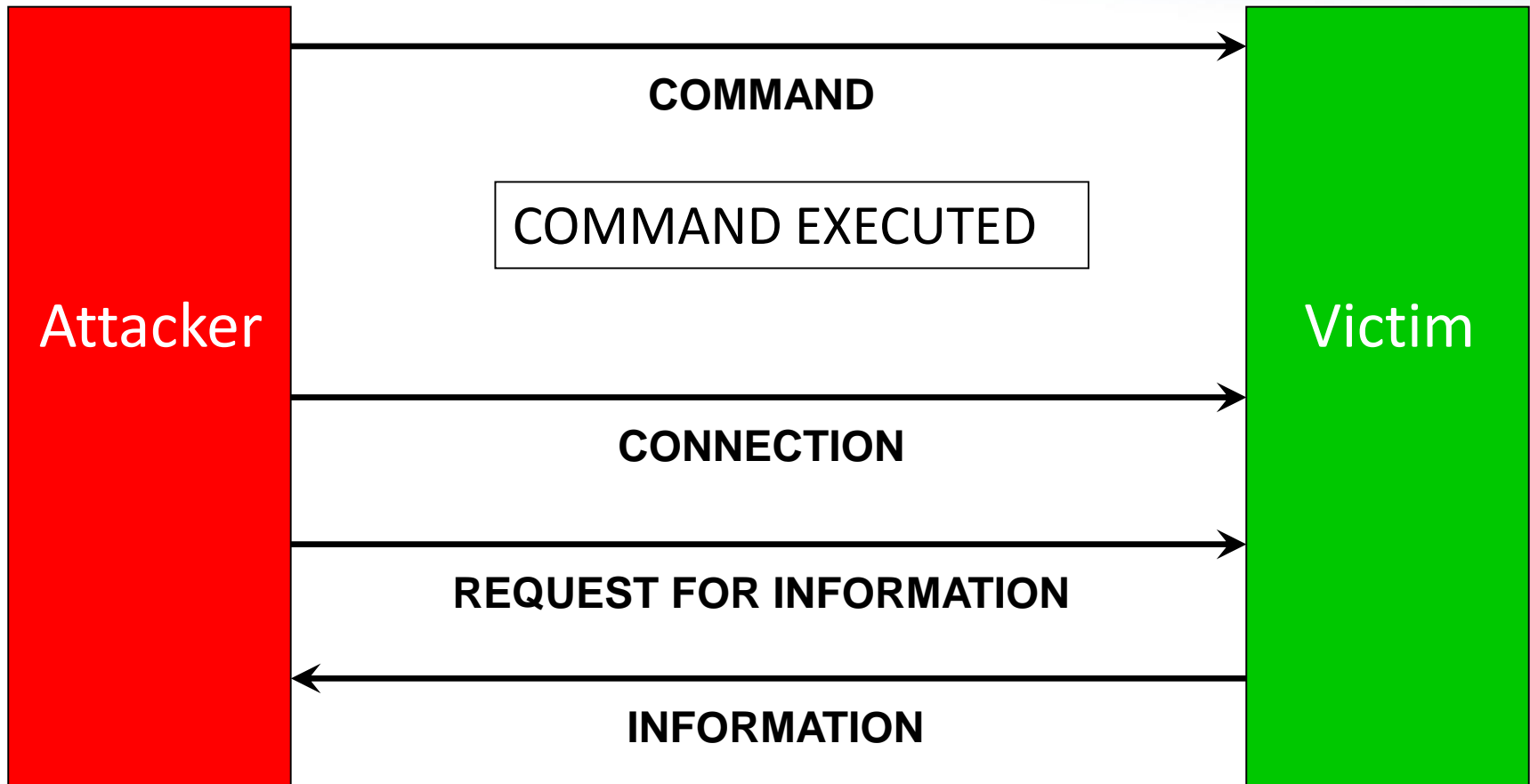
BO: Protocol

- Modular authentication
- Modular encryption
 - AES and CAST-256 modules available
- UDP or TCP
- Variable port
 - Avoids most firewalls
- IP Notification via. ICQ
 - Dynamic IP addressing not a problem

