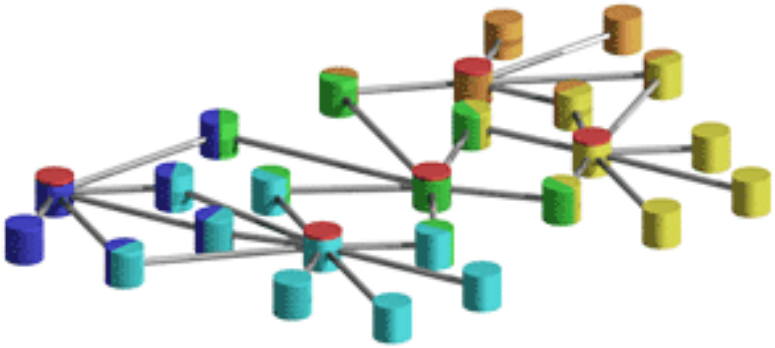
Πανεπιστήμιο Θεσσαλίας
Τμήμα Πληροφορικής

Introduction to Malware Analysis



Partially based on “Practical Malware Analysis
Kris Kendall and Chad McMillan

Malware Analysis Basics

Malware Analysis

- Dissecting malware to understand
  - How it works
  - How to identify it
  - How to defeat or eliminate it
- A critical part of incident response

Why Analyze Malware

- To assess damage
- To discover indicators of compromise
- To determine sophistication level of an intruder
- To identify a vulnerability
- To catch the “bad guy”
- To answer questions...

The Goals of Malware Analysis

- Information required to respond to a intrusion
  - Exactly what happened
  - Ensure you've located all infected machines and files
  - How to measure and contain the damage
  - Find signatures for intrusion detection systems

General Rules for Malware Analysis

- Don’t Get Caught in Details
  - You don’t need to understand 100% of the code
  - Focus on key features
- Try Several Tools
  - If one tool fails, try another
  - Don’t get stuck on a hard issue, move along
- Malware authors are constantly raising the bar

Business Questions

- What is the purpose of the malware?
- How did it get there?
- Who is targeting us and how good are they?
- How can I get rid of it?
- What did they steal?
- How long has it been there?
- Does it spread on its own?
- How can I find it on other machines?
- How do I prevent this from happening in the future?

Technical Questions

- Network Indicators?
- Host-based Indicators?
- Persistence Mechanism?
- Date of Compilation?
- Date of Installation?
- What language was it written in?
- Is it packed?
- Was it designed to thwart analysis?
- Does it have any root kit functionality?

What is Malware

- Generally
  Any code that “performs evil” Today
- Executable content with unknown functionality that is resident on a system of investigative interest
  - Viruses
  - Worms
  - Intrusion Tools
  - Spyware
  - Rootkits

Analysis techniques

- **Types of Malware I**
  - **Backdoor**. Malicious code that installs itself onto a computer to allow the attacker access. Backdoors usually let the attacker connect to the computer with little or no authentication and execute commands on the local system.
  - **Botnet**. Similar to a backdoor, in that it allows the attacker access to the system, but all computers infected with the same botnet receive the same instructions from a single command-and-control server.
  - **Downloader**. Malicious code that exists only to download other malicious code. Downloaders are commonly installed by attackers when they first gain access to a system. The downloader program will download and install additional malicious code.
  - **Information-stealing malware**. Malware that collects information from a victim's computer and usually sends it to the attacker. Examples include sniffers, password hash grabbers, and keyloggers. This malware is typically used to gain access to online accounts such as email or online banking.
  - **Launcher**. Malicious program used to launch other malicious programs. Usually, launchers use nontraditional techniques to launch other malicious programs in order to ensure stealth or greater access to a system.

Analysis techniques

- **Types of Malware II**

  - **Rootkit**. Malicious code designed to conceal the existence of other code. Rootkits are usually paired with other malware, such as a backdoor, to allow remote access to the attacker and make the code difficult for the victim to detect.

