



*cutting through complexity™*

# A Primer on Reverse Engineering Malwares

24<sup>th</sup> September 2011

Sony Anthony

Associate Director

Management Consulting – IT Advisory



# Agenda

---

Setting the Stage

Myths

Malware & the Art of Reverse Engineering

Malware Detection & Analysis Life Cycle

Behavior Analysis and Code Analysis

---



# Setting the Stage

# Cyber weapon (July 2010)

STUXNET

## The Epoch Times

Home Nation World China Business Opinion Science Technology Arts & Entertainment

### Cyber Cold War Becomes More Dangerous Stuxnet malware heralds a new era of cyberwarfare

by Joshua Philipp  
Epoch Times Staff

Created: Nov 9, 2010  
Last Updated: Nov 9, 2010

[Facebook](#) [Digg](#) [StumbleUpon](#) [Twitter](#) TEXT SIZE PRINT | EMAIL | FEEDBACK

[Related articles](#) : [United States](#) > [National News](#)

Stuxnet is different from much other malware. The [program](#) does not hack into finances, but experts suspect that it was developed through [millions of dollars](#) of research. Stuxnet is a cyber weapon that can take control of machinery that is guided by computers, even if the mechanisms are not connected to [the Internet](#).

The creator of Stuxnet is unknown, and the program has fired the starting gun for a new type of war.

Iran's state-run media announced on Sept. 26 that the malware was found in the country's Bushehr nuclear power plant and had reached the IP addresses of more than 30,000 computer systems. The malware has continued to spread, affecting systems worldwide, including in the United States, India, and China.

Cyber Weapon to control Industrial computer systems

Strong Financial Backing for Development

Pre-Defined Target Segment

Source: [www.theepochtimes.com](http://www.theepochtimes.com) 11-09-2010

# Malware's growing at alarming rate (2010)

ZEUS

## Malware growth reaches record rate

Wamick Ashford

Wednesday 17 November 2010 08:25

Malware growth has reached its highest levels, with an average of 60,000 new pieces of malware identified every day, according to the latest threat report from security firm McAfee.

Cyber criminals are becoming more savvy and attacks increasingly more severe, said the threat report for the third quarter of 2010.

The Zeus botnet is identified as one the most sophisticated pieces of malware to plague users, with US small businesses losing \$70m to Ukrainian cybercriminals.

Most recently, cybercriminals unleashed the Zeus botnet aimed at mobile devices, designed to intercept SMS messages to validate transactions. As a result, the report said criminals can perform the full bank operation, stealing funds from unsuspecting victims.

"Cybercriminals are doing their homework, and are aware of what's popular, and what's insecure," said Mike Gallagher, senior vice-president and chief technology officer of Global Threat Intelligence for McAfee.

Criminals are attacking mobile devices and social networking sites, so education about user activity online,



Efficient Enterprises do more with Dell EqualLogic.

Discover how, before your boss does >

Sophisticated

USD\$70M lost to Ukrainian Cyber criminals

Initial Target : US Small Businesses via Intercepting of SMS based Banking Transactions on Mobile devices

Source: [www.computerweekly.com](http://www.computerweekly.com) 17-11-2010

# And their variants at work (2011)

## ZEUS – V2

July 12, 2011, 12:29PM

### Zeus Banking Trojan Comes to Android Phones

by Paul Roberts

Follow @paulfroberts



Share



Comment



The Zeus banking Trojan has jumped the bridge to the large and growing ecosystem of mobile devices powered by Google's Android operating system, according to security researchers at Fortinet.

Researchers say they have obtained a Zeus variant, dubbed "Zitmo," that can run on Android phones and that has the ability to intercept one time pass codes sent to mobile phones as an added, "two factor" security measure.

#### Editor's Pick

[Ramnit Worm Evolves Into Financial Malware](#)

[Researchers: Square Card Reader Provides Straight Line to Illicit Cash?](#)

[Apple, Google Need Mobile Security Rethink](#)

[Threatpost Newsletter Sign-up](#)

The new Android variants are just the latest evidence that malware authors are expanding their operations to mobile devices. Earlier Zeus variants that run on [Nokia Symbian, RIM Blackberry and Microsoft Windows Mobile devices were identified in February](#). The post, by Fortinet researcher Axelle Aprville, claims that Fortinet researchers have observed conversations relating to Zeus for Android, but were finally able to obtain and test a sample. The malware they obtained looks much like known Android malware variants. It masquerades as a banking security application by the firm Trusteer. The malware is intended to thwart online banking security systems that rely on so-called out-of-band (OOB) authentication: sending pass codes to pre-registered cell phones that are required to start an online banking

Most Sophisticated / An Evolution

Man In the middle attack by marrying PC-based Zeus infections with a mobile component

Mobile variant, gives fraudsters control of both the user's PC and the user's phone  
And  
Generate a fraudulent transaction on behalf of the user by intercepting the SMS verification message

Source: [http://threatpost.com/en\\_us/blogs/zeus-banking-trojan-comes-android-phones-071211](http://threatpost.com/en_us/blogs/zeus-banking-trojan-comes-android-phones-071211)

# Cyber War

## Virtual Wars

The New York Times

## Europe

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION /  
AFRICA AMERICAS ASIA PACIFIC EUROPE MIDDLE EAST

### Cyberattack on Estonia stirs fear of 'virtual war'

By Steven Lee Myers  
Published: Friday, May 18, 2007

**MOSCOW** — The computer attacks, apparently originating in Russia, first hit the Web site of Estonia's prime minister on April 27, the day the country was mired in protest and violence. The president's site went down, too, and soon so did those of other ministries in a wired country that touts its paperless government and likes to call itself E-stonia.

Then the attacks, coming in waves, began to strike newspapers and television stations, then schools and finally banks, raising fears that an initial nuisance could have economic consequences.

The attacks have peaked and tapered off since then, but they have not ended, prompting officials there to declare Estonia the first country to fall victim to a virtual war

Source - <http://www.nytimes.com> 18-05-2007

TWITTER

SIGN IN TO  
E-MAIL

PRINT

SHARE

Probable attacks from Russia

Attack against Estonia's critical websites

Attacks lead to Economic Consequences

# Worms

Defences Down

**DEFENSE SYSTEMS**  
INFORMATION TECHNOLOGY AND NET-CENTRIC WARFARE

About Us Email Us Free sub

HOME LATEST NEWS DEFENSE SYSTEMS MAGAZINE BLOGS NEWSLETTERS RESOURCE C

C4ISR

Communications

Command and Control

Geospatial and  
Intelligence

Net-Centric Training

Sensors and UAVs

DEFENSE IT

Battlespace IT

Cyber Warfare

Enterprise IT

Information Security

Printable Format E-Mail this page

## Malware attack leaves Pentagon scrambling for answers

By [Dan Campbell](#)

Dec 02, 2008

Pentagon officials have acknowledged that the malware known as Agent.btz recently affected some Defense Department systems. Although it has been in circulation for several months, the malware was not yet known to have penetrated military networks.

The incident has left DOD officials scrambling to clean infected systems, institute new policy and security measures to thwart future incidents, and perform forensics to discover the source of the attack.