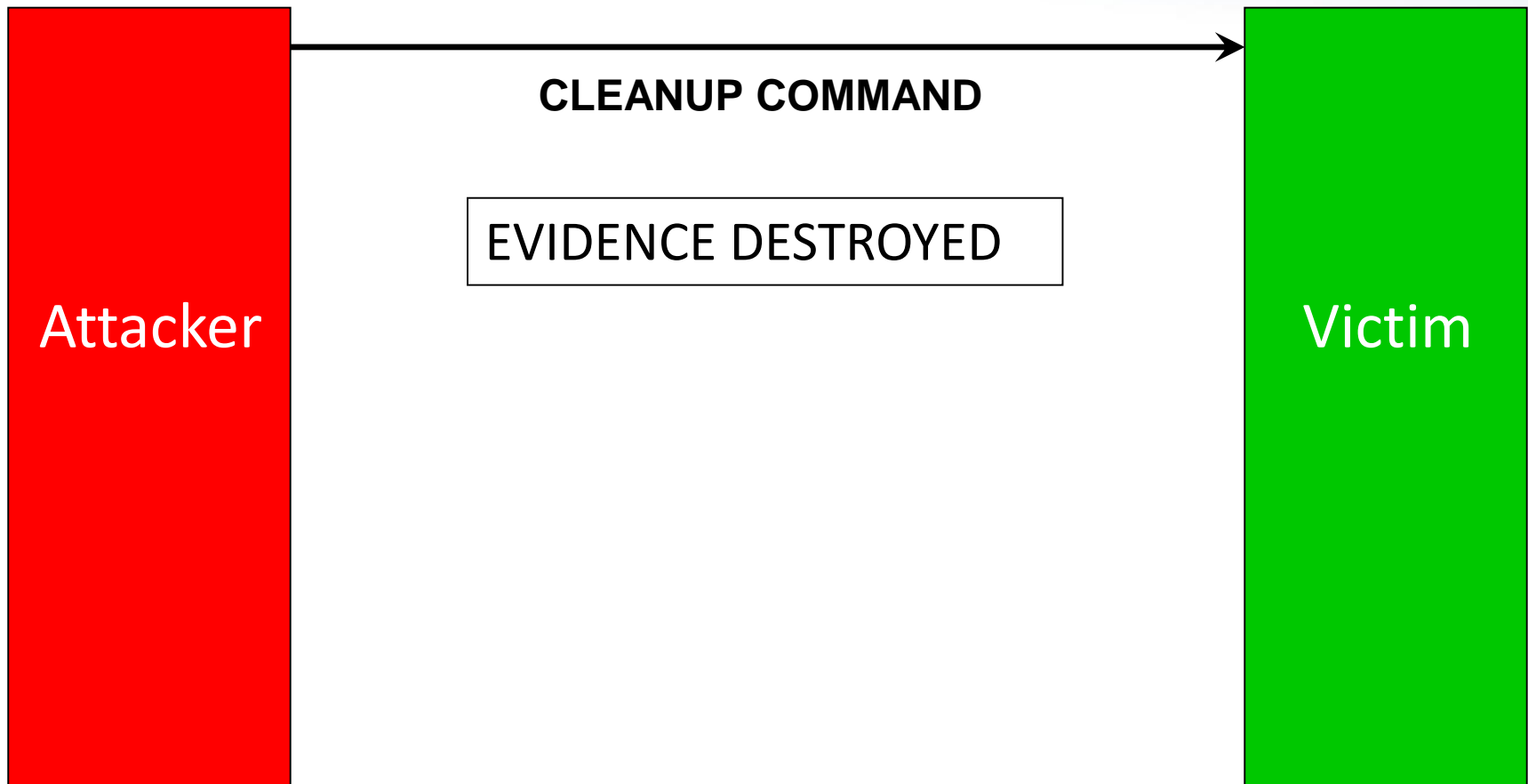
BO: Protocol Example (1)



BO: Protocol Example (2)



