The InMAS Approach

- EWNI 2010 -

Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITY OF MANNHEIM

InMAS

- *InMAS* - "Internet Malware Analysis System"
- In cooperation with the German Federal Office for Information Security (BSI)

- Markus Engelberth, Felix C. Freiling, Jan Göbel, Chistian Gorecki, Thorsten Holz, Ralf Hund, Philipp Trinius, Carsten Willems

Motivation

- The Internet is a critical infrastructure
- Failure/attacks occur every day

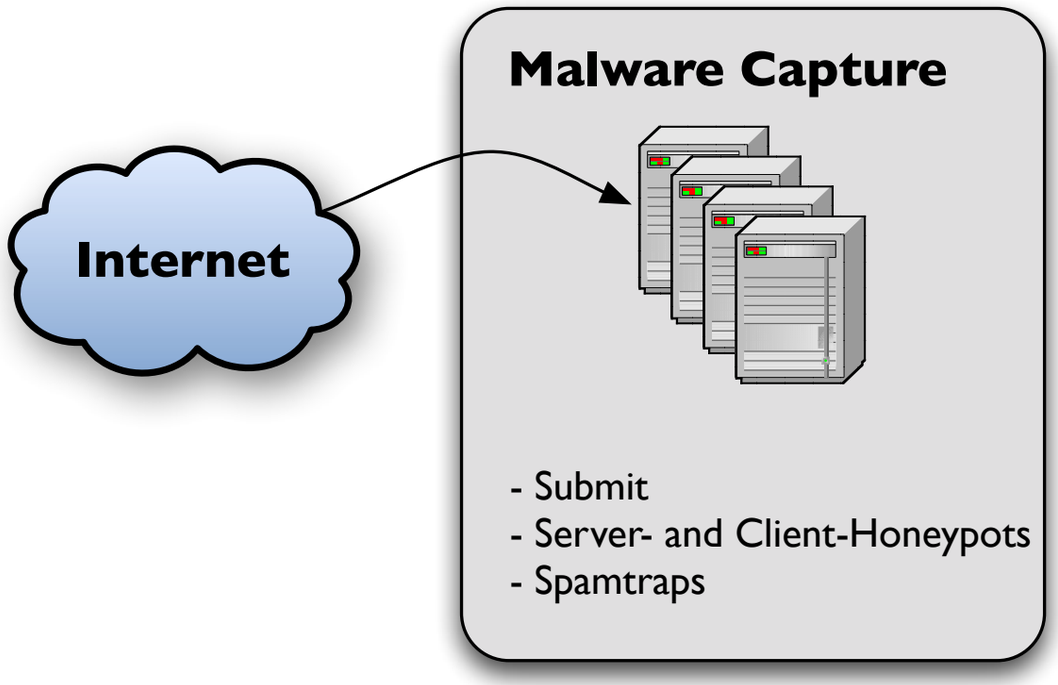
- Early warning systems to anticipate the attacks
  - Detect and classify incidents
  - Analyze attacks and tools involved
  - Perform a suitable reaction

InMAS

- Focus on Malware
  - *“Malware is involved in most attacks.”*
- Modular monitoring and analysis system
  - Distributed and large-scaled system
  - Integration of well known tools
  - Static and dynamic analyses
  - Easy to use and simple to extend