The issue was serious enough to prompt Adm. Mike Mullen, chairman of the

Source - <http://digital-works.net> 02-12-2008

Malware Attack

Worm Agent.btz spreads by creating AUTORUN.INF. Infects HD's, USB's etc.

Affected US Command centers in Iraq & Afghanistan



# Scenario @ home

## Penetration into High Profile targets in India



### Internet

## China Cyberspies Strike Indian Military, Tibetan Exiles, and Embassies in U.S.

Jason Mick (Blog) - April 7, 2010 9:11 AM

Print



ShareThis

New



listen now



26 comment(s) - last by dsx724.. on Apr 11 at 12:16 PM

### Report authors say Chinese government is cooperating to investigate the situation

Cybersecurity researchers at the University of Toronto's Munk School of Global Affairs claim to have discovered a [massive campaign of cyberespionage](#) carried out by members of China's underground hacking rings. The campaign zeroed in on high profile targets in India, including Tibetan exiles and the Indian Defense Ministry.

The attackers used attacks on social networking, blogging, and email services, such as Twitter, Google Groups, and Yahoo Mail to gain access to individual computers, forcing them to communicate with attack



Chinese hackers stole information from a variety of parties. While the attacks related to rivals or enemies of the government, the Chinese government claims not to have been involved and

Malware Attack

Use of social networking sites to attack personal PC's

Probable Military secret documents related security situations in north eastern states etc. stolen

Source – [www.dailytech.com](http://www.dailytech.com) 07-04-2010

# Scenario @ home

## Infiltration into Indian Military Network

### Chinese Army Broke Into Secret Indian Military Network In North-East: Report

[ Updated 04 Dec 2009, 14:04:14 ]



SHARE

COMMENTS

EMAIL | PRINT

FONT SIZE



#### Rs. 1500 Free Advertising

Start Running Your Own Ads Here. Fill Out the Form & We'll Help You!

[www.Google.com/AdWords](http://www.Google.com/AdWords)



Ads by Google

The Mumbai newspaper DNA on Friday reported that Chinese intelligence agencies had infiltrated into the computer network of Indian Army's 33 Corps stationed at Sukhna near Siliguri in North Bengal and obtained many reliable army-related information.

Source [www.indiatvnews.com](http://www.indiatvnews.com) 4-12-2009

Malware Attack

Infected 33 Corps headquarters at Sukhna near Silliguri in North Bengal

Possible leakage of details of military posts along the borders

# Malware Entry Points

Universal Serial Bus – Portable Storage – Internet

## USB Malware Attacks On the Rise

By: [Sean Carroll](#)

11.04.2010

Malware slips in via many weak points. It can come through e-mail, drive-by downloads, or ill-advised clicking, perhaps on a misleading popup. Increasingly, it also comes via USB devices. In fact, according to AVAST Software, 13.5 percent of more than 700,000 attacks recorded by its avast! Community IQ system in October came via USB.

The main way that malware is delivered by USB is via the AutoRun feature in Windows. AutoRun is a convenience feature that pops up a dialog to help users choose what to do with a USB device upon connection to their PCs. When a USB device infected with a particular type of worm is connected to the PC, an executable file starts that begins downloading malware onto the PC. This malware infects the OS and can replicate itself each time the computer is restarted.

Auto Run Feature

Malware affects the OS

Applies to Phones, digital cameras, PSP's, mp3 players

Source: [www.pcmag.com](http://www.pcmag.com) 11-04-2010

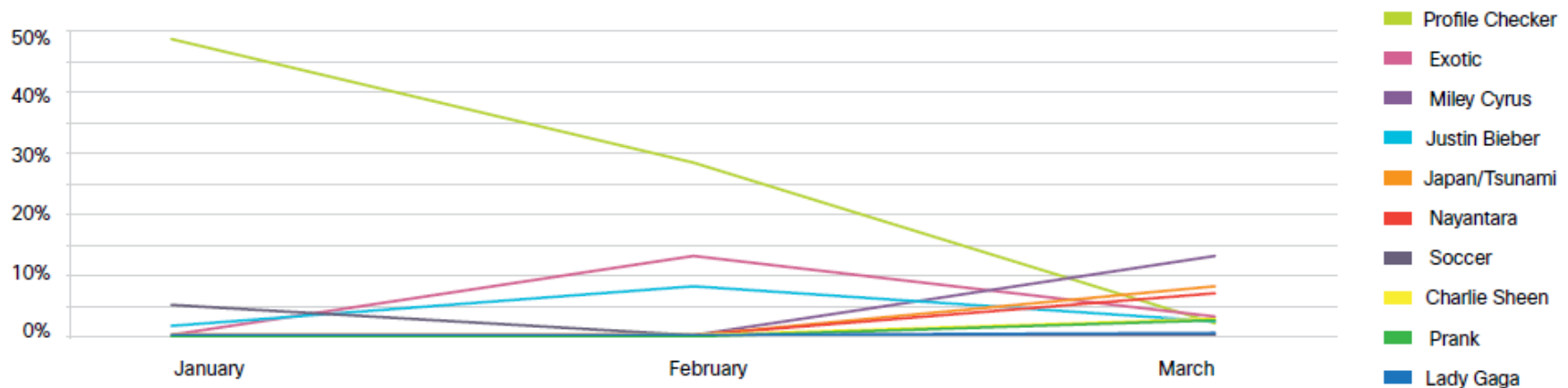
# Probable variants in the Future (Social Networks Based)

## Likejacking

“Likejacking” refers to a method of clickjacking that uses image overlays to forcibly cause a Facebook user to “Like” a particular page.

In turn, this causes a link to the page to appear on the user’s Facebook wall, exposing their Facebook friends to the likejacking scam.

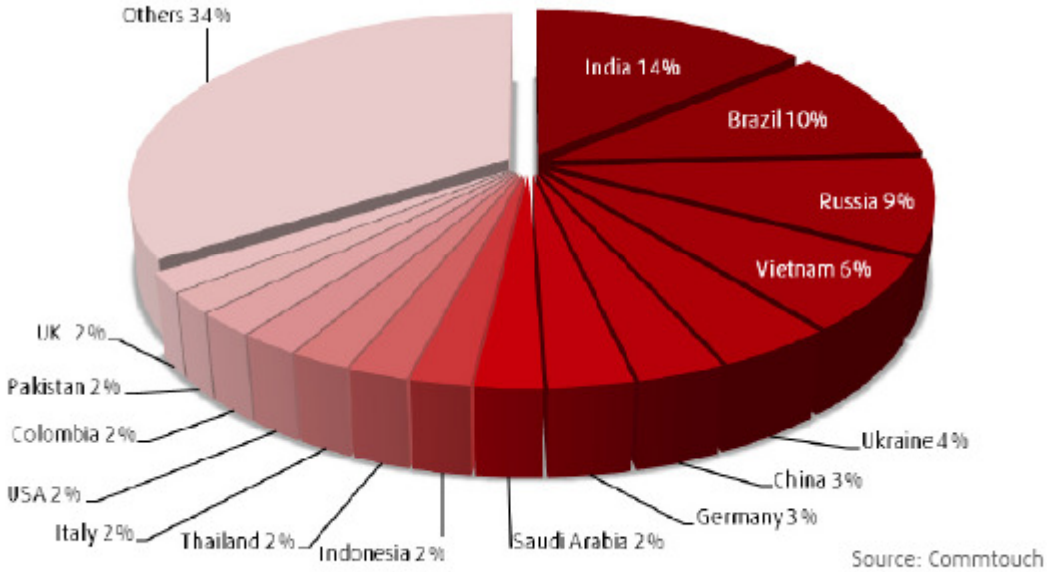
This worm-like scam is often accompanied by a phishing segment whereby the victim is also tricked into providing their Facebook username and password. (Not completely a Malware, but a method)