BO: Protocol Example (3)



Trojan Horse Examples

- M\$ Rootkit
 - Integrates with the NT kernel
 - Very dangerous
 - Virtually undetectable once installed
 - Hides from administrator as well as user
 - Private TCP/IP stack (LAN only)

Trojan Horse Examples

- iSpyNOW
 - Commercial
 - Web-based client
- Assassin Trojan
 - Custom builds may be purchased
 - These are not found by virus scanners
 - Firewall circumvention technology

Trojan Horse Examples

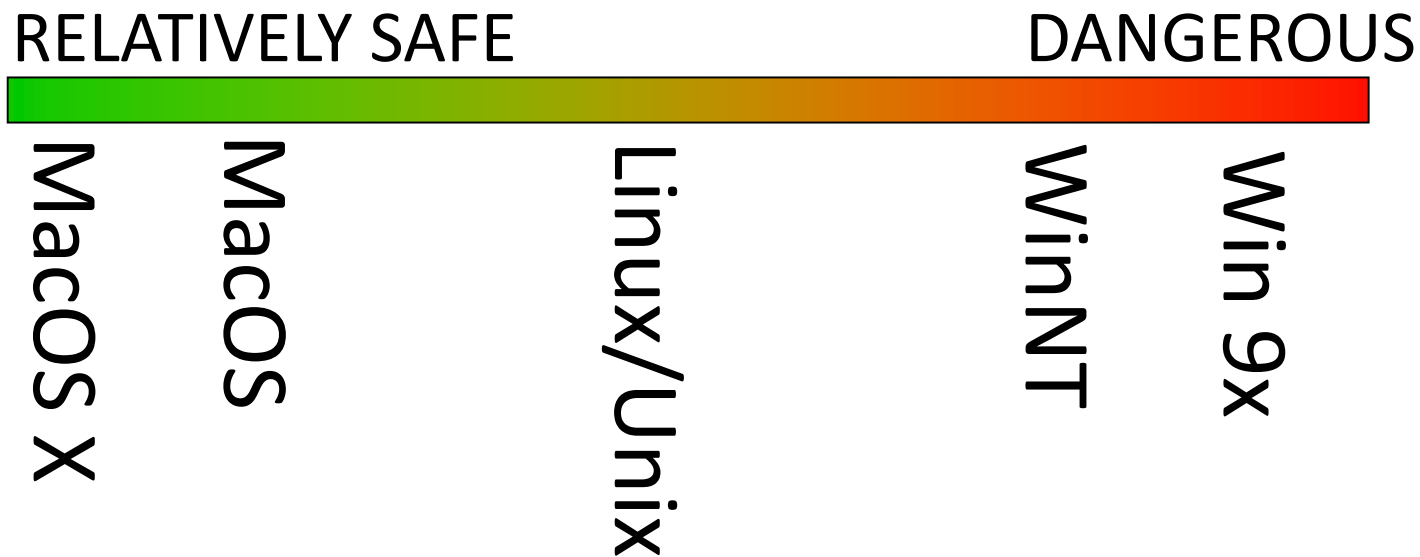
- Hardware
 - Key loggers
 - More advanced?
- Magic Lantern
 - FBI developed
 - Legal grey area (until recently!)
 - Split virus checking world

The background features a series of overlapping, semi-transparent blue shapes that create a sense of depth and movement. A prominent white curved line sweeps across the middle of the image, separating the blue abstract pattern from the white space below.

Demonstration

Vulnerable Systems

Number of trojans in common use...



WinNT refers to Windows NT 4, 2000, XP and Server 2003/8 , Winwdows 7/8/10.

Win9x refers to Windows 95, 95SE, 98 and ME.

Information Source: McAfee Security - <http://us.mcafee.com/>

Vulnerable Systems

Ease of compromise...

RELATIVELY SAFE

DANGEROUS



Linux/Unix

MacOS X

WinNT

MacOS

Win 9x

WinNT refers to Windows NT, 2000, XP , Server 2003/8, Winwdows 7/8/10.

Win9x refers to Windows 95, 95SE, 98 and ME.