  - **Scareware/Ransomware**. Malware designed to frighten an infected user into buying something. It usually has a user interface that makes it look like an antivirus or other security program. It informs users that there is malicious code on their system and that the only way to get rid of it is to buy their “software,” when in reality, the software it’s selling does nothing more than remove the scareware.

  - **Spam-sending malware**. Malware that infects a user’s machine and then uses that machine to send spam. This malware generates income for attackers by allowing them to sell spam-sending services.

  - **Worm or virus**. Malicious code that can copy itself and infect additional computers.

Exams Questions example

- Πολλαπλής Επιλογής
  - **Το Incident Management περιλαμβάνει τις παρακάτω φάσεις**
    - A. Preparation, Integration, Containment, Recovery, After-Action-Reporting
    - B. Preparation, Identification, Collaboration, Erasure, Recovery, Lessons Learned
    - C. Prioritazion, Identification, Containment, Eradication, Recovery, lessons learned
    - D. Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.
- Σωστό / Λάθος
  - **Η συγκέντρωση στοιχείων με συστηματικό (forensic solid) τρόπο είναι σημαντικό βήμα της identification φάσης.**
    - **A. Σωστό**
    - **B. Λάθος**

Malware Analysis Basics

SSD Analysis tools: Digital Forensics

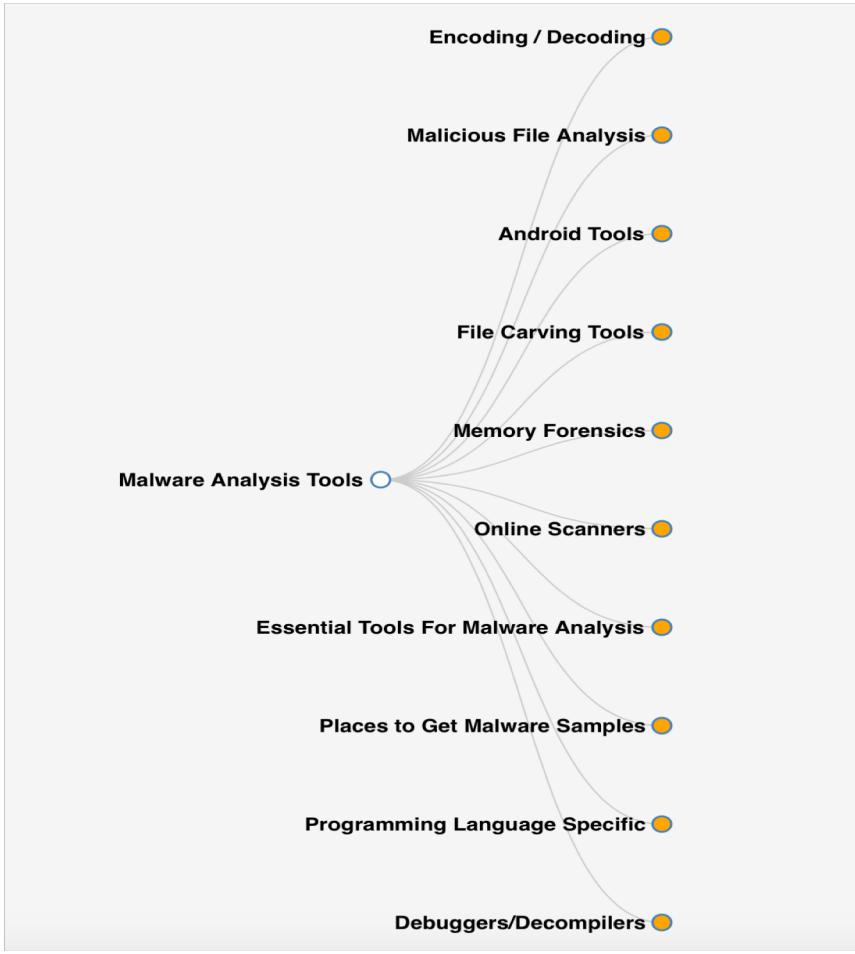
- Complicated due to the way SSDs manage / store information:
  - Almost all present-day SSDs have hardware data encryption.
  - Today's SSDs are manufactured based on NAND Flash microchips
  - All SSDs come with a pre-manufactured Techno Mode:
    - This special mode is designed to debug devices; manufacturers use it to examine broken drives in order to identify the damaged part of a microcode and address the cause in future firmware versions.
  - A set of tools are available to force SSD in this mode in order to recover the stored information:
    - https://github.com/CyberShadow/trimcheck
    - https://belkasoft.com/ec

