SYSTEMS AND APPLICATION SECURITY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

IDENTIFY AND ANALYZE MALICIOUS CODE AND ACTIVITY

SSCP®

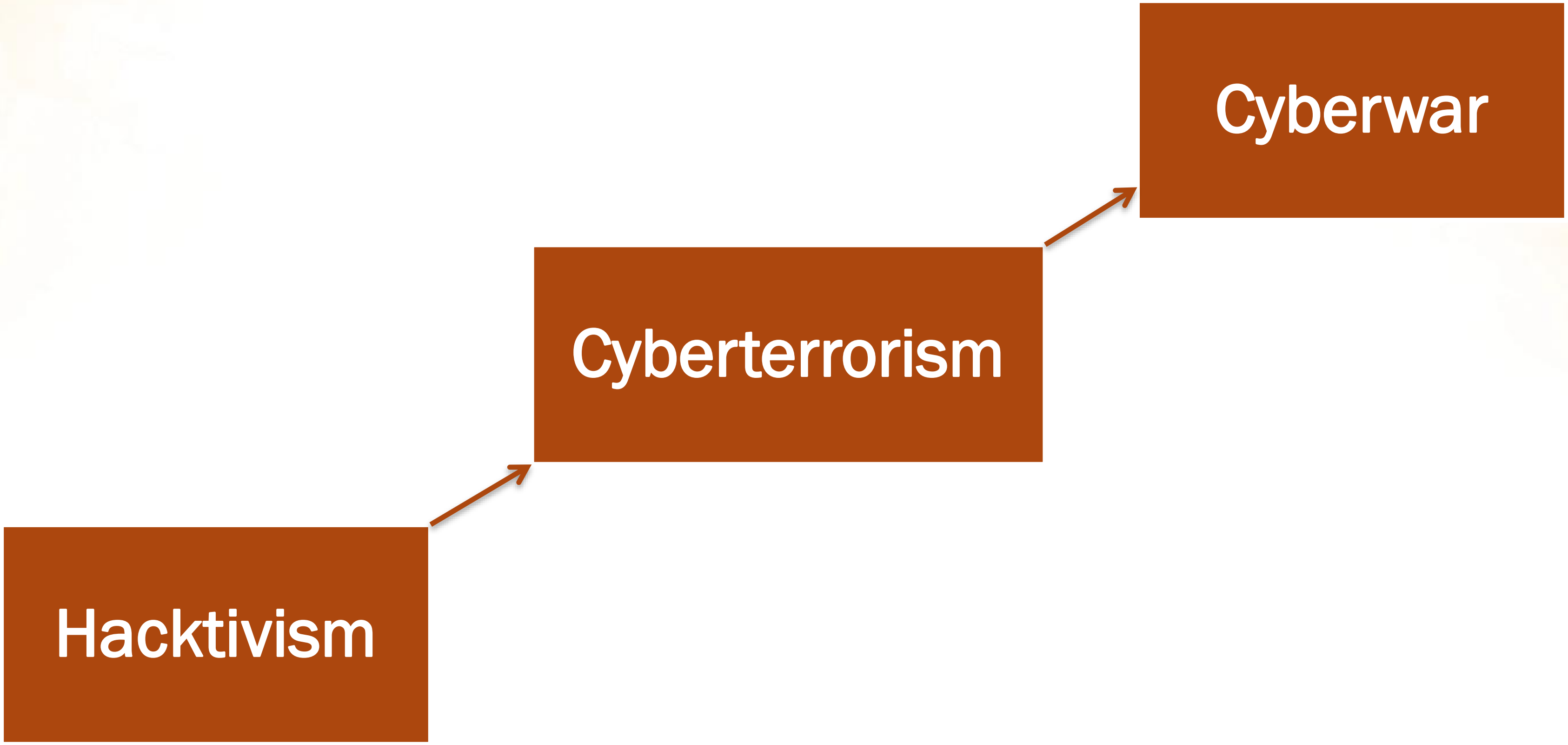
Systems Security
Certified Practitioner

(ISC)²®

Malicious Code

Malicious code (sometimes called malware) is a type of software designed to take over or damage a computer's operating system without the user's knowledge or approval

Hacktivism Moving Toward Cyberwar and Cyberterrorism?



