빠르게 끝내는 악성코드 분석 및 대응

Dalgomtaeng

dalgomtaeng@gmail.com

Dalgomtaeng.blogspot.kr

@dalgomtaeng

Who Am I ?

- 관심사 : DFIR, Elastic, Opensource

CATHOLIC UNIVERSITY OF KOREA

F-INSIGHT

AhnLab

목차

악성코드 분석

- 빠르게 빠르게~

- 왜 빠르게 분석해야 하는가?
  - 한정된 분석 시간
  - 침해 원인 파악에 비중
  - 또 다른 침해 자산에 대한 확인을 위함

- 어떤 결과가 필요한가?
  - 분석가가 쉽고 간편하게 볼 수 자료
  - 고객이 이해할 수 있는 쉬운 자료

virustotal

SHA256: 620a4a2c4e3c48df68c13fe531e07aabf88cb7a348a4781496889ca2fc9321bb

파일 이름: 620a4a2c4e3c48df68c13fe531e07aabf88cb7a348a4781496889ca2fc9321bb....

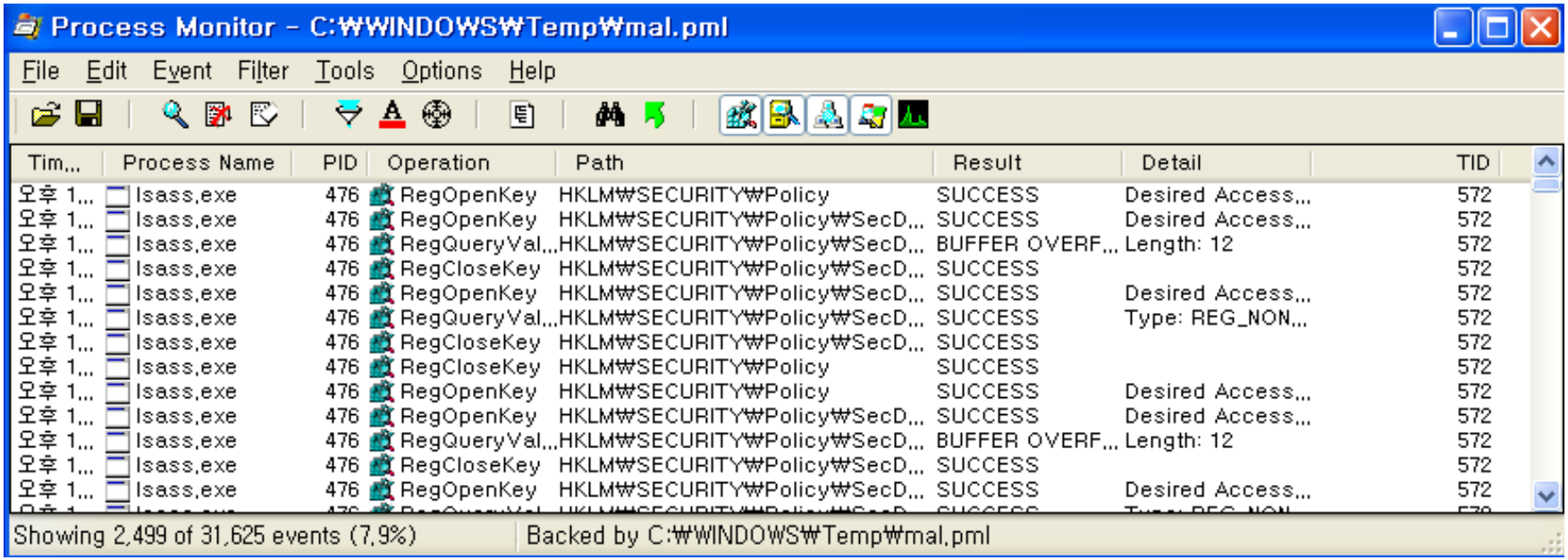
탐지 비율: 5 / 55

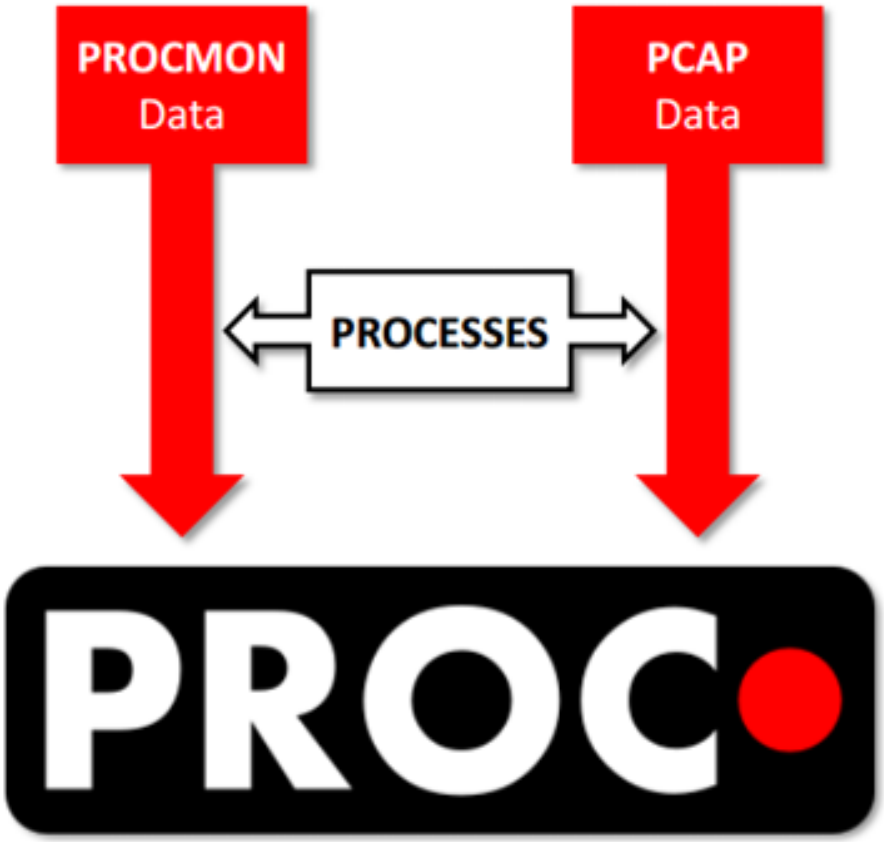
분석 날짜: 2015-08-20 20:40:42 UTC (17시간, 59분 전)