Information Source: McAfee Security - <http://us.mcafee.com/>

Security Implications

Short Term

- Divulge personal data
- Backdoors into system
- System corruption
- Disruption / Irritation
- Aids identity theft
- Easy virus distribution
- Increased spam

Long Term

- Mass data collection
- Consequences unknown
- Web becomes unusable
- Web cons outweigh pros
- Cost of preventions
- More development work
- More IP addresses (IPv6)

Solutions

Short Term

- Firewall
- Virus Checker
- Spyware Remover
- Frequent OS updates
- Frequent back-up
- Learning problems

Long Term

- Add Spyware to Anti-Virus
- Automatic maintenance
- Legislation
- Education on problems
- Biometric access
- Semantic web (and search)

Firewalls

Network / Internet

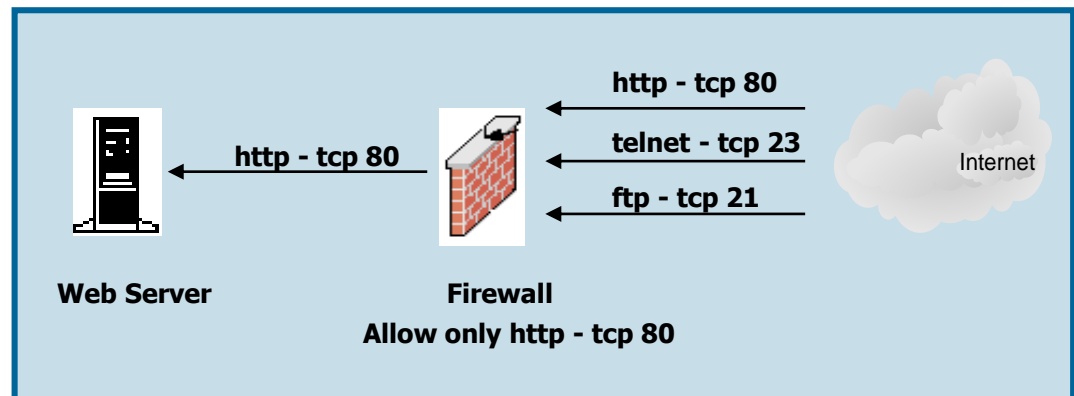
- **3 Types...**

- **Packet Filtering** – Examines attributes of packet.
 - **Application Layer** – Hides the network by impersonating the server (proxy).
 - **Stateful Inspection** – Examines both the state and context of the packets.
- Regardless of type; must be configured to work properly.
 - Access rules must be defined and entered into firewall.