Malicious Code Countermeasures

At the gateway

At workstations that access information services

Malicious Code Detection System Requirements

Allow access to all services available on the WAN

Be able to locate the source and type of an infection

Be able to react to such intrusions

Be able to fully reconstitute the system following intrusions

Have minimal operational effect on the user

Have minimal operational effect on performance

Malicious Code Detection System Requirements

Have appropriate documentation

Allow automatic malicious code prevention programs to run in the background

Allow a disaster recovery plan to recover data

Provide adequate scanning tools

Have appropriate means to trace all incoming and outgoing data

If Internet is unavailable, be able to access to virus updates

Countermeasures for Malware

- Antivirus software on user machines
- Install and use several different antivirus software
- User awareness training
- Disable scripts when previewing or viewing e-mail
- Block attachments at network borders
- Prevent download of software from the Internet
- Strict software installation policies
- Block the use of removable drives
- Antivirus scanners on e-mail gateways

Behavior-Blocking Software

Integrates with the operating system of a host computer and monitors program behavior in real time for malicious actions

Code Signing

A digital signature serves as a means of confirming the authenticity of an object, its origin, and its integrity

Sandboxing

A secluded environment on a computer where you can run untested code or malware to study the results without having any ill effects on the rest of your software

Security Awareness Training

Never trust unsolicited e-mails, instant messages, or other communications

Situational-specific awareness based on their roles and responsibilities

Long File Extensions

- On Windows NTFS-based operating systems, the filename can be up to 255 characters long
- Filenames that are very long are abbreviated with three dots "…" concealing the true extension of the file

Double File Extensions

The use of double file extensions is often combined with long filenames to show only the first extension, such as:

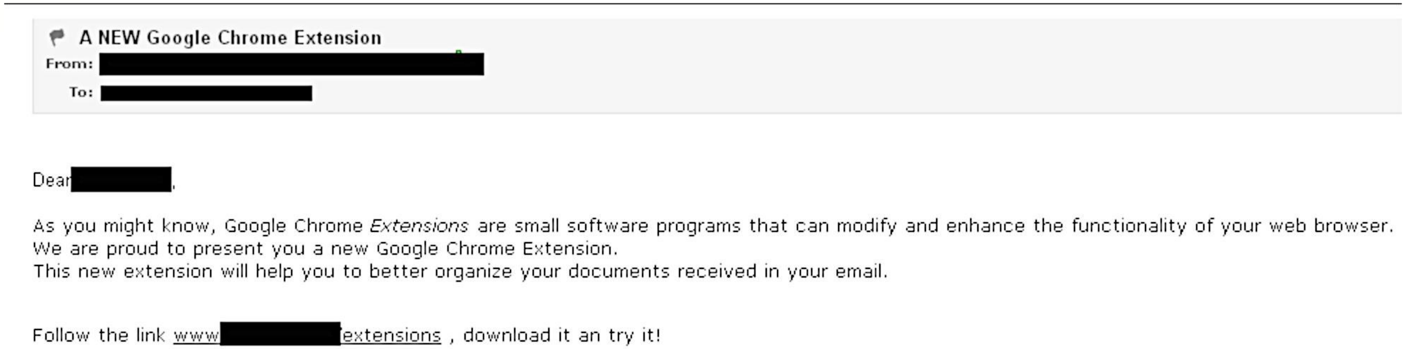
“Madonna.jpg”

followed by many spaces and then the real extension, such as .exe:

“Madonna.jpg.exe”

E-mail

One of the most well-known vectors for spreading malcode



A NEW Google Chrome Extension

From: [redacted]

To: [redacted]

Dear [redacted],

As you might know, Google Chrome *Extensions* are small software programs that can modify and enhance the functionality of your web browser.
We are proud to present you a new Google Chrome Extension.
This new extension will help you to better organize your documents received in your email.