분석 | File detail | Relationships | 추가 정보 | 댓글 2 | 투표

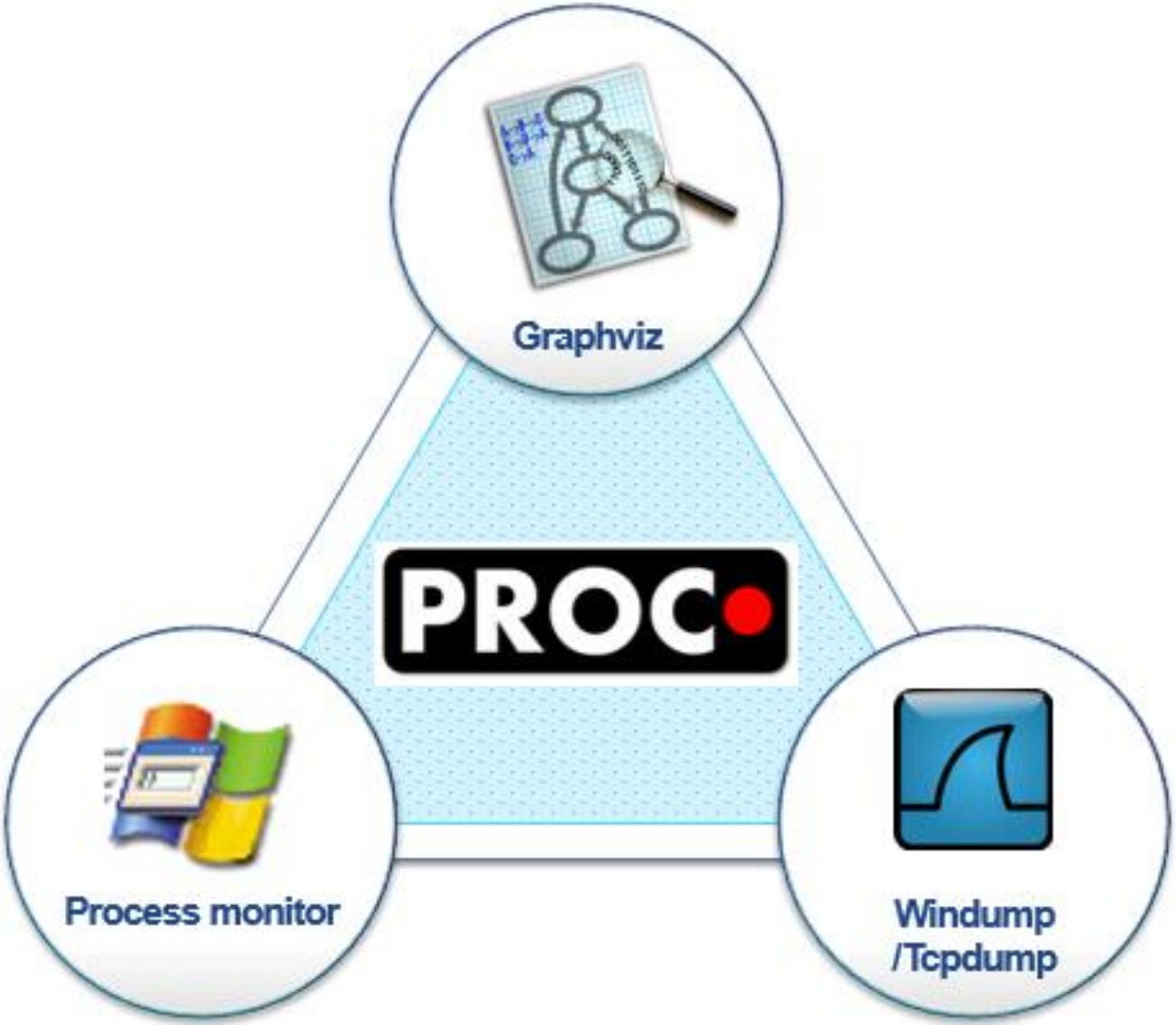
안티바이러스	결과	업데이트
Baidu-International	Trojan.MSIL.Injector.LLW	20150817
Kaspersky	UDS:DangerousObject.Multi.Generic	20150818
McAfee	Artemis!AD8B1D7BF608	20150818
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.dc	20150818
Rising	PE:Trojan.Win32.Generic.18F97855!419002453	20150817
ALYac		20150818

