Malware Analysis Workshop

June 5, 2012

Michael Theuerzeit
Norman Data Defense Systems BV
michael@norman.nl
Veterans in the security industry

- Founded in 1984 - HQ in Oslo, Norway
- Pioneer in proactive security solutions
- Consumers, SMB, Enterprise & Government
  - Partner network worldwide
- Strong partnerships with key industry leaders
Agenda

• Malware trends
• Attack Vectors
• Malware Analysis methods
• Run-time Analysis with Malware Analyzer G2
Cyber threat spectrum

Who?
- Nation States
- Terrorists
- Irregular warriers
- Activists
- Criminals
- Cybervandals

Cyberspionage
- Duqu
- Flame

Cyberactivism
- Anonymous (Wikileaks)
- Stuxnet
- Magenta

Cyberterrorisme
- Attacks on Estland, Korea

Purpose
- Fun Money Control
- Limited purpose
- Terror Revolution
- (State) Power
Malware trends

• Malicious code growth
  • Mobile malware growing at extreme rates
    • 400 -> 13,000 (June ’11 – Jan ’12)
    • Mainly Trojans
  • Apple malware growing steadily
  • PC malware growth increasing again

• Size of malware
  • iframe 80 Bytes
  • Tinba 20KB
  • Stuxnet 1 MB
  • Flame 20 MB
Flame

- 650,000 lines of code
- Websites
- Trojan → phishing
- Worm
- Spreading via network & USB

- Sniffing the network traffic
- Taking screenshots
- Recording audio conversations, Skype
- Intercepting the keyboard, chats
Flame

- LUA - run in Virtual Machine → avoiding detection?
- After emails → maktoob.com / gawab.com
Flame units

- **Beetlejuice**
  - Enumerates Bluetooth devices & beacon

- **Microbe**
  - Records audio

- **Infectmedia**
  - Defines infection method
  - Autorun_infector (like stuxnet)
  - Euphoria juction point directory

- **Limbo**
  - Creates backdoor accounts in network domain
Flame units

- **Frog**
  - Infect with predefined user accounts
- **Munch**
  - HTTP server
- **Snack**
  - Listens to network interfaces and logs data
- **Boot_dll_loader**
  - Configuration
- **Weasel**
  - Creates directory listing of infected PC
Flame units

• **Boost**
  • Create list of specific files

• **Telemetry**
  • Logging

• **Gator**
  • Connects to C7C servers

• **Security**
  • Identifies hazardous files like AV, firewalls, etc

• **Bunny / Dbquery / Driller / Headache / Gadget**
  • Yet unknown
Flame
Malware trends

• SSL isn’t so safe
  • Grabbing username / password before encryption
• Targeted malware is on the rise
  • Malware looking at browser history and infect upon criteria
• New malware is hard to spot and remove
• Ransomware is increasing
  • It won’t go away unless you pay
• Old problems resurface
• Mobile malware increasing
Classes of malware

- Based on spreading mechanism, actions or attack vector

- Backdoors, trojans, worms, adware, bots, dialers, droppers, hijackers, loggers

- Ransomware, rogueware, scareware, spyware

- PC, Mac, mobile devices, SCADA
Attack vectors

• Drive-by infections

• Social media
  • Proliferation
  • Likes from ‘friends’
    • Fake facebook pages “Oops... divx plugin needed”
  • http://bit.ly/LtrZ3V ???
  • Many services
    • Legitimate: Bitly.com / Goo.gl / Tiny.cc
    • Hack.er have their own
  • QR codes

• 0-Day vulnerabilities
Attack vectors

• The internet of things
  • Everything is connected
  • RFID is everywhere

• What about security?
  • BYOD
  • Internet TV
  • Cable box
  • Fridge
Future Outlook 2012

• **Targeted attacks and APTs**
  • Regular malware will benefit from this

• **Consumerization of IT & Cloud computing**
  • US Army using Android tablets and phones?
  • Army Software Marketplace prototype

• **Anything SCADA**
  • What’s being PLC-controlled in your environment?
Future Outlook 20xx

• Crossing domains
  • Biologic viruses infecting computers?
    • DNA computers
    • Cotton based circuits (Cornell University)
  • Integrated chemical chips (Linköping University, Sweden)

