MALWARE SANDBOXING – THE XANDORA WAY

Lau Kai Jern, Chief Development Officer – kj@xandora.net

INTRODUCTION

PANDA SECURITY

9am – 6pm Weekday

Working in Panda Security since year 2005

- Runing the technical team
- In charge of APAC malware incidents

Most of the time

Running xandora.net project.

- The coder
- The administrator
- The everything

VNSECURITY

Sometimes

Member of vnsecurity.net

- Good friends
- Can't really recall what I did for my good friends

hack in the box

Once a year

Crew

- Yet to be define

AGENDA

- Introduction
- Malware Analysis 101
- Define: Sandbox
- What is xandora
- Architecture
- Infrastructure
- Technical Problems
- identification
- Global Partnership
- Sector
- Roadmap
- References & Acknowledgements

MALWARE ANALYSIS 101

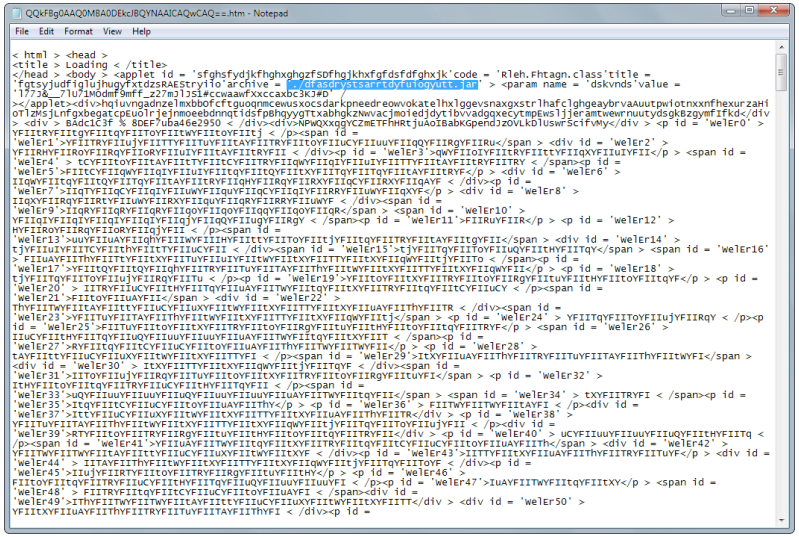
Static Analysis

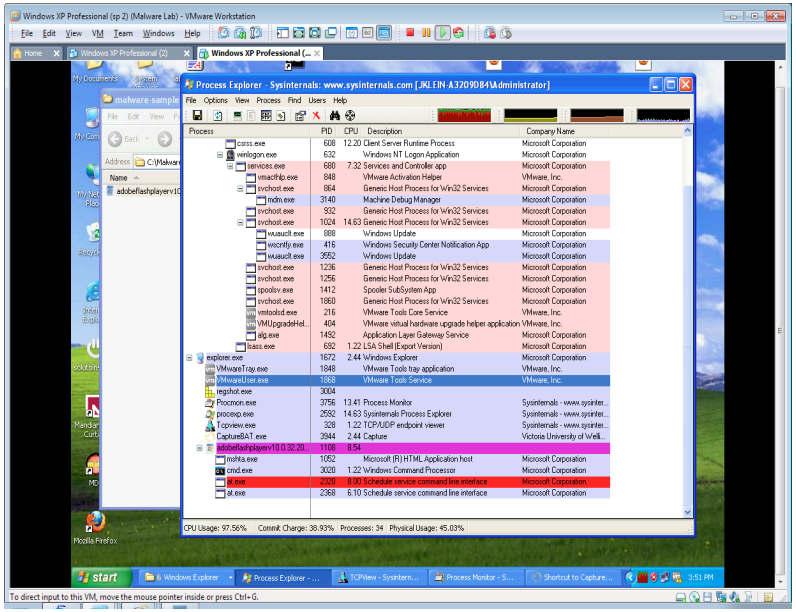
- Reading the binary
- Understanding the binary
- Become crazy

OllyDbg
Win32 Symbolic Debugger

IDA Pro
by Ilfak Guilfanov

PEiD





Dynamic Analysis

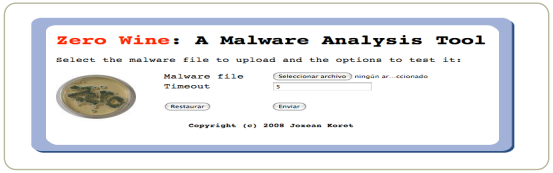
- Virtual Machines
- Analysis tools/ debugger
- Human Analysis

vmware

DEEPFREEZE
STANDARD

Sandboxie

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 comes with network access
- Provide file behavioral report

PROBLEMS

Objectives

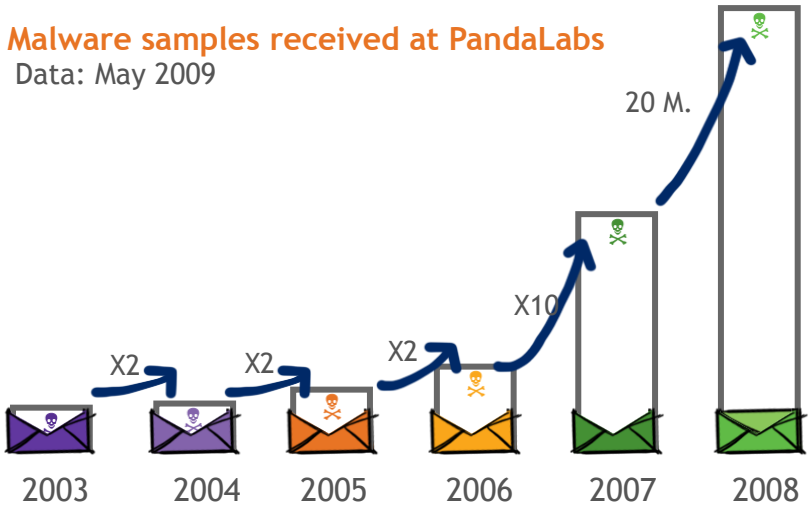
OTHER MALWARE SANDBOX

- Too many malware sandboxes out there
- Most the 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