Procmon

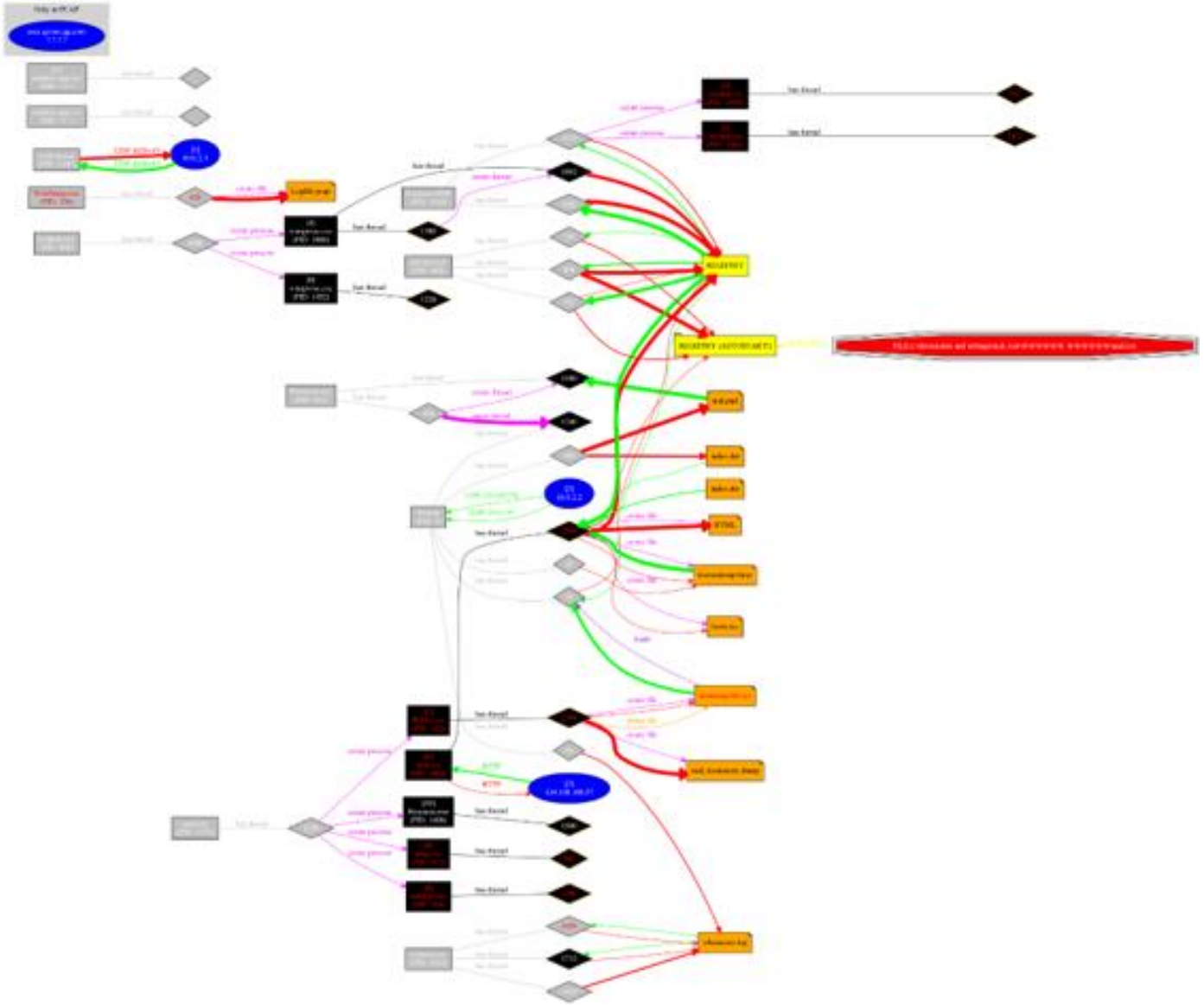

Process Monitor - C:₩WINDOWS₩Temp₩mal.pml
File Edit Event Filter Tools Options Help
Tim... Process Name PID Operation Path Result Detail TID
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy SUCCESS Desired Access... 572
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS Desired Access... 572
오후 1... lsass.exe 476 RegQueryVal... HKLM₩SECURITY₩Policy₩SecD... BUFFER OVERF... Length: 12 572
오후 1... lsass.exe 476 RegCloseKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS 572
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS Desired Access... 572
오후 1... lsass.exe 476 RegQueryVal... HKLM₩SECURITY₩Policy₩SecD... SUCCESS Type: REG_NON... 572
오후 1... lsass.exe 476 RegCloseKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS 572
오후 1... lsass.exe 476 RegCloseKey HKLM₩SECURITY₩Policy SUCCESS 572
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy SUCCESS Desired Access... 572
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS Desired Access... 572
오후 1... lsass.exe 476 RegQueryVal... HKLM₩SECURITY₩Policy₩SecD... BUFFER OVERF... Length: 12 572
오후 1... lsass.exe 476 RegCloseKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS 572
오후 1... lsass.exe 476 RegOpenKey HKLM₩SECURITY₩Policy₩SecD... SUCCESS Desired Access... 572
Showing 2,499 of 31,625 events (7.9%)
Backed by C:₩WINDOWS₩Temp₩mal.pml