Infosec tools

- General list:
  - https://isc.sans.edu/tools/
  - https://sectools.org
  - https://securitytrails.com/blog/top-15-ethical-hacking-tools-used-by-infosec-professionals
- Malware Analysis:
  - https://cuckoosandbox.org
  - http://malwareanalysis.tools/index.html
  - https://www.joesecurity.org
  - http://www.toolwar.com

Malware Analysis tools

- Source: http://malwareanalysis.tools/index.html



Malware Analysis Basics

- Analysis techniques
- On-line Analysis
- Dynamic Analysis
- Static Analysis

Analysis techniques

- Malware Analysis Techniques
  - Static Analysis
    - Basic: consists of examining the executable file without viewing the actual instructions.
    - Advanced: analysis consists of reverse-engineering the malware's internals by loading the executable into a disassembler and looking at the program instructions in order to discover what the program does
  - Dynamic Analysis
    - Basic: techniques involve running the malware and observing its behavior on the system in order to remove the infection, produce effective signatures, or both.
    - Advanced: analysis uses a debugger to examine the internal state of a running malicious executable

Analysis techniques

- **General Rules for Malware Analysis**

  - **First**, don’t get too caught up in the details. Most malware programs are large and complex, and you can’t possibly understand every detail. Focus instead on the key features.

  - **Second**, remember that different tools and approaches are available for different jobs. There is no one approach. Every situation is different, and the various tools and techniques that you’ll learn will have similar and sometimes overlapping functionality.

  - **Finally**, remember that malware analysis is like a cat-and-mouse game. As new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis.

Basic Analysis

- Basic static analysis
  - View malware without looking at instructions
  - Tools: VirusTotal, strings
  - Quick and easy but fails for advanced malware and can miss important behavior
- Basic dynamic analysis
  - Easy but requires a safe test environment
  - Not effective on all malware

