The golden age of hacking

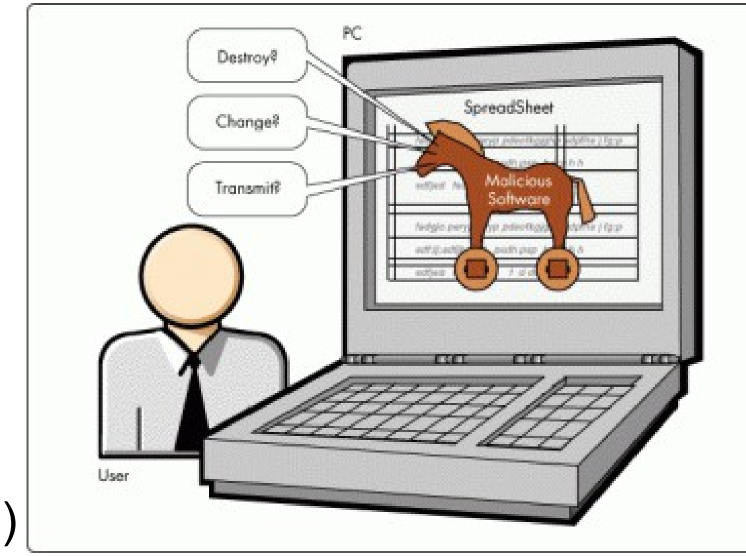
Maintaining access

Trojans

Backdoors

Rootkits

Trojan horses, backdoors and rootkits



- Trojan horses
  - Does just about anything
  - Be suspicious about freeware
- Backdoors
  - Ex. Netcat must be compiled with GAPING_SECURITY_HOLE option attach stdin/stdout to network (-e option)
- Trojans and backdoors = RAT (Remote Access Trojan)
- Application-level trojan
  - Separate application gives attacker control
- User-mode rootkit
  - Critical key system executables or libraries are replaced or modified in memory in order to hide attacker and form backdoors
- Kernel-mode rootkit
  - The OS kernel itself is modified in order to hide attacker and form backdoors

RATs

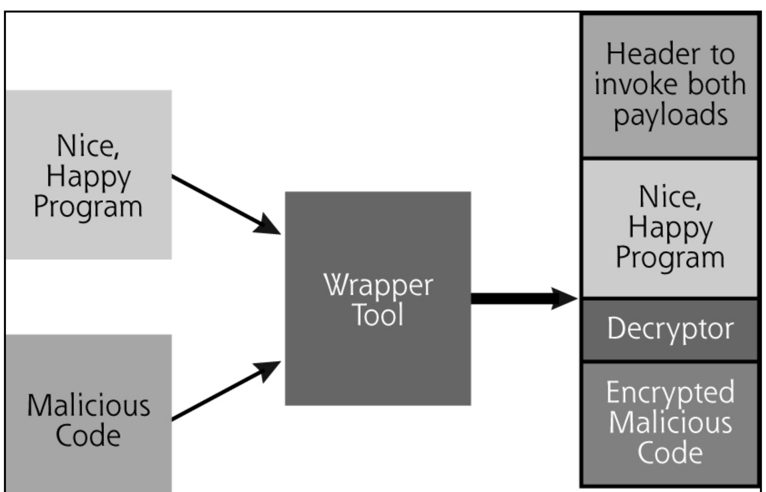
- Trojan horses are rarely used in penetration tests. However they constitute a large portion of the post exploitation process
- Trojan horses can be categorized into three main families
  - Binary (closed source) Trojans
  - Open Source Trojans
  - World Domination Trojans (bots – hybrid worms)
    - Includes built in spreading methods as Storm Worm (Storm botnet)
    - http://en.wikipedia.org/wiki/Storm_Worm
- Trojans can further be categorized depending on their connectivity architecture
  - Bind connection
  - Reverse connection
- More information about Trojan horses
  - http://en.wikipedia.org/wiki/Trojan_horse_(computing)

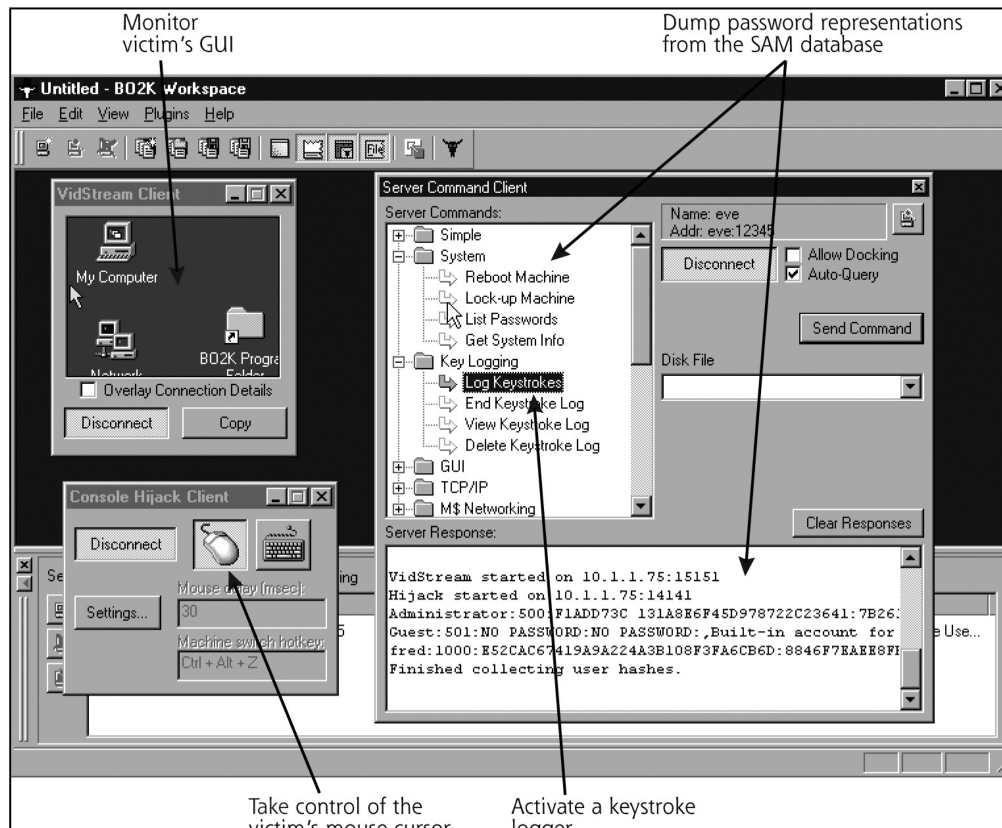
Advanced persistent threat (APT)

- **Advanced** – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.
- **Persistent** – Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.
- **Threat** – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded.