Source: Cisco Global Threat Report 1Q2011

# Zombie Hotspots @ Home

India leading as Zombie Hotspots (14 %)



\* Source: Commtouch Internet Threats Trend Report Q3 2010

# Malware News Bytes

**Daily more than 60,000  
malwares introduced**

**Trojan's account for 60% of  
malwares followed by  
crimeware & spyware**

**13.5 % of the recorder Malware  
attacks are thru USB / Flash  
drives**

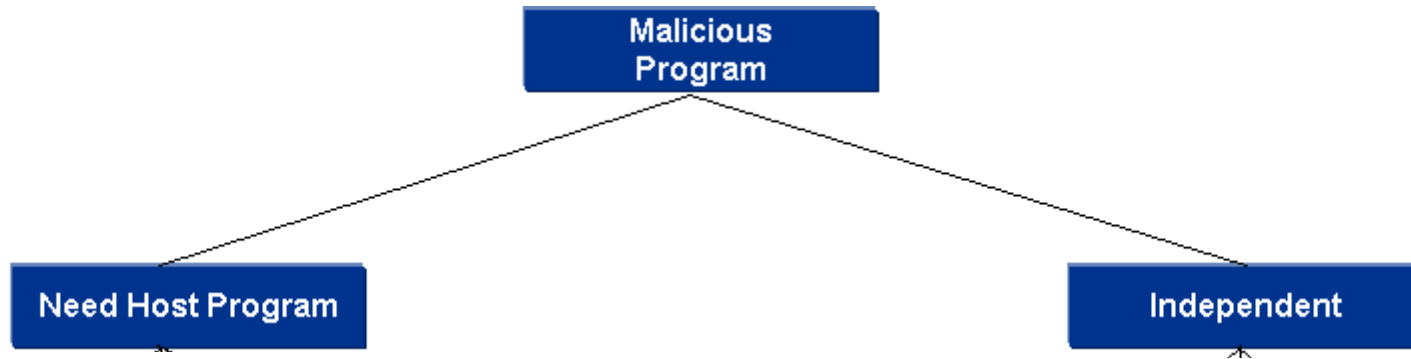
**McAfee saw 55,000 & 280,00  
AutoRun attacks in April & May  
2010**

**In 2009 India accounted for 15 %  
of malicious activities in APJ  
region**

**Indian Embassy Website in Spain  
was defaced and used to spread  
Malwares**

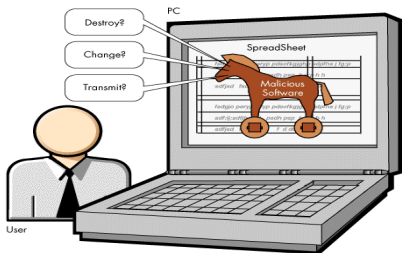
# Introduction

# What is a Malware?





# Malwares & their Variants



**Trojan Horse** – Malicious software running in background in context of a valid program. Appears to perform a valid desirable function.

Possible Operations that can be performed using Trojan Horse:

- Use of the system as Botnet
- Uploading / Downloading of files
- Unauthorized access
- Keystroke Logging and DOS

**Computer Worms** - Self Replication malware variant. Independent Execution. Spreads across the network

Most popular Worms in the Wild:

- Morris worm
- Mydoom
- Conficker



**Adware** – Malware variants which automatically plays, displays & downloads advertisements.

**Purpose**

- Advertisement
- Marketing
- Forcibly displaying vendor contents

**Spyware** – Malware that stealthily obtains user's information

**Purpose**

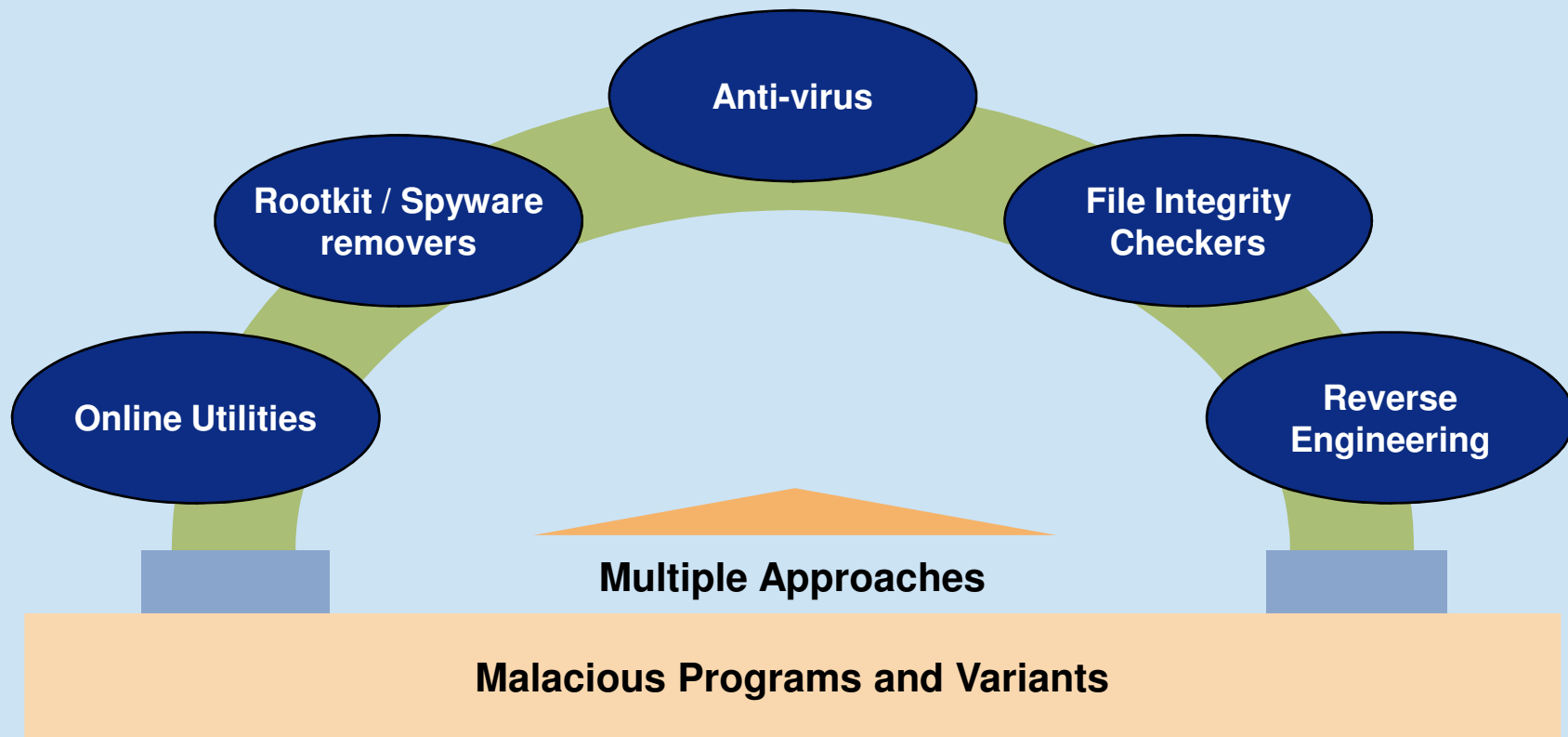
- Passwords
- Credit Card details
- Confidential Information