• Computer viruses infecting people?
  • Medical implants
  • Function enhancing implants
  • Manipulating DNA databases
Future Outlook 20xx

- Malware and nanotechnology
  - 1st: Passive nanostructures (1st generation products)
    - a. Dispersed and contact nanostructures. Ex: aerosols, colloids
    - b. Products incorporating nanostructures. Ex: coatings; nanoparticle reinforced composites; nanostructured metals, polymers, ceramics
  - 2nd: Active nanostructures
    - a. Bio-active, health effects. Ex: targeted drugs, biodevices
    - b. Physico-chemical active. Ex: 3D transistors, amplifiers, actuators, adaptive structures
  - 3rd: Systems of nanosystems
    - Ex: guided assembling; 3D networking and new hierarchical architectures, robotics, evolutionary
  - 4th: Molecular nanosystems
    - Ex: molecular devices "by design", atomic design, emerging functions

- What about Singularity?
The need for analysis
Blackbox Analysis

• Consider the program as a black box (Bird watch 😊)

• Run it in a controlled environment and watch its actions
  • Registry, Files, Network traffic
  • Controlled access to different resources
    • DNS names
    • Network services
    • Other machines
Pros ‘n’ Cons – Blackboxing

• **Pros**
  - Quick and Easy for first insights
  - Automated extraction of many relevant information
  - No (human) effort required for known protocols
Pros ‘n’ Cons – Blackboxing

• Cons
  • Encrypted traffic, registry, file content
  • Communication peers need to be reachable
  • Large number of samples - only limited time
  • Timed functionality (updates, timed malcode)
  • Observes only one-time run for that specific sandbox (no NAT/non-NAT check, ...)
  • Sometimes easy to evade: Intentional Timeouts
    • Sleep(300000)
Static Analysis?

Analysis of binary code **without execution**

- 0x80485e0 <main>: push %ebp
- 0x80485e1 <main+1>: mov %esp,%ebp
- 0x80485e3 <main+3>: sub $0x68,%esp

- **Static information** (about data)
- Strings
- Binary data (JPGs, BMPs, executables)
- Sections
- Constants / immediate values
- Number of functions
- ...

**Structural relationships**

- Functions calls
- Sections usage
- Data origin/usage

- Packer/Obfuscation
- Encryption
- Rootkit
- Propagation
- Anti-Debug
Pros ‘n’ Cons – Static Analysis

• Pros
  • Examine all parts of executable
  • Ability to reveal timed behavior
  • No execution ⇒ No wait times / synchronization
  • See possible values for different locations in executable
  • Independent from environment
    • Connectivity
    • Communication endpoints (peers)
    • Operating System
  • Often faster results than with execution
Pros ‘n’ Cons – Static Analysis

- Disadvantages
  - Often no concrete values / memory contents
  - Difficult to extract information about comm. Endpoints
  - Sometimes very time consuming
  - Requires expertise / experience
Dynamic Analysis

Analysis of binary code at run-time

- **Dynamic information**
  - Network connections
  - Open files
  - Processes

- Normally information from the *binary’s inside* is taken into consideration
- Real data exchange
- Memory contents
- Register contents
- Program states
- Threads
- API calls
- Function parameters
- …

Blackboxing is a special form of dynamic analysis
Pros ‘n’ Cons – Dynamic Analysis

• Pros
  • “Hands-on” investigation/observation (a single run)
  • Concrete data for registers / memory locations
  • Full memory contents available
  • Recognize same data
Pros ‘n’ Cons – Dynamic Analysis

• Cons
  • One execution path only
  • Only one possible value (for each memory location)
  • (No “step back” – Norman Sandbox and GDB can)
  • Depends on working environment
    (network connectivity, communication peers, ...)
  • Waiting (timeouts / thread synchronization)
  • May be detected (by bot herder)
  • Contribution to the botnet
    (spam, ddos, ...)
Runtime Analysis with Norman Malware Analyzer G2
Our Security Peers Say.....

Virus Bulletin 2010 Awards Norman Sandbox®
“THE MOST INNOVATIVE IDEA IN 10 YEARS”
What is Analyzer G2?