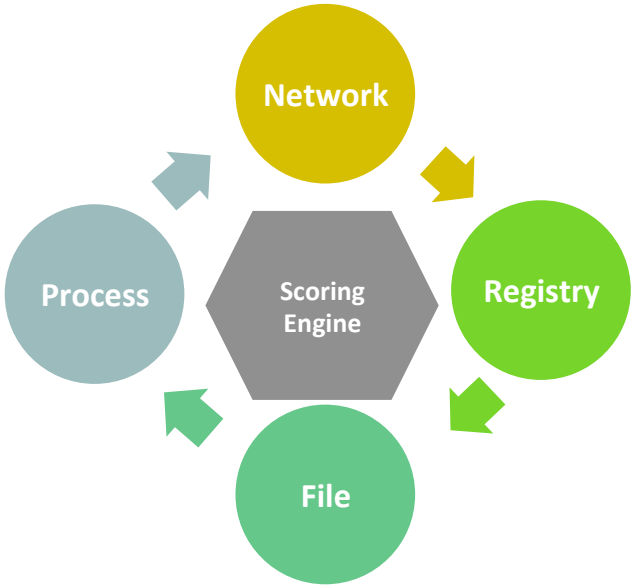
Performance

How to solve this problem and why this is important



Source: PandaLabs

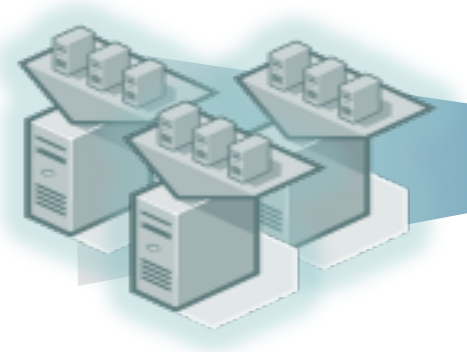
Scoring System



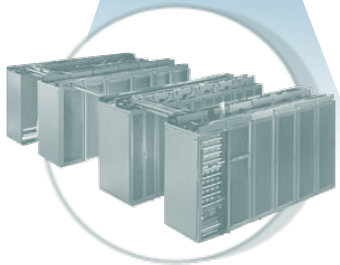
WHAT IS XANDORA

Online Global Collaboration
Partnership

Virtualization Management



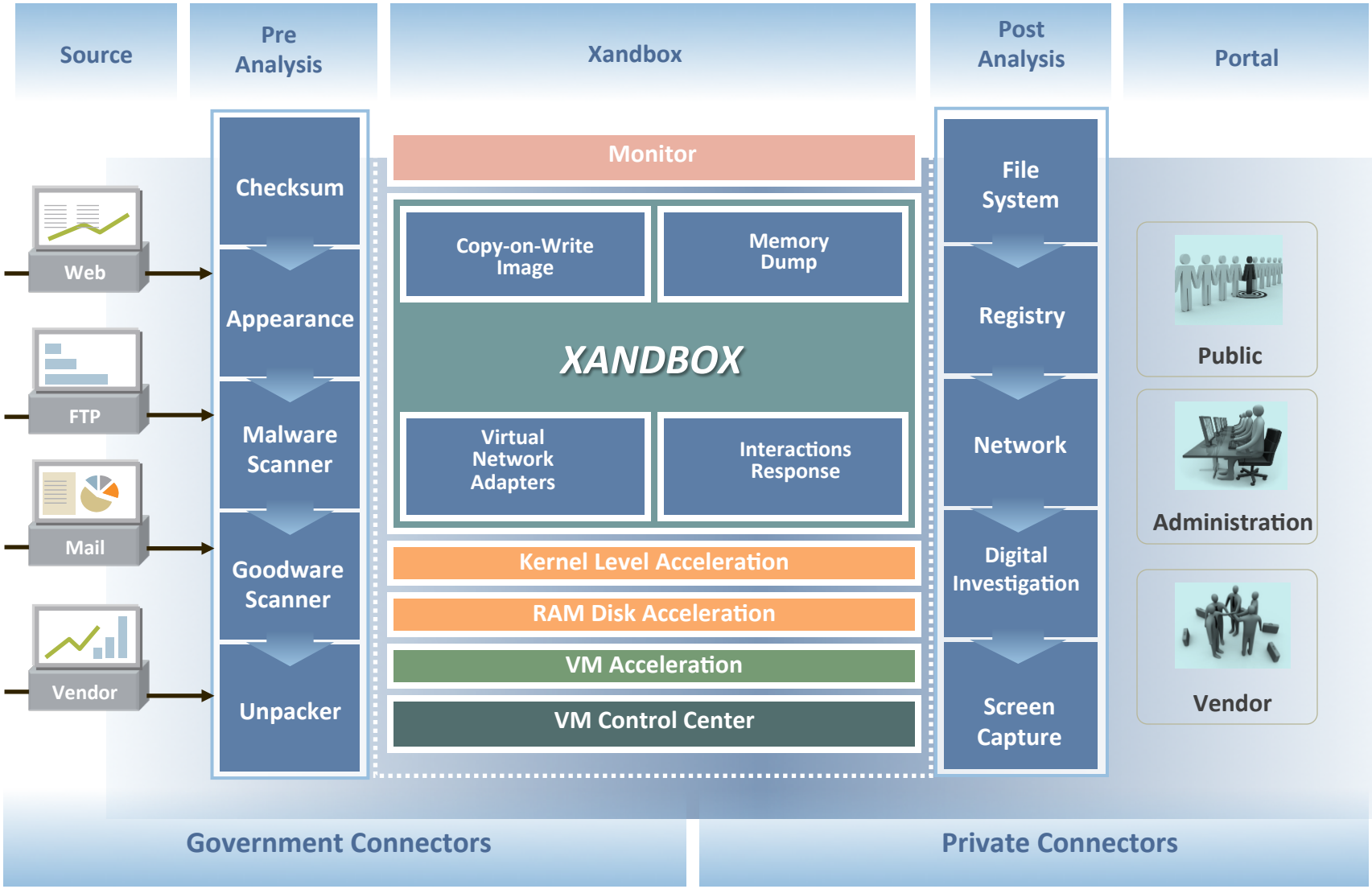
Possible Malware

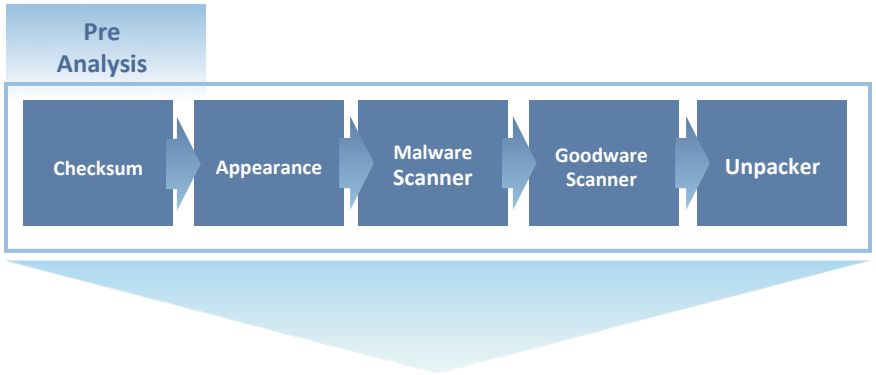


Automated Malware Analysis
Platform

ARCHITECTURE

Architecture Overview





Checksum

- Common unique identification
- Generate SHA1 and MD5

Appearance

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

Malware Scanner

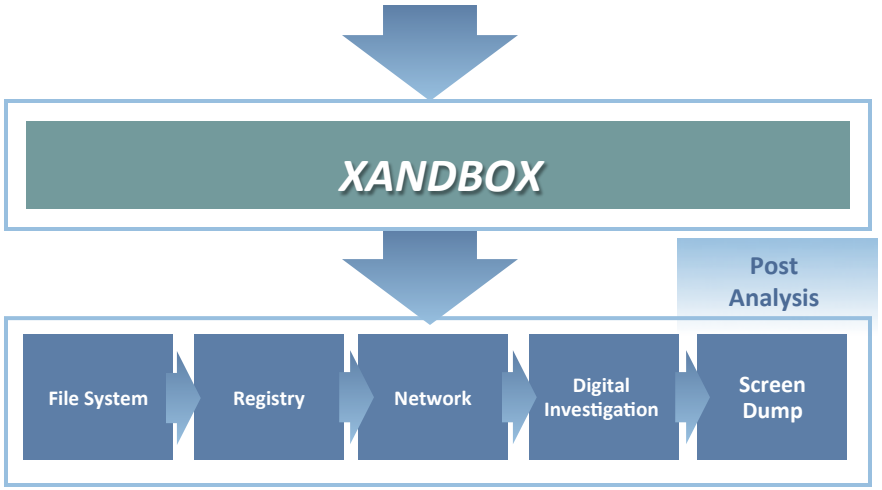
- VirusTotal
- Compare against all antivirus vendor listed in VirusTotal
- Private access to VirusTotal database