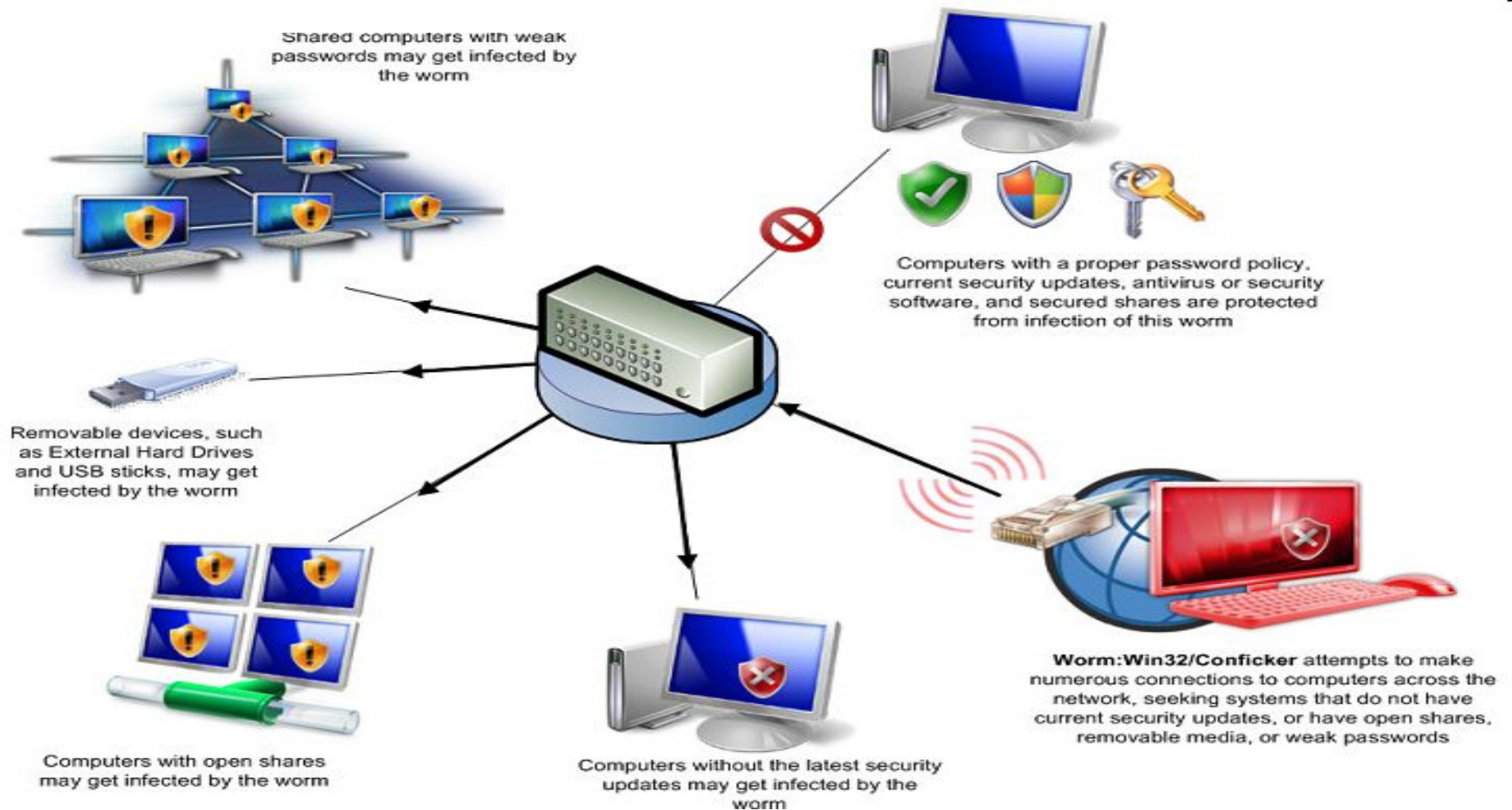
**Myths**

## Myth I – I bought an Anti-virus and it is good enough



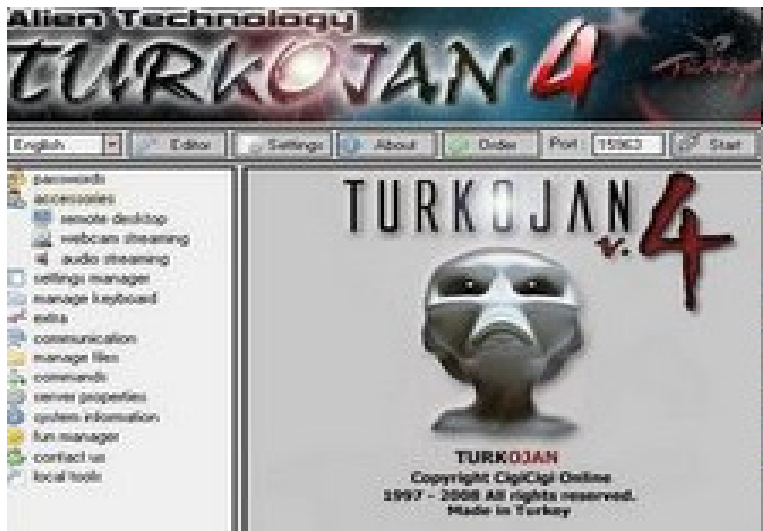
# Myth II – Malwares spread only if the System is connected to the INTERNET

Is it really so ?



# Myth III – Malwares creation requires an extraordinary effort

Not Really !