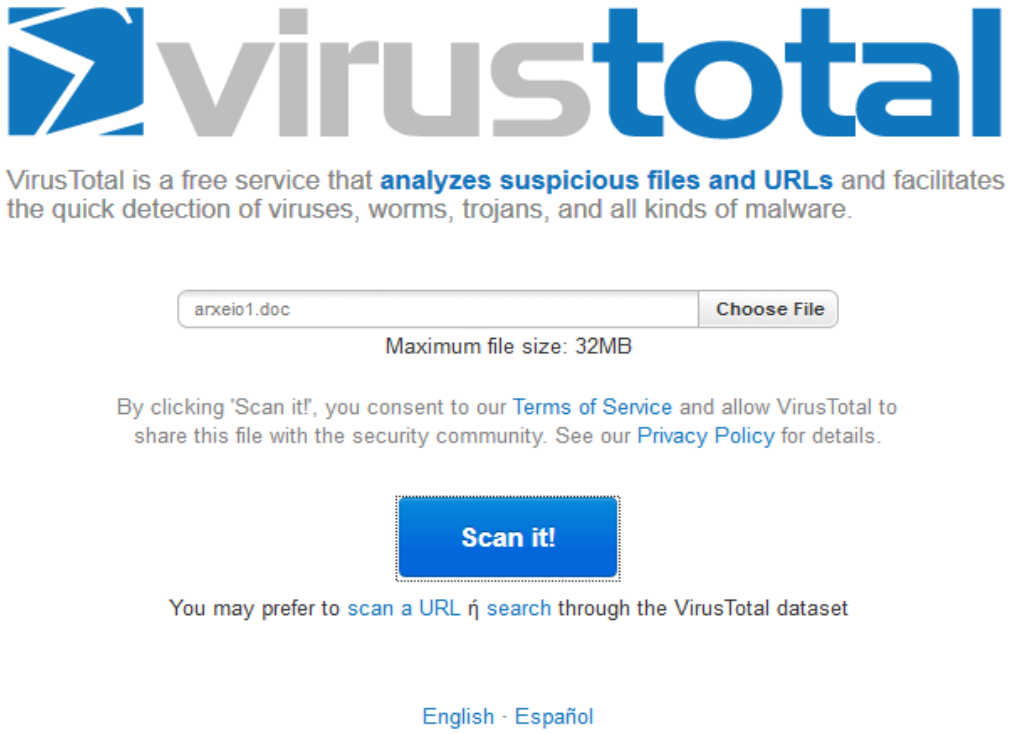
Advanced Analysis

- Advanced static analysis
  - Reverse-engineering with a disassembler
  - Complex, requires understanding of assembly code
- Advanced Dynamic Analysis
  - Run code in a debugger
  - Examines internal state of a running malicious executable

