<table>
<thead>
<tr>
<th><strong>9am – 6pm Weekday</strong></th>
<th><strong>Most of the time</strong></th>
<th><strong>Sometimes</strong></th>
<th><strong>Once a year</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Working in Panda Security since year 2005</td>
<td>Running xandora.net project.</td>
<td>Member of vnsecurity.net</td>
<td>Crew</td>
</tr>
<tr>
<td>➔ Running the technical team</td>
<td>➔ The coder</td>
<td>➔ Good friends</td>
<td>➔ Yet to be define</td>
</tr>
<tr>
<td>➔ In charge of APAC malware incidents</td>
<td>➔ The administrator</td>
<td>➔ Can’t really recall what I did for my good friends</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Analysis 101</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define: Sandbox</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What is xandora</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Problems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Partnership</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sector</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roadmap</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>References &amp; Acknowledgements</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Static Analysis

- Reading the binary
- Understanding the binary
- Become crazy

Dynamic Analysis

- Virtual Machines
- Analysis tools/ debugger
- Human Analysis
DEFINE: SANDBOX
Sandbox

- Isolated environment to run untrusted code
- Run a suspicious file within a locked down environment
- “Locked” but not overly restrictive. Eg: Sandbox must come with network access
- Provide file behavioral report
PROBLEMS
OBJECTIVES

OTHER MALWARE SANDBOX

- Too many malware sandboxes out there
- Most the sandbox design have only one objective, which is to provide complete analysis report for a file being processed. This will lead to:

  i. Lengthy report, 40-60 pages
  ii. Too much information
  iii. Too Enterprise
  iv. Takes too much resources to process
  v. Process files in-time. 24 hours malware

Performance

How to solve this problem and why this is important

Malware samples received at PandaLabs
Data: May 2009

Source: PandaLabs

Source: PandaLabs
WHAT IS XANDORA
Automated Malware Analysis Platform

Online Global Collaboration Partnership

Virtualization Management

Possible Malware
ARCHITECTURE OVERVIEW

Source

Pre Analysis

Checksum
Appearance
Malware Scanner
Goodware Scanner
Unpacker

Xandbox

Monitor
Copy-on-Write Image
Memory Dump
Virtual Network Adapters
Interactions Response

XANDBOX

Kernel Level Acceleration
RAM Disk Acceleration
VM Acceleration
VM Control Center

Post Analysis

Portal

File System
Registry
Network
Digital Investigation
Screen Capture

Public
Administration
Vendor

Government Connectors
Private Connectors

Vendor

Government Connectors
Private Connectors
**Pre Analysis**

- **Checksum**
  - Common unique identification
  - Generate SHA1 and MD5

- **Appearance**
  - Check against database
  - Update the last time file being received

- **Malware Scanner**
  - VirusTotal
  - Compare against all antivirus vendor listed in VirusTotal
  - Private access to VirusTotal database

- **Goodware Scanner**
  - shaodowserver.org
  - Check file belongs to which Company and Product

- **Unpacker**
  - Unpack binary for static analysis
  - Able to automatically unpack ASPack, NSPack, UPX and PE_Compact

---

**XANDBOX**

**Post Analysis**

- File System
- Registry
- Network
- Digital Investigation
- Screen Dump
VM Monitor Access
- Capture screen dump when there is a screen change
- Issue specific command such as mouse movement and key stroke
- Able to accept VM dump for analysis

Xanbox
- Fork disk image from master VM Image
- Both images master and running images are stored in RAM
- Gain full access to RAM
- Dump full RAM snapshot from VM
- Suspicious file able to access network from VM
- Monitor request from the suspicious file to create a new file or made changes in the registry

Acceleration
- Use different kinds of hardware and software acceleration to make sure all the VM fork by Xandora is being optimized

VM Control Center
- Monitor process and process queue
- Ensure CPU usage is not overloaded
- Only one network adapter for one VM
**Pre Analysis**