Follow the link www[redacted]extensions , download it an try it!

Insider Threats

Authorized access to an organization's network

Intentionally misuse

Negatively affect confidentiality, integrity, or availability

Indicators of Malicious Threat Activity

- Remotely accesses the network while on vacation, sick, or at odd times
- Works odd hours without authorization
- Notable enthusiasm for overtime, weekend, or unusual work schedules
- Unnecessarily copies material
- Interest in matters outside of the scope of duties
- Signs of vulnerability

Countermeasures

- Train employees to recognize threats
- Conduct training on risk perception and cognitive biases
- Improve usability of security tools and software
- Enhance awareness of unintentional insider threat
- Provide effective security practices
- Maintain staff values and attitudes that align with organizational mission and ethics

Detection, Prevention, and Deterrence Methods

- Data/file encryption
- Data access monitoring
- SIEM or other log analysis
- DLP
- Data redaction
- IAM
- Data access control
- IDS/IPS

Insider Hardware Threats

Monitor phone activity logs

Monitor and control privileged accounts

Monitor and control external access

Protect critical files

Disable accounts upon employee termination

Prevent unauthorized removable storage mediums

Identify all access paths

Spoofing

A situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage

Phishing

The attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication

Common Characteristics of Forged E-Mail Messages

Use of the names of existing companies

Use of the name of a real company employee

Web addresses that seem to be correct

Fear factor

Techniques

Man-in-the-middle

Exploitation of cross-site scripting vulnerabilities in a website

Vulnerabilities in Internet Explorer

Exploits hosted in malicious websites

Protecting Users From Spam

Do not publish personal e-mail addresses

Never click on the “unsubscribe” link in spam

Never reply to a spam message

Do not resend chain letters

Do not open the spam message

Disable the Preview Pane of the e-mail client

Botnets

A botnet is an army of compromised machines, also known as "zombies," that are under the command and control of a single "botmaster”

Botnet-Led Exploits

- DDoS Attacks
- Spyware and Malware
- Identity Theft
- Adware
- E-mail Spam
- Click Fraud
- Phishing

Botnet Detection and Mitigation

Botnets use multiple attack vectors; no single technology can provide protection against them