• Next generation technologies for superior threat intelligence
  • Analyzes and supplies intelligence on the full spectrum of threats
  • Saving manpower, time, and money

• Malware Analysis Framework
  • Integration of Analysis Modules
  • Analysis Management Center
  • Scalability & Flexibility
Analyzer G2 – Key technologies

• Hybrid SandBoxing – Unmatched Intelligence
  • Norman SandBox
    • Unique to Norman
  • IntelliVM
    • Norman goes deeper
    • Adaptable to YOUR needs
Virtualization Methods – SandBox

- Software x86 emulator
- Custom Windows 98 XPish OS
- Generates lots of low-level events
  - pagefaults, exceptions
- Easy to add new events
- Emulated network access and services (e.g. HTTP, SMB)
- "hook" based event capture
Virtualization Methods - IntelliVM

- Hardware virtualization
- Full Windows XP SP3 OS
- Generates high-level events
  - file, registry, network, process
- Real network access
- KernelScout
  - Filter driver based event capture
- Customizable
Virtualization Methods - IntelliVM

- **VM Introspection monitoring “events”**
- **Flexibility for non-traditional threats**
  - PDF, Office, Web
  - Customization for mirroring customer’s environment for targeted attacks
- **KernelScout**
  - Kernel & Application Level Monitoring
  - Transparency – Intelligence you will not otherwise see
  - Accuracy - Intelligence Integrity
  - Speed – Accelerate you analysis process
  - Avoid Anti-VM Techniques & Increase Security
  - Rootkit Monitoring
Why 2 different blackbox technologies?

• No system is un-evadable (not even anti-virus ;) )

• Some malware doesn’t run in VMs
• Some malware doesn’t run in Norman Sandbox
Code Interrogator

• Integrate 3rd party technologies & signatures
• Predefine & Configure Advanced Event Triggers
  • Generate threat risk scores
  • Customized Intelligence & Reporting
  • Alerting
    • Detect APT indicators
  • Analysis Optimization
MAG2 Workflow

Input | Processing | Output

Input: Browser, Remote API, Honeypots, Spam Traps

Processing: SandBox, IntelliVM

Output: Report
Operation & Management

• Web Based Dashboard & Analysis Center
  • Easy operation
    • Ready to go lab environment.
  • Intelligence Database
    • Store, Search, and Retrieve intelligence
  • Intuitive Presentation
    • Drill down for technical details

• G2 Integration APIs
  • Integrate features with other analysis systems & tools
  • Retrieve and Search intelligence data
  • Import samples from honeypots and sample feeds
Flexible Solutions

• Appliance
• Software
• Cloud
BLACKBOXING
WITH
NORMAN MALWARE ANALYZER G2
MAG2 interface

Lets have a look
MAG2 interface

MalwareAnalyzer2 interface showing a list of samples and a quick analysis section. The quick analysis section is highlighted, suggesting users can select files or drag and drop files into this box to start a quick analysis using default settings.
MAG2 as Blackboxing tool

• Blackboxing - identifying malicious behavior
  • Malicious executables
  • Malicious PDFs (Adobe Acrobat 8.1)
  • Malicious web pages (Internet Explorer 6)
  • Arbitrary file types requires installation of (exploitable) host application
MAG2 – other use cases

• (Un-)installation verification

• Threat analysis in mail filtering (integrate into MTA)

• DLP / APT via specific behaviors

• Threat detection (drives, net-shares, …)
Malicious files have several behavioral patterns

- **Installation (infection)**
  - Become persistent on a system

- **Self-protection / hiding**
  - Hide from detection (attacker’s dilemma)
  - Protect from analysis (e.g. packers)
  - Evade removal

- **Propagation**

- **Command & control communication**
USE OF LIVE MALWARE
USE AT OWN RISK
Let’s get our feet wet

- Connect Wifi

- Logging into Malware Analyzer G2
  - [https://mag2.norman.com](https://mag2.norman.com)
  - User: ccdcoe
  - pw: ccdcoe
Hands-on 1: Malicious? – Sample 5885

Hands-on 1: Malicious? – Sample 5885

![MalwareAnalyzerG2](image-url)

**Task 3530 Report**

<table>
<thead>
<tr>
<th>Activity Report</th>
<th>Process/Thread</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Risk Level:** 9