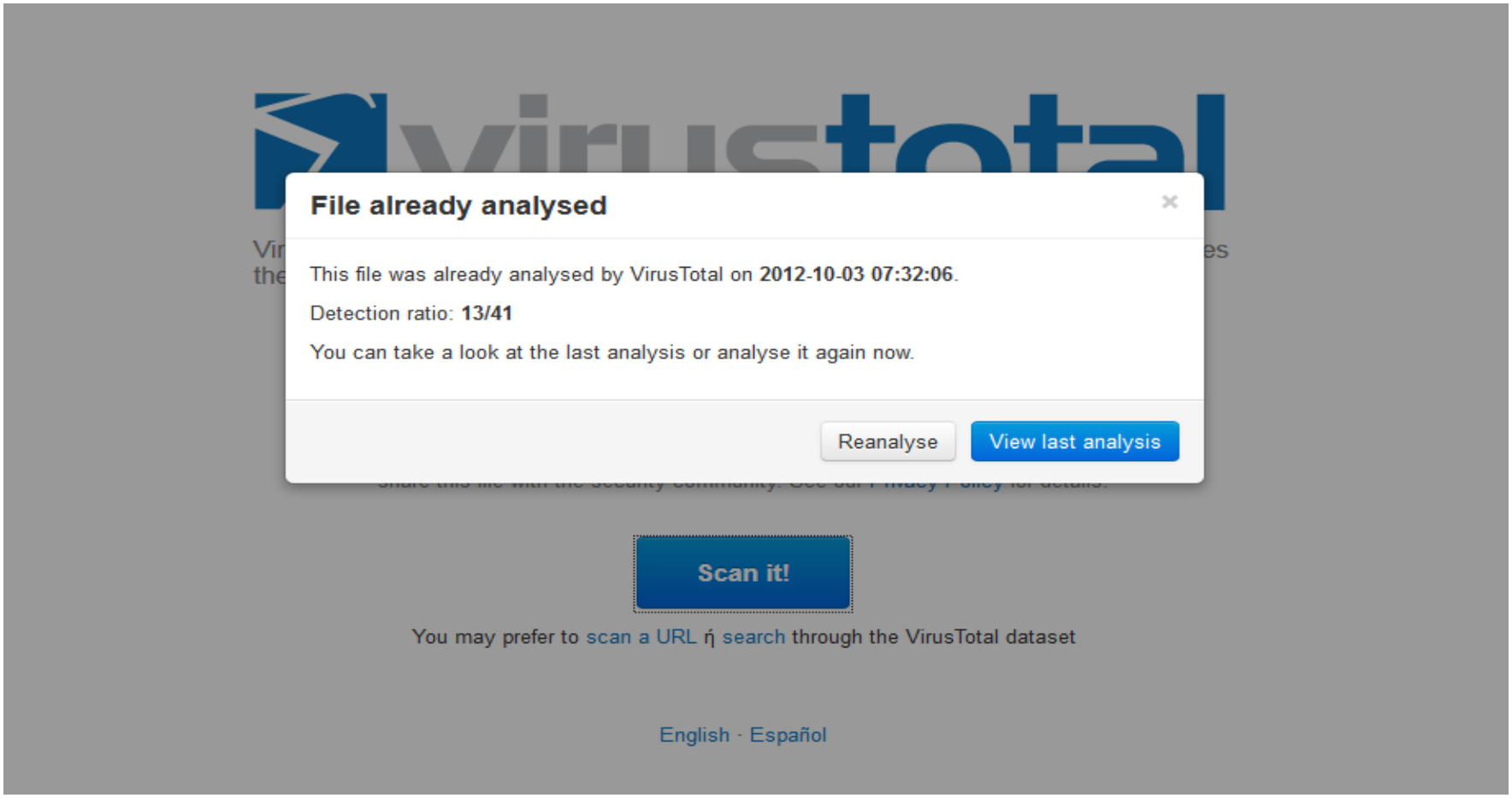
On-line Analysis

- Malware on-line analysis
  - Submission of the malicious file to a web site that offers malware analysis services.
  - Virus Total
    - Online malware scanning engine
    - Includes 41 AV vendor engines
    - Two options:
      - File submission
      - Hash search

On-line Analysis



On-line Analysis



On-line Analysis

virustotal

SHA256:	5fe53a960bc2031a185c575ea05ac466f26739a34c651c14260e4cfbc123e87f
SHA1:	d967d8ffe28ceb6f3c15954bf8f761a4233e2ae7
MD5:	cb51ef3e541e060f0c56ac10adef37c3
File size:	1.2 MB (1206576 bytes)
File name:	mal.doc
File type:	unknown
Tags:	cve-2010-3333 exploit
Detection ratio:	13 / 41
Analysis date:	2012-10-03 07:32:06 UTC (1 εβδομάδα, 2 ημέρες ago)

Less details

Analysis | Comments | Votes | Additional information

Antivirus	Result	Update
Agnitum	-	20121002
AntiVir	EXP/CVE-2010-3333.A.744	20121002
Antiy-AVL	-	20121002
Avast	RTF:CVE-2010-3333-AR [Expl]	20121003
AVG	-	20121002
BitDefender	Exploit.RTF.Gen	20121002
CAT-QuickHeal	RTF_Exploit_2010_3333	20121002

On-line Analysis

virustotal

SHA256:	5fe53a960bc2031a185c575ea05ac466f26739a34c651c14260e4cfbc123e87f
SHA1:	d967d8ffe28ceb6f3c15954bf8f761a4233e2ae7
MD5:	cb51ef3e541e060f0c56ac10adef37c3
File size:	1.2 MB (1206576 bytes)
File name:	mal.doc
File type:	unknown
Tags:	cve-2010-3333 exploit
Detection ratio:	13 / 41
Analysis date:	2012-10-03 07:32:06 UTC (1 εβδομάδα, 2 ημέρες ago)

Less details

Analysis | Comments | Votes | Additional information

ssdeep
24576:StL8dw0eGJ2TqeyInhaXluoi7oTUE/yFGGaYubhdsFSKLYs7TodK4cbuSp:N

TrID
Rich Text Format (100.0%)

First seen by VirusTotal
2012-09-27 11:31:06 UTC (2 εβδομάδες, 1 ημέρα ago)

