Week-3

Part I-Malware Overview

分类：1. Propagation：如何抵达目标，传播方式；

2. Payload：病毒到达目标之后采取的行动。

•Virus：Almost always attached to an executable file

- Propagates：only when infected software or document is transferred to another computer by a user via Email attachment, USB Drive, Network File Share, etc.
- Viruses cannot propagate on their own!
- Payload:
  - Infect/overwrite other software or documents with copies of itself
  - Erase files and programs
  - Reformat hard disk

4 Types of Viruses：

1. File infector viruses
2. Boot sector & Master Boot Record (MBR) viruses
3. Multipartite viruses
4. Macro viruses

•Worm：Seeks out computers to infect and each infected computer acts as automated launching pad for attacks on even more computers.

•Propagates via:

- Network connections, shared media, can email copy of itself
- Worm macro inside Word, Excel, PP documents
- Unlike Viruses, Worms propagate on their own!

Payload:

- Creation of backdoor
- Turns computers into spam engines
- Can disable security software
- Damage systems
- Cause Denial of Service (DoS) attacks

•Conficker (AKA Downadup)

•Worm that:

- Replicates and joins infected hosts to a botnot
- Could also download and install other malware such as scareware.

•Uses Windows Server Service vulnerability

•Windows Remote Procedure Call (RPC)

- Lets program request a service from a program on a remote computer
- Provides file/print/named pipe sharing across a network

•Payload:

- Copies itself with random name into %systemroot%\system32 and registers itself as a service.
- Adds itself to the Windows registry

•Uses following sites to determine infected machine‘s IP:

- http://www.getmyip.org
- http://checkip.dyndns.org
- http://getmyip.co.uk

•Then, downloads small HTTP server to infected machine to:

- Scan for other vulnerable computers as targets
- Sends infected computer URL to targets

•Conficker can also use infected computer to crack passwords of remote computers:

•Vulnerable target computer downloads worm from the initially infected computer’s HTTP server via the URL provided

•Target starts infecting other machines in the same manner.

**Confickeralso patches vulnerability to prevent other worms from getting into Conficker infected computers.

Conficker Prevention：

•Keep security patches up to date

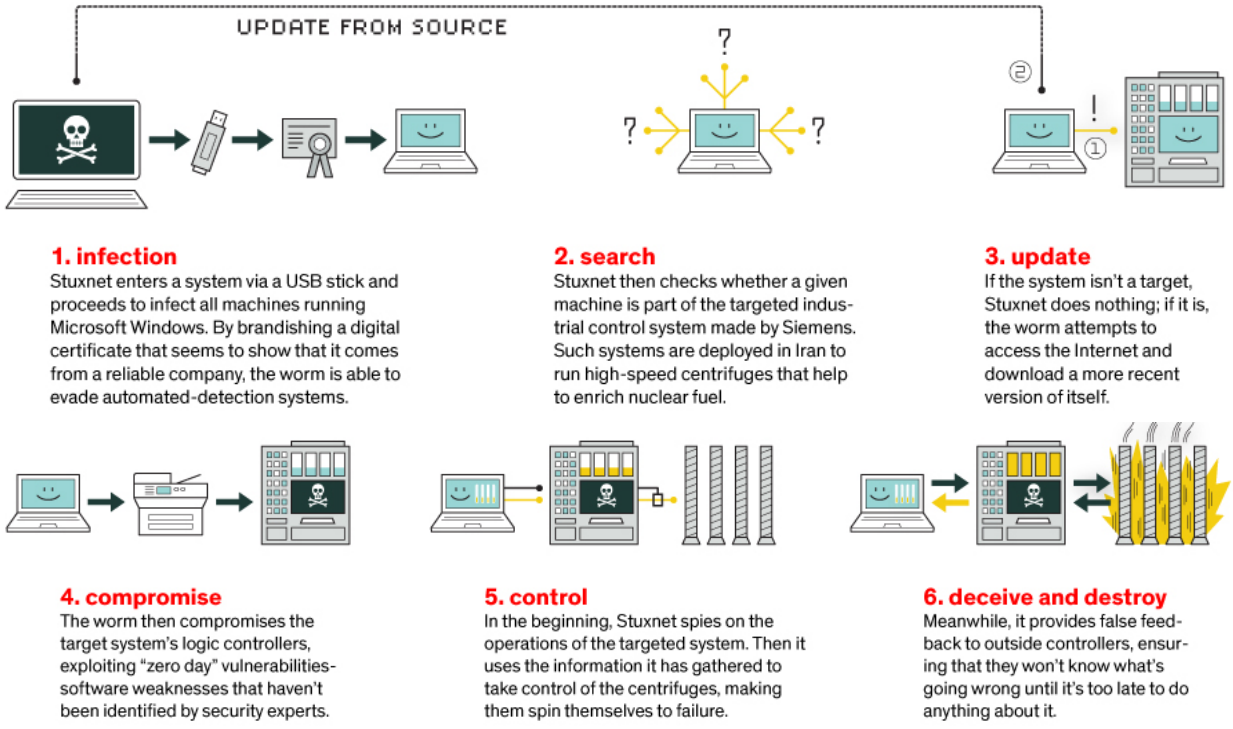
•Could use firewall to block SMB (445) and NetBios(139)