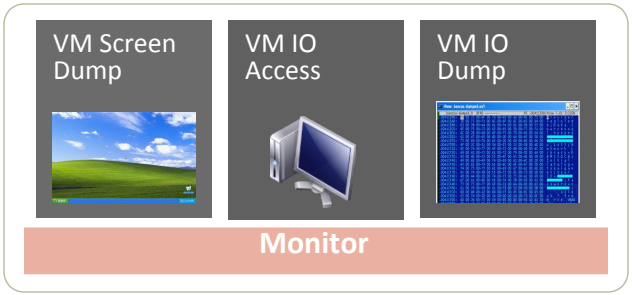
Goodware Scanner

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

Unpacker

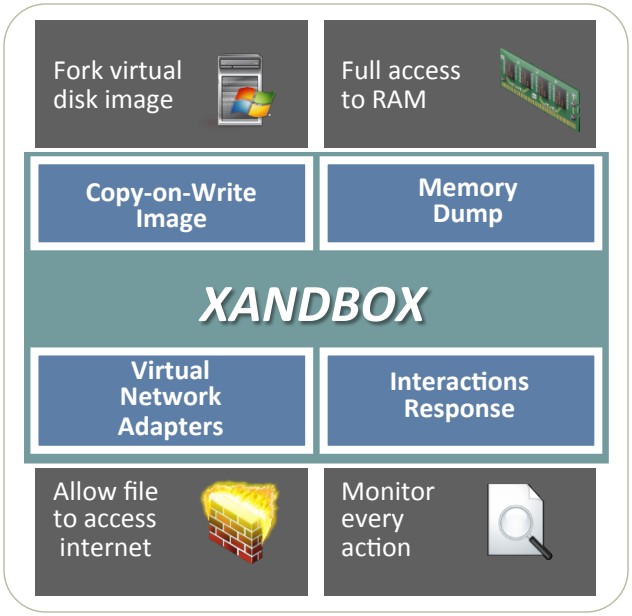
- Unpack binary for static analysis
- Able to automatically unpack ASPack, NSPack, UPX and PE_Compact