Turkojan a commercial Malware creator



GUI based Virus & Malware Creator

# Malwares & Art of Reverse Engineering

# So we know why they are written...

**Stealing of Confidential Information**

**Destroying of Files**

**Covert Channels**

**Defacing Websites**

**Forced Advertising**

**Pranks**

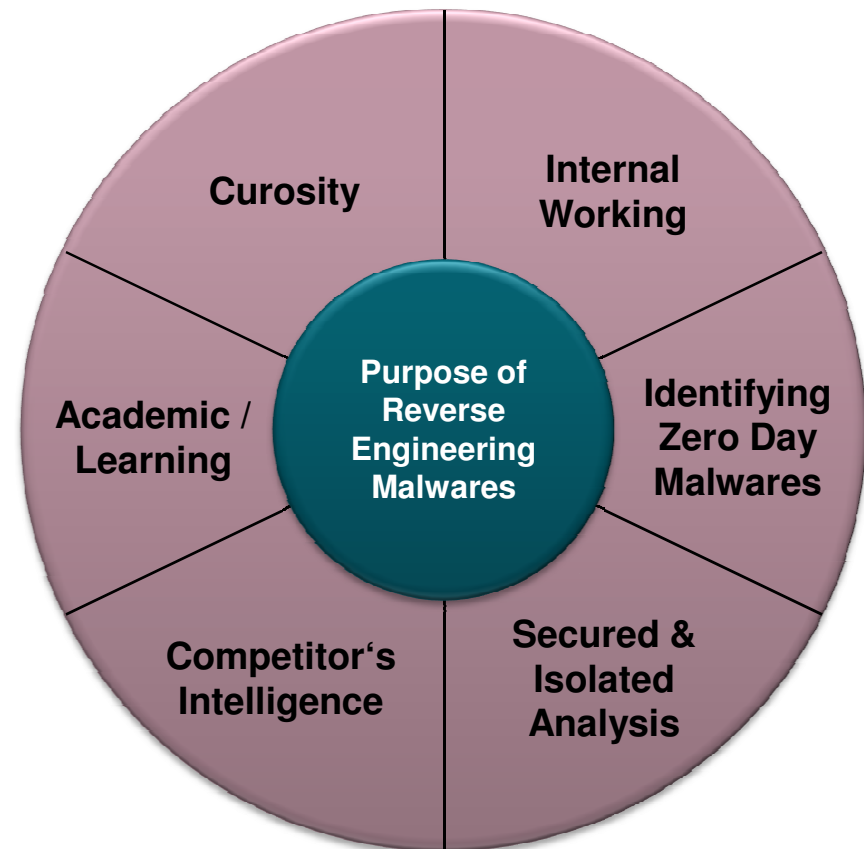
**Back Doors**

# Lets Demystify them with the ART OF REVERSE ENGINEERING

Reverse Engineering is a science

It is a science where the working of an object is analyzed by

- Breaking it down;
- Tearing it apart; and then
- Putting it together





# Malware Detection & Analysis Life Cycle

# Malware Detection & Analysis Life Cycle



# Data Collection & Analysis



Data  
Collection

## Spotting malicious behavior

To identify systems & network components which are showing suspicious behavior



Data  
Analysis

## Malware Discovery or Behavior Analysis (Reverse Engineering)

To gather / analyze information relevant to identification & collection of suspicious files, services and interconnections

# Code Analysis

Code  
Analysis

## Code Analysis – Reverse Engineering

**Understanding the internal working of the malware to prevent spread and further infection by using Debuggers and Disassemblers**

- **OllyDBG (Free Debugger and Disassembler)**
- **IDA Pro**

Modify  
Data  
Collectors

## Developing Indicators & Modifying Data Collectors

**Identify other infected systems and improvise on malware detection analyzing techniques**

# Ad-Hoc Utilities used for Malware Detection / Analysis

## In Built System Commands / Utilities

- “netstat”
- “dir”
- “Search” in start menu
- “regedit”
- “sigverif”

## Browser Plug In's

- McAfee Site Advisor
- Firefox Plug In's / Add On's - Malware Search, WOT, Interclue

## Sandbox

- Sandboxie

## Online Tools / Utilities

- Google Safe Browsing
- Virus Total
- Anubis



# **Behavior Analysis**

## **– A Construct**

# Behavior Analysis

## 3 Stage Approach

Source - <http://zeltser.com/reverse-malware/live-messenger-malware.zip>

Infect a laboratory system with the specimen

Observe how the malicious executable accesses the file system, the registry, and the network

Adjust the laboratory infrastructure to evoke additional behavior from the program also attempt to interact with the program to discover additional characteristics it may exhibit



Behaviour Analysis Source - <http://zeltser.com>

# Behavior Analysis

## Setup the Lab (Controlled Environment)

Virtualized Environment (Multi Instance for Comparison)

Multiple snapshots, which comes in very handy for “bookmarking” different stages of your analysis and for reverting back to system’s pristine state

Malware may have defenses that prevent it from executing properly in a virtualized environment. In these cases, the easiest step might be to use a set of physical systems (DD)



Behaviour Analysis Source - <http://zeltser.com>



# Behavior Analysis

## Mitigating Risk

Virtualized Environment (Not Airtight – Physical Systems)

Virtualization Software Bugs – Could be Vulnerable to the Malicious code being analyzed

No Connection to the Production Environment and Updated Patches is a MUST.



Behaviour Analysis Source - <http://zeltser.com>

# Behavior Analysis

## The Approach and Infection

Examine the new files.

1<sup>st</sup> Snapshot of Registry prior to upload of malicious code

(<http://sourceforge.net/projects/regshot>) → Multiple Registry Shots and Comparison Tool

Launch malicious code, Interact, Login, Kill process and take 2<sup>nd</sup> Snapshot of Registry

Compare the registry files to see for major system changes

(In this case, we see that two files were added to the system → msnsettings.dat and pas.txt)

```
pas.txt - Notepad
File Edit Format View Help
www. .com
Username: abc@example.com
Password: pass
www. .com

msnsettings.dat - Notepad
File Edit Format View Help
hello
0
-1
-1
0
0
-1
Please type in an error message
C:\Program Files\MSN Messenger\msnmsgr.exe
0
0
0
0
C:/
```

It looks like pas.txt has captured the login credentials we used when logging into the malicious executable.

The msnsettings.dat file looks like a configuration file

Behaviour Analysis Source - <http://zeltser.com>

# Behavior Analysis

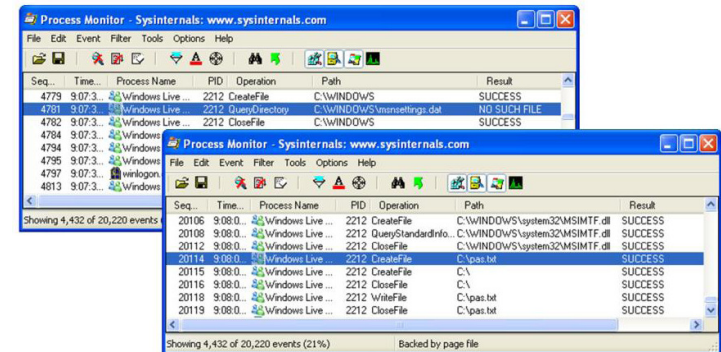
## Monitoring

Process Monitor records API calls it observes on the system that deal with file system and registry access. It shows the details of how programs create, delete, read or modify the local environment

Process Monitor's log is very comprehensive. However, it is also very noisy

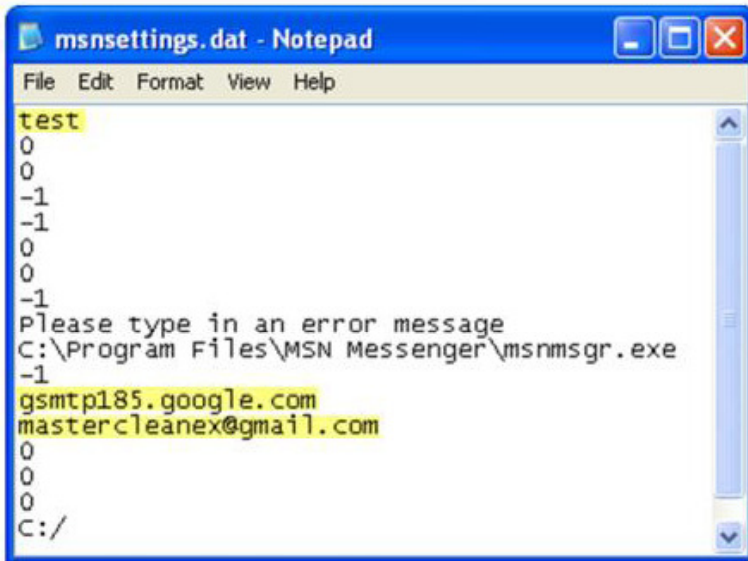
Attempts by malware specimen to create pas.txt file and to locate the msnsettings.dat file → screenshot

Process Monitor observes malware as it infects the system.