Last seen by VirusTotal
2012-10-03 07:32:06 UTC (1 εβδομάδα, 2 ημέρες ago)

File names (max. 25)
1. mal.doc
2. arxeio1.doc

On-line Analysis

virustotal

SHA256: 5fe53a960bc2031a185c575ea05ac466f26739a34c651c14260e4cfbc123e87f

File name: arxeio1.doc

Detection ratio: 17 / 44

Analysis date: 2012-10-12 21:59:08 UTC (0 λεπτά ago)

More details

Analysis | Comments | Votes | Additional information

Antivirus	Result
Agnitum	-
AhnLab-V3	-
AntiVir	EXP/CVE-2010-3333.A.744
Antiy-AVL	-
Avast	RTF:CVE-2010-3333-AR [Expl]
AVG	-
BitDefender	Exploit.RTF.Gen
ByteHero	-
CAT-QuickHeal	RTF_Exploit_2010_3333
ClamAV	-
Commtouch	-
Comodo	UnclassifiedMalware
Kaspersky	Exploit.MSWord.CVE-2010-3333.bw
Kingsoft	-	20121008
McAfee	-	20121012
McAfee-GW-Edition	-	20121012
Microsoft	Exploit:Win32/CVE-2010-3333	20121012
MicroWorld-eScan	Exploit.RTF.Gen	20121012
Norman	-	20121012
nProtect	Exploit/W32.CVE-2010-3333.AAI	20121012
Panda	-	20121012
PCTools	-	20121012
Rising	-	20121012
Sophos	Exp/20103333-A	20121012
SUPERAntiSpyware	-	20121012
Symantec	-	20121012
TheHacker	-	20121009
TotalDefense	-	20121012
TrendMicro	-	20121012
TrendMicro-HouseCall	TROJ_GEN.F47V0927	20121012
VBA32	-	20121012
VIPRE	Exploit.RTF.CVE-2010-3333 (v)	20121012

On-line Analysis

- Online automated behavioral analysis tools
  - Anubis
  - GFI Sandbox (CWSandbox)
  - Joebox
  - Norman SandBox
  - ThreatExpert

On-line Analysis

GFI ThreatTrack™

Home

Submit an unknown sample for a FREE behavior analysis

GFI Sandbox™ (formerly CWSandbox) is an industry leading dynamic malware analysis tool. It gives you the power to analyze virtually any Windows application or file including infected: Office documents, PDF's, malicious URL's and Flash ads.

Once you submit your sample below we will email you an executive level PDF and an XML report containing all the behavior information gathered during analysis

File: * Αναζήτηση...

Email: *

Confirm Email: *

Enter the words you see above: *

Get new words

Choose captcha format: Image or Audio

By clicking on the 'Accept and submit my file' below you are agreeing to the Terms of Service.

Accept and submit my file

Due to heavy load, this public site does not support zipped files. Please contact us directly for sample analysis of this file type. Please note we only accept the following file types: PDF, PPT, PPTX, XLS, XLSX, EXE , DLL, DOC, DOCX, JAR, MSG, HTML, HTM, URL and executable files with no extension.

GFI Website | Support

For more information please contact ATG at ATG@gfi.com or by calling (855) 4-GFI-ATG (+1-855-443-4284)

On-line Analysis

Hello,

Thank you for submitting your sample for analysis by GFI SandBox.

Attached are the XML and PDF reports generated by GFI SandBox for analysis 20697. The PDF report contains an executive-level summary, incluc behavioral information gathered during analysis.