- **Analyzed:** 2912-04-10 11:20:53 UTC
- **Processing Time:** 390.01s
- **Status:** Success (Maximum runtime reached)
- **Environment:** Sandbox
- **Execution Arguments:** 
- **Recreate Task:**
- **Recreate Task with Detailed Capture**

**Pattern Matching Results**

- Creates process in suspicious location
- Possible Botnet Client
- Non standard DLL loaded
- Excessive API usage
- Writes to system folder
- Creates run key
- Writes to Windows folder
- Connects to IRC server
- Sandbox Detection
  - [NORMAN]: Creates process in suspicious location
  - [NORMAN]: Possible Botnet Client
  - [NORMAN]: Non standard DLL loaded
  - [NORMAN]: Excessive API usage
  - [NORMAN]: Writes to system folder
  - [NORMAN]: Creates run key
  - [NORMAN]: Writes to Windows folder
  - [NORMAN]: Connects to IRC server
  - [NORMAN]: Sandbox Detection
  - [NORMAN]: Creates Autorun Registry

**Sandbox Details**

<table>
<thead>
<tr>
<th>Task Queue</th>
<th>Available Processors</th>
<th>Storage Space</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>391.19GB</td>
</tr>
</tbody>
</table>

Logged In As: 
Notifications:
- vodafone (vodafone Fun)
Choosing your preferred setup

• Default:
  • IVM runs for 60 seconds (+startup +cleanup)
  • Sandbox runs for fixed cycle count or 5 minutes (watchdog)

• File system and registry are normally “filtered”
  • Well known (malicious) registry keys
  • Windows folder and files starting with “MZ”, batch files, ...
Hands-on 2: Malicious? – Sample 6188

Task 3528 Report

- Risk Level: 9
- Analyzed: 2012-04-10 11:20:02 UTC
- Processing Time: 300s
- Status: Success (Maximum runtime reached)
- Environment: SandBox
- Execution Arguments: {sample}
  - Recreate Task
  - Recreate Task with Detailed Capture

Pattern Matching Results
- ACCESS_VIOLATION
- Possible Botnet Client
- Checks for debugger
- Excessive API usage
- Writes to system folder

Hands-on 2: Malicious? – Sample 6188
Overview report includes

• **Obviously: malware actions**
  • Files, Registry, Processes, Named Objects, Network

• **IVM:**
  • Pcaps
  • Screenshots (if there are)
  • Dropped files

• **Sandbox**
  • (Reconstructed) PE memory dumps
  • API histogram
Task – Sandbox vs. IVM

- Look at Sandbox network activities
- Compare to IVM network activities
- What are possible reasons for the difference?
Full Connectivity

• **Advantages**
  • Real behavior / no detection by malware (if dependent on connectivity)
  • Observe currently ongoing actions
Full Connectivity

- **Disadvantages**
  - Participate in malicious actions (sending spam, DDoS)
  - Actions may be observed by botherder
Being Monitored - AVTracker
Isolated Lab

• No Internet connectivity
• All services are provided locally (e.g. INetSim, MAG2)
• Advantages
  • No possibility to be detected by botherder (think other communication channels – WiFi, Bluetooth, USB sticks)
  • No participation in malicious activities
Isolated Lab

- Disadvantages
  - More sophisticated malware checks the connectivity
  - Different or no actions if incomplete connectivity
ANALYST’S FAVORITE FEATURES
Other activities – leveraging the MAG2 potential

• Looking at the sandbox report...

• What about the .bat file? What might it be used for?

• What’s the C&C channel? What’s the channel password?
Full event view = full potential

- All collected data is indexed (searchable)
  - Including pcap/network data
- Index exists in browser (offline)

- Examples:
  - Full network data index (see packets)
  - Full file writes
  - Event types (IP_, Reg_, ...)
  - Process / thread IDs
MalwareAnalyzerG2

Full Event List For Task 3628

Show 25 entries

Filter results: a.bat

Event Number | PID | TID | Type       | Summary
-------------|-----|-----|------------|--------
335          | 265 | 19  | FS_Create  | cia.bat
339          | 265 | 19  | FS_Write   | cia.bat
346          | 265 | 19  | OBJ_CreateProcess | "C:\WINDOWS\system32\cmd.exe" [new PID: 256]
367          | 265 | 21  | FS_Open    | cia.bat
375          | 265 | 21  | FS_Read    | cia.bat
4751         | 267 | 22  | FS_Create  | cia.bat
4754         | 267 | 22  | FS_Write   | cia.bat