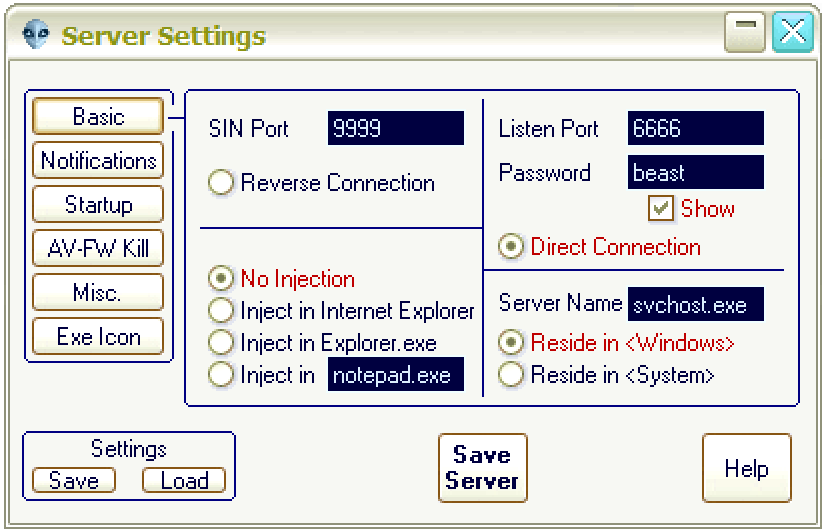
Trojan horses and backdoors I

- Remote control trojan backdoors - can do anything… almost
  - www.megasecurity.org - inventory and technical info of all backdoor tools
- Popular remote control tools
  - VNC (Virtual Network Computing) and Dameware mini RC
  - Back Orifice 2K - www.bo2k.com and SubSeven - www.subseven.org
- How get onto victim?
  - Mass or directed e-mail
  - Wrapper tools with morphing capabilities
  - Notification functionality

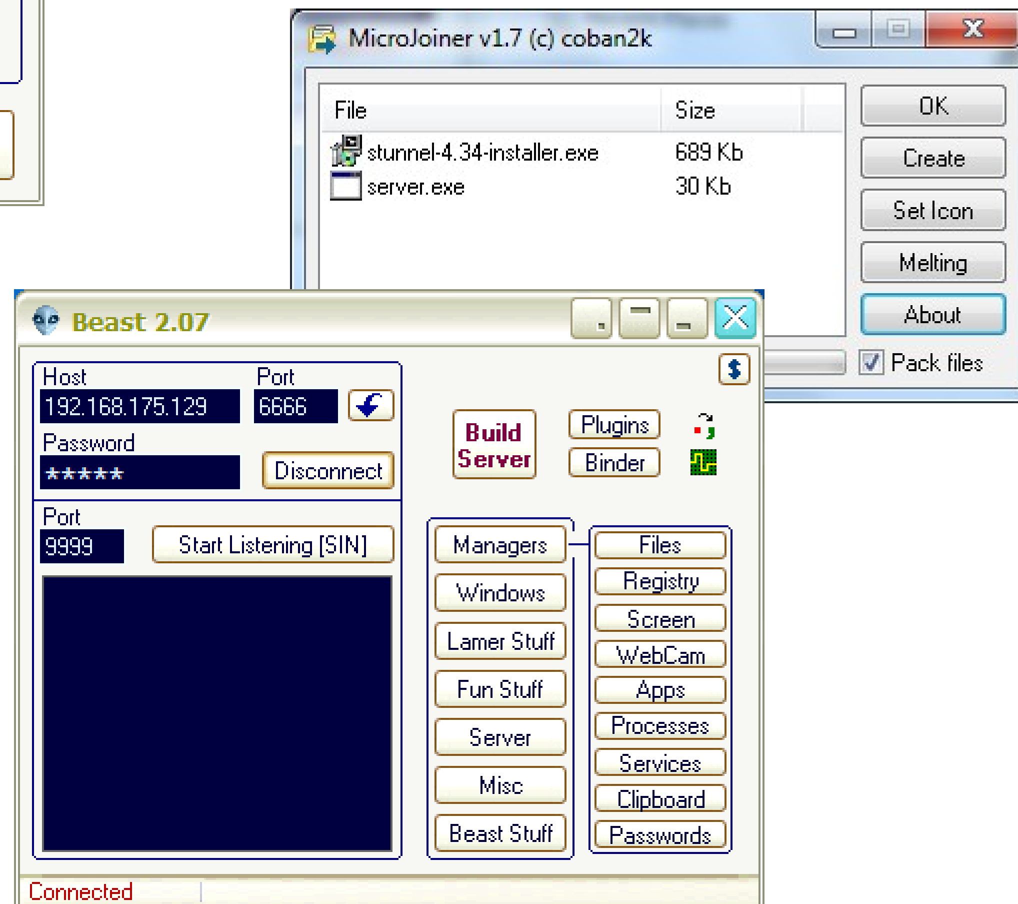




Beast RAT and MicroJoiner demo



- Configure and create server
- Join/bind evil and good file
- Distribute
- Take remote control



Spoofning and Phishing

- Spoofning
  - Use a forged sender address in the email which contain malicious code etc.
- Phishing
  - Try to acquire information such as usernames, passwords, and credit card details from web sites etc.

MS Program Security Section, 9/20/2003 07:05 PM -0400, New Security Update

Subject: New Security Update

FROM: "MS Program Security Section" <bsunoqplozaso@support.ms.net>
TO: "Commercial Consumer" <ilep.ivuomhed@support.ms.net>
SUBJECT: New Security Update
Date: Sat, 20 Sep 2003 19:05:35 -0400

Microsoft | All Products | Support | Search | Microsoft.com Guide

Microsoft Consumer

this is the latest version of security update, the "September 2003, C
which fixes all known security vulnerabilities affecting MS Internet Ex
MS Outlook Express as well as three new vulnerabilities. Install now
from these vulnerabilities, the most serious of which could allow an r
on your computer. This update includes the functionality of all previo

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest
How to install	Run attached file. Choose Yes on displayed dialog
How to use	You don't need to do anything after installing this i

Microsoft Product Support Services and Knowledge Base articles can
Microsoft Technical Support web site. For security-related informatior
products, please visit the Microsoft Security Advisor web site, or Con

Thank you for using Microsoft products.

Please do not reply to this message. It was sent from an unmonitored e-mail address a
any replies.