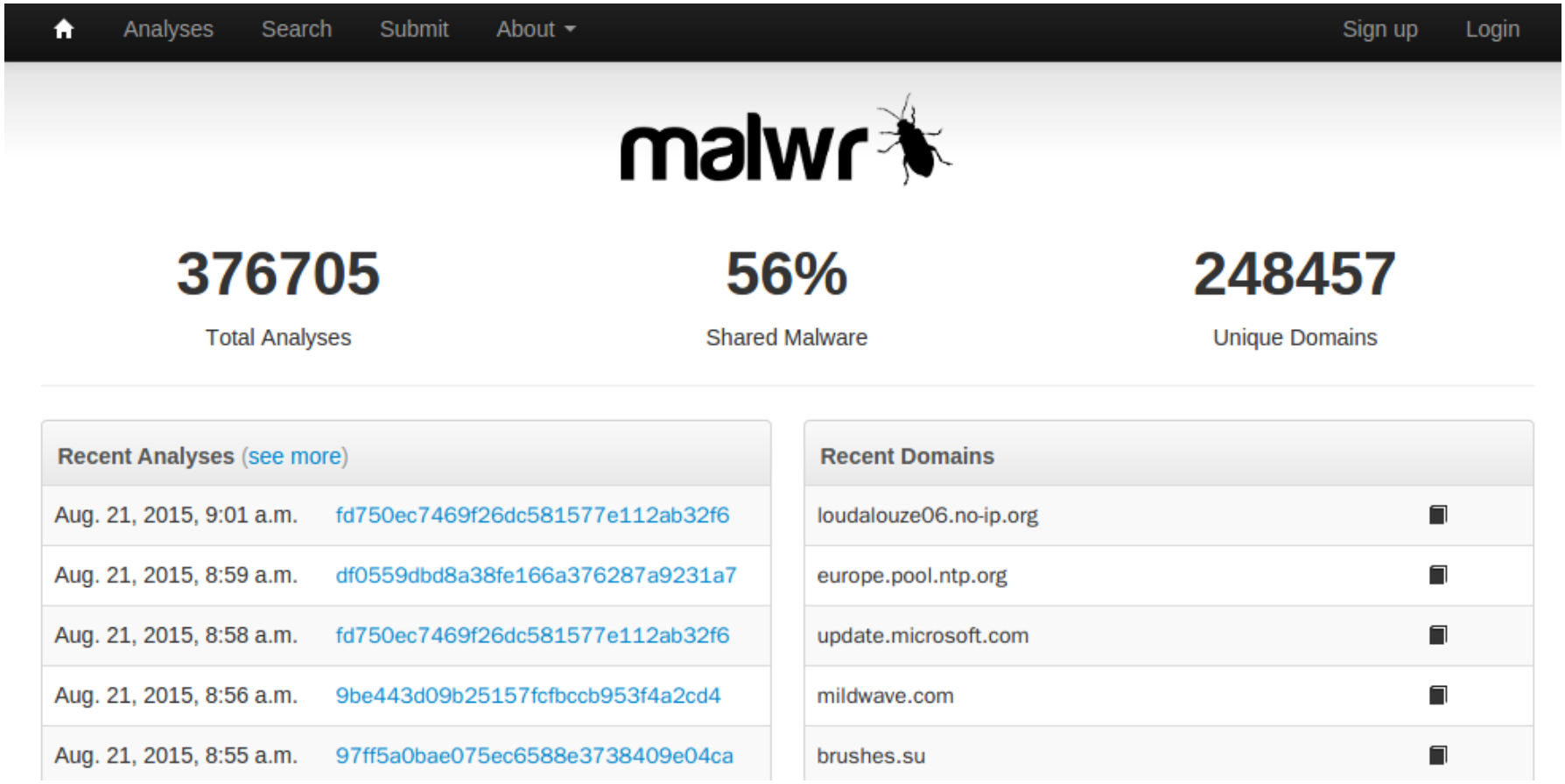

PROCMON
Data
PCAP
Data
PROCESSES
PROC

활동	Procmon	PCAP(Windump, Tcpdump, Wireshark)
Filesystem	✓	✗
Network	✓	✓
Registry	✓	✗
Process-Management	✓	✗
Thread-Management	✓	✗