# Behavior Analysis

## Reading the Contents



```
msnsettings.dat - Notepad
File Edit Format View Help
test
0
0
-1
-1
0
0
-1
Please type in an error message
C:\Program Files\MSN Messenger\msnmsgr.exe
-1
gsmtmp185.google.com
mastercleanex@gmail.com
0
0
0
C:/
```

### Analysis of Content

1. String "Test"
2. Gsmtp185.google.com → DNS
3. mastercleanex@gmail.com → SMTP

### Theories

### Inference

1. Processing the DAT File
2. Capability to connect outside
3. Capability to send email



**To Confirm - We Read the Network**

Behaviour Analysis Source - <http://zeltser.com>

# Behavior Analysis

## Verifying the Theory

CaptureBAT is similar to Process Monitor in that it records local processes' interactions with their environment. (Less Noisy – Filters)

Load the .cap file created by CaptureBAT into a full-feature network sniffer, such as Wireshark (<http://www.wireshark.org>).

Attempts by malware specimen to create pas.txt file and to locate the msnsettings.dat file → screenshot

```
C:\>capturebat -c -n
```

```
Option: Capturing network packets
Option: Collecting modified files
Loaded kernel driver: CaptureProcessMonitor
Loaded kernel driver: CaptureRegistryMonitor
Loaded filter driver: CaptureFileMonitor
```

```
-----
process: created C:\WINDOWS\explorer.exe -> ...Windows Live Messenger.exe
file: Write ...Windows Live Messenger.exe -> C:\WINDOWS\msnsettings.dat
file: Write ...Windows Live Messenger.exe -> C:\pas.txt
```

No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:0c:29:ca:2a:f2	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.11.129? Tell 192.168.11.129
2	0.038277	00:0c:29:15:71:e1	00:0c:29:ca:2a:f2	ARP	192.168.11.129 is at 00:0c:29:15:71:e1
3	0.039666	192.168.11.128	192.168.11.129	DNS	Standard query A gsmtpl85.google.com
4	0.067907	192.168.11.129	192.168.11.128	ICMP	Destination unreachable (Port unreachable)

Frame 3 (79 bytes on wire, 79 bytes captured)  
Ethernet II, Src: 00:0c:29:ca:2a:f2 (00:0c:29:ca:2a:f2), Dst: 00:0c:29:15:71:e1 (00:0c:29:15:71:e1)  
Internet Protocol, Src: 192.168.11.128 (192.168.11.128), Dst: 192.168.11.129 (192.168.11.129)  
User Datagram Protocol, Src Port: blackjack (1025), Dst Port: domain (53)  
Domain Name System (query)  
Transaction ID: 0x1bad  
Flags: 0x0100 (Standard query)  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
Queries  
gsmtpl85.google.com: type A, class IN

The hostname suggests SMTP, but use DNS resolution

**Theory  
Confirmed**

Behaviour Analysis Source - <http://zeltser.com>

# Behavior Analysis

## The Interaction with Malware

The Fake DNS window shows a request for tp185.google.com. The network traffic analysis shows a SYN packet from 192.168.11.128 to 192.168.11.129 on port 25, followed by an RST, ACK response.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.11.128	192.168.11.129	TCP	1078 > 25 [SYN] Seq=0 win=64240 L
2	0.005603	192.168.11.129	192.168.11.128	TCP	25 > 1078 [RST, ACK] Seq=1 Ack=1

Redirect all DNS Queries to IP: C:\127.0.0.1 User defined 192.168.11.129

Confirmed SMTP attempt.

### Servers in the LAB

1. DNS Server (Host File or Fake DNS)
2. SMTP Server (Mail Pot Tool)
3. Add Additional Services as you learn
4. Repeat till no new discoveries

Move on to Code Analysis

The Mailpot Active window shows a listening log for port 25. The Notepad window shows the raw SMTP data received, including the sender's email address and password.

```
Received From: 127.0.0.1
TO:<mastercleanex@gmail.com>
s FROM:<yourpassword@password.com>

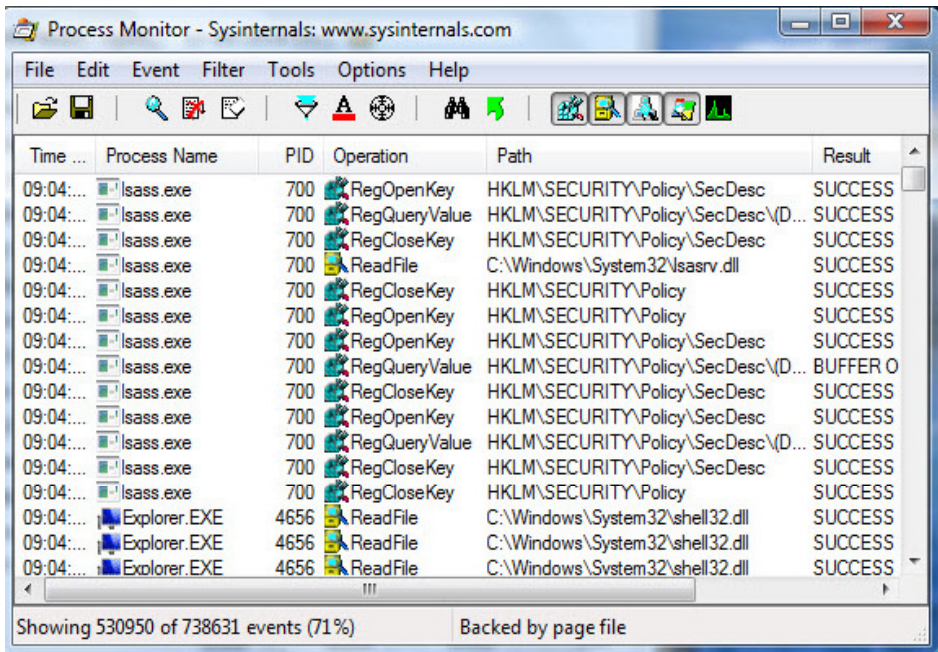
P DEBUGMODE RAW DATA FOLLOWS

EHLO labbox
RSET
MAIL FROM:<yourpassword@password.com>
RCPT TO:<mastercleanex@gmail.com>
DATA
From: yourpassword@password.com
Subject: Username: abc@example.com
To: mastercleanex@gmail.com
Date: Sat, 7 Mar 2009 22:20:15 -0500
X-Priority: 3
X-Library: Indy 9.00.10

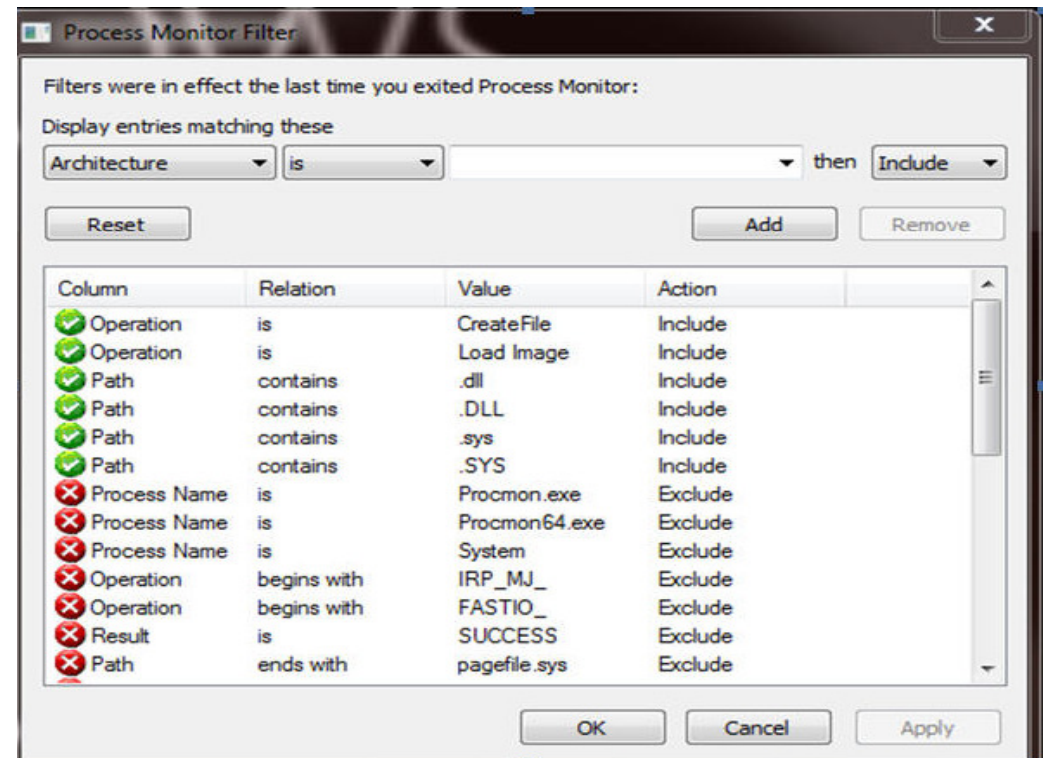
Password: pass
```