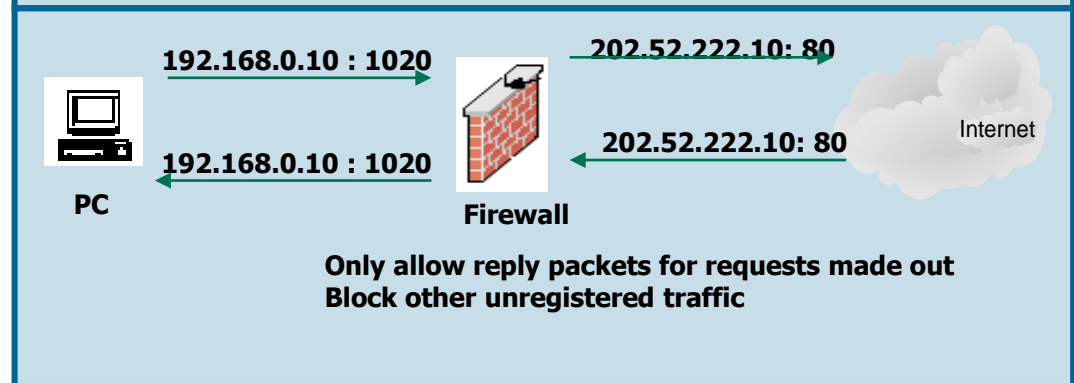
Firewalls

Network / Internet

Packet Filtering

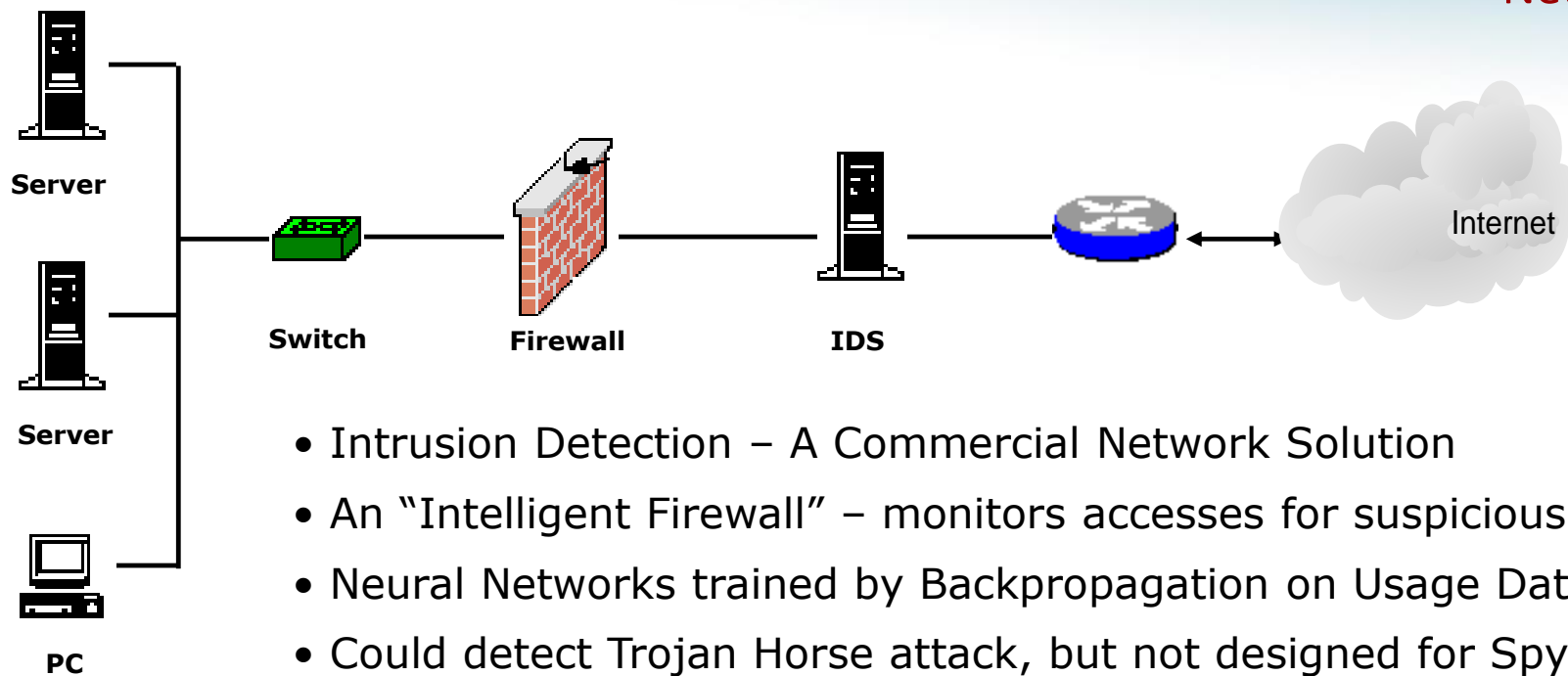


Stateful Inspection



Intrusion Detection Systems

Network



- Intrusion Detection – A Commercial Network Solution
- An “Intelligent Firewall” – monitors accesses for suspicious activity
- Neural Networks trained by Backpropagation on Usage Data
- Could detect Trojan Horse attack, but not designed for Spyware
- Put the IDS in front of the firewall to get maximum detection
- In a switched network, put IDS on a mirrored port to get all traffic.
- Ensure all network traffic passes through the IDS host.