The names of the actual companies and products mentioned herein are the trademarks

Contact Us | Legal | TRUSTe

©2003 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Stateme

INSTALL.exe

Från: nordea@nordea.se [mrjk@bkkmail.com]
Skickat: den 4 oktober 2005 08:55
Till: Sfoe
Ämne: InternetBank NORDEA sakerhetssystem

Lägg märke till!

Extraförnyelse av elektronbetalingars säkerhetssystem!!

Ärade kunder av InternetBank NORDEA. Vi låtar komma
om vår bankens säkerhetssystem.

Den förnyade teknologi och den nya server tillåtar att gå
säkerhets nivå av era online-betalingarna.

Banken Nordea insisterar på det bindande förfarande att
upprepade autentifisering, för att få er personalinformatio
fort som möjligt på den nya, mera säker server av vår bai

För att få ert kontots normal funktions fortgång, behövar
konto på den nya server, som är skyddad, med utnyttjan
motsatt fall skall ert Internet konto blockeras provisoriskt
för er säkerhet för tillgångarsbortförande, för att undgå "F
antal, som stiger ständigt.

Ni har infört den felaktiga TAN kod (engångskod) var så s

http://www.nordea-se.com

From: UNIVERSITY EMAIL REGISTRATION UNIT <universitywebmailunit2@gmail.com>
To: undisclosed-recipients:
Subject: CONFIRM YOUR HOGSKOLAN DALARNA EMAIL ACCOUNT TO AVOID CLOSURE

Please Submit Your e-mail account information to this
E-mail: (universityaccountprocessunit2@live.com)

DEAR HOGSKOLAN DALARNA webmail holders

This is a message from the HOGSKOLAN DALARNA
Carolina WEBMAIL ACCOUNT Message Center for
Communication to all of our HOGSKOLAN DALARNA
Webmail owners.

We are currently working on our database e-mail
In users.We are delecting all old unused
HOGSKOLAN DALARNA Webmail Account,

for more space for new users. To prevent your account not be
deleted from our database you are advised to confirm
your HOGSKOLAN DALARNA webmail account
immediately.

Submit your account information below

Login Website ....
Username :..........................
Password ....
Date of Birth: ....
Country or territory: ....

Warning! E-mail owners who refuse to submit E-mail
account details, within seven days from this date
of receipt will loses his/her Webmail account
permanetly.

Thank you,

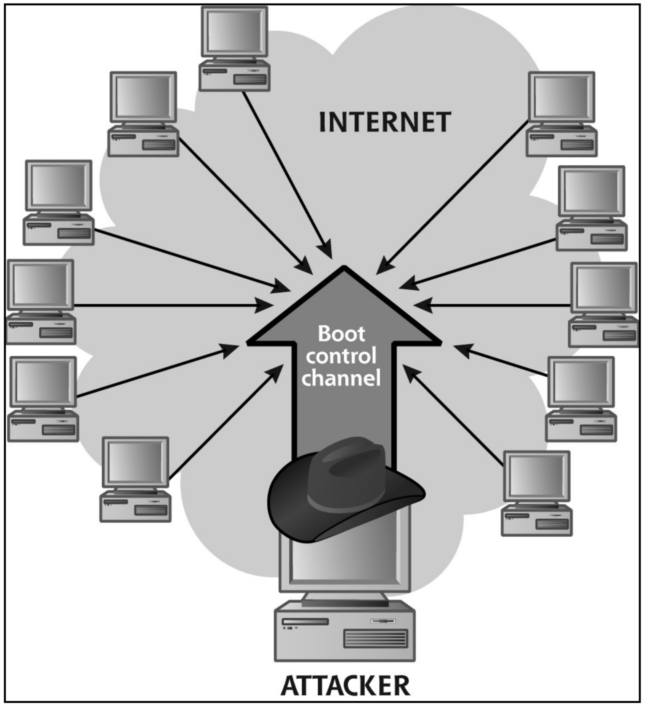
HOGSKOLAN DALARNA
Webmail Team

Please Submit Your e-mail account information to this
E-mail: (universityaccountprocessunit2@live.com)

CONFIRM YOUR HOGSKOLAN DALARNA EMAIL ACCOUNT TO AVOID CLOSURE

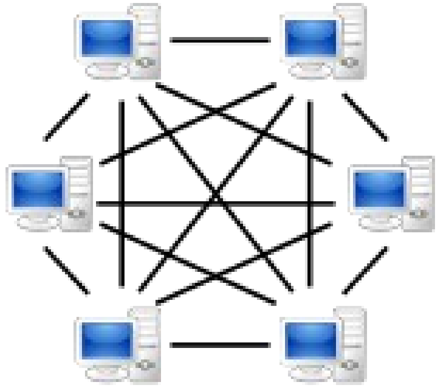
Trojan horses and backdoors II

- Via web sites
  - ActiveX controls – no sandbox
  - Signed with MS authenticode - possible to disable by user
- Phishing and URL obfuscation
  - <A HREF="http://badwebsite.com">goodwebsite.com</A>
  - URL shortening – tinyurl.com/site_url and bit.ly/site_url
  - URL in hex or Unicode "%77%77%77%2e…
  - Javascript which decode URL/message
  - Fake SSL certificates
- Controlling many trojans - bots
  - Bot-nets
  - Bot-herder
    - Controlling thousands of victims
  - History of the IRC bots
    - http://en.wikipedia.org/wiki/IRC_bot