Common Botnet Detection and Mitigation Techniques

Flow data monitoring

Anomaly detection

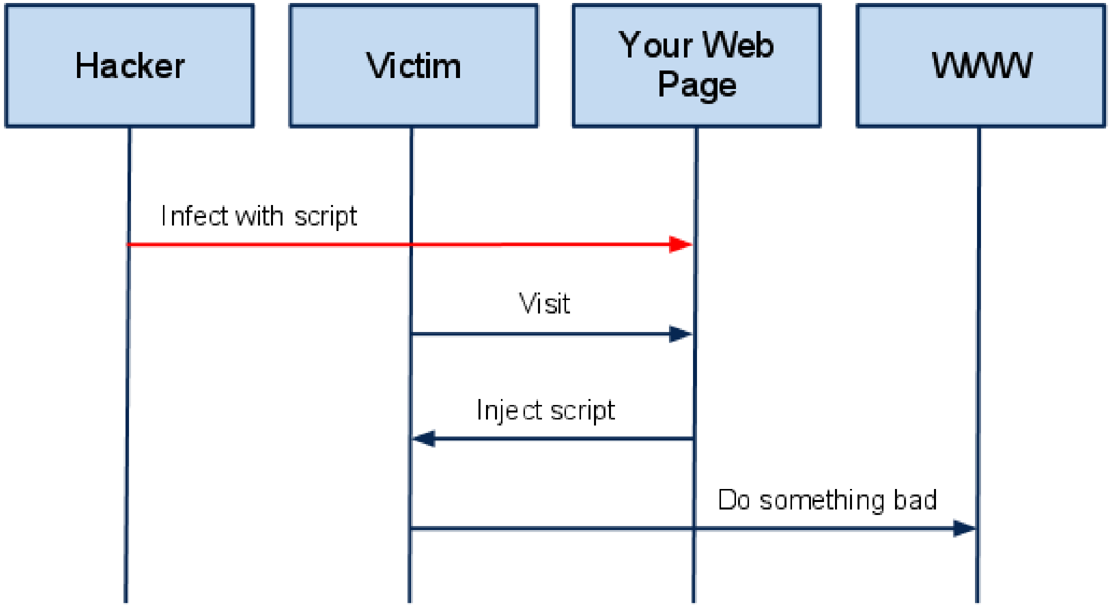
DNS log analysis

Honeypots

Cross-Site Scripting (XSS) Attacks

Hacking technique that leverages vulnerabilities in the code of a web application to allow an attacker to send malicious content from an end user and collect some type of data from the victim

The Theory of XSS



A High Level View of a typical XSS Attack

Example of a Cross-Site Scripting Attack

1. Search Results for "XSS Vulnerability”
2. Next, try to send the following query to the search engine
3. Upon loading the results page, the test search engine would probably display no results for the search, but it will display a JavaScript alert that was injected into the page by using the XSS vulnerability

How to Check for Cross-Site Scripting Vulnerabilities

Web Vulnerability Scanner:

- Automatically checks for cross-site scripting vulnerabilities
- Indicates which URLs/scripts are vulnerable to these attacks

Zero-Day Exploits and Advanced Persistent Threats (APTs)