“System X”

Network / Internet / Standalone

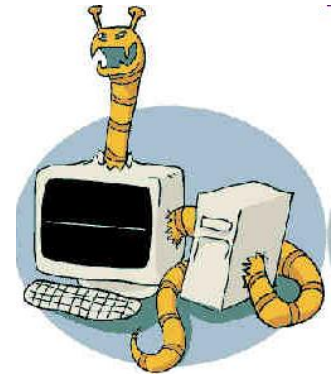
- Composed of...
 - Open Source OS
 - Mozilla / Opera / Lynx (!) Browser (Not IE)
 - Stateful Inspection Firewall
 - Anti-Virus Software
 - Careful and educated user
 - Secure permissions system
 - Regularly updated (possibly automatically)

Worms

Special features of the worms

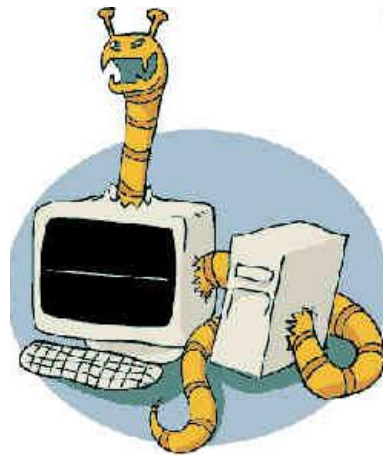
Viruses and Trojans require some human actions, such as sharing a USB stick, clicking on web sites, opening ;doc email attachments etc.

- spread is slow.
- Worms don't require human presence.
 - Spread is **MUCH** faster



Moreover worms do hack/break into computers, viruses and Trojans they use legitimate access channels and just abuse these privileges.

Famous Historical Worms - Unix



Morris Worm (first major network attack)

- Released November 1988
 - spreading on Digital and Sun workstations
 - exploited several Unix security vulnerabilities
- Consequences
 - no immediate damage
 - replication
 - load on network,
 - load on CPUs
 - many systems were shut down
 - fearing damage (only later people found it was not harmful)

***Morris - Author

Robert T. Morris, released it November 1988

- His father, another Robert Morris was
 - a cryptologist and code-breaker (broke codes for the FBI),
 - worked for the NSA “National Computer Security Center”,
 - wrote a book about UNIX Operating System Security (1984).

Morris Worm

- **program to spread worm**
 - looks for other machines that could be infected, several methods used: 'netstat -r -n', /etc/hosts,
 - when worm successfully connects, forks a child to continue the infection while the parent keeps trying new hosts
- **vector program (99 lines of C)**
 - re-compiled and run on the infected machines

Three ways the worm spread

- Sendmail
 - exploited debug option in sendmail to allow shell access
- Fingerd
 - exploited a buffer overflow in the fgets function
- Remote shell
 - reading list of trusted hosts known to local OS
 - password cracking

*sendmail

- Worm used debug feature
 - opens TCP connection to machine's SMTP port
 - invokes debug mode
 - sends a RCPT TO that pipes data through shell
 - shell script retrieves worm main program
 - places 40-line C program in temporary file called x\$\$,l1.c where \$\$ is current process ID
 - compiles and executes this program
 - opens socket to machine that sent script
 - retrieves worm main program, compiles it and runs



*fingerd

- written in C and runs continuously
- Array bounds attack
 - Fingerd expects an input string
 - Worm writes long string to internal 512-byte buffer
- Attack string
 - Includes machine instructions
 - Overwrites return address
 - Invokes a remote shell
 - Executes privileged commands

*remote shell

- Unix trust information
 - /etc/host.equiv – system wide trusted hosts file
 - /.rhosts and ~/.rhosts – users' trusted hosts file
- Worm exploited this information
 - assumed reciprocal trust: maybe Y trusts X as well..
- Password cracking
 - worm was running as daemon (not root) so needed to break into accounts to use .rhosts feature
 - read /etc/passwd, used 400 common password strings & local dictionary to do a dictionary attack

Not so bad...