Bots I

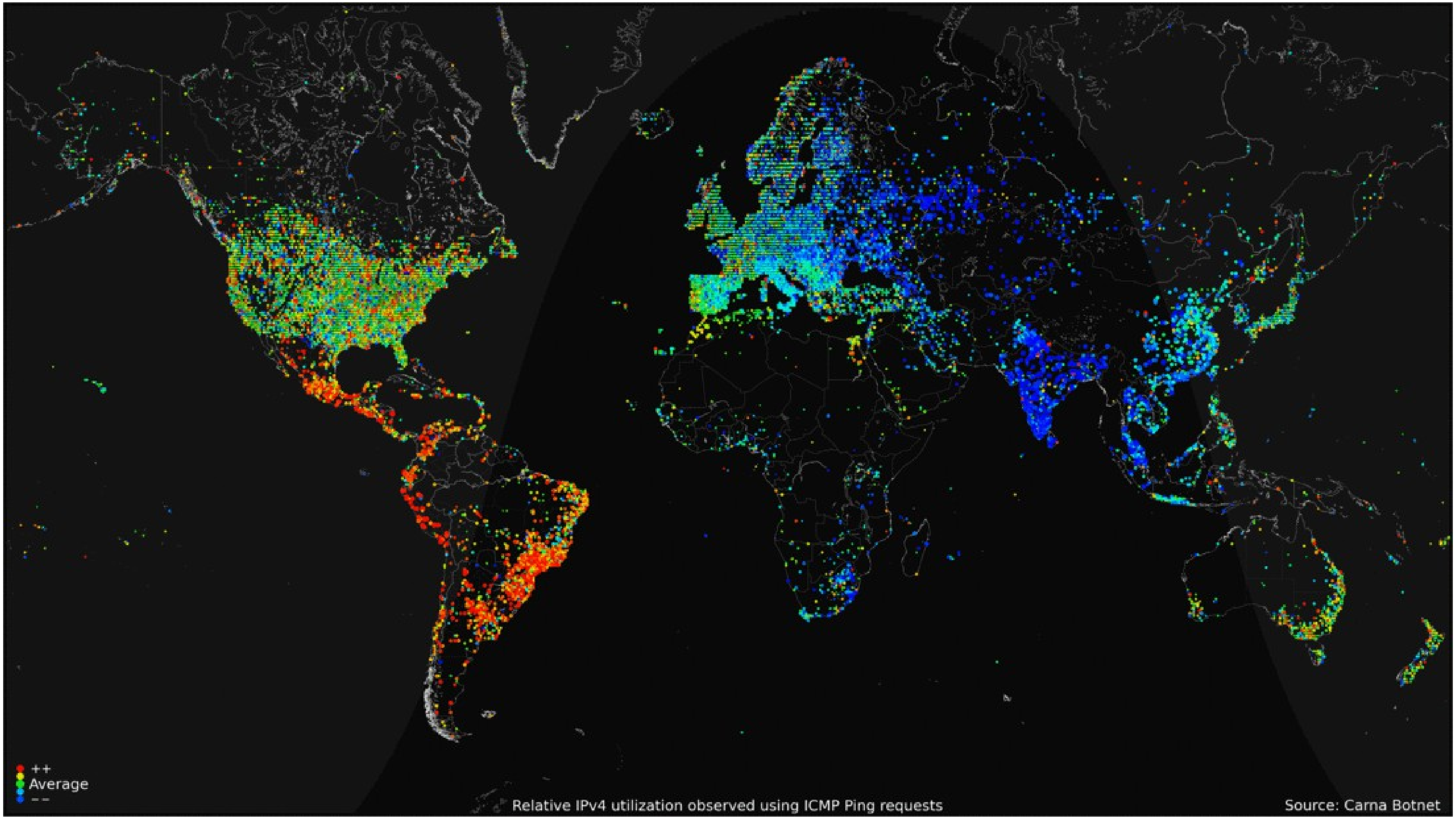
- Modular code usually controlled over IRC
- Sdbot - Zotob
  - http://en.wikipedia.org/wiki/Zotob_%28computer_worm%29
- Phatbot - Agobot, gaobot… > 500 variants, > 100 functions
  - http://en.wikipedia.org/wiki/Agobot_%28computer_worm%29
  - All the common trojan functionality – plus
    - DDoS flood attacks
    - Vulnerability and port scanning, sniffing
    - File morphing and rootkit installer
    - Information gathering, spyware
    - HTTP client - anonymizing HTTP proxy
    - SMTP client - e-mail address harvester, spamming



- WASTE - peer-to-peer (P2P) bot-control
- Virtual machine environment awareness
- Rxbot - “Analysis of RXBOT” thesis
  - [server]\malware\bots, source code attached, a good read!

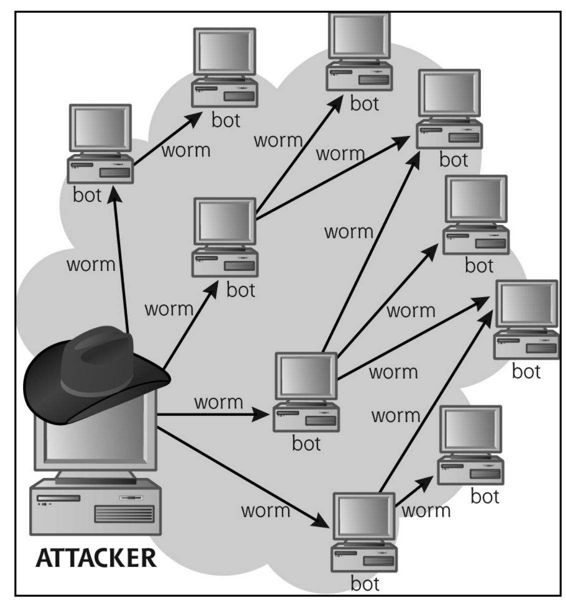
Bots II

- World map of 24 hour relative average utilization of IPv4 addresses observed using ICMP ping requests
- Carna Botnet: http://en.wikipedia.org/wiki/Carna_Botnet



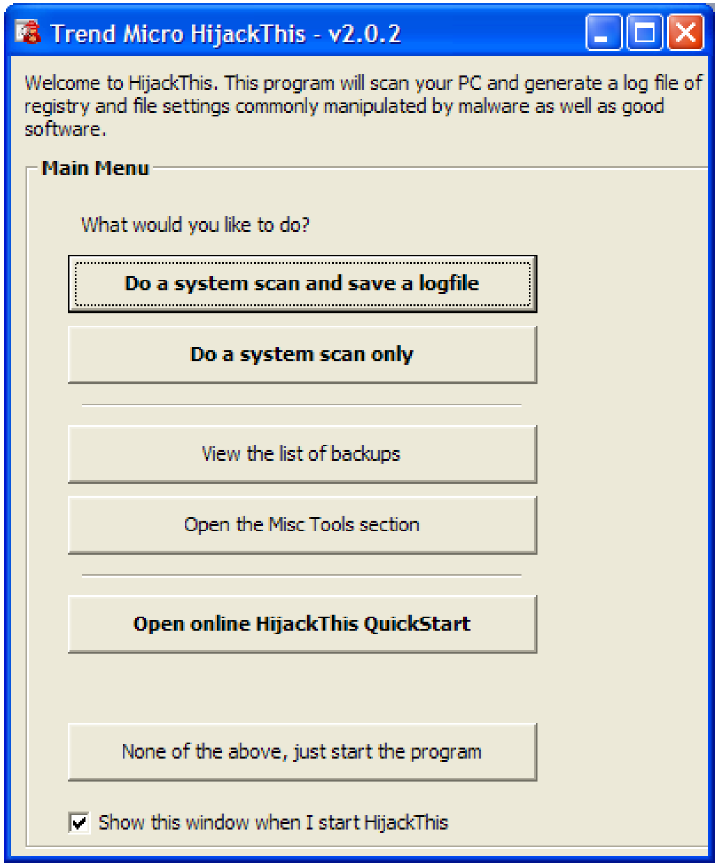
Bots, worms and spyware

- Spreading bots with worms
  - Worm = automatic self replicating
  - Having the bot as payload
  - Via buffer overflows and e-mail is common
- Spyware - may grab and pull
  - Surfing statistics/habits
  - Personal info
  - Filter web search results
  - Logging keystrokes
  - Show customized ads and pop ups
  - Usually bundled with free/needed add-ons, games etc.
- Defense
  - Be suspicious of to good to be true deals
  - Check for unusual open ports