Behaviour Analysis Source - <http://zeltser.com>

# Dynamic Malware Analysis – Process Monitor



**Process Monitor**



**Process Monitor Filter**

# Code Analysis



# Code Analysis

## Expands and Reinforces Behavior Analysis

Code analysis can be tricky and time-consuming,  
You never get to see the source code

A Disassembler converts the specimen's instructions from  
their binary form into the human-readable assembly form

A debugger lets you interact and observe the effects of its  
instructions

Behaviour Analysis Source - <http://zeltser.com>

# Code Analysis

## Strings and their meaning

A good way to start analyzing the specimen's code often involves looking at the strings embedded in its executable.

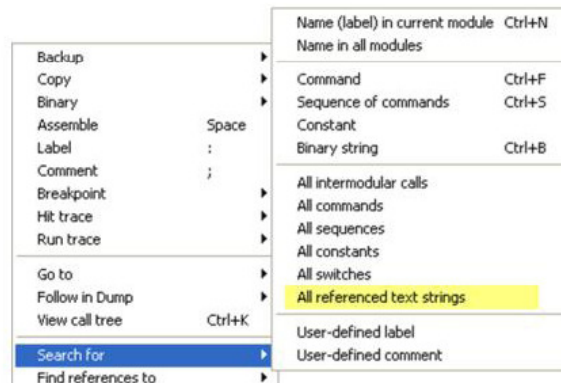
The string "test" is not visible anywhere within the body of the malicious executable when it's not running.

2

Address	Disassembly	Text string
00496EC0	PUSH Windows_.004973BC	ASCII "msnsettings.dat"
00496EE5	MOV EDX,Windows_.004973D4	ASCII "hello"
00496F12	MOV EDX,Windows_.004973F0	ASCII "-1"
00496F21	MOV EDX,Windows_.004973F0	ASCII "-1"
00496F4E	MOV EDX,Windows_.004973F0	ASCII "-1"
00496F5D	MOV EDX,Windows_.004973FC	ASCII "Please type in an error m
00496F6C	MOV EDX,Windows_.00497424	ASCII "C:\Program Files\MSN Mess
00496F8A	MOV EDX,Windows_.00497458	ASCII "C:/"

Looks like default msnsettings.dat content.

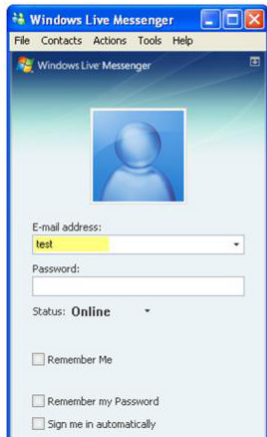
1



# Code Analysis

.....with patience...

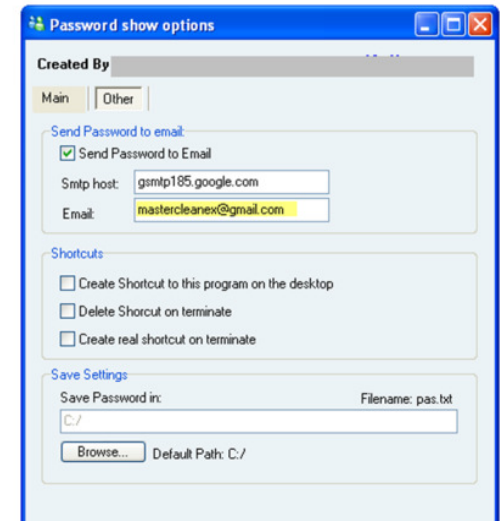
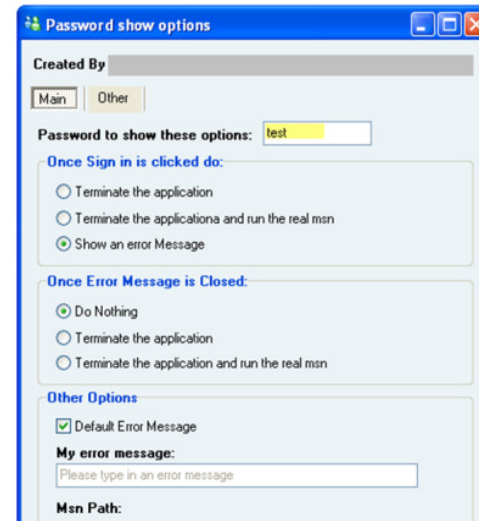
The trojan seems to be looking for the string "test" in the "E-mail address" field.  
Launch the trojan and enter "test" to see what happens



Enter "test" in the field to see what happens (outside the debugger).