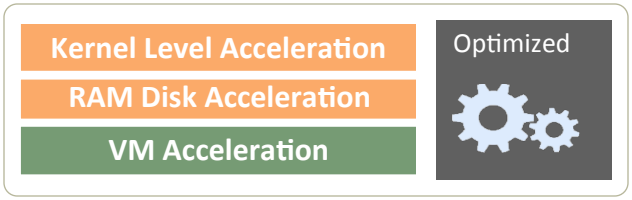
VM Monitor Access

- 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



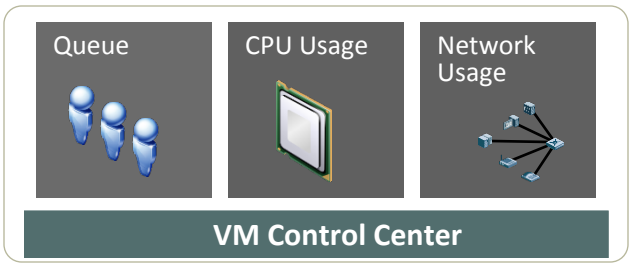
Xanbox

- 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



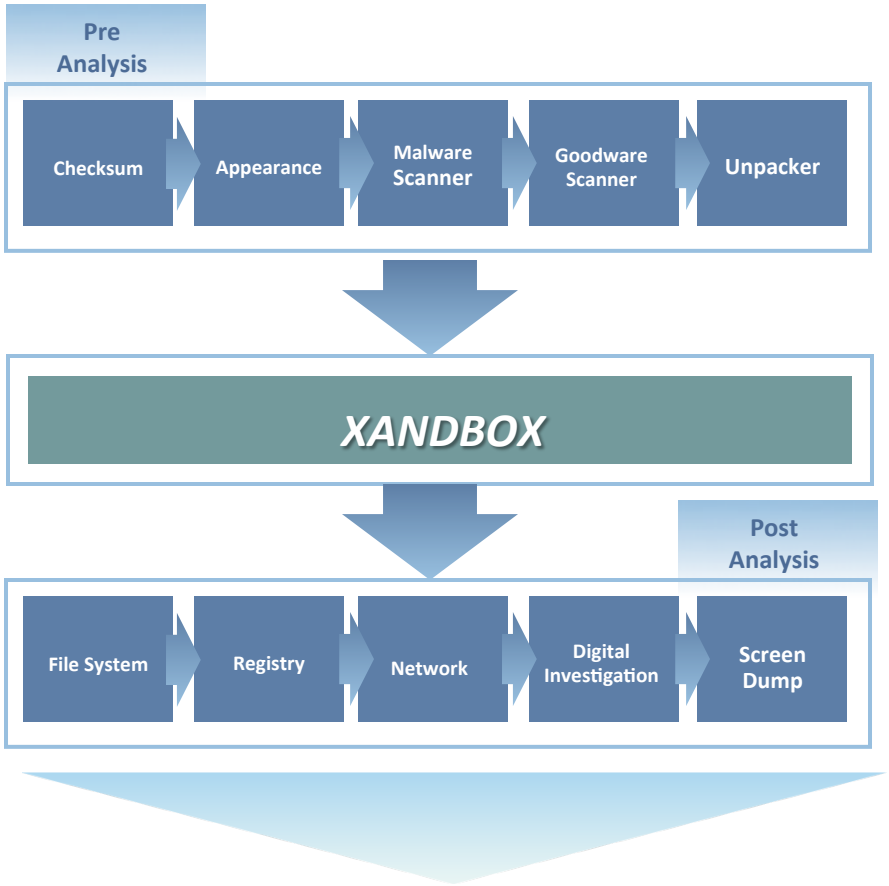
Acceleration

- 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



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

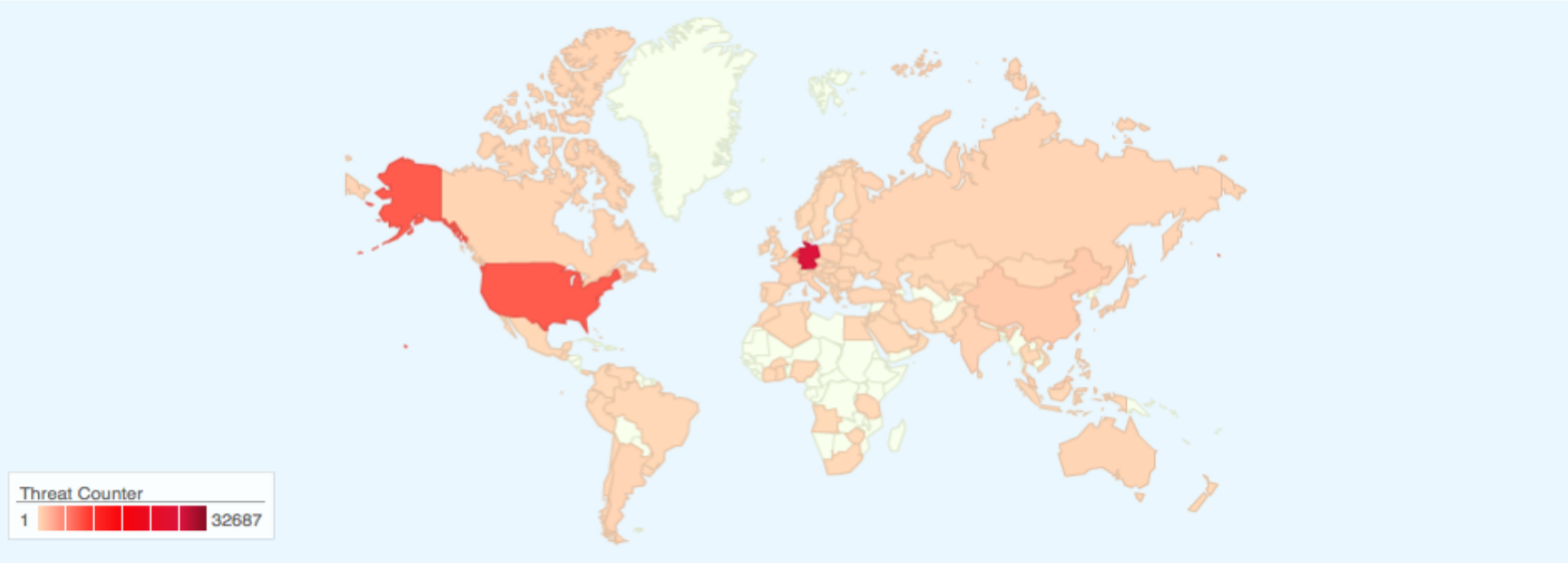
IN ACTION

PORTAL

Xandora - Your Online Binary Analyzer

Home | Dashboard | Users

md5 Search



24H Top Received Malware rss
Heuristic.gen
Trojan.Gen
Trojan.Win32.Generic!BT

24H Top Connection by IP rss	
NL	62.212.74.67
TR	88.238.143.71
US	208.73.210.29

24H Top Connection by Domain rss	
NL	skuj4ugfddsj.com
QA	asyueu37yhd.com
CN	img001.com

PORTAL

Xandora - Your Online Binary Analyzer

Home | Dashboard | Users

md5 Search

2,098,108	522	8,960	620	30,432	98,177
Processed	Queued	Processing	Analyzed today	Analyzed This Week	Analyzed This Month

1 2 3 83923 83924 83925 Next Last

No.	Name	MD5	Date	Time	Score	Size	Ext	VT
1	Unidentified	60502ea64aff008d9094eb3488a61c37	2011-10-12	03:15:00	59	221696	dll	0
2	Backdoor.Win32.Bifrose.dstn	8801e59b078e3f478a3ebb0b16deba09	2011-10-12	03:15:00	92	513000	exe	27
3	Hoax.MSIL.ArchSMS.clt	65425da20e1990fac7056d36aa6a6eaf	2011-10-12	03:15:00	33	1951729	exe	16
4	Net-Worm.Win32.Allaple.b	287dd90eb8c37f0a10d5573b276e6191	2011-10-12	03:15:00	146	57856	exe	35
5	HEUR:Backdoor.Win32.ZAccess.gen	31e5aaa62457f7089ba4869eada19b71	2011-10-12	03:15:00	126	48016	exe	28
6	Unidentified	b7dd267f9986872a281713d8fdf10b02	2011-10-12	03:15:00	34	73904	exe	0
7	Unidentified	102f6b881218f7572d013caa90c3ad99	2011-10-12	03:15:00	73	1189424	exe	0
8	W32/Behav-Heuristic-CorruptFile-EP	145f99b35923ecd0e411d329c7744a5f	2011-10-12	03:15:00	52	515728	dll	3
9	Unidentified	f85507291f052d00d168075f9be7a9c6	2011-10-12	03:15:00	55	512000	exe	0
10	W32/Behav-Heuristic-CorruptFile-EP	f943bec2f77cb2e962c2e6d3d410eec6	2011-10-12	03:15:00	67	512000	exe	4
11	Unidentified	96c3720900b4f0fa2b8ae4f638228d9e	2011-10-12	03:12:00	81	1579644	exe	0
12	Unidentified	ef4c739afc76d1460399dbaaa1942c69	2011-10-12	03:12:00	52	230912	dll	0

File Information

Unidentified

Like Tweet 0 Share

Download File

File Details

MD5	e9d23dd5bd55bd36b224d5a7d09af329
SHA-1	db939a875958f784066f67f1cbb8d1053e2c86cd
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

++++++++++++++++++++++++ FILE HEADER INFORMATION ++++++++++++++++++++++++

TimeStamp: 2A425E19 Sat Jun 20 06:22:17 1992
Subsystem: 2 (Windows GUI)
Image Base: 00400000 Size: 00028000
Code Base: 00001000 Size: 0001B800
Data Base: 0001D000 Size: 00007000
Entry Point: 0001AE44 (file offset 0001A244)

++++++++++++++++++++++++++++++++ SECTIONS ++++++++++++++++++++++++++++++++

1: CODE RVA: 00001000 Offset: 00000400 Size: 0001B800 Flags: 60000020 (CER)
2: DATA RVA: 0001D000 Offset: 0001BC00 Size: 00001400 Flags: C0000040 (DRW)
3: BSS RVA: 0001F000 Offset: 0001D000 Size: 00000000 Flags: C0000000 (RW)
4: .idata RVA: 00020000 Offset: 0001D000 Size: 00000C00 Flags: C0000040 (DRW)
5: .tls RVA: 00021000 Offset: 0001DC00 Size: 00000000 Flags: C0000000 (RW)
6: .rdata RVA: 00022000 Offset: 0001DC00 Size: 00000200 Flags: 50000040 (DSR)
7: .reloc RVA: 00023000 Offset: 0001DE00 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
- **yaigay.exe**, pid: 488
- **awhost.exe**, pid: 112
- **dwwin.exe**, pid: 940
- **cwhost.exe**, pid: 544
- **439017316**, pid: 1536

File system and Registry

Filesystem Change

The following file was changed in the system

- "/WINDOWS/439017316"
- "/WINDOWS/Temp/Perflib_Perfdata_7a0.dat"
- "/WINDOWS/system32/CatRoot2/tmp.edb"

Registry Change

The following Registry Keys were changed

- software_Microsoft_Windows_CurrentVersion_Group_Policy_State_Machine_Extension-List
- software_Microsoft_Windows_CurrentVersion_Group_Policy_State_Machine_Extension-List
- 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_ProfileList
- software_Microsoft_Windows_NT_CurrentVersion_Prefetcher
- software_Microsoft_Windows_NT_CurrentVersion_ProfileList
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Applets_SysTray
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Applets_SysTray
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Explorer_CD_Burning_Drives
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Explorer_CLSID
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Explorer_CD_Burning_Drives
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Explorer_CLSID
- NTUSER_Software_Microsoft_Windows_CurrentVersion_Explorer_Desktop