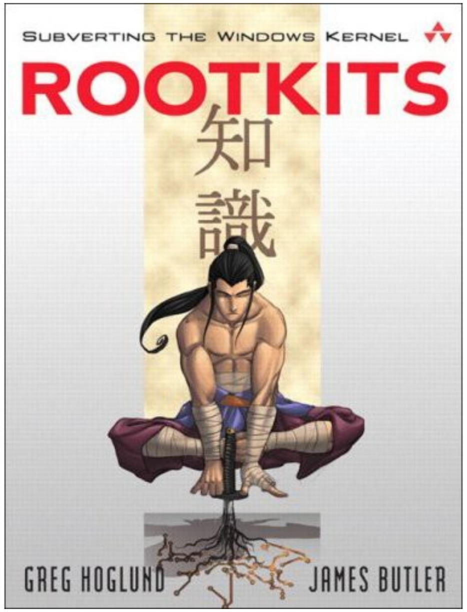
Defense cont.

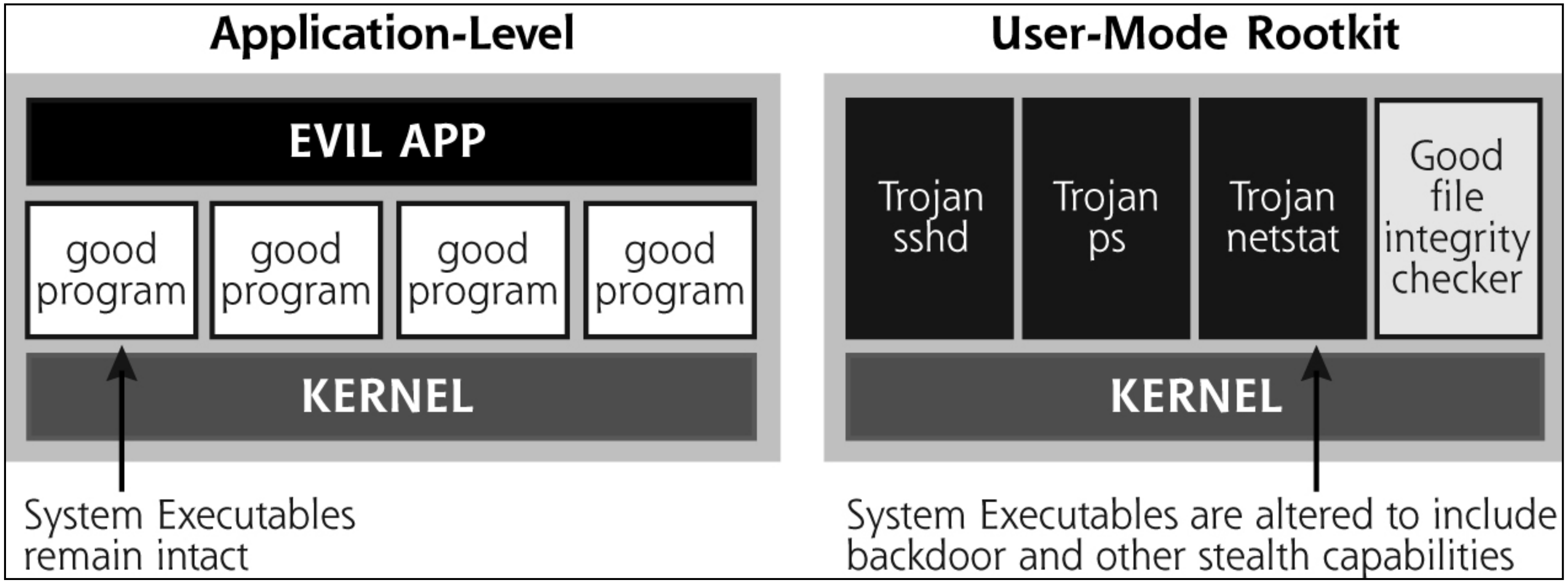
- Antivirus programs – the bare minimum
  - AVG, Avira and Avast! are free good offers
  - Microsoft Security Essentials / Defender are good as well
  - http://en.wikipedia.org/wiki/List_of_antivirus_software
- Trusted software
  - Digital fingerprint (hash)
  - Code signed (certificate)
- User education
  - Web browser configuration
  - Phishing attacks
- Potentially Unwanted Programs (PUPs)
  - Ad-aware
  - Trend Micro



User mode rootkits

- Unix - alters or replace existing OS software
- Windows – alters the process memory
- Purpose is to hide and maintain access to system via trojans etc.
- Rootkit downloads
  - Must look for mirrors now
  - http://www.rootkit.com





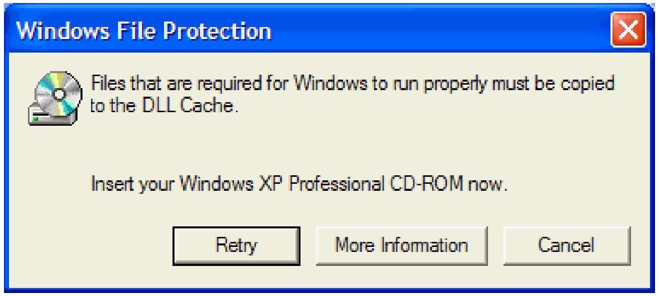
as Tripwire

Unix/Linux user mode rootkits

- Usually replaces critical OS files as
  - Login, sshd
    - Contains hard-coded backdoor password with root access
    - Skips updating utmp and wtmp files (who, last)
  - Ifconfig
    - Sniffers
      - Check if network card is in PROMISC mode
  - Du, find, ls, netstat, ps, syslogd, md5sum etc.
  - Detection
    - Check for foreign strings in executables
    - Modified size is sometimes the same so Tripwire is better!
- Lrk6 and shv4 are popular rootkits
  - Have trojan horses of many OS files
  - http://packetstormsecurity.org/UNIX/penetration/rootkits/