- Checksum
- Appearance
- Malware Scanner
- Goodware Scanner
- Unpacker

**XANDBOX**

**File System**
- Look for newly generated file
- Store newly generated executable file

**Registry**
- Dump VM registry
- Look for newly generated, edited and deleted registry entries

**Network**
- Analyze network traffic
- Destination host and port
- Destination URL
- Extract downloaded file

**Digital Investigation**
- Full memory dump from VM
- Analyze active and suspicious process

**Screen Dump**
- Capture screenshot from VM
- Do not store if there are no activities
- Do not store if screen is duplicated
<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>MD5</th>
<th>Date</th>
<th>Time</th>
<th>Score</th>
<th>Size</th>
<th>Ext</th>
<th>VT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unidentified</td>
<td>60502ea64aff008d9094eb3468a61c37</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>59</td>
<td>221696</td>
<td>dll</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Backdoor.Win32.Bifrose.dsn</td>
<td>8801e59b078e3f478a3eb0b16deba09</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>92</td>
<td>513000</td>
<td>exe</td>
<td>27</td>
</tr>
<tr>
<td>3</td>
<td>Hoax.MSIL.ArchSMS.cl</td>
<td>65425da20e1990fac705636a6afeaf</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>33</td>
<td>1951729</td>
<td>exe</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Net-Worm.Win32 Allaple.b</td>
<td>287dd90eb8c37f0a10d5573b276e6191</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>146</td>
<td>57856</td>
<td>exe</td>
<td>35</td>
</tr>
<tr>
<td>5</td>
<td>HEUR:Backdoor.Win32.ZAccess.gen</td>
<td>315e5aa62457f7089a4859eada19b71</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>126</td>
<td>48016</td>
<td>exe</td>
<td>28</td>
</tr>
<tr>
<td>6</td>
<td>Unidentified</td>
<td>b7dd267f9986872a281713d8fd11b02</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>34</td>
<td>73904</td>
<td>exe</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Unidentified</td>
<td>102f6b812187572d013caa90c3ad99</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>73</td>
<td>1189424</td>
<td>exe</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>W32/Behav-Heuristic-CorruptFile-EP</td>
<td>145f99b35923edc3e411d329c7744a5f</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>52</td>
<td>515728</td>
<td>dll</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>Unidentified</td>
<td>f86507291f052d00d160875f9e7a9c6</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>55</td>
<td>512000</td>
<td>exe</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>W32/Behav-Heuristic-CorruptFile-EP</td>
<td>f943bec2f77cbe2e962ca2e6d34d10eed6</td>
<td>2011-10-12</td>
<td>03:15:00</td>
<td>67</td>
<td>512000</td>
<td>exe</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>Unidentified</td>
<td>96c37209000b4f0fa2bbae4f63228d9e</td>
<td>2011-10-12</td>
<td>03:12:00</td>
<td>81</td>
<td>1579644</td>
<td>exe</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>Unidentified</td>
<td>ef4c739afc76c1460399daba1942c69</td>
<td>2011-10-12</td>
<td>03:12:00</td>
<td>52</td>
<td>230912</td>
<td>dll</td>
<td>0</td>
</tr>
</tbody>
</table>
File Information

Unidentified

File Details

- **MD5**: e9d23dd5bd55bd36b224d5a7d09af329
- **SHA-1**: db939a8759587f984066f67f1cb8d1053a2c86cd
- **First Received (GMT+8)**: 2011-10-12 03:11:00
- **Last Received (GMT+8)**: 2011-10-12 03:11:00
- **Size (bytes)**: 399606
- **Weightage**: 151
- **virustotal.com**: 0 vendors detected