Graphviz
PROCDOT
Process monitor
Windump
/Tcpdump

Procdot

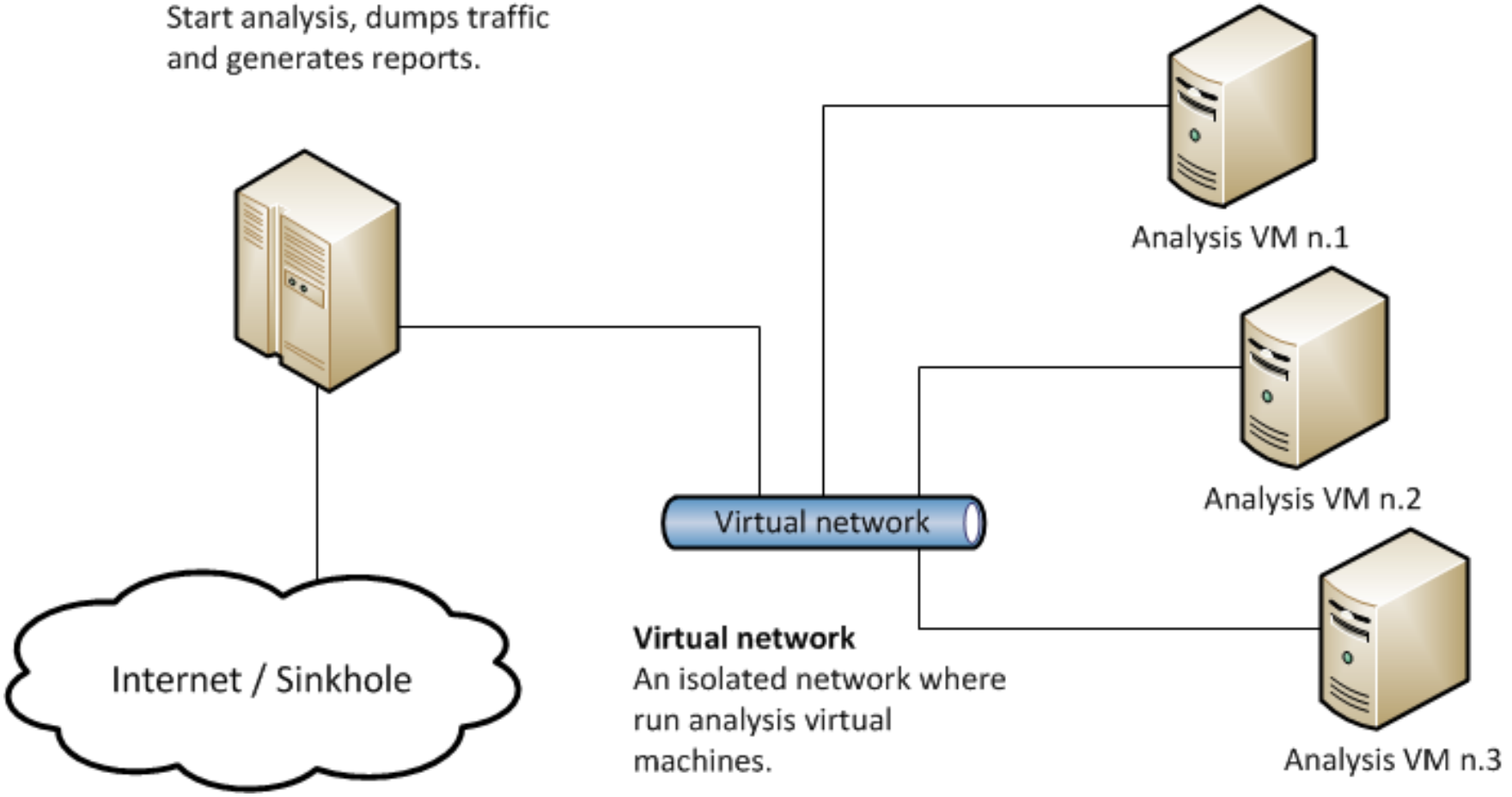



Analyses
Search
Submit
About
Sign up
Login
malwr
376705
Total Analyses
56%
Shared Malware
248457
Unique Domains
Recent Analyses (see more)
Aug. 21, 2015, 9:01 a.m. fd750ec7469f26dc581577e112ab32f6
Aug. 21, 2015, 8:59 a.m. df0559dbd8a38fe166a376287a9231a7
Aug. 21, 2015, 8:58 a.m. fd750ec7469f26dc581577e112ab32f6
Aug. 21, 2015, 8:56 a.m. 9be443d09b25157fcfbccb953f4a2cd4
Aug. 21, 2015, 8:55 a.m. 97ff5a0bae075ec6588e3738409e04ca
Recent Domains
loudalouze06.no-ip.org
europe.pool.ntp.org
update.microsoft.com
mildwave.com
brushes.su

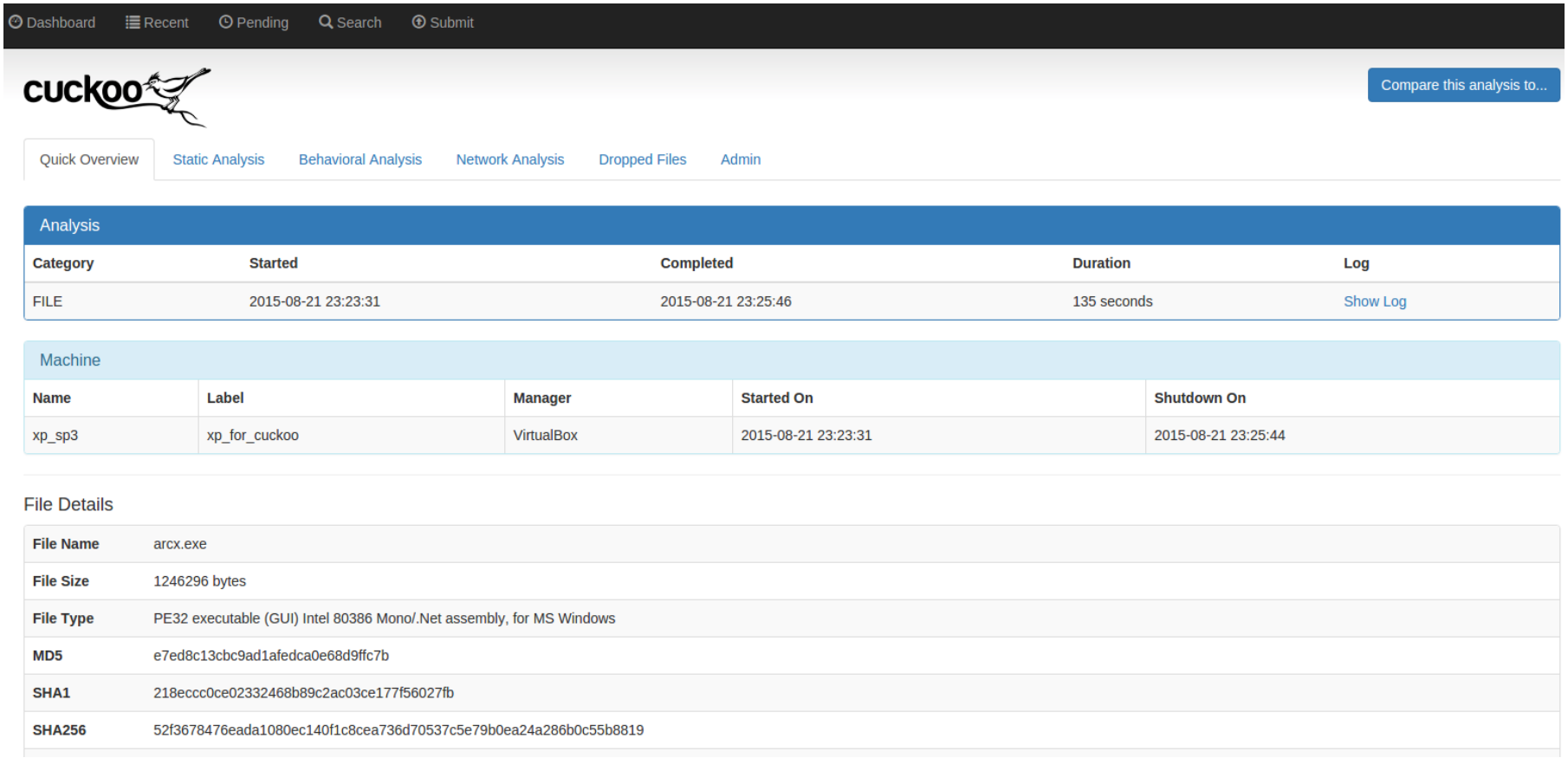
Cuckoo Sandbox

Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.



Virtual network
An isolated network where run analysis virtual machines.