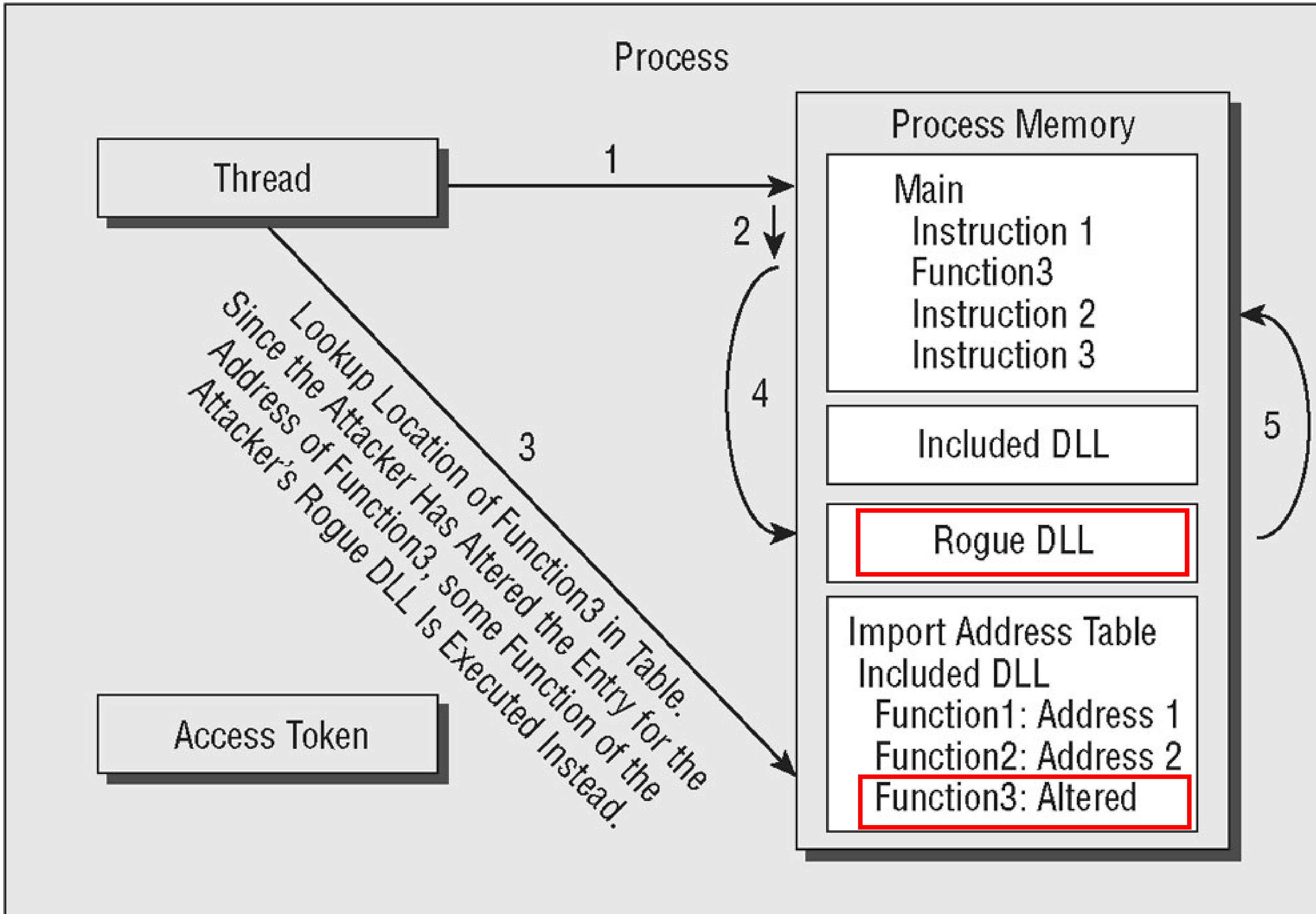
Windows user mode rootkits I

- Usually altering the memory of running OS processes instead of changing executable file
  - Windows File Protection (WFP)
    - Difficult to fool
    - http://support.microsoft.com/kb/222193
  - Easy API to connect to another process and change behavior and capabilities (debug rights which admins got default)



- A handful of API calls to Windows system libraries supports most of the programs admins use
  - ntdll.dll
- The rootkit overwrites the address these calls point to so it instead point to attackers code, called: API hooking
  - http://www.hook-api.com/
  - http://jacquelin.potier.free.fr/winapioverride32/

Hooking and DLL injection

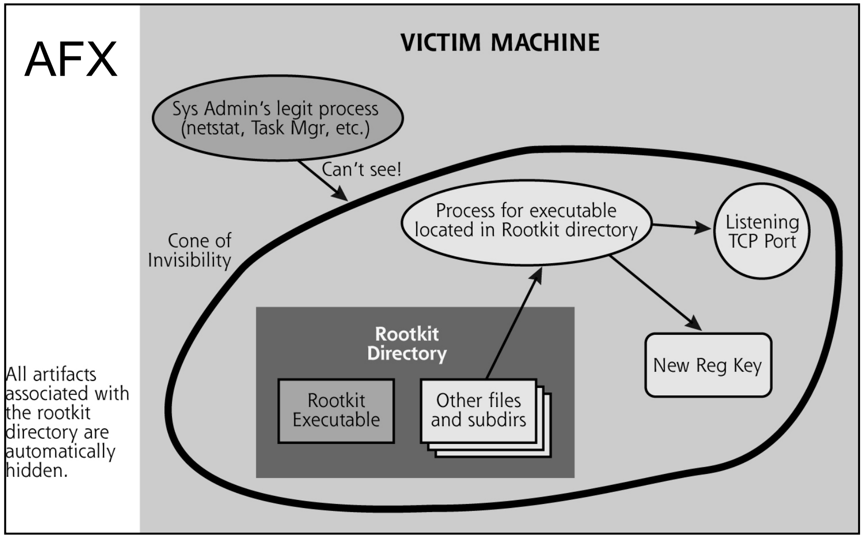


Windows user mode rootkits II

- Ex. task manager call
  - Task manager make API call to NtQuerySystemInformation … to get a list of running processes
  - Attackers code intercept and filters out attackers processes
- Most popular API calls used by rootkits
  - NtQuerySystemInformation
    - Hide particular running process
  - NtQueryDirectoryFile
    - Hide particular files
  - NtEnumerateKey
    - Hide particular registry keys
  - NtReadVirtualMemory
    - Prevent rootkit-detection tools detecting hooked API-calls
- Backdoors and other nasty stuff is of course included