InMAS - platform

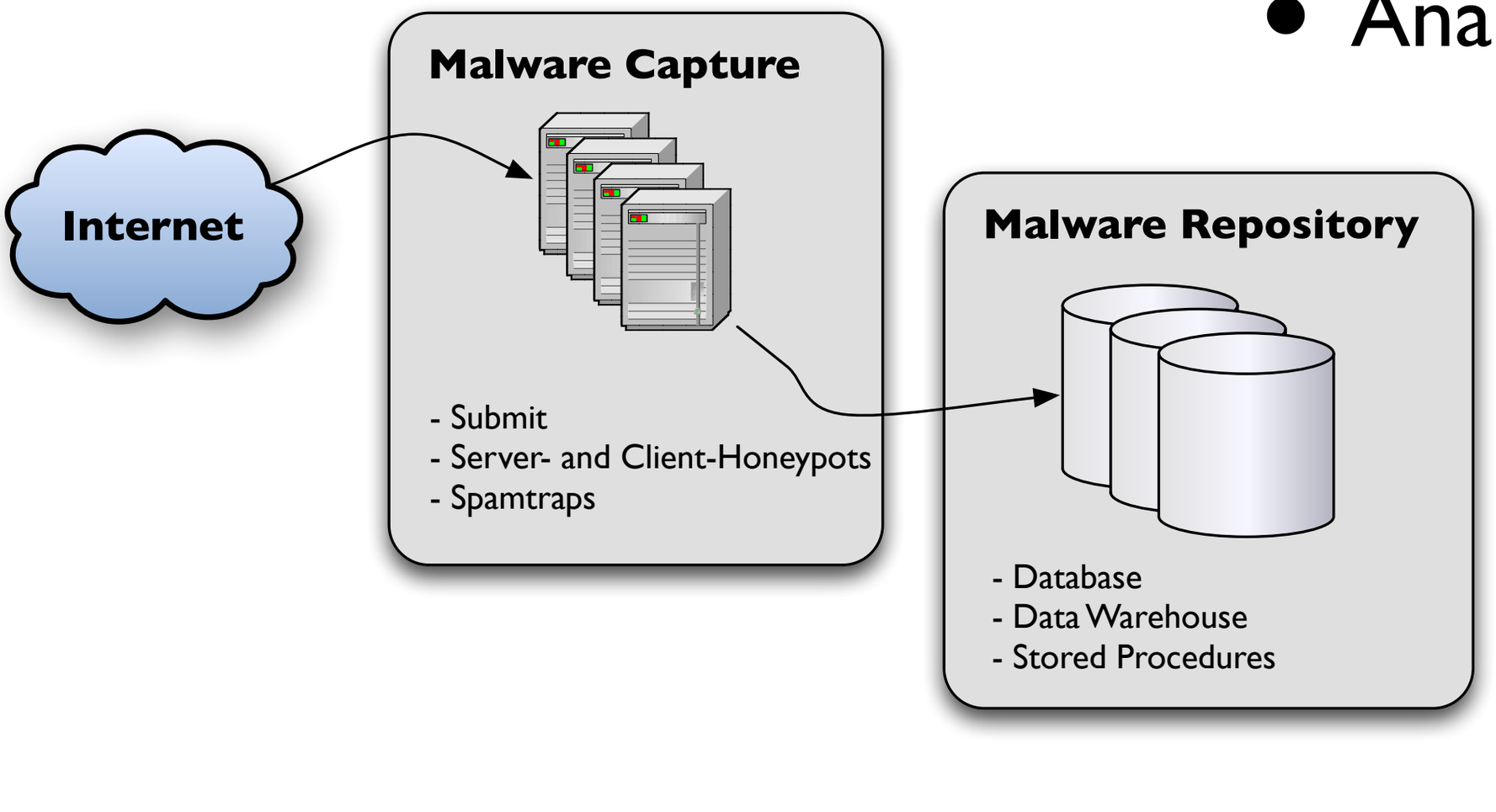
Malware - Capture



- Server honeypots
- Client honeypots
- Spamtraps
- http://cwsandbox.org

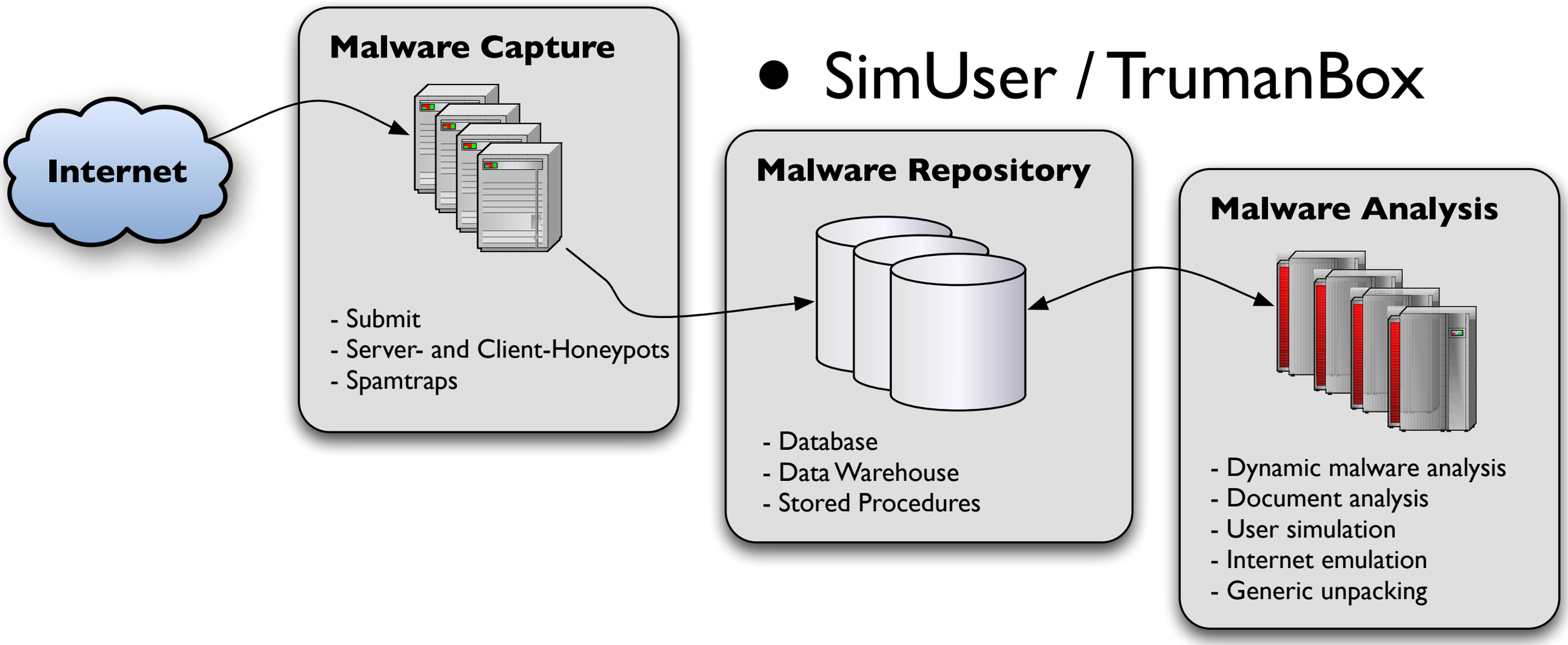
Malware - Repository

- Attack data
- Malware binaries
- Analyses results