Dashboard
Recent
Pending
Search
Submit
cuckoo
Compare this analysis to...
Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Admin
Analysis
Category
Started
Completed
Duration
Log
FILE
2015-08-21 23:23:31
2015-08-21 23:25:46
135 seconds
Show Log
Machine
Name
Label
Manager
Started On
Shutdown On
xp_sp3
xp_for_cuckoo
VirtualBox
2015-08-21 23:23:31
2015-08-21 23:25:44
File Details
File Name
arcx.exe
File Size
1246296 bytes
File Type
PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5
e7ed8c13cbc9ad1afedca0e68d9ffc7b
SHA1
218eccc0ce02332468b89c2ac03ce177f56027fb
SHA256
52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819

Quick Overview | Static Analysis | Behavioral Analysis | Network Analysis | Dropped Files | Admin

Static Analysis | Strings | Antivirus

PE Compile Time

2015-02-05 14:26:30

PE Imphash

f34d5f2d4577ed6d9ceec516c1f5a744

Version Infos

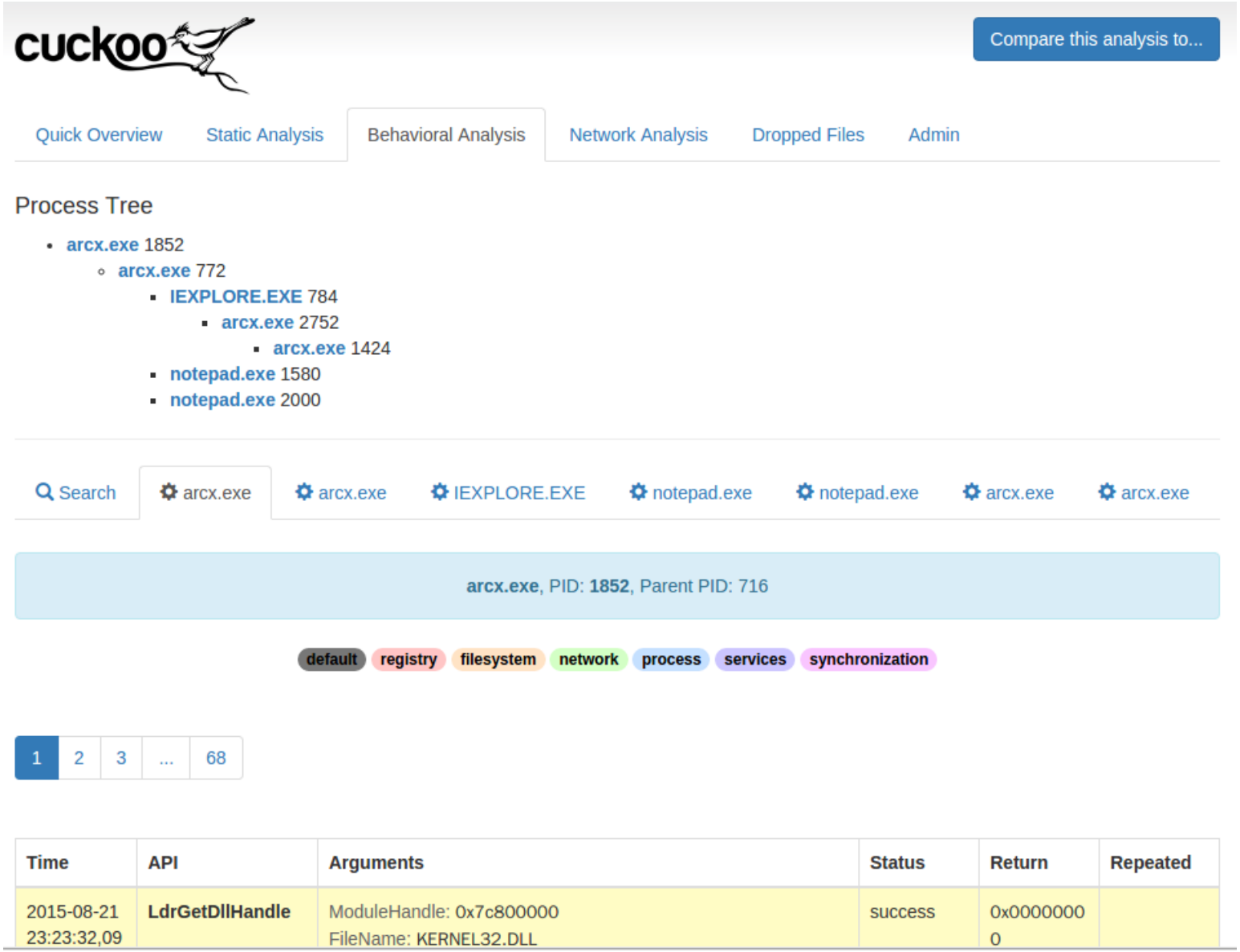
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2002-2008 Canneverbe Limited
Assembly Version	4.5.4.4852
InternalName	cdbxpp.exe
FileVersion	4.5.4.4852
CompanyName	Canneverbe Limited


cuckoo
Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Admin
Static Analysis
Strings
Antivirus
!This program cannot be run in DOS mode.
`.rsrc
@.reloc
lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
hSystem.Drawing.Bitmap, System.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3aPADPAD
QSystem.Drawing, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
System.Drawing.Bitmap
IDATx^
CO*UXV
O)7x,8
?W-836
BhZk7"
)SwOC~]d
$0:CxB

Quick Overview | Static Analysis | Behavioral Analysis | Network Analysis | Dropped Files | Admin

Static Analysis | Strings | Antivirus

Antivirus	Signature
Bkav	Clean
MicroWorld-eScan	Trojan.GenericKD.2145091
nProtect	Trojan.GenericKD.2145091
CMC	Clean
CAT-QuickHeal	TrojanDropper.Injector.g3
ALYac	Trojan.GenericKD.2145091
Malwarebytes	Trojan.Agent.ASGen
VIPRE	Trojan.Win32.Generic!BT
TheHacker	Clean
BitDefender	Trojan.GenericKD.2145091


cuckoo
Compare this analysis to...
Quick Overview
Static Analysis
Behavioral Analysis
Network Analysis
Dropped Files
Admin
Process Tree
arcx.exe 1852
arcx.exe 772
IEXPLORE.EXE 784
arcx.exe 2752
arcx.exe 1424
notepad.exe 1580
notepad.exe 2000
Search
arcx.exe
arcx.exe
IEXPLORE.EXE
notepad.exe
notepad.exe
arcx.exe
arcx.exe
arcx.exe, PID: 1852, Parent PID: 716
default
registry
filesystem
network
process
services
synchronization
1
2
3
...
68
Time
API
Arguments
Status
Return
Repeated
2015-08-21 23:23:32,09
LdrGetDllHandle
ModuleHandle: 0x7c800000
FileName: KERNEL32.DLL
success
0x00000000

cuckoo

Compare this analysis to...