File Header

**Static File Header**

```
+-----------------------------------------------+
<table>
<thead>
<tr>
<th>FILE HEADER INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem: 2 (Windows GUI)</td>
</tr>
<tr>
<td>Image Base: 00400000 Size: 0028000</td>
</tr>
<tr>
<td>Code Base: 00001000 Size: 00019800</td>
</tr>
<tr>
<td>Data Base: 00010000 Size: 0007000</td>
</tr>
<tr>
<td>Entry Point: 0001A244 (file offset 001A244)</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
+-----------------------------------------------+
```

**SECTIONS**

1. CODE RVA: 00001000 Offset: 00000400 Size: 0001B800 Flags: 60000020 (CER)
2. DATA RVA: 0001D000 Offset: 0001BC00 Size: 00014000 Flags: C0000040 (DRW)
3. BSS RVA: 0001F000 Offset: 0001D000 Size: 00000000 Flags: C0000000 (RW)
4. Idata RVA: 00020000 Offset: 0001D000 Size: 0000C000 Flags: C0000040 (DRW)
5. tis RVA: 00021000 Offset: 0001D000 Size: 00000000 Flags: C0000000 (RW)
6. .data RVA: 00022000 Offset: 0001D000 Size: 00002000 Flags: 50000040 (DSR)
7. .reloc RVA: 00023000 Offset: 0001E000 Size: 00002000 Flags: 50000040 (DSR)
8. .rsrc RVA: 00025000 Offset: 0001FE00 Size: 00002E00 Flags: 50000040 (DSR)

Process

**Running Process**

- smss.exe, pid: 288
- csrss.exe, pid: 388
- winlogon.exe, pid: 420
- services.exe, pid: 540
- lsass.exe, pid: 552
- svchost.exe, pid: 700
- svchost.exe, pid: 748
- svchost.exe, pid: 812
- svchost.exe, pid: 904
- explorer.exe, pid: 1024
- svchost.exe, pid: 1056
- alg.exe, pid: 1592
- yagay.exe, pid: 488
- awhost.exe, pid: 112
- dvw.exe, pid: 940
- cwhost.exe, pid: 544
- 439017316, pid: 1536

Download File
Portal Network Support

File system and Registry

### Filesystem Change
The following file was changed in the system
- "C:\WINDOWS\436017316"
- "C:\WINDOWS\Temp\perfil_perfdata\700.dat"
- "C:\WINDOWS\system32\catRoot2\tmp.edb"

### Registry Change
The following Registry Keys were changed
- software_Microsoft_Windows_CurrentVersion_Group_Policy_State_S-1-5-21-790525478-1390067357-1417001333-500_Extension-List
- software_Microsoft_Windows_CurrentVersion_Group_Policy_State_S-1-5-21-790525478-1390067357-1417001333-500_Extension-List
- software_Microsoft_Windows_NT_CurrentVersion_AeDebug
- software_Microsoft_Windows_NT_CurrentVersion_AeDebug
- software_Microsoft_Windows_NT_CurrentVersion_Prefetcher
- software_Microsoft_Windows_NT_CurrentVersion_Prefetcher
- NTUSER\Software\Microsoft\Windows_CurrentVersion_AppCompat\SysTray
- NTUSER\Software\Microsoft\Windows_CurrentVersion_AppCompat\SysTray
- NTUSER\Software\Microsoft\Windows_CurrentVersion_Explorer_CDMurning_Drives
- NTUSER\Software\Microsoft\Windows_CurrentVersion_Explorer_CLSID
- NTUSER\Software\Microsoft\Windows_CurrentVersion_Explorer_CDMurning_Drives
- NTUSER\Software\Microsoft\Windows_CurrentVersion_Explorer_CLSID
- NTUSER\Software\Microsoft\Windows_CurrentVersion_Explorer_Desktop