•Use security software

•Use strong passwords

•Scan USB drives before inserting into your computer

•Stuxnet



Stuxnet Prevention：

•Disable local USB ports.

•Integrity scanners of the logic controller software that ran the centrifuges could have detected a change.

•Stuxnetwas a 0-day attack at the time

- Hence, there were no patches or signatures for A/V or IDS/IPS created yet.

•Trojan Horse: Malicious software that appears to be legitimate

•Propagates via user interaction:

- Opening email attachments
- Downloading and executing a file from the internet

•Payloads:

- Data theft or loss
- Creation of backdoor
- Downloading of other malware

•Trojans do not self replicate like Worms or reproduce by infecting other files like Viruses

Early Trojans：

•Pirated Software

•Screen Savers

•Useful Utilities

•Keygens

•Download and install the software above

- Get hit with malware payload

Recent Trojan Types：

•Scareware/ FakeAV

•Ransomware

•Remote Administration Trojan (RAT)

•Also called a backdoor

•Includes client and server program

•Attacker can remotely control system

- Log keystrokes
- Access webcam and audio
- Take screenshots
- Packet sniffing
- Steal files
- Modify system

•PDF Malware

1.User opens malicious PDF in a viewer

2.Embedded script set to execute “On Open”

3.Script either:

- extracts and decodes embedded malware on system
- downloads new malware from an internet site

4.Malware is installed on victim’s system

•Customizable Trojans –Zeus/Zbot

- Build a bot package

- Botnet Admin panel

•Can be customized to:

- Gather passwords from Windows Protected Storage (IE, FTP, POP3)
- Monitor web sites in config file to intercept web forms
    - oSometimes creating additional fields in page such as date of birth

•Spread by:

- Phishing emails
- Infected sites

•New variants in 2014 shown to:

- Use Windows Program Information Files (PIF) for execution.
- Can be slightly modified to avoid A/V detection
- Communicates with Command and Control (C&C) servers (aka Botnet Master Server) using HTTPS to transmit stolen data.

•Bot/Botnets

•Can be used to:

- Steal information (Zeus/Zbot)
- Send spam/phishing campaign emails
- Participate in Distributed Denial-of-Service attacks (DDoS)
- Crack passwords
- Bitcoin mining

•Bot Master (aka C&C Server) communicates with bots via covert channel.