An attack that exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch

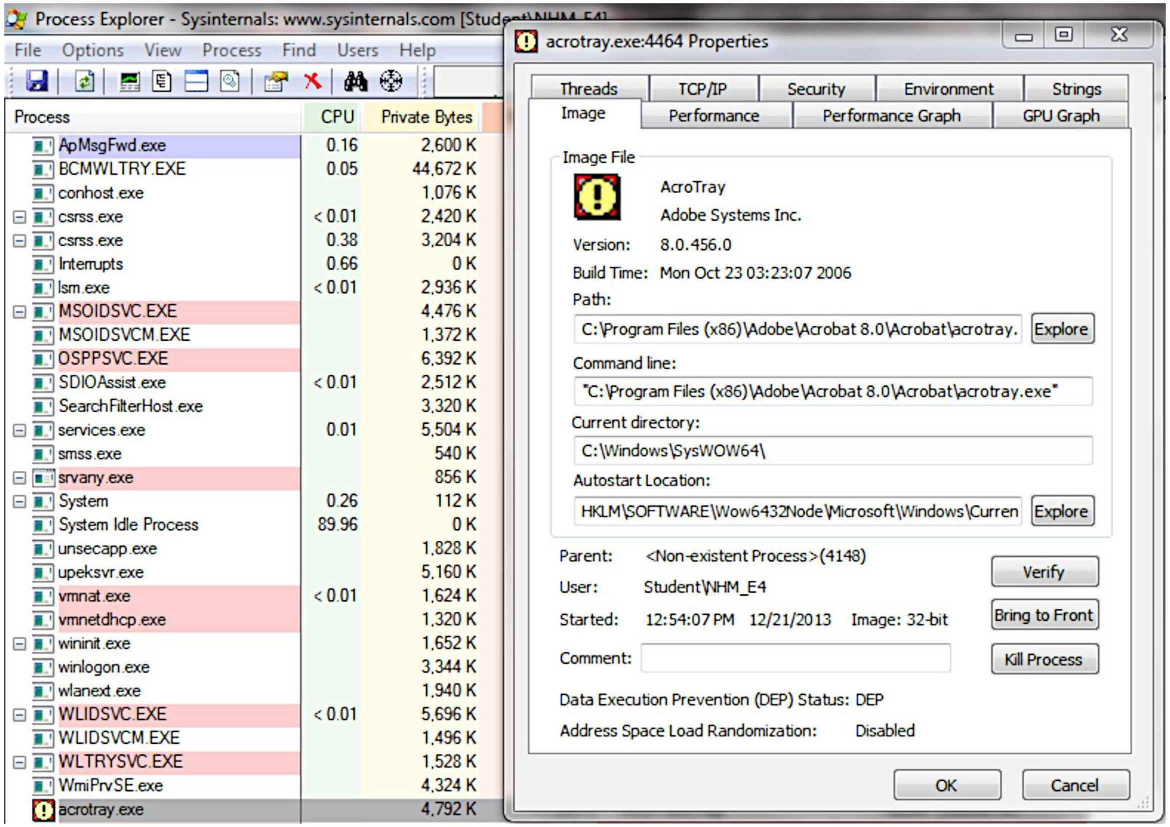
Instant Messaging

Instant messaging (IM) threats may involve exploitation of software to spread code but more frequently rely on social engineering

Peer-to-Peer Networks

Peer-to-peer (P2P) networks involve hosts sharing files with one another, either directly or through a centralized P2P server

Process Explorer


Process Explorer - Sysinternals: www.sysinternals.com [Student\NHM_E4]
File Options View Process Find Users Help
acrotray.exe:4464 Properties
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
GPU Graph
Explore
Explore
Verify
Bring to Front
Kill Process
OK
Cancel

Process	CPU	Private Bytes
ApMsgFwd.exe	0.16	2,600 K
BCMWLTRY.EXE	0.05	44,672 K
conhost.exe		1,076 K
csrss.exe	< 0.01	2,420 K
csrss.exe	0.38	3,204 K
Interrupts	0.66	0 K
lsm.exe	< 0.01	2,936 K
MSOIDSVC.EXE		4,476 K
MSOIDSVCM.EXE		1,372 K
OSPPSVC.EXE		6,392 K
SDIOAssist.exe	< 0.01	2,512 K
SearchFilterHost.exe		3,320 K
services.exe	0.01	5,504 K
smss.exe		540 K
srvany.exe		856 K
System	0.26	112 K
System Idle Process	89.96	0 K
unsecapp.exe		1,828 K
upeksvr.exe		5,160 K
vmnat.exe	< 0.01	1,624 K
vmnetdhcp.exe		1,320 K
wininit.exe		1,652 K
winlogon.exe		3,344 K
wlanext.exe		1,940 K
WLIDSVC.EXE	< 0.01	5,696 K
WLIDSVCM.EXE		1,496 K
WLTRYSVC.EXE		1,528 K
WmiPrvSE.exe		4,324 K
acrotray.exe		4,792 K

Image File

AcroTray
Adobe Systems Inc.

Version: 8.0.456.0

Build Time: Mon Oct 23 03:23:07 2006

Path:
C:\Program Files (x86)\Adobe\Acrobat 8.0\Acrobat\acrotray.

Command line:
"C:\Program Files (x86)\Adobe\Acrobat 8.0\Acrobat\acrotray.exe"

Current directory:
C:\Windows\SysWOW64\

Autostart Location:
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Curren

Parent: <Non-existent Process>(4148)

User: Student\NHM_E4

Started: 12:54:07 PM 12/21/2013 Image: 32-bit

Comment:

Data Execution Prevention (DEP) Status: DEP

Address Space Load Randomization: Disabled

Application Layer

Signature Detection

Heuristic Analysis

Modified Hosts File and DNS Changes

- Malicious code may modify the hosts file to block or redirect traffic on the host
- Normally has just a few entries
- If it has additional entries that point to questionable content or loopback, it may indicate a malicious code infection

Inspection of Processes

- Look for new processes taking up lots of memory
- Find a new or unexpected process in the list of running processes
- Process Explorer

Behavioral Analysis of Malcode

- A test system must be in place to properly analyze malcode behavior
- This should contain a known set of applications, processes, and tools that establish a behavioral baseline
- Changes to the system can then be identified