Quick Overview | Static Analysis | Behavioral Analysis | Network Analysis | Dropped Files | Admin

Download PCAP

Hosts (6) | DNS (5) | TCP (5) | UDP (2) | HTTP (6) | ICMP (0) | IRC (0)

UDP

Source	Source Port	Destination	Destination Port
192.168.56.11	1025	168.126.63.1	53
192.168.56.11	138	192.168.56.255	138

▲192.168.56.11:1025 → 168.126.63.1:53

```
00000000: 77f1 0100 0001 0000 0000 0000 0463 726c  w
...........crl
00000010: 3308 6469 6769 6365 7274 0363 6f6d 0000  3
.digicert.com..
00000020: 0100 01                                  .
..
```

▲192.168.56.11:1025 → 168.126.63.1:53

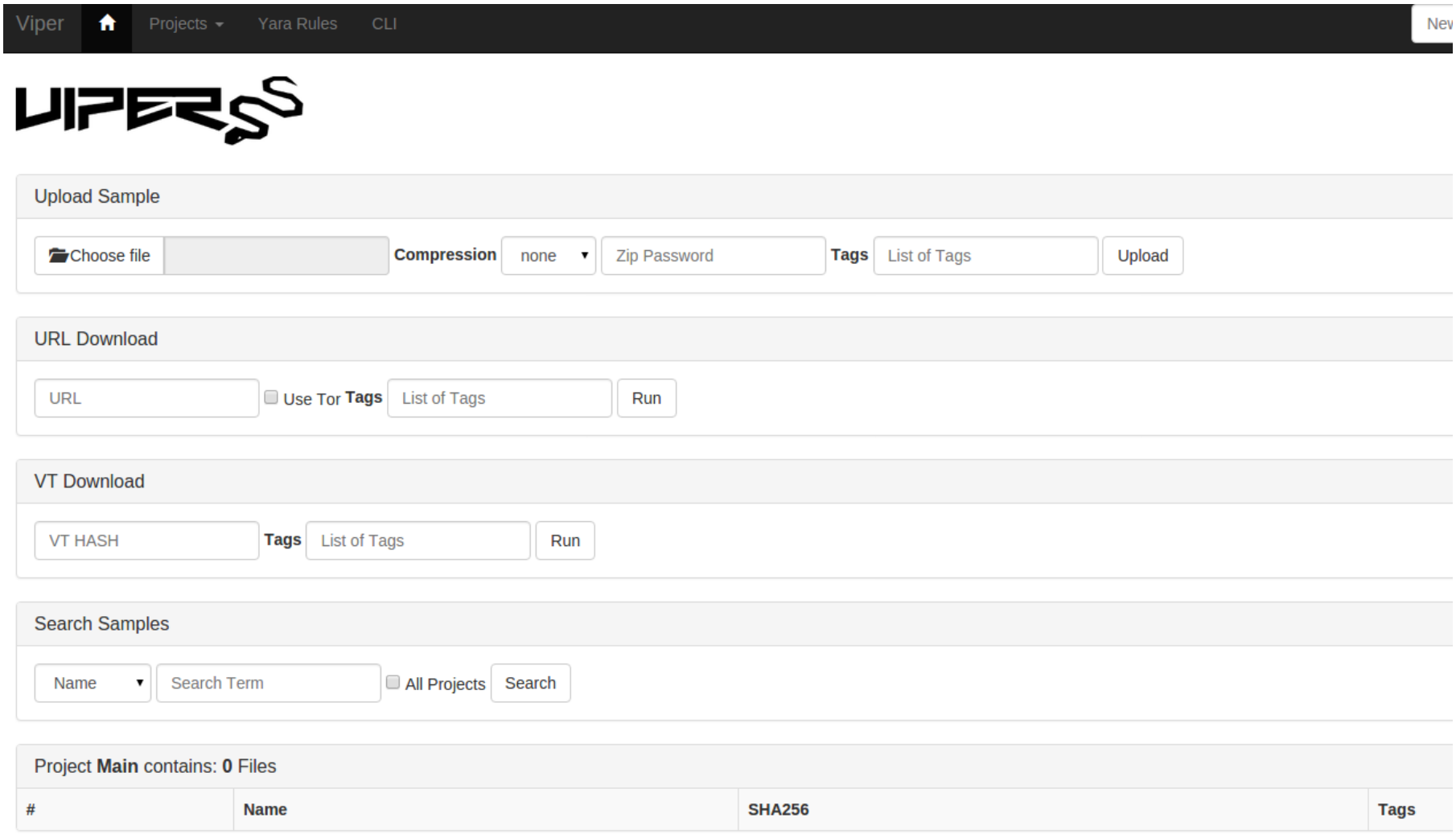
```
00000000: 77f1 0100 0001 0000 0000 0000 0463 726c  w
...........crl
00000010: 3308 6469 6769 6365 7274 0363 6f6d 0000  3
.digicert.com..
00000020: 0100 01                                  .
..
```

▼168.126.63.1:53 → 192.168.56.11:1025

```
00000000: 77f1 8180 0001 0002 000d 000b
 0463 726c  w...........crl
00000010: 3308 6469 6769 6365 7274 0363
 6f6d 0000  3.digicert.com..
```

Quick Overview | Static Analysis | Behavioral Analysis | Network Analysis | Dropped Files | Admin