Hacker Defender and AFX rootkits

- HXDef INI-config file where everything is controlled
  - Hiding files, processes, system services, system drivers, registry keys/values and TPC/UDP ports via a configuration file
  - Lying about free disk space
  - Hiding the alterations in processes when debugging
  - Remote access backdoor and relay/redirector functions as in Netcat
  - Backdoor intercept other programs listening on ports
    - Almost all present network services will be potential backdoors!
    - http://rootkit.com/newsread.php?newsid=60
- AFX
  - Generates a system patch that hides what is filtered by attacker



  - http://rootkit.com/newsread.php?newsid=194

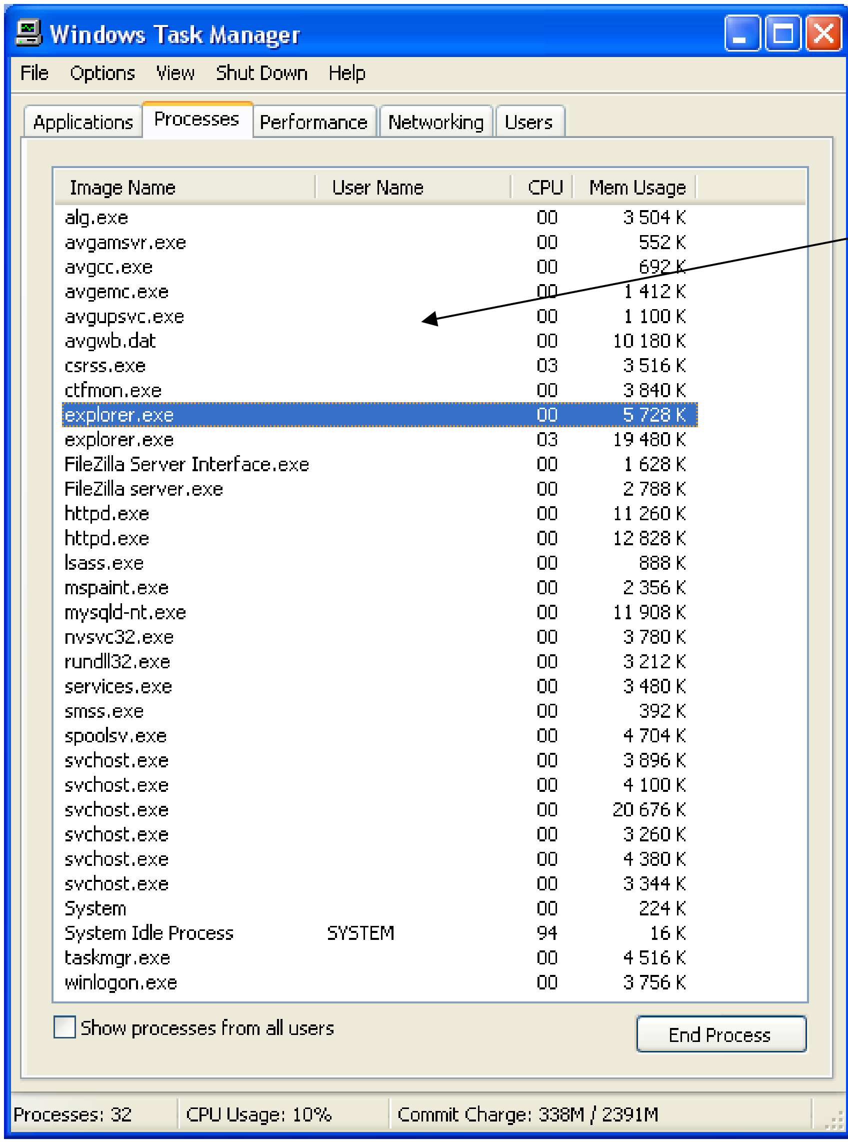
Hacker Defender I

- Case review: My XP got root-kitted!
- Windows XP SP2 (WAMP), DMZ
  - Apache 2.2, MySQL 5.0, PHP 5.21
  - FileZilla, AVG Free

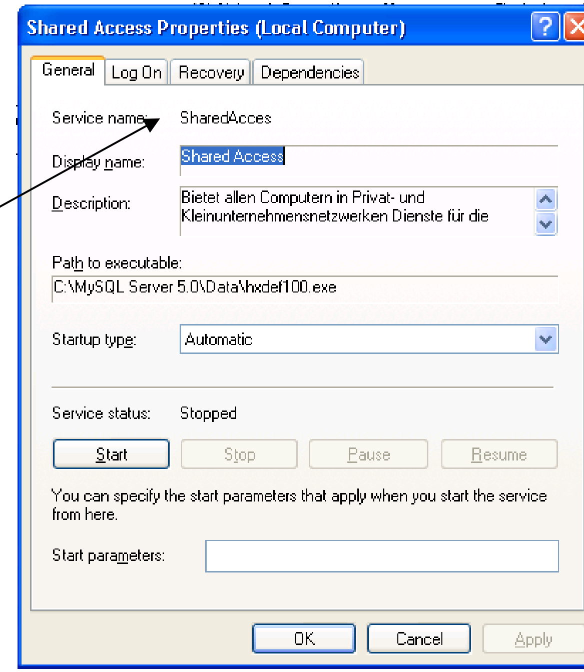
- Suspect behavior
  - Services down, unstable etc.
- Batch file found in c:\
  - Full of commands as: net stop "AVG7 Alert Manager Server" /y
  - Executed as administrator (admin account 8 char - LM passwd)
- Restart + up with services
  - Hacker Defender (hxdef) installed!
- MS MRT reported hackdef as well
  - http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=38058