Network

Traffic - by TCP/IP Connections

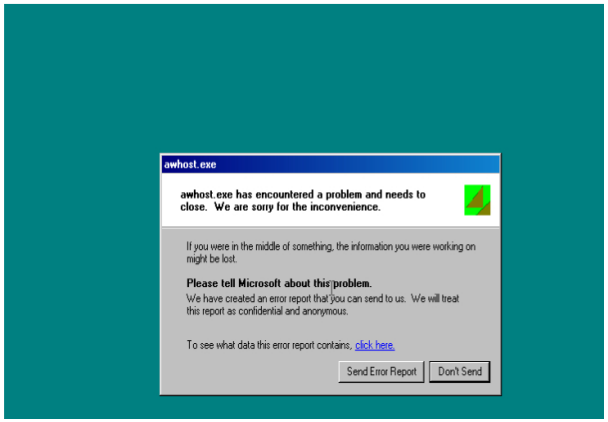
Produces outbound traffic, view by host and port

- 105.142.238.162 : 34354
- 109.54.49.235 : 34354
- 173.169.154.120 : 34354
- 173.3.172.129 : 34354
- 173.80.230.1 : 34354
- 174.101.90.246 : 34354
- 174.65.23.52 : 34354
- 178.89.152.177 : 34354
- 178.89.155.217 : 34354
- 178.89.56.132 : 34354
- 178.90.46.9 : 34354
- 178.91.82.85 : 34354
- 183.179.9.127 : 34354
- 186.180.61.186 : 34354
- 186.34.194.101 : 34354
- 2.133.69.183 : 34354
- 2.50.129.94 : 34354
- 201.255.185.198 : 34354
- 216.227.104.37 : 34354
- 24.184.199.219 : 34354
- 24.57.252.252 : 34354
- 41.70.180.249 : 34354
- 41.75.116.113 : 34354

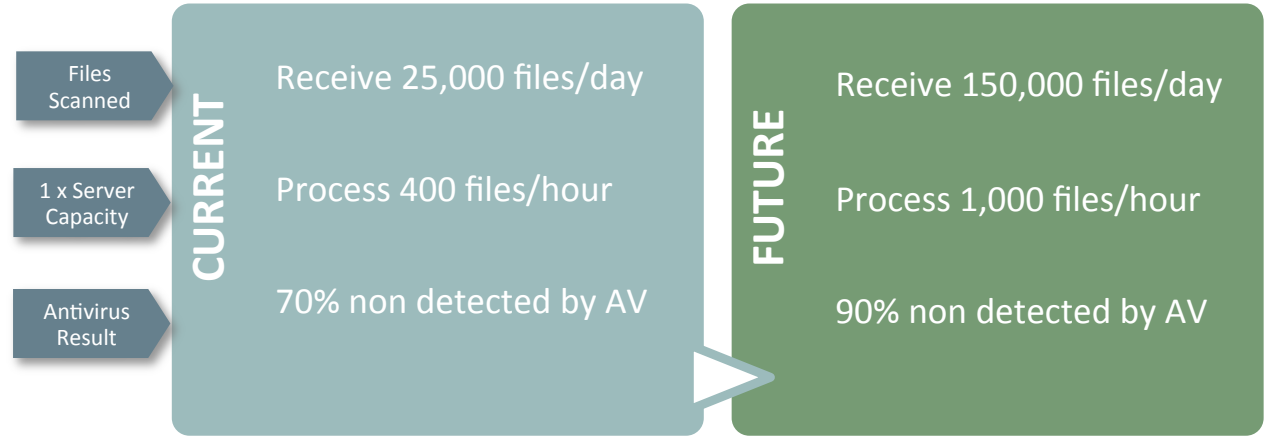
Screen Shot

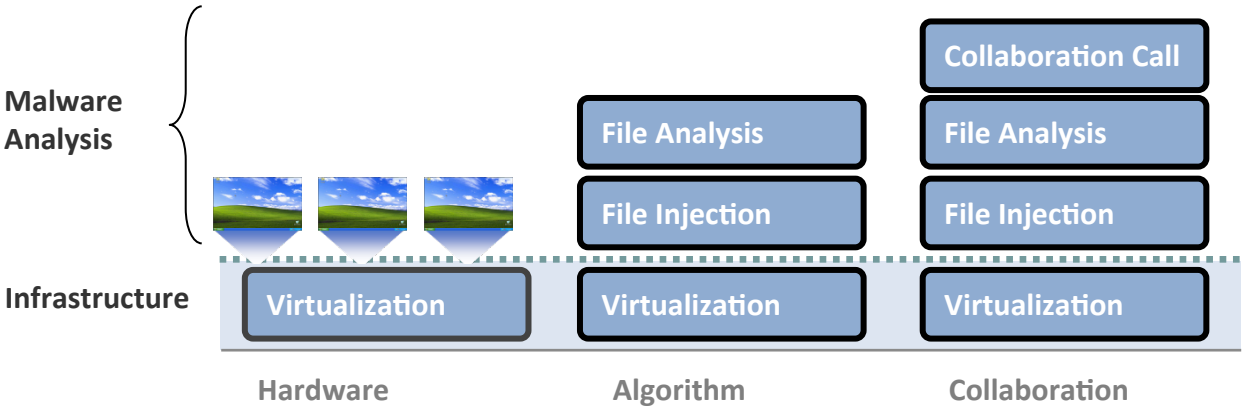
Screen Capture

The new window was created



INFRASTRUCTURE





Virtualization

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

Sandboxing

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

Collaboration

- Request for information from our analysis partners
- Expertise and focus

TECHNICAL PROBLEMS

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

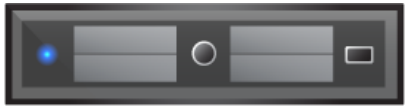
- Reduce mount and umount at preprocess
- Post process qcow +NTFS problems

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



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

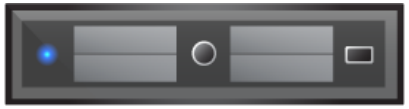
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

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



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

Detect VM ENV

- Detect samples not able to run under VM
- **Possible Malware**

Execution Timing

- Fixed time between 3 to 5 minutes
- Execution and no response from binary
- **Possible Malware**

Volume

- Small scale Windows
- VM monitoring and queuing engine
- Task allocation

Hiding Client

- No client required
- Possible malware scoring algorithm

Report

- Simple
- Ensure readability

THE XANDORA WAY

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

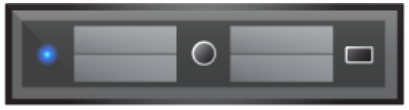
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM

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

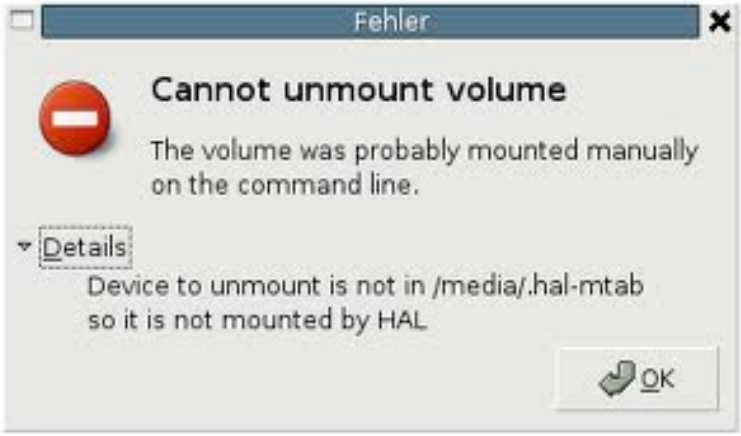
Input/Output

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



Problems

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



Preprocessing

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

Sandbox

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

Post Processing

i. Mount ntfs over tcpip
ii. Mount ntfs over ramfs
iii. Modding ntfs-3g
    a. Disable checking
    b. Force read only
    c. Fix to one NTFS version