SandBox results for arxeio1.doc

Analysis ID:	20697
Date Analyzed:	2012-09-30 15:56:58
Sandbox Attributes:	IE 9, Office 2003, Adobe Reader 9.4, Flash 10.1, Java 6
MD5 Hash:	cb51ef3e541e060f0c56ac10adef37c3
Filename:	arxeio1.doc
File Type:	Rich Text Format data, version 1, unknown characte

Digital Behavior Traits		VirusTotal Results	
Injected Code	NO	Last Scanned:	2012-09-30 19:45:56
More than 5 Processes	NO	nProtect	Exploit/W32.CVE-2010-3333.AAI
Copies to Windows	NO	CAT-QuickHeal	RTF_Exploit_2010_3333
Windows/Run Registry Key Set	NO	McAfee	Not Detected
Makes Network Connection	NO	K7AntiVirus	Not Detected
Creates EXE in System	NO	TheHacker	Not Detected
Starts EXE in System	NO	F-Prot	Not Detected
Starts EXE in Documents	NO	Symantec	Not Detected
Deletes File in System	NO	Norman	Not Detected
Hooks Keyboard	NO	TotalDefense	Not Detected
Creates Hidden File	YES	TrendMicro-HouseCall	Not Detected
Creates DLL in System	NO	Avast	RTF:CVE-2010-3333-AR [Expl]
Creates Mutex	YES	eSafe	Not Detected
Alters Windows Firewall	NO	ClamAV	Not Detected
Checks For Debugger	YES	Kaspersky	Not Detected
Could Not Load	NO	BitDefender	Exploit.RTF.Gen
Opens Physical Memory	NO	Agnitum	Not Detected
Modifies Local DNS	NO	SUPERAntiSpyware	Not Detected
Starts EXE in Recycle	NO	Sophos	Exp/20103333-A
Creates Service	NO	Comodo	Not Detected
Modifies File in System	NO	F-Secure	Exploit.RTF.Gen
Deletes Original Sample	NO	DrWeb	Exploit.CVE2010-3333.7
		VIPRE	Exploit.RTF.CVE-2010-3333 (v)
		AntiVir	EXP/CVE-2010-3333.A.744
		TrendMicro	Not Detected
		McAfee-GW-Edition	Not Detected
		Emsisoft	Not Detected
		Jiangmin	Not Detected

On-line Analysis

NORMAN Proactive IT Security

Trials & Downloads | About Norman

Products | Personal | Business | Partner | Security Center | Support

Home > Security Center > SandBox Information Center

Security Center

- SandBox Information Center
- Malware Analysis Search
- Security articles
- Security blog
- Threat level
- Current virus threats
- Malware types
- Virus descriptions
- Email statistics
- Books, general white papers etc.
- Our Technology

SandBox Information Center

Print page

Submit a Suspicious File for a FREE Malware Analysis

Email: isiace@yahoo.gr

Filename: I:\VM Share Folder\malware\αρχειο1.doc Αναζήτηση...

Upload

Latest Submissions

SandBox Name	Signature Name	Executable type	Date
W32/Downloader	Not detected by signature	Application	2012-10-12 17:25:23
W32/Downloader	Not detected by signature	Application	2012-10-12 15:49:08
W32/VBKrypt.SE	Not detected by signature	Application	2012-10-12 14:31:22
W32/Crypt.AWHI	Not detected by signature	Application	2012-10-12 14:21:13

View all

Global Threats Overview

Based on submissions to Norman

Dynamic Analysis

- Dynamic analysis is any examination performed after executing the malware
- Involves
  - Monitoring malware as it runs
  - Examining the system after the malware has executed
- Pros
  - Observation of malware's true functionality
- Cons
  - May put your network or system at risk
  - Limitations of execution due to restricted malware functionality

Dynamic Analysis

- Establish a malware analysis lab (virtual or physical)
  - Virtual analysis lab
    - Best and most popular approach but…mind that malware may detect the virtual environment
    - Multiple virtual systems on the same machine with interaction between them
    - Ability to take snapshots
  - Lab isolation form the production environment

Dynamic Analysis

- Prepare the virtual environment
  - The objective is to mirror the production environment to the lab in order to simulate the same conditions
  - Install a clean guest OS
  - Identify normal behavior
  - Take a snapshot of the clean machine
  - Install behavioral analysis tools