Network

### Traffic by TCP/IP Connections
Produces outbound traffic, view by host and port

- 105.142.238.162 : 34534
- 109.54.49.238 : 34384
- 173.199.104.129 : 34384
- 173.3.172.129 : 34384
- 173.3.172.129 : 34384
- 173.8.230.1 : 34384
- 174.101.90.246 : 34384
- 174.65.23.52 : 34384
- 178.89.102.177 : 34384
- 178.89.102.217 : 34384
- 178.89.102.132 : 34384
- 178.90.46.9 : 34384
- 178.91.62.85 : 34384
- 183.179.1.127 : 34384
- 186.100.61.160 : 34384
- 186.34.104.101 : 34384
- 213.133.183 : 34384
- 250.129.94 : 34384
- 201.255.188.198 : 34384
- 216.227.104.37 : 34384
- 216.227.104.37 : 34384
- 24.97.220.252 : 34384
- 41.70.190.249 : 34384
- 41.73.116.133 : 34384

Screen Shot

### Screen Capture
The new window was created

[Image of a computer screen showing a message about a security alert and the option to send a report.]
**Malware Analysis**

**Infrastructure**

**CURRENT**

- Receive 25,000 files/day
- Process 400 files/hour
- 70% non detected by AV

**FUTURE**

- Receive 150,000 files/day
- Process 1,000 files/hour
- 90% non detected by AV

**Virtualization**

- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

**File Analysis**

**File Injection**

**Sandboxing**

- Threat evolution will increase the amount of analysis and processing requirements
- Fundamental

**Collaboration Call**

- Request for information from our analysis partners
- Expertise and focus
Detect VM ENV
- Binary that do not run under virtual machine
- Find solutions for malware to run under actual machine

Execution Timing
- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

Volume
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

Hiding Client
- Hiding sensors
- Kernel driver
- Hidden process

Report
- Demand for more information snapshots
- Demand for more detailed analysis

File System
- Reduce mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM
- How many VMs
- How to check
- Which process with highest CPU load

Input/Output
- Base image protection
- Faster read/write for VM
- Faster read write for post processing
Detect VM ENV
- Binary that do not run under virtual machine
- Find solutions for malware to run under actual machine

Execution Timing
- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

Volume
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

Hiding Client
- Hiding sensors
- Kernel driver
- Hidden process

Report
- Demand for more information snapshots
- Demand for more detailed analysis

File System
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM
- How many VMs
- How to check
- Which process with highest CPU load

Input/Output
- Base image protection
- Faster read/write for VM
- Faster read write for post processing
<table>
<thead>
<tr>
<th>Detect VM ENV</th>
<th>Execution Timing</th>
<th>Volume</th>
<th>Hiding Client</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Binary that do not run under virtual machine</td>
<td>• Requires specific time</td>
<td>• Increase in numbers</td>
<td>• Hiding sensors</td>
<td>• Demand for more information snapshots</td>
</tr>
<tr>
<td>• Find solutions for malware to run under actual machine</td>
<td>• Improvement only in the number of virtual machines in each server</td>
<td>• Increase in variants</td>
<td>• Kernel driver</td>
<td>• Demand for more detailed analysis</td>
</tr>
<tr>
<td></td>
<td>• Foundation</td>
<td>• Delay in processing</td>
<td>• Hidden process</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Vendors process files without sandbox</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect VM ENV</td>
<td>Execution Timing</td>
<td>Volume</td>
<td>Hiding Client</td>
<td>Report</td>
</tr>
<tr>
<td>• Detect samples not able to run under VM</td>
<td>• Fixed time between 3 to 5 minutes</td>
<td>• Small scale Windows</td>
<td>• No client required</td>
<td>• Simple</td>
</tr>
<tr>
<td>• Possible Malware</td>
<td>• Execution and no response from binary</td>
<td>• VM monitoring and queuing engine</td>
<td>• Possible malware scoring algorithm</td>
<td>• Ensure readability</td>
</tr>
<tr>
<td></td>
<td>• Possible Malware</td>
<td>• Task allocation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**SANDBOX PROBLEMS**

**Detect VM ENV**
- Binary that do not run under virtual machine
- Find solutions for malware to run under actual machine