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

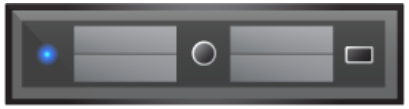
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

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

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

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

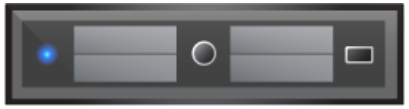
- Reducing mount and umount at preprocess
- Post process qcow +NTFS problems

Concurrent VM

- How many VMs
- How to check
- What the most heave process

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

IDENTIFICATION

File System

- What is good, what is bad.

Registry

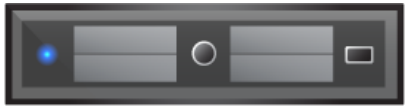
- How to know changes in registry is good or malicious

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

Filesystem Change

The following file was changed in the system

- "/WINDOWS/Prefetch/NET.EXE-01A53C2F.pf"
- "/WINDOWS/Prefetch/NET1.EXE-029B9DB4.pf"
- "/WINDOWS/Prefetch/RUNOUCE.EXE-37141743.pf"
- "/WINDOWS/system32/runouce.exe"

Filesystem Change

The following file was changed in the system

- "/Autorun.inf"
- "/WINDOWS/Help/HelpCat.exe"
- "/WINDOWS/Prefetch/ATTRIB.EXE-39EAFB02.pf"
- "/WINDOWS/Sysinf.bat"
- "/WINDOWS/Tasks/At1.job"
- "/WINDOWS/Tasks/At2.job"
- "/WINDOWS/Tasks/At3.job"
- "/WINDOWS/Tasks/At4.job"
- "/WINDOWS/Tasks/At5.job"
- "/WINDOWS/Tasks/At6.job"
- "/WINDOWS/regedt32.sys"
- "/WINDOWS/system/KavUpda.exe"
- "/WINDOWS/system32/CatRoot2/tmp.edb"
- "/WINDOWS/system32/Folderdir"
- "/WINDOWS/system32/Option.bat"
- "/ntldr~6"
- "/ntldr~8"

File System

- What is good, what is bad.

Registry

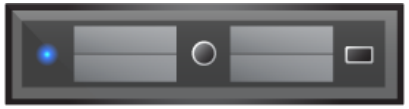
- How to know changes in registry is good or malicious

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_IEXPLORE.EXE_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

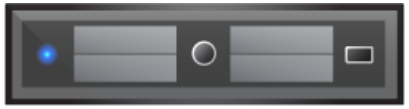
- How to know changes in registry is good or malicious

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 (svch0st.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: 848
- **svchost.exe**, pid: 892
- **explorer.exe**, pid: 1080
- **alg.exe**, pid: 1616
- **wuauclt.exe**, pid: 1316
- **DIDfuRcLeJEc.ex**, pid: 1400
- **P1kAIMiG2Kb7Fz.**, pid: 972

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
- **explorer.exe**, pid: 1036
- **svchost.exe**, pid: 1060
- **SAMPLE.EXE**, pid: 1680
- **alg.exe**, pid: 1808
- **lvvm.exe**, pid: 968
- **wuauclt.exe**, pid: 1572
- **conhost.exe**, pid: 1592

File System

- What is good, what is bad.

Registry

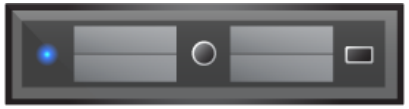
- How to know changes in registry is good or malicious