- Often IRC
- Newer botnets use P2P network and encryption

ZeroAccess Botnet

•Uses ZeroAccess Trojan rootkit on bots

•Spread by:

- Compromised web sites (Drive by download)

•Payload:

- Click Fraud : conducts web searches and clicks on results
- Can download other malware such as scareware
- Bitcoin mining
- Backdoor for C&C owner

•Rootkits:

•Has system level/root access to system

•Attempts to hide fact that system is infected

•Two types:

- User-Mode Rootkits
- Kernel-Mode Rootkits

ZeroAccess Rootkit:

•Started as kernel-mode rootkit

- Created new kernel device driver object called __max++>
- Maintains persistence on reboot

•Now it has been changed to a user-mode rootkit

- Loads DLL into services.exe and explorer.exe
- Maintains persistence by hijacking COM object in Windows Registry called wberness.dll

%systemroot%\system32\wbem\wbemess.dll Correct value

\\.\globalroot\systemroot\Installer\{e051c979-bddd-5d1f-8953-4b8c940e9b4d}\n.

Hijacked value

TDSS Rootkit (Alureon)

•PC gets infected by Trojan such as ScarewareSecurity Essentials 2010

•Hooks hardware driver and joins botnet

•Network traffic interception to:

- Steal usernames, passwords, credit card data

How to detect Rootkits?

•A/V might detect signatures

•Monitor outbound traffic to C&C

•File Integrity Software might detect changes

•chkrootkit–tool to locally check for signs of a rootkit.

•Rootkit Hunter: Checks for over 50 different rootkits.

•Rootkit Revealer

•F-Secure'sBlackLight

•ICE Sword

•Sophos Anti-Rootkit

•McAfee Rootkit Detective

Rootkit Remediation:

•A lot of Enterprise Organizations will just:

- Wipe the drive
- Reformat drive
- Reinstall OS, Apps, and Data
- Apply all security patches
- Change all admin/root passwords

•This is the safest option to know definitively that the rootkit is gone!

•If you can't wipe/reformat:

- Remediation Software
  - oMcAfee RootkitRemover
    - Removes ZeroAccessand TDSS family of rootkits
  - oKaspersky Lab TDSSKiller
  - oGMER

oMalwarebytes Anti-Rootkit

•Logic Bombs

•Code embedded into an application or a simple script that executes in response to an event:

- Specific date/time
- User performs a specific action such as open an application

•Backdoors

•A backdoor is simply a way for an attacker to enter a system at a later date

•It is a method of persistence

•The best backdoors will be loaded as a service so that they will restart if the computer is restarted

•Remote Access Trojans (RAT)

A Backdoor with Metasploit

•Metasploit is a penetration testing tool and is included in Kali Linux.

•Meterpreter is a backdoor shell that can be placed onto the victim's computer to steal data, passwords, etc.

•Meterpreter has a persistence mechanism in case the victim's computer is rebooted.

•Spyware

- Usually used to access a user's private data and send information to a third party
  - oKeyloggers
  - oBrowser Hijackers
  - oWebcam Loggers
  - oClipboard Loggers
  - oCan download other malicious programs

•Adware

- Learn a user's browsing habits to deliver targeted advertising

oPop-up ads

oToolbars

Part II- Detecting Malware

Look for Indicators of Compromise (IOC) through:

A. Use of AntiVirus& AntiMalwaretools

B. Analysis of system/server changes

C. Monitoring outbound communications

Part II -A: Detecting Malware (A/V & AntiMalwareTools)

AntiVirus(A/V) vs. AntiMalware(A/M)

•Industry vendors have created some confusion in their terms:

Virus: Malicious software that can damage a computer

Malware: Malicious software that consists mainly of spyware, adware, ransomware, and trojans.

•Technically, a virus is "malware" but vendors often consider viruses in their own category

•We will consider all malicious software as "malware"

How Does A/V & A/M Typically Work?