**Execution Timing**
- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

**Volume**
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

**Hiding Client**
- Hiding sensors
- Kernel driver
- Hidden process

**Report**
- Demand for more information snapshots
- Demand for more detailed analysis

**File System**
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

**Concurrent VM**
- How many VMs
- How to check
- Which process with highest CPU load

**Input/Output**
- Base image protection
- Faster read/write for VM
- Faster read write for post processing
### Problems

1. Too many mount/umount kill the system – Kernel Panic

### Preprocessing

1. Group all required files in to a ISO, using `mkisofs`

### Sandbox

1. Start VM with ISO image as ISO
2. Run the ISO while VM boots up
   1. Register runonce
   2. Autorun.inf

### Post Processing

1. Mount ntfs over tcpip
2. Mount ntfs over ramfs
3. Modding ntfs-3g
   1. Disable checking
   2. Force read only
   3. Fix to one NTFS version
**Detect VM ENV**
- Binary that do not run under virtual machine
- Find solutions for malware to run under actual machine

**Execution Timing**
- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

**Volume**
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

**Concurrent VM**
- How many VMs
- How to check
- Which process with highest CPU load

**Hiding Client**
- Hiding sensors
- Kernel driver
- Hidden process

**File System**
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

**Input/Output**
- Base image protection
- Faster read/write for VM
- Faster read write for post processing

**Report**
- Demand for more information snapshots
- Demand for more detailed analysis

**Volume**
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox
**Problems**

i. Too many mount/umount kill the system – Kernel Panic

**Preprocessing**

i. File queue
   a. Priority
   b. Balanced for multiple sandbox

**Sandbox**

i. Pick up files and insert into VM
ii. VM monitoring
   a. Total running VMs
   b. Heavy process – RAM Dump
iii. Process RAM Dump.

**Post Processing**

i. Process output files
Detect VM ENV
- Binary that do not run under virtual machine
- Find solutions for malware to run under actual machine

Execution Timing
- Requires specific time
- Improvement only in the number of virtual machines in each server
- Foundation

Volume
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

File System
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM
- How many VMs
- How to check
- What the most heavy process

Hiding Client
- Hiding sensors
- Kernel driver
- Hidden process

Report
- Demand for more information snapshots
- Demand for more detailed analysis

Input/Output
- Base image protection
- Faster read/write for VM
- Faster read/write for post processing

Volume
- Increase in numbers
- Increase in variants
- Delay in processing
- Vendors process files without sandbox

File System
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM
- How many VMs
- How to check
- What the most heavy process

Hiding Client
- Hiding sensors
- Kernel driver
- Hidden process

Report
- Demand for more information snapshots
- Demand for more detailed analysis

Input/Output
- Base image protection
- Faster read/write for VM
- Faster read/write for post processing
### Problems

i. So far the only problem is slow
ii. No disk error yet

### Preprocessing

i. Move required file to RAM Disk
ii. SSD saves the world

### Sandbox

i. Protect Master Image
   a. chattr +i
ii. SSD saves the world

### Post Processing

i. Move required files to RAM disk
ii. SSD saves the world
**File System**
- What is good, what is bad.

**Registry**
- How to know changes in registry is good or malicious

**Process**
- Good or malicious process

**Networking**
- Identify good and malicious traffic
File System

Clean and easy to identify a bad file

i. Compare old and new file system change
ii. Malicious change
   a. Dropping exe
   b. Dropping dll
   c. Dropping sys
iii. Dropped location
   a. c:\windows\fonts
File System
• What is good, what is bad.