FS_Write

event_number: 4754
event_start: 67110474
pid: 267
tid: 22
actual_size: 5894
data: @echo off Echo REGEDIT4 &@temp\1.reg Echo &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBTParameters] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000}\Protocol\NetBT\Client\Policy] &@temp\1.reg Echo [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{1DF21E22-0C75-1574-445F-000000000000\]path: cia.bat
size: 5894

4751          | 267 | 22  | OBJ_CreateProcess | "C:\WINDOWS\system32\cmd.exe" [new PID: 256]
4815          | 268 | 24  | FS_Open    |

Task Queue
SandBox: 0
IntellIVM: 1

Availability Processors:

<table>
<thead>
<tr>
<th>Task Queue</th>
<th>Available Processors</th>
<th>Storage Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>SandBox</td>
<td>0</td>
<td>Operating System: 391.4 GB</td>
</tr>
<tr>
<td>IntellIVM</td>
<td>1</td>
<td>Store: 391.4 GB</td>
</tr>
</tbody>
</table>

Logged In As: vadafone (Vodafone Fun)
Virus Total Integration

Event Distribution Chart

AVG
- Detected: true
- Result: Worm/Spybot
- Update: 2012.02.15
- Version: 10.0.0.1180

AhnLab-V3
- Detected: true
- Result: Win32/IRCBot worm.varial
- Update: 20120214
- Version: 2012.02.15.00

Avast
- Detected: true
- Result: Win32 SpyBot-gen [Wzn]
- Update: 20120215
- Version: 6.0.1289.0

BitDefender
- Detected: true
- Result: Generic.Keylogger.2.330...
- Update: 20120215
- Version: 7.2

ClamAV
- Detected: true
- Result: Trojan.Spybot.gan-3
- Update: 20120215
- Version: 0.97.3.0

Comodo
- Detected: true
- Result: Worm.Win32.SpyBot.MH
- Update: 20120215
- Version: 11531

DrWeb
- Detected: true
- Result: Win32.HLLW.SpyBot
- Update: 20120215
- Version: 7.0.0.11250

Emisoft
- Detected: false
- Result: null
- Update: 20120211
- Version: 1.0.0.1

CAT-QuickHeal
- Detected: false
- Result: null
- Update: 20120214
- Version: 12.00

F-Prot
- Detected: true
- Result: Worm.Win32.SpyBot.gen
- Update: 20120215
- Version: 5.3.2.6

F-Secure
- Detected: true
- Result: Virus.Win32.SpyBot.gen-4
- Update: 20120215
- Version: 6.66.0.0

At least 36 vendors detect this sample.
MORE TO PLAY
Hands-on 3: Malicious? – Sample 5933

Hands-on 3: Malicious? – Sample 5933
Hands-on 4: Malicious? – Sample 6190

Hands-on 4: Malicious? – Sample 6190
Searching

• MAG2 has its own database built-in
• Normal blackbox systems only store reports – MAG2 stores every event

• Enables fast search for specific events globally

• TASK:
  Search for samples that create “a.bat”
Pattern groups – power to the people

• **Use cases:**
  • Point out special behaviors
  • Assign rating to task (maximum pattern score)
  • Seniors create pattern groups to guide juniors
  • When company specific aspects occur (e.g. checking for Norman services)
Playing with pattern groups

• Look at our sample / tasks

• Select a (set of) interesting events

• Create a pattern group ("Patterns") (! not global !)