•Signature Based (Known Malware)

Compares contents of file against dictionary of virus signatures

•Heuristic/Behavior Based (Unknown Malware)

File Emulation

oSandbox testing

File Analysis

oDetermine intent of file

Generic Signature Detection

oLocate variations of known viruses

Popular Business Security Software Vendors

•Symantec

•McAfee

•Kaspersky

•Trend Micro

•Sophos

•Eset

•F-Secure

Popular Business Security Software Vendors

•Bitdefender

•Panda

Popular Business Security Software

•Many offer distributed protection that is centrally managed

•Example: Symantec Endpoint Protection (SEP)

- SEP: Installed on endpoint client devices & provides:
  - oSignature based A/V and A/M protection
  - oHeuristic based protection
  - oNetwork Threat Protection (Local firewall and IDS)
  - oNetwork Access Control (Quarantines infected computers)
- SEP Manager: Communicates and manages all clients, can run reports, etc.

Popular Business Security Software -Limitation

•Some endpoint protection vendors don't detect "malware" very well

•Companies can submit a sample to the vendor to have a signature added or can install an additional A/M product

Popular "AntiMalware" Software

•MalwareBytes

•Webroot

Security Software Challenges

•Endpoint software becomes corrupt

•Endpoint software stops communicating with the management server

•Some endpoint software uses substantial host resources

Part II -B: Detecting Malware (System/Server Changes)

Cheat Sheet

•Lenny Zeltsercreated a great cheat sheet for Linux and Windows Server Administrators to assess suspicious hosts

•https://zeltser.com/security-incident-survey-cheat-sheet/

Note

•During investigation, use the command line (as opposed to Windows Explorer) to avoid modifying important file system metadata

Event Logs

•cmd: **eventvwr**

•Windows Event Viewer

- Holds various logs for local system

•Expand “Windows Logs”

- Application

  oEvents unrelated to OS but related to installed Apps

- **Security**

  oLogon info, File/Folder Access, Security Modifications

- System

  oEvents related to Windows services, drivers, reboots, etc.

•Event ID

- 4624 = Successful Logon
- 4634 = Successful Logoff
- 4625 = Failed Logon

Enable Security Logging

•cmd**: secpol.msc**

Network Configuration

•What does ARP do?

Maps MAC addresses to IP addresses

•arp–a

To view current arptable mapping

•netstat–nr

View interfaces and routes

Network Connections

•netstat –nao

-n Displays addresses and port numbers

-a Displays all connections and listening ports

-o Displays owning PID associated with connection

•netstat –nvb

-v Displays components involved in creating connection

-b Displays executable involved in listening port or connection

-n shows foreign addresses as IPs

•netstat –fvb

-f resolves foreign address into domains

•net session

Shows computer names and user names of users on a server

•net use

Shows current connections to network resources such as file shares

New Users/Groups

•net users

Displays user accounts for the host

•net localgroup administrators

Shows who is a local administrator of the host

•net group administrators

- Only can be run on a domain controller

•lusrmgr

- GUI version to show users and groups

Secheduled Jobs

•schtasks

- Shows next run time for various tasks and if ready, running, or disabled

Lists Processes and Services

•taskmgr

- Most should be familiar with this GUI process viewer

•wmic process list full

- Shows verbose detail about processes

•net start

- Shows what services are running

•tasklist /svc

- Shows what services are running under what executable processes

Check DNS Settings and Hosts File

•ipconfig /all

- Shows interface and DNS information

•ipconfig /displaydns

- Shows recent queries from DNS Resolver Cache

•more %systemroot%\system32\drivers\etc\hosts

- Shows hosts file which can bypass network DNS to resolve hostnames to IPs locally.
- Malware often tries to use the hosts file to send web browser requests to malicious servers

Recently Modified Files

•dir/a/o-d/p %systemroot%\System32

- Shows recently modified files along with modification date and time sorted by most recent

Programs Starting at Boot

•msconfig

Shows programs that start at boot in Startup tab

•Autoruns Application

We used this GUI program previously in the lecture

More verbose than msconfig

Part II -C: Detecting Malware (Monitoring Outbound Comms.)