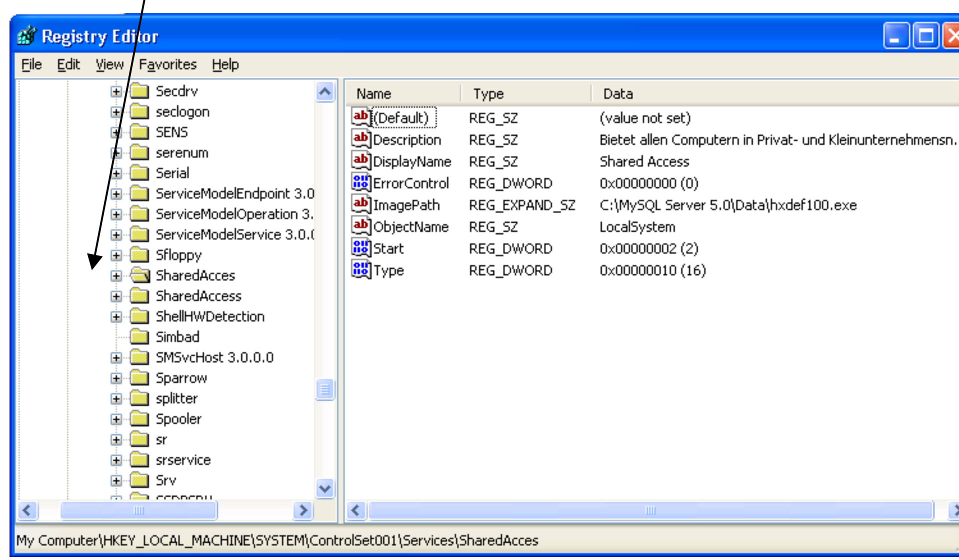
http://www.microsoft.com/security/encyclopedia/details.aspx?name=VirTool%3aWinNT%2fHackdef.I

Hacker Defender II



Note!
Hxdef
hiding
Service
etc.



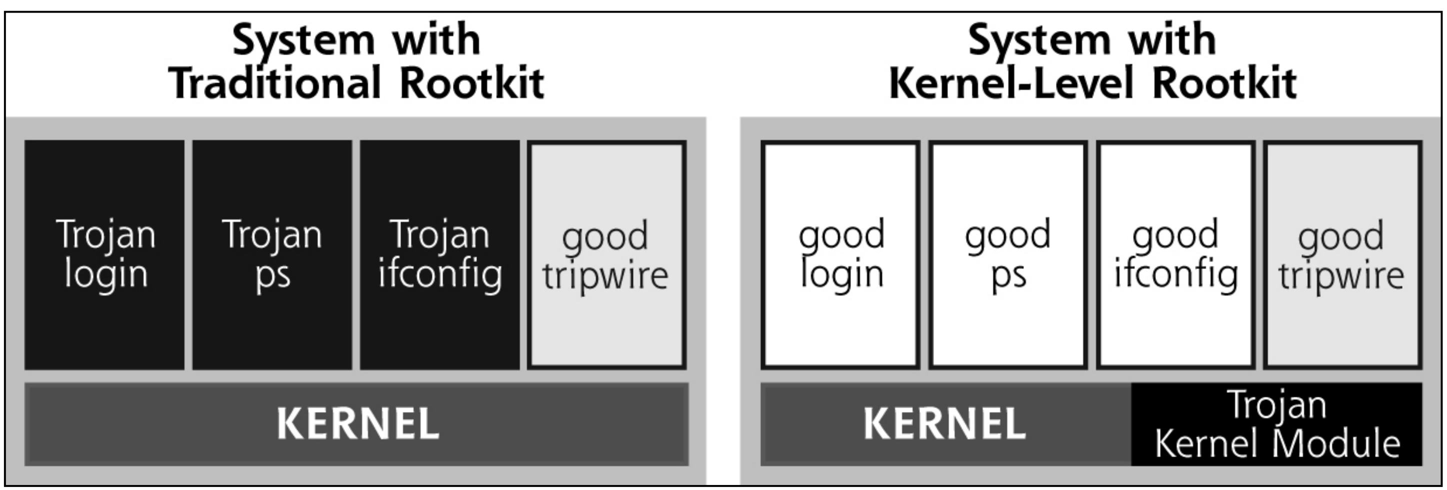


Defend against user mode rootkits

- Do not give superuser access
  - Windows XP etc. have as default no password for Administrator!
- Harden the system
  - Templates from CIS (Center of Internet Security)
    - http://www.cisecurity.org - it's called benchmarks
- File integrity checkers
  - Hashar på filer garanterar äkthet och korrekthet
  - Automatiska verktyg/script finns som t.ex. Tripwire och Open Source Tripwire: http://sourceforge.net/projects/tripwire/
  - MS Windows File Signature Verification (sigverif.exe)
- Antivirus software
- Rootkit checkers (see list in later slide)
- Recover from rootkit?
  - May be possible but you never know when something will pop up again
  - Reinstall from verified ROM media is the only sure thing to do

Kernel mode rootkits I

- Alters the kernel
  - The kernel itself becomes the trojan!
  - File integrity checkers don't work…
- Often include powerful execution redirection (Unix)
  - Runs another program than intended which resides in a hidden area
  - Sshd, taskmanager, netstat etc.
- Hides just about anything as user mode rootkits are capable of (but implemented in the kernel) which makes all programs lie
  - Files, processes, network etc. - nothing can be trusted...



Kernel mode rootkit examples

- Unix/Linux
  - Adore-ng, supports
    - Execution redirection, hiding files, processes, network etc.
    - Promiscuous mode hiding (intelligent)
    - Kernel module hiding (itself) using lsmod
    - Backdoor present in kernel module
    - http://packetstorm.linuxsecurity.com/groups/teso/
- Windows
  - FU, a special device driver named msdirectx.sys
    - Hide processes etc. with direct kernel object manipulation
    - Process privilege elevation on the fly
    - Hides selected events and device drivers (itself)
    - https://www.rootkit.com/board_project_fused.php?did=proj12

Defend against kernel rootkits I

- All the previous defense methods for user mode rootkits
- Honeypots
  - For “know your enemy” learning
  - Sebek2 a kernel mode rootkit for monitoring attackers
    - http://www.honeynet.org/papers/kye.html
- Host based IPS software
  - Control action between user mode <-> kernel mode
    - Limit calls specific applications can do
  - Systrace
    - Strace (shows system calls) on steroids
  - CSA (Cisco Security Agent)
  - McAfee Entercept
- Manual detection?
  - May work, but probably not…

Defend against kernel rootkits II

- Automated tools that (in best case) can find rootkits
  - Chkrootkit - http://www.chkrootkit.org
    - Scan executables for fingerprint
    - Search for hidden processes comparing /proc with ps
    - Check for inconsistency in directory structure
  - Rootkit hunter - http://www.rootkit.nl/projects/rootkit_hunter.html
  - RootkitRevealer (Sysinternals)
  - GMER - http://www.gmer.net
  - Radix - http://www.usec.at/rootkit.html
  - Strider GhostBuster
    - http://www.research.microsoft.com/rootkit/
  - OSSEC HIDS and Rootcheck
    - http://www.ossec.net/main/rootcheck

Lists of freeware antirootkit and AntiRootkit Tools

http://freeware.wikia.com/wiki/Lists_of_freeware_antirootkit

http://lists.thedatalist.com/pages/AntiRootkit_Tools.htm

http://www.sophos.com