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

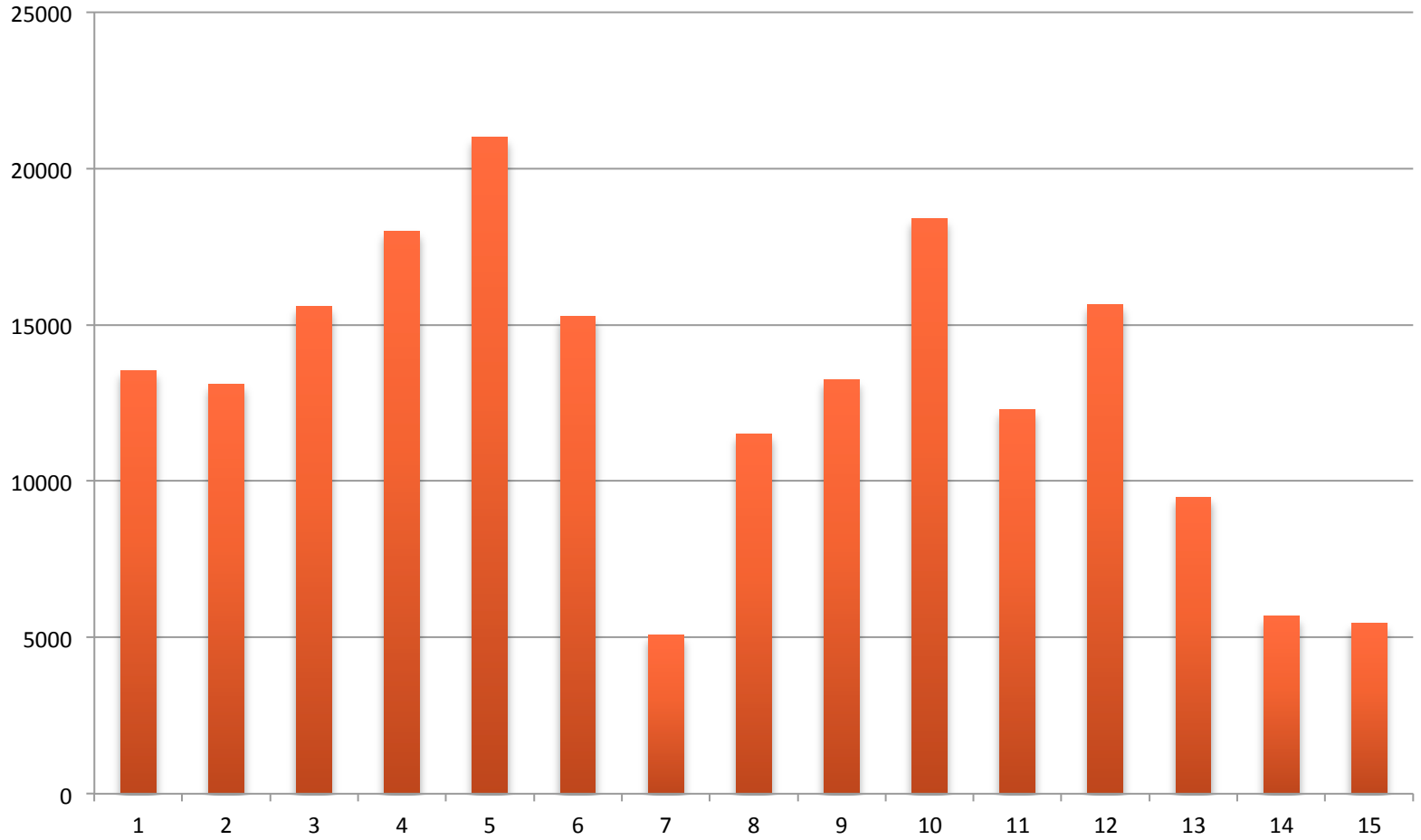
Traffic - by URL

Produces outbound traffic, view by URL

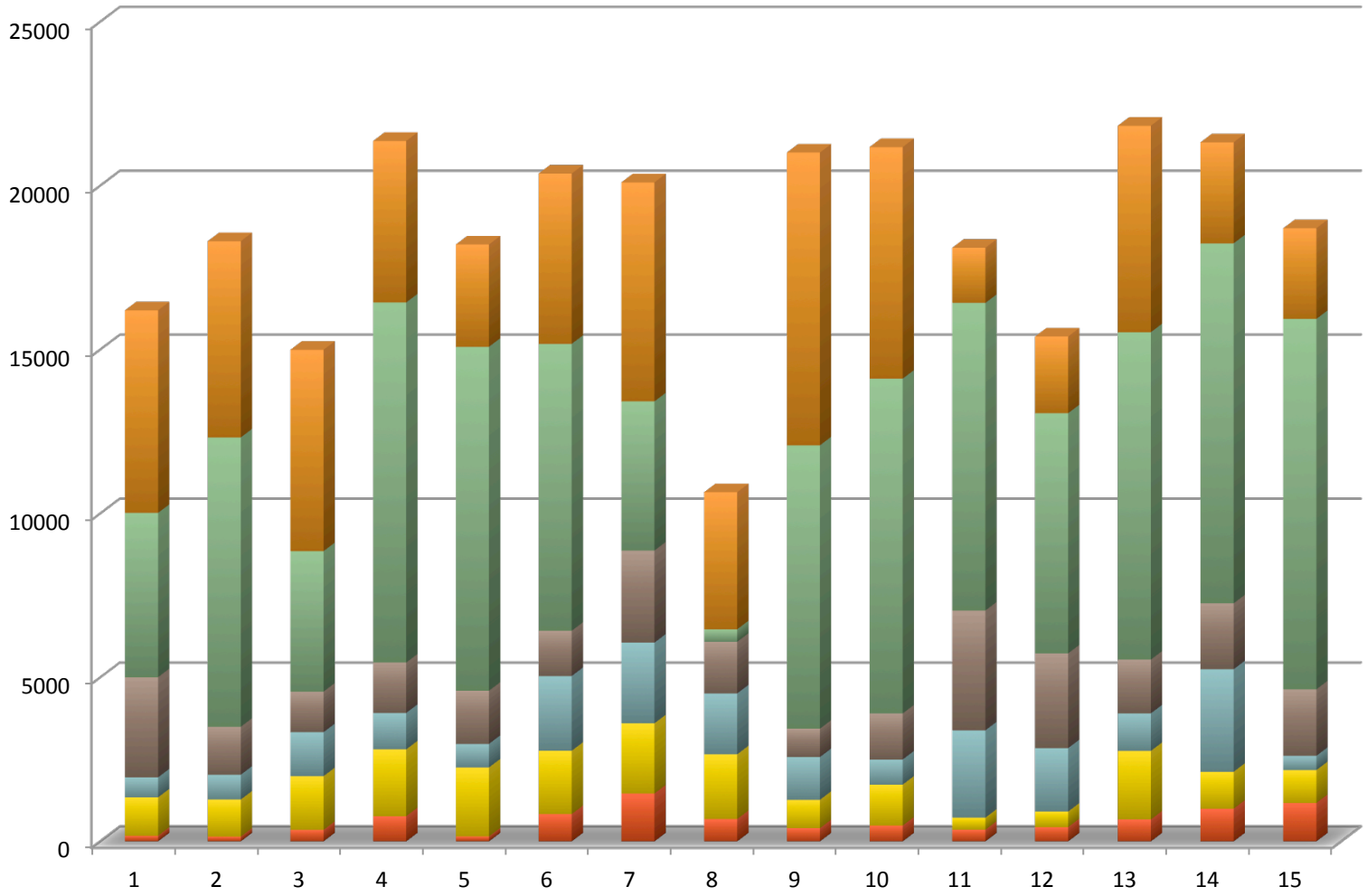
- **www.dnf01.com**/gg
- **www.dnf01.com**/gg
- **www.dnfboshi.com**/
- **new.egooad.com**/show
- **new.egooad.com**/TESTPage
- **new.egooad.com**/TESTPage
- **activex.microsoft.com**/objects
- **codecs.microsoft.com**/isapi
- **new.egooad.com**/egjpm.aspx?apid=10988&isr=FD99E8D17CEDF9BAAB69F82AD57DB12A&ibmm=1209&syykj=2011-10-12+11%3a05%3a50&zpuc=202.190.74.20&bi=COOKIE%3Atrue%3BCPU_MODEL%3Ax86%3BOS_LANG%3Aen-us&chti=1&ref=&bl=http%3A%2F%2Fwww.dnf01.com%2Fgg%2Flvbu.htm&sh=600&sw=800&ws=&fsz=69&fcd=10%2F11%2F2011&fmd=10%2F11%2F2011&htl=0&chs=windows-1252&cpj=true&tzo=-7&plgn=0&mimen=0&srlt=298&srtp=328&psrh=31&ms=
- **tc.100tjs.com**/gvo001.php?id=3&uid=24199&ams=X6jkoaCcW%2fo%3d
- **t.100tjs.com**/tdyx