File name	**C27229390F3F6926292942FB717A1F0F**
File Size	120 bytes
File Type	data
MD5	45a2263b02ff3e8f23c19ffb7d33de1c
SHA1	116b73d856ea5a04a45d51e44b85a9ae6338db15
SHA256	efa3538c629495f550d55efd5878a5e3df0044a6164dc0c107c864e566d27ac8
CRC32	6765AEAD
Ssdeep	3:nklZl0T15/hD8WXdA31y+9lbABYyWSNlPUAlj:nRTv/FAUalkBQS/UAj
Yara	None matched
VirusTotal	Search for analysis
	Download

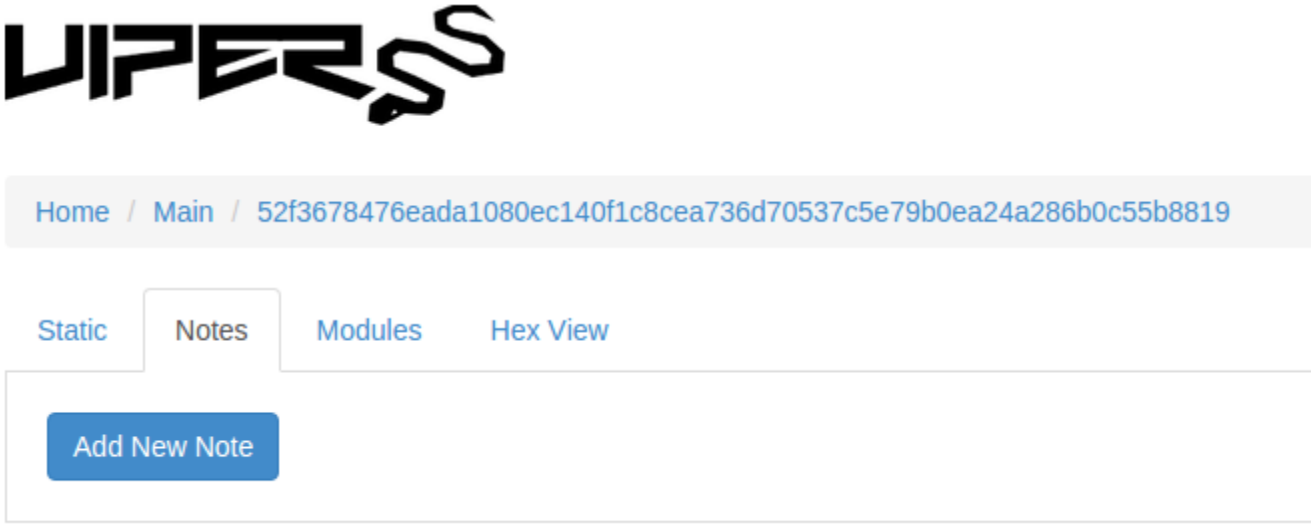

Viper
Projects
Yara Rules
CLI
Upload Sample
Choose file
Compression
none
Zip Password
Tags
List of Tags
Upload
URL Download
URL
Use Tor
Tags
List of Tags
Run
VT Download
VT HASH
Tags
List of Tags
Run
Search Samples
Name
Search Term
All Projects
Search
Project Main contains: 0 Files
#
Name
SHA256
Tags

Home / Main / 52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819

Static | Notes | Modules | Hex View

File Name	arcx.exe
File Size	1246296 bytes
File Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File Mime	application/x-dosexec
MD5	e7ed8c13cbc9ad1afedca0e68d9ffc7b
SHA1	218eccc0ce02332468b89c2ac03ce177f56027fb
SHA256	52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819
SHA512	e525ef9c077c6b7ac328ffd0b6543673e3fe0892a40b57f580f426573380d82249f16c4994d1c72dd30d1b0fd03767868fe78c6aaeddc2c4b0b98580fad7f532
CRC32	FECD27F5
Ssdeep	24576:d7tLYbgis0gvhzfHjfmNxuA8vKqZQnMyy99H51maqvHnod2:JlYboBhfHJA8v9+Myy99H51dqvo0 | Fuzzy Search
	Download Cuckoo

Tags:


Home / Main / 52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819
Static
Notes
Modules
Hex View
Add New Note

Home / Main / 52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819

Static | Notes | Modules | Hex View

Select a module or run a command

Viper Command Module ▾ ▾ Enter CLI Commands Run

Module Output

Home / Main / 52f3678476eada1080ec140f1c8cea736d70537c5e79b0ea24a286b0c55b8819

Static | Notes | Modules | Hex View

Load More

Hex Viewer

```
00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 |MZ..............|
00000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |........@.......|
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
00000030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 |................|
00000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 |........!..L.!Th|
00000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f |is program canno|
00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 |t be run in DOS |
00000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 |mode....$.......|
00000080 50 45 00 00 4c 01 03 00 06 ff d2 54 00 00 00 00 |PE..L......T....|
00000090 00 00 00 00 e0 00 02 01 0b 01 08 00 00 40 11 00 |.............@..|
000000a0 00 90 01 00 00 00 00 00 4e 5a 11 00 00 20 00 00 |........NZ... ..|
000000b0 00 60 11 00 00 00 40 00 00 20 00 00 00 10 00 00 |.`....@.. ......|
000000c0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 |................|
000000d0 00 00 13 00 00 10 00 00 00 00 00 00 02 00 40 85 |..............@.|
000000e0 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 |................|
000000f0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |................|
```


Demo

악성코드 대응

방화벽 차단

- C&C 서버 차단
  - 악성코드와 통신하는 서버의 IP
- DNS 차단
  - 침해 자산에 설정된 DNS 서버가 아닌 악성코드 내에 고정된DNS서버 IP
- URL 차단
  - 악성코드에서 접근하는 URL주소

- 차단 만으로 끝?

- Indicator Of Compromise-침해지표
- 자산의 침해여부를 알 수 있는 흔적

- http://forensicinsight.org/slides

[2013-05-11]
- kevinkoo : [F-INSIGHT] Network Forensics and its Role and Scope
- proneer : [F-INSIGHT] Utilization of IOC, IOAF and SigBase
- proneer : [F-INSIGHT] Trends in dForensics (Apr, 2013)

Question and Answer