Network Indicators of Compromise (IOCs)

•Monitor network traffic to determine if hosts are communicating with command and control (C2) servers or downloading additional malware

Splunk

•Log aggregator which can allow analysis of logs from network firewall and proxy devices

•Watchlistsare used to look for hosts communicating with malicious domains

•Splunkcan send alerts to an analyst via email to investigate

•Good way to tell if user gets hit with malware after clicking on a phishing email

Part III Web Exploit Kits

Web Exploit Kits

•Pre-packaged malicious software toolkits for rent referred to as “Crimeware”

•Renter receives Control Panel that contains customizable installer and can display statistics.

•Renter installs redirector on legitimate website

•Victim receives phishing or spam email with link to legitimate website that has been compromised

Goal of Web Exploit Kits

•Exploit user’s browser in order to deliver malware payload

•Payload:

- Scareware
- Spyware
- Bot

- Backdoor
- Etc.

Chain of Events

1.Victim connects to the compromised website

2.Victim is redirected through intermediary servers

3.Victim lands at rogue server hosting the exploit kit

4.Exploit kit enumerates victim's browser/PC and determines exploit to deliver

5.Exploit is delivered

6.If exploit succeeds, a malicious payload is downloaded to the victim's computer and executed

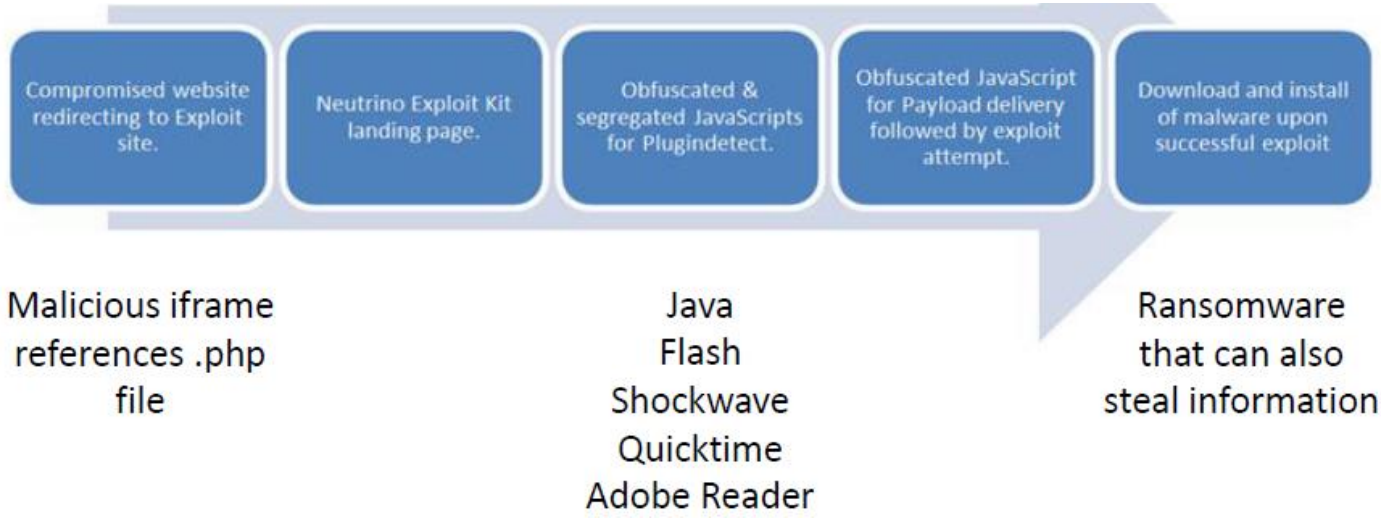
- Payload could be Trojan, Backdoor, Locker, Spyware, Fake A/V, etc

1. Neutrino Exploit Kit

•Most prevalent web threat in 2013

- Russian creator is unknown but has reportedly put Neutrino up for sale.