STATISTICS

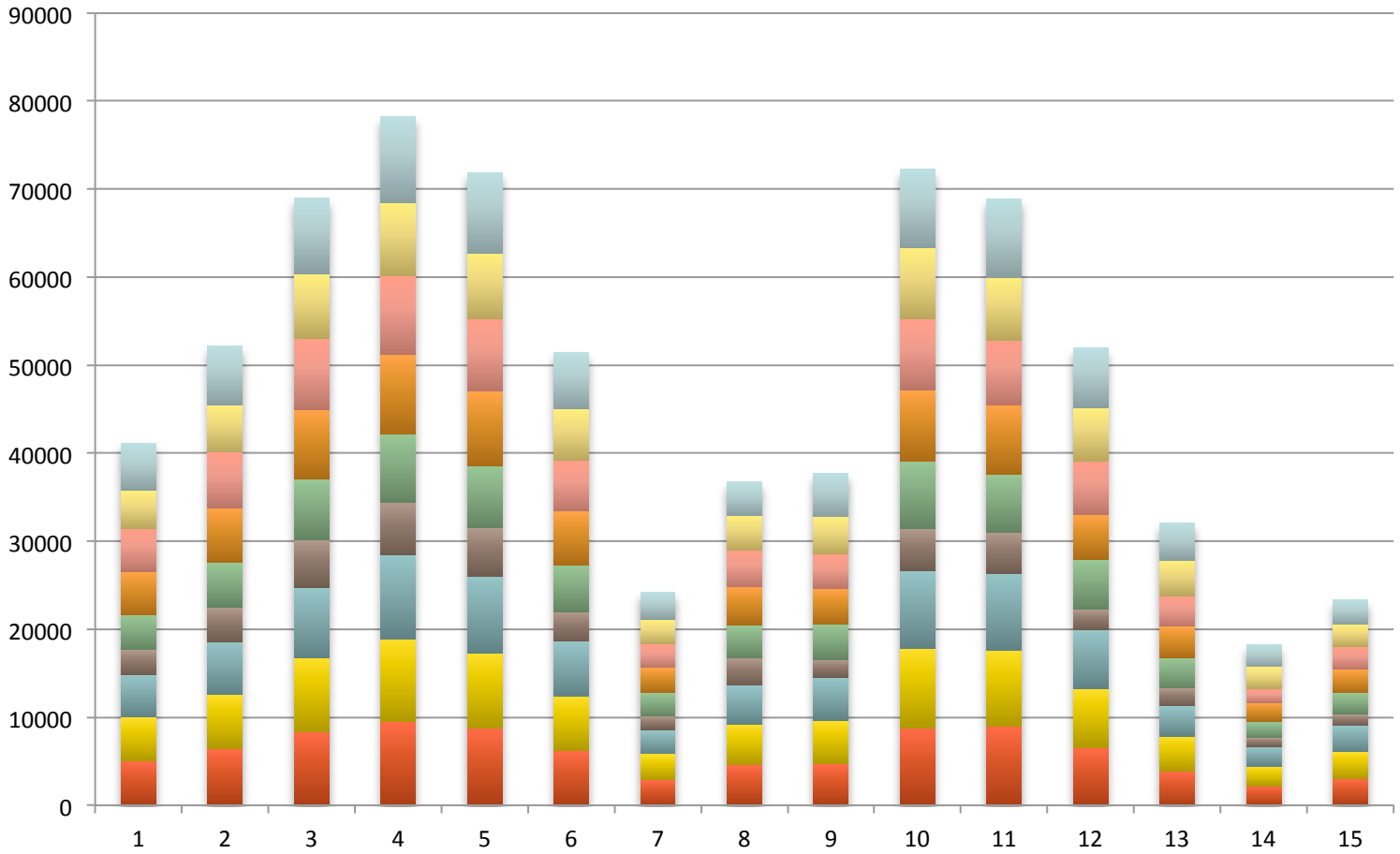
15 Days Received Files



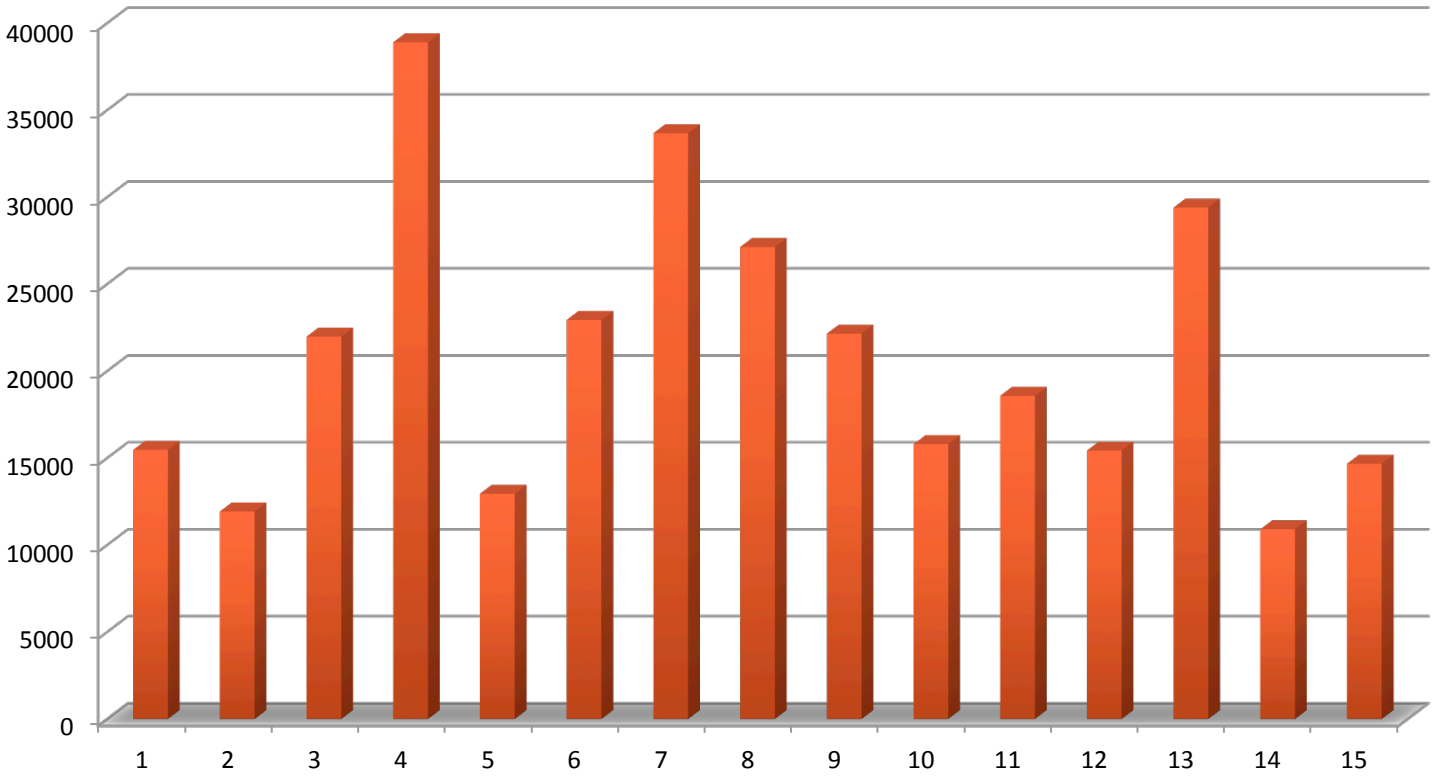
15 DAYS RECEIVED SAMPLES – BY VENDORS



Vendors Detection



URL – 15 DAYS


40000
35000
30000
25000
20000
15000
10000
5000
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

GLOBAL PARTNERSHIPS

Global Partnership

SECTOR

Meeting Future Needs

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

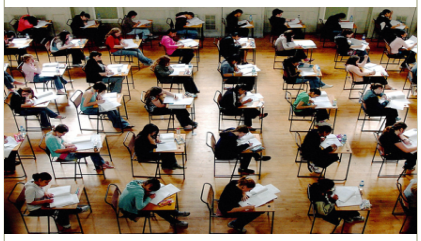
Country CERTs should have operations to monitor targeted attacks which can affect its economy and security.

- 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.

ROADMAP


2012
Jan - March
New Reporting Interface
April
Multi Vendor Profiling
May/June
Binary Profiling
July/August
Translation
Aug/Sept
NoSQL Conversion
Oct
Executive Reporting
Nov/Dec
PDF/Office/ APK File Analysis

REFERENCES & ACKNOWLEDGEMENTS

References

1. Nguyen Anh Quynh, Virt-ICE: next generation debugger for malware analysis
2. Nguyen Anh Quynh, eKimono: A Malware Scanner for Virtual Machines
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

kj@xandora.net | http://xandora.net | http://www.facebook.com/xandora | @kaijern | @susPEciousfile