Behaviour Analysis Source - <http://zeltser.com>



Enter "test", the trojan brings you to a brand new screen that seems to allow you to configure the trojan's operation.

The configuration options let you define the passphrase to activate this string, the address where the trojan will send captured logon credentials, etc.

# Case Study

# Case Study – Operation Aurora

## Aurora Demystified

### Overview

Highly sophisticated and targeted attacks on major cooperates from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors.

Targeted companies included Google, Adobe Juniper Rackspace etc.

Attack targeted source code repositories and tried to gain access and modify source codes

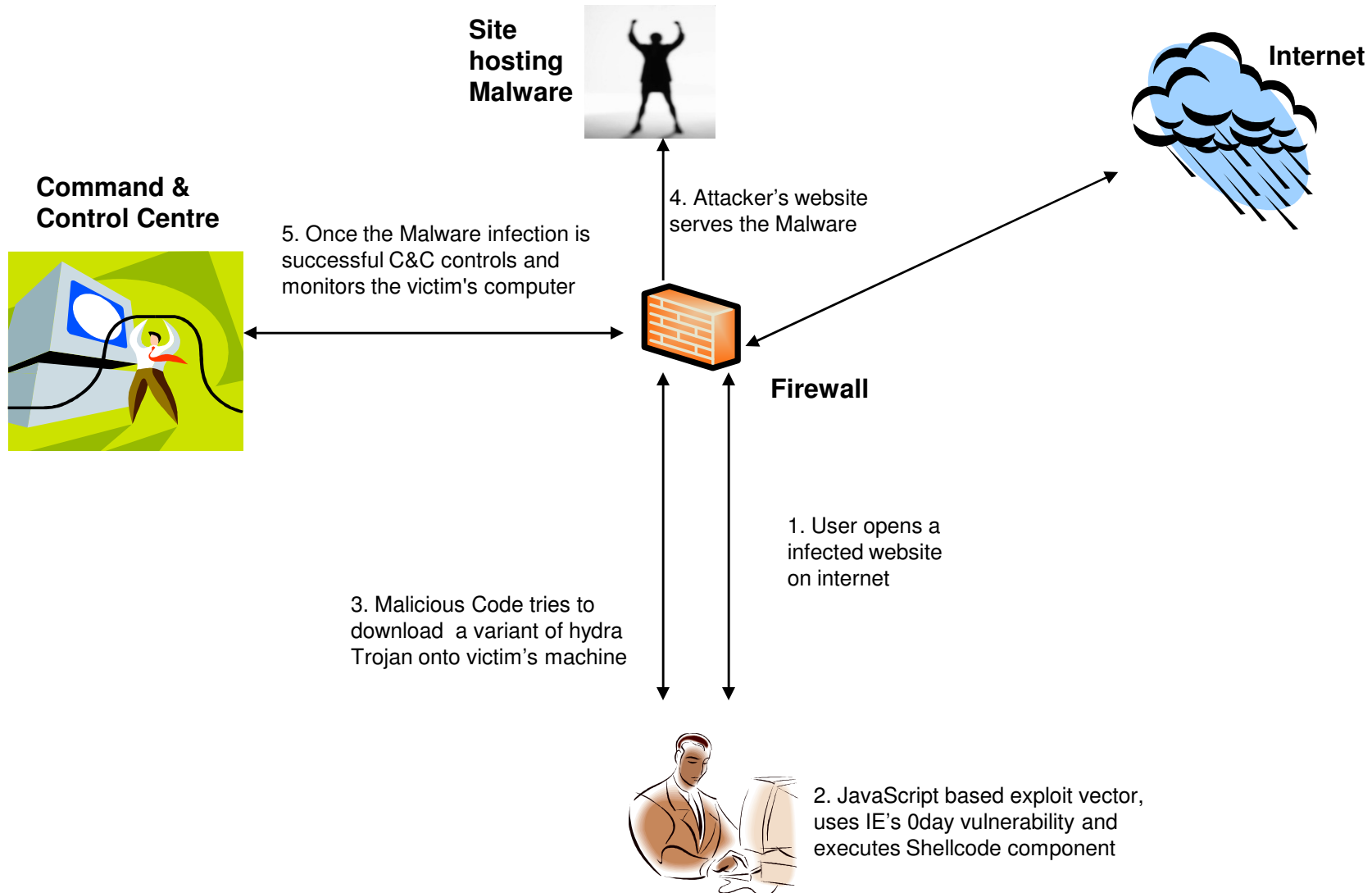
### Mode of attack

- Typical example of a Drive by Download attack
- Attack exploited 0day vulnerability(cve-2010-0249) in Internet Explorer versions 6, 7, and 8 on Windows 7, Vista, Windows XP, Server 2003, Server 2008 R2, as well as IE 6 Service Pack 1 on Windows 2000 Service Pack 4
- Multiple layers of code obfuscation and encryption to avoid antivirus detection
- Custom encryption protocol, a non-standard SSL channel used for communicating with Command & control
- Post exploit variant of Hydra Trojan was used inject and monitor the target system

### Impact

- Compromised Corporate Network
- Theft of Intellectual property
- Large scale theft of customer data and company source code

# Case Study – Operation Aurora



# Reverse-Engineering Malware (Cheat Sheet)

## Approach

Set up a controlled, isolated laboratory in which to examine the malware specimen.

Perform behavioral analysis to examine the specimen's interactions with its environment

Perform static code analysis to further understand the specimen's inner-workings.

Perform dynamic code analysis to understand the more difficult aspects of the code.

If necessary, unpack the specimen.

Repeat steps 2, 3, and 4 (order may vary) until sufficient analysis objectives are met.

Document findings and clean-up the laboratory for future analysis.

1. Be ready to revert to good state via dd, VMware snapshots, CoreRestore, Ghost, SteadyState, etc.
2. Monitor local (Process Monitor, Process Explorer) and network (Wireshark, tcpdump) interactions.
3. Detect major local changes (RegShot, Autoruns).
4. Redirect network traffic (hosts file, DNS, Honeyd).
5. Activate services (IRC, HTTP, SMTP, etc.) as needed to evoke new behavior from the specimen.

IDA Pro is a Windows or Linux or Mac OS X hosted multi-processor disassembler and debugger

OllyDbg is a 32-bit assembler level analysing debugger for Microsoft Windows. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable.

<http://zeltser.com/reverse-malware/reverse-malware-cheat-sheet.html>

# Case Study – Operation Aurora

## References

1. HB GARY THREAT REPORT: OPERATION AURORA  
[http://www.hbgary.com/wp-content/themes/blackhat/images/hbgthreatreport\\_aurora.pdf](http://www.hbgary.com/wp-content/themes/blackhat/images/hbgthreatreport_aurora.pdf)
2. The Command Structure of the Aurora Botnet  
[http://www.damballa.com/downloads/r\\_pubs/Aurora\\_Botnet\\_Command\\_Structure.pdf](http://www.damballa.com/downloads/r_pubs/Aurora_Botnet_Command_Structure.pdf)
3. Operation “Aurora” Hit Google, Others  
<http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others>



# Thank You

Presentation by Sony Anthony  
Associate Director, IT Advisory  
KPMG, Bangalore

© (2010) KPMG, an Indian Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International Cooperative ("KPMG International").