- Typical Neutrino Infection Sequence



Example of Neutrino Exploit Chain

•Redirector from compromised web site

- http://first.com/mdvmYEri/js.js

•Traffic Direction Script (TDS) by Browser, OS, Geo, etc.

- http://second.com/clicker.php

•Main Neutrino landing page

http://third.com:8000/afscm?qomseteng=7559371

•PluginDetectfile to determine best exploit

http://third.com:8000/scripts/js/plg.js

•Payload Executable Downloaded

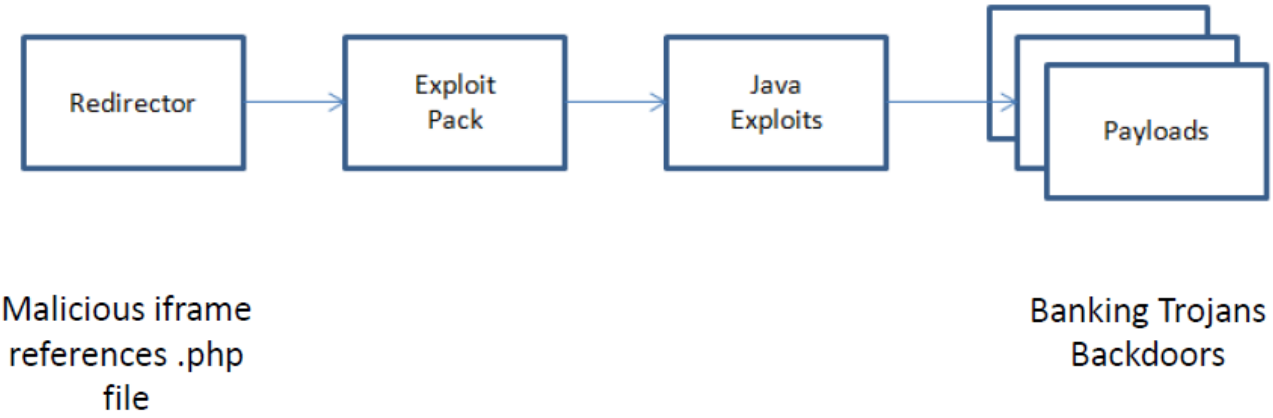
http://third.com:8000/agofydqhtbubuy?qvtghxlw=7559371