• See how this shows up in our report
Graph view – more than you think

- “Full Event Timeline”
- Seems like “yeah, nice” but not useful
Nice but also “ooooh”

- Clicking on the bottom: enable/disable event types
- Sandbox page-faults help to see end of unpacking
Customizable to your needs
PDF ANALYSIS
Hands-on 5: Malicious PDF? - Sample 6193

Infection? Actions?
Hands-on 5: Malicious PDF? – Sample 6193
**Hands-on 6: Malicious PDF? – Sample 6192**

<table>
<thead>
<tr>
<th>Task Details</th>
<th>Activity Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level: 8</td>
<td></td>
</tr>
<tr>
<td>Analyzed: 2012-04-10 11:34:09 UTC</td>
<td></td>
</tr>
<tr>
<td>Processing Time: 0m 56.5s</td>
<td></td>
</tr>
<tr>
<td>Status: Success</td>
<td></td>
</tr>
<tr>
<td>Environment: IntellVM</td>
<td></td>
</tr>
<tr>
<td>Execution Arguments: <code>c:\windows\tem...173e7dca2cab1a5.pdf</code></td>
<td></td>
</tr>
<tr>
<td>Properties: Firewall Mode: Unlimited</td>
<td></td>
</tr>
</tbody>
</table>

**Pattern Matching Results**
- Non standard user-agent
- Writes to system folder
- Writes to Windows folder
- Downloads executable
- Related process checks certificate
- [NORMAN] Writes to system folder
- [NORMAN] Writes to Windows folder
- [NORMAN] Downloads executable
- [NORMAN] Related process checks certificate
- [NORMAN] pdf drops exe

**Infection? Actions?**
Hands-on 6: Malicious PDF? – Sample 6192
URL ANALYSIS
Use MAG2 to spot exploits against IE6

- Go to “Submit URLs”
- Enter a URL (malicious or not)
- Task -> “Custom” -> Firewall = “Unlimited”
- (Timeout = 15 if you are impatient 😊)
- Look at the result
Hands-on 7: Malicious web page? – Task 9880

### Task 9880 Report

**Task Details**
- **Risk Level:** 8
- **Analyzed:** 2012-06-01 13:43:10 UTC
- **Processing Time:** 59.54s
- **Status:** Success
- **Environment:** Intel64M

**Execution Arguments:**
- iprocess24.com/report.htm

**Pattern Matching Results**
- Non standard user-agent
- Creates process in suspicious location
- Crash
- Writes to system folder
- Writes to Windows folder
- Downloads executable
- Related process checks certificate
  - [NORMAN] Creates process in suspicious location
  - [NORMAN] Crash
  - [NORMAN] Writes to system folder
  - [NORMAN] Writes to Windows folder
  - [NORMAN] Downloads executable
  - [NORMAN] Related process checks certificate
  - [NORMAN] pdf drops exe

**Sample Details**
- **ID:** 6195
- **File Exists:** No
- **Received:** 2012-06-01 13:43:08 UTC
- **Name:** iprocess24.com/report.htm

### Activity Report

#### Process/Thread Events

- Creates process: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ce8v0k.exe
- Creates process: C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe
- Creates process: C:\Program Files\Common Files\Adobe\Updater3\AdobeUpdate.exe
- Creates process: C:\Program Files\Internet Explorer\EXPLORER.EXE

#### Infection Actions?

- UPN: Infection detected
- Actions required: Further analysis and remediation
Hands-on 7: Malicious web page? – Task 9880

Task 9880 Report

Risk Level: 8
Analyzed: 2012-06-01 13:43:10 UTC
Processing Time: 59.54s
Status: Success
Environment: Int8VM
Execution Arguments: iprocess24.com/report.htm
Recreate Task
Recreate Task with Detailed Capture

Pattern Matching Results
- Non standard user-agent
- Creates process in suspicious location
- Crashes
- Writes to system folder
- Writes to Windows folder
- Downloads executable
- Related process checks certificate
  - [NORMAN] Creates process in suspicious location
  - [NORMAN] Crashes
  - [NORMAN] Writes to system folder
  - [NORMAN] Writes to Windows folder
  - [NORMAN] Downloads executable
  - [NORMAN] Related process checks certificate
  - [NORMAN] pdf drops exe

Sample Details
- ID: 6195
- File Exists: No
- Received: 2012-06-01 13:43:09 UTC
- Name: iprocess24.com/report.htm
Hands-on 8: Malicious web page? – Task 9906

Infection? Actions?
Hands-on 8: Malicious web page? – Task 9906

Task 9906 Report

Task Details
- Risk Level: 8
- Analyzed: 2012-06-01 16:16:07 UTC
- Processing Time: 60.22s
- Status: Success
- Environment: IntelliVM
- Execution Arguments: sowler.tw/main...age=1a38e197e2c1e8a
- Properties: Firewall Mode: Unlimited