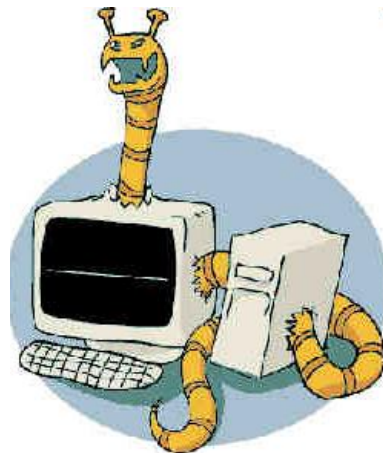
- Morris worm **did not**:
 - delete system's files,
 - modify user files,
 - install Trojans,
 - make any other use of cracked passwords
 - e.g. record or re-transmit elsewhere
 - it never took superuser privileges...

Detecting Morris Internet Worm

- Files
 - Strange files appeared in infected systems
 - Strange log messages for certain programs
- System load
 - Infection generates a number of processes
 - Password cracking uses lots of resources
 - Systems were reinfected => number of processes grew and systems became overloaded
 - Apparently not intended by worm's creator

Thousands of systems were shut down

Famous Windows Worms



Increasing propagation speed

- Code Red, July 2001
 - fascinating story, see Brad Karp slides
 - Released AFTER Microsoft released the patch
 - affecting like 500 000 hosts in hours
- SQL Slammer, January 2003
 - See Brad Karp too.
 - vulnerable population infected in less than 10 minutes
 - its growth was limited... by the speed of the Internet

Remark: both exploited an already known and already patched buffer overflow vulnerability!

Nimda worm

- Spreads via 5 methods to Windows PCs and servers
 - e-mails itself as an attachment (every 10 days)
 - runs once viewed in preview plane (due to bugs in IE)
 - scans for and infects vulnerable MS IIS servers
 - exploits various IIS directory traversal vulnerabilities
 - copies itself to shared disk drives on networked PCs
 - appends JavaScript code to Web pages
 - surfers pick up worm when they view the page.
 - scans for the back doors left behind by the "Code Red II" and "sadmind/IIS" worms

Nimda worm

- Nimda worm also
 - enables the sharing of the c: drive as C\$
 - creates a "Guest" account on Windows NT and Win7/8/10 systems
 - adds this account to the "Administrator" group.

Malware Defences



Virus Defenses

Today's "anti-virus software":

Just a name.

Virus + firewall + etc...

Defends against all sorts of malware.

classical viruses are only about 5% nowadays...

Tips

- do not execute programs obtained by email
- maybe do not install any new software
 - ???
 - very few software companies can be trusted to care about their customers,
 - lack of liability, lack of legal obligations, culture of irresponsibility, need to renew products range etc etc...
 - do they even understand how secure is their own software?



Automated Virus Defenses

White list:

accept only trusted digitally signed programs. Examples:
Sumsung Suit: OS updates, drivers, anti-virus

Prevalent methods in PCs:

- Black-list, signature-based detection.
- Networks firewalls
- control application calls and IPC
- monitor and prevent “privileged” system calls, e.g. registry modification, plug-ins install etc.
- track changes to executables (hash/MAC/sign)

Network Defences



Internet-Wide Defences

Cyberspace:

- a new dimension of national defense.
- a critical infrastructure

Goal: monitor the Internet at a larger scale, detect anomalies.

*Traditional Military Doctrine

- Each country has **3 frontiers**:
 - land
 - sea
 - air, space

as a consequence they have 3 armies.



Now, we have a new frontier, the digital frontier.
Shouldn't we have a fourth army?

- It would be totally useless and waste of money?
 - Arguably less than the 3 above (better technical education for young people).

Network Telescopes



Monitor traffic arriving at large sizeable regions of Internet address space. Reveals, e.g.,:

- “Backscatter”
= responses to randomly source-spoofed DDoS attacks
- Worms’ random scanning of IP addresses
- Attackers randomly scanning for a particular port, servers running a particular service, etc...

Examples:

- LBNL: $1/2^{15}$ of Internet address space
- UCSD/Univ. Wisconsin: covers $1/2^8$.

Questions