Registry
• How to know changes in registry is good or malicious

Process
• Good or malicious process

Networking
• Identify good and malicious traffic
Registry

i. Registry change
   a. Disable antivirus
   b. Add in autorun at startup

Registry Change

The following Registry Keys were changed

- software_Flowmix
- software_Clients_StartMenuInternet_IEXPLOREREXE_shell_open_command
- software_Gemplus
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Run
- NTUSER_Software_Microsoft_Windows_CurrentVersion_RunOnce
- NTUSER_Software_Microsoft_Windows_CurrentVersion_WindowsUpdate
- NTUSER_Software_Microsoft_Windows_CurrentVersion_WinTrust
File System
  • What is good, what is bad.

Registry
  • How to know changes in registry is good or malicious

Process
  • Good or malicious process

Networking
  • Identify good and malicious traffic
How to hunt for a malicious process

i. List down all processes
ii. Full process path
iii. Process file name (svchost.exe)
iv. File MD5 or SHA1 for comparison

Running Process

smss.exe, pid: 288
csrss.exe, pid: 388
winlogon.exe, pid: 416
services.exe, pid: 536
lsass.exe, pid: 548
svchost.exe, pid: 696
svchost.exe, pid: 744
svchost.exe, pid: 804
svchost.exe, pid: 852
svchost.exe, pid: 892
explorer.exe, pid: 1080
alg.exe, pid: 1616
wuauctl.exe, pid: 1316
DIDfuRcLeJEc.exe, pid: 1400
P1kA1MIg2Kb7Fz., pid: 972
File System
- What is good, what is bad.

Registry
- How to know changes in registry is good or malicious

Process
- Good or malicious process

Networking
- Identify good and malicious traffic
Networking

None of these being implemented yet.

i. IP Blacklisting
ii. Domain blacklisting

Traffic - by TCP/IP Connections

Produces outbound traffic, view by host and port

- 16.209.6.79 : 1034
- 16.55.147.53 : 1034
- 16.57.210.8 : 1034
- 16.83.200.22 : 1034
- 172.22.104.41 : 1034
- 193.41.153.254 : 1034
- 194.4.224.121 : 1034
- 203.76.97.63 : 1034

Traffic - by URL

Produces outbound traffic, view by URL

- www.dnf01.com/gg
- www.dnf01.com/gg
- www.dnfbochi.com/
- new.egoood.com/show
- new.egoood.com/TESTPage
- new.egoood.com/TESTPage
- activex.microsoft.com/objects
- codecs.microsoft.com/isapi
- tc.100tjs.com/qvo001.php?id=3&uid=24199&ams=X6jkoaCcw%2f0%3d
- t.100tjs.com/tjxy
15 Days Received Samples – by Vendors
SECTOR
**Community**

Collaborate with experts globally to outnumber and outsmart cybercriminals. Even cybercriminals collaborate.

- From security experts to endless possibilities of collaboration
- Xandora platform enables global collaboration

**Government**

Country CERTs should have operations to monitor targeted attacks which can affect its economy and security.

- Monitors country-wide activities
- Collaboration between all Government departments
- Proactive effort towards security

**Enterprise**

Enable large enterprises to monitors its security.

- Business disasters such as downtime, data leakage, etc. widely affected large enterprises in recent times.
- Corporate espionage
- Shareholders must be proactively protected

**Education**

Establish long-term working partnership with universities to train future experts in CERT.

- Providing Xandora for FREE
- Universities can be collaborators and contributors.
Jan - March
New Reporting Interface

Apr/May
Multi Vendor Profiling

Nov/Dec
PDF/Office/ APK File Analysis

Oct
Executive Reporting

Aug/Sept
NoSQL Conversion

July/Aug
Translation
References

1. Nguyen Anh Quynh, Virt-ICE: next generation debugger for malware analysis
3. Georg Wicherski, dirtbox, A x86/Windows Emulator
4. Daniel Raygoza, Automated Malware Similarity Analysis
5. Project: Cuckoo
6. Book: Malware analysis cookbook

Acknowledgements

1. Very good friends from vnsecurity.net
2. Rodrigo Rubira Branco
3. Meling Mudin
4. PandaLabs
THANK YOU