Dynamic Analysis

- Behavioral analysis tools
  - File system and registry monitor
    - Process monitor, CaptuteBAT
  - Process monitoring
    - Process Explorer, Process Hacker
  - Network monitoring
    - Wireshark
  - Change detection
    - Regshot
  - Internet simulation
    - Fakenet, Inetsim

Dynamic Analysis

- Detect malicious behavior durng and after execution
  - Transfer malware to the guest machine
  - Forward all network traffic to the Internet simulator
  - State snapshot with regshot
  - Run CaptureBAT
  - Execute the malware
  - Detect changes with Regshot, CaptureBAT, processexplorer and processmonitor
  - Analyze traffic with Wireshark
  - Identify new processes, created files, deleted files, registry entries, registry modifications, network connections

Dynamic Analysis

- Automated dynamic malware analysis
  - Using a sandbox
    - a sandbox is a security mechanism for separating running programs.
  - Automated malware analysis systems
    - automatically run and analyze files and collect comprehensive analysis results that outline what the malware does.
    - Cuckoo Sanbox (also online malwr.com)
    - Buster Sandbox Analyzer (with Sandboxie)
    - REMnux (light Linux distribution focused on malware analysis)

Dynamic Analysis

- A report from an automated malware analysis includes:
  - General information
  - Changes to file system
  - Changes to registry
  - Network services
  - Process/window information
  - Screenshots during malware execution (Cuckoo)

Static Analysis

- Code analysis to determine its function without execution
  - AV scanning, file hashing
  - Strings
    - A program contains strings if it prints a message, connects to a URL, or copies a file to a specific location.
    - Very useful unless program is…packed
  - *Packed* programs
    - are obfuscated programs in which the malicious program is compressed and cannot be analyzed.
    - PEid to detect the type of packer or compiler employed to build an application.
    - LordPE to dump the malicious process image from memory (after executed and deobfuscated)

Static Analysis

- Portable Execution File Format (PE)
  - is a data structure that contains the information necessary for the Windows OS loader to manage the wrapped executable code.
  - Linked Libraries and functions
    - Dependency Walker explores dynamically linked functions
    - Identify imported and exported functions
  - PE file headers and sections
    - Useful Tools:
      - PEview , Resource hacker , PEBrowse, PE Explorer

Static Analysis

Sections of a PE File for a Windows Executable

Executable	Description
`.text`	Contains the executable code
`.rdata`	Holds read-only data that is globally accessible within the program
`.data`	Stores global data accessed throughout the program
`.idata`	Sometimes present and stores the import function information; if this section is not present, the import function information is stored in the `.rdata` section
`.edata`	Sometimes present and stores the export function information; if this section is not present, the export function information is stored in the `.rdata` section
`.pdata`	Present only in 64-bit executables and stores exception-handling information
`.rsrc`	Stores resources needed by the executable
`.reloc`	Contains information for relocation of library files

Static Analysis

- Disassembling and debugging
  - translates machine language into assembly language, test and debug.
    - IDA Pro
    - OllyDbg
  - More advanced techniques for static malware ananlysis

Static Analysis

- Other file formats for static analysis…
  - Microsoft Office files
    - OfficeMalScanner (locates shellcode and VBA macros)
    - Offvis (shows raw contents and structure)
  - Adobe PDF files
    - PDFid (identifies PDFs that contain strings associated with scripts and actions)
    - PDF-parser, Origami's pdfwalker(examine the structure and decode contents of PDF files)
    - Origami's pdfextract, Jsunpackn's pdf.py (extract JavaScript from PDF files)
    - pyew, peepdf (navigate through pdf)
  - Adobe Flash files
    - Swfdump, flare
  - Javascript code
    - Spidermonkey, firebug (javascript deobfuscation)
- Remember that all of the above extract or download and execute a PE file…

Questions