Recreate Task
Recreate Task with Detailed Capture

Pattern Matching Results
- Non standard user-agent
- Creates process in suspicious location
- Creates threads in windows processes
- Writes to windows processes
- Writes to system folder
- Creates run key
- Writes to Windows folder
- Writes to system processes
- Injects thread into Windows process
- Injects thread into Norman process
- Downloads executable
- Related process checks certificate

Activity Report
- Process/Thread Details
  - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\cs8v0k.exe
  - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\wpbt0.dll
  - C:\Users\Administrator\9ea5db1.exe

Download PDF Report
Hands-on 9: Malicious web page? – Task 9905

Task 9905 Report

- **Risk Level:** 8
- **Analyzed:** 2012-06-01 16:16:07 UTC
- **Processing Time:** 60.29s
- **Status:** Success
- **Environment:** IntelliVM
- **Execution Arguments:** u54s.info/main...age=8643fa265298a92
- **Properties:** Firewall Mode: Unlimited

**Activity Report**

- Creates process: C:\Documents and Settings\Administrator\Application Data\AcroRd32.exe
- Creates process: C:\Documents and Settings\Administrator\Application Data\AcroRd32.exe
- Creates process: C:\Program Files\Adobe\Reader DC\AcroReader DC.exe
- Creates process: C:\Program Files\Adobe\Reader DC\AcroReader DC.exe
- Creates remote thread: C:\WINDOWS\explorer.exe

**Pattern Matching Results**

- Non standard user-agent
- Writes to system folder
- Creates run key
- Writes to Windows folder
- Dumps executable in application
- Writes to system processes
- Injects thread into Windows process
- Dumps and runs batch script
- Related process checks certification
- [NORMAN] Writes to system folder
- [NORMAN] Creates run key
- [NORMAN] Opens file

**Infection? Actions?**
Hands-on 9: Malicious web page? – Task 9905

Task 9905 Report

Task Details
- Risk Level: 8
- Analyzed: 2012-06-01 16:18:07 UTC
- Processing Time: 60.29s
- Status: Success
- Environment: IntelliVM
- Execution Arguments: u54s.info/main...age=8643fa265298a92
- Properties: Firewall Mode: Unlimited

Recreate Task
Recreate Task with Detailed Capture

Pattern Matching Results
- Non standard user-agent
- Writes to system folder
- Creates run key
- Writes to system processes
- Dumps executable in application
- Dumps and runs batch script
- Related process checks certificate
- [NORMAN] Writes to system folder
- [NORMAN] Creates run key

Event Number vs. Cycles
Hands-on 10: Malicious file? – Sample 6221

Infection? Actions?
Hands-on 10: Malicious file? – Sample 6221

Task Details
- Risk Level: 8
- Analyzed: 2012-06-03 14:10:59 UTC
- Processing Time: 59.69s
- Status: Success
- Environment: IntellIVM
- Execution Arguments: c:\windows\temp...e3adde70b868dc13...
- Properties: Keep Reg Events: 1

Activity Report
- Process: C:\WINDOWS\Temp\dllinjection.exe
- Process: PID: 1568 C:\WINDOWS\explorer.exe

Pattern Matching Results
- Writes to system processes
- Injects thread into Windows process
  [NORMAN] Writes to system processes
  [NORMAN] Injects thread into Windows process

Sample Details
- ID: 6221
- File Exists: Yes
PREVALENCE
Google Protocol Buffers (GPB)

- Like XML but not bloated
- Like ASN.1 but works
- Like Corba IDL but usable
- C++, Python, Java, (C#, C, Perl, Ruby)

**What Are Protocol Buffers?**

Protocol buffers are Google's language-neutral, platform-neutral, extensible mechanism for serializing structured data – think XML, but smaller, faster, and simpler. You define how you want your data to be structured once, then you can use special generated source code to easily write and read your structured data to and from a variety of data streams and using a variety of languages – Java, C++, or Python.
JSON

- Easily parse-able (not like XML)
- Libraries for most languages
- Text – easy to read/debug
**Norman MalwareAnalyzerG2**