2. CrimebossExploit Kit

•Launched in 2011

Author may be “Psychlo” a Brazilian cyber criminal

- Typical CrimebossInfection Sequence



Example of CrimebossExploit Chain

•Redirector from compromised web site

http://first.com/index.php?setup=d

•Main Crimebosslanding page, checks Java

http://first.com/cb.php?action=jv&h=1048356750

•Java exploits delivered

http://second.com/jex/amor1.jar

http://second.com/jex/java7.jar

•Payload Executable Downloaded

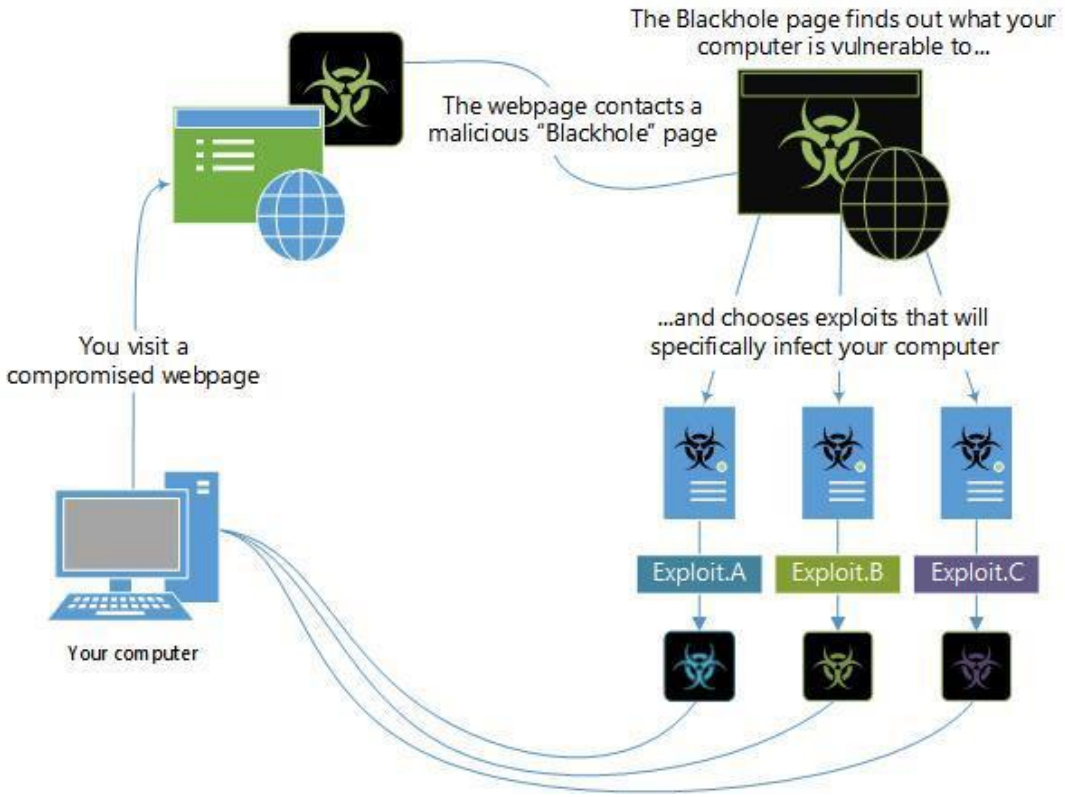
http://uploads.boxify.me/48548/gforcea.bmp

3. BlackholeExploit Kit

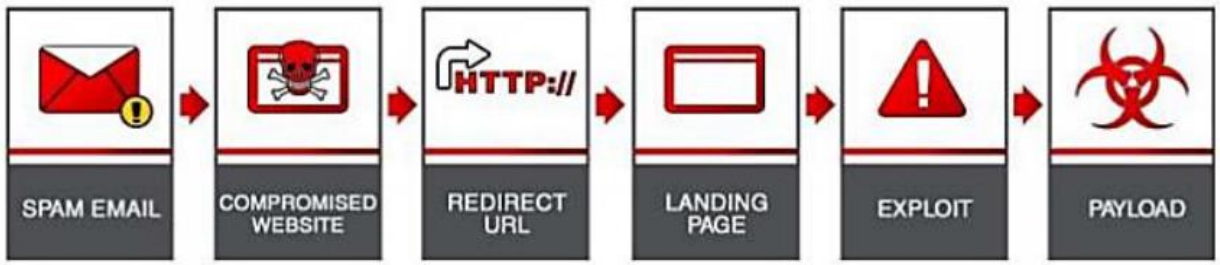
•Was most prevalent web threat in 2012

Kit is nearly extinct now

- BlackholeExploit Kit -Example Diagram



- Typical BlackholeInfection Sequence



US Airways
LinkedIn
Intuit
ADP
Facebook
Amazon

Java - .jar
Flash -.swf
PDF - ap2.php?f=

Zeus/Zbot
ZeroAccess
Fake AV
TDSS
Ransomware

Example of BlackholeExploit Chain

•Link in Spam email

http://first.com/T3xXwMv9/index.html

•Redirector

http://second.com/mdvmYEri/js.js

•Main BlackholeLanding page

http://third.com/showthread.php?t=d44175c6da768b70

•Java Browser Exploit

http://third.com/content/GPlugin.jar

•Payload Executable Downloaded

http://third.com/q.php?f=<diek&e=9854648634319485