**Task Details**

<table>
<thead>
<tr>
<th>Task ID:</th>
<th>3531</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level:</td>
<td>8</td>
</tr>
<tr>
<td>Date Processed:</td>
<td>2012-04-10 11:31:37 (UTC)</td>
</tr>
<tr>
<td>Processing Time:</td>
<td>59.67 seconds</td>
</tr>
<tr>
<td>Virtual Environment:</td>
<td>IntelIVM</td>
</tr>
<tr>
<td>Execution Arguments:</td>
<td>&quot;c:\windows\temp\2769a1276913c36ebc984679d4564c12.exe&quot;</td>
</tr>
<tr>
<td>Sample ID:</td>
<td>1581</td>
</tr>
<tr>
<td>Type:</td>
<td>basic</td>
</tr>
<tr>
<td>Owner:</td>
<td>vodafone</td>
</tr>
<tr>
<td>Label:</td>
<td>2769a1276913c36ebc984679d4564c12</td>
</tr>
<tr>
<td>Date Added:</td>
<td>2012-04-10 11:31:14 (UTC)</td>
</tr>
<tr>
<td>File Type:</td>
<td>PE32:win32gui</td>
</tr>
<tr>
<td>File Size:</td>
<td>80896 bytes</td>
</tr>
<tr>
<td>MD5:</td>
<td>2769a1276913c36ebc984679d4564c12</td>
</tr>
<tr>
<td>SHA256:</td>
<td>08ce4719878081f87e6e2c63be859bf795a240d4122013ae186867091a4b3100e</td>
</tr>
<tr>
<td>Description:</td>
<td>None</td>
</tr>
</tbody>
</table>

**Process/Thread Events**

- Creates process: C:\WINDOWS\Temp\2769a1276913c36ebc984679d4564c12.exe
- Creates process: C:\WINDOWS\System32\vqiuadni.exe
- Writes to process: PID:1548 C:\WINDOWS\explorer.exe
- Terminates process: C:\WINDOWS\Temp\2769a1276913c36ebc984679d4564c12.exe
- Creates remote thread: C:\WINDOWS\explorer.exe
DIY – Create your own output...

- ...based on HTML style-sheets

curl https://<host>/rapi/widgets/task_report/<task_id>
Remote API

• (Almost) everything you saw can also be scripted

• For full API see manual
RAPI examples

• GET sample overview:
curl https://<host>/rapi/samples?md5=<md5>

• GET tasks for a specific sample:
curl https://<host>/rapi/samples/<sampleid>/tasks

• GET tasks overview
curl https://<host>/rapi/tasks/<taskid>

• GET all events
curl https://<host>/rapi/tasks/<taskid>/events
More than just retrieving information

• Remote API can...
• Upload samples
• Create tasks
• Delete files
• Retrieve resources (screen-shots, PE dumps, pcaps, dropped files)
• Retrieve, create pattern groups (matches)
• (system info & maintenance)
OPEN ARCHITECTURE
Architecture is open

• Root-ssh access

• User interface is open (modify to your needs)

• (Almost) everything accessible via RAPI
ADMIN PANEL
**Firewall**

![Firewall Management Interface](image)

### Details for Firewall #2

- **Owner**: Charlie Root
- **Name**: Limited
- **Delete**: Yes

<table>
<thead>
<tr>
<th>ID</th>
<th>Priority</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.0.0.0/0:</td>
<td>0.0.0.0/0: 25</td>
<td>tcp</td>
<td>DROP</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.0.0.0/0:</td>
<td>0.0.0.0/0: 139</td>
<td>tcp</td>
<td>DROP</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0.0.0.0/0:</td>
<td>0.0.0.0/0: 445</td>
<td>tcp</td>
<td>DROP</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0.0.0.0/0:</td>
<td>0.0.0.0/0:</td>
<td>all</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>
Maintenance mode

- Customize IntelliVM
  - Install customs programs
  - Change default handler (in Windows)
  - RDP (& VNC)
Various admin features

• Firewall
• Maintenance mode
• User management
• Virus Total key
• Network setup
• License information
• Restart / Shutdown
Use case

BEHAVIOR CLUSTERING
Security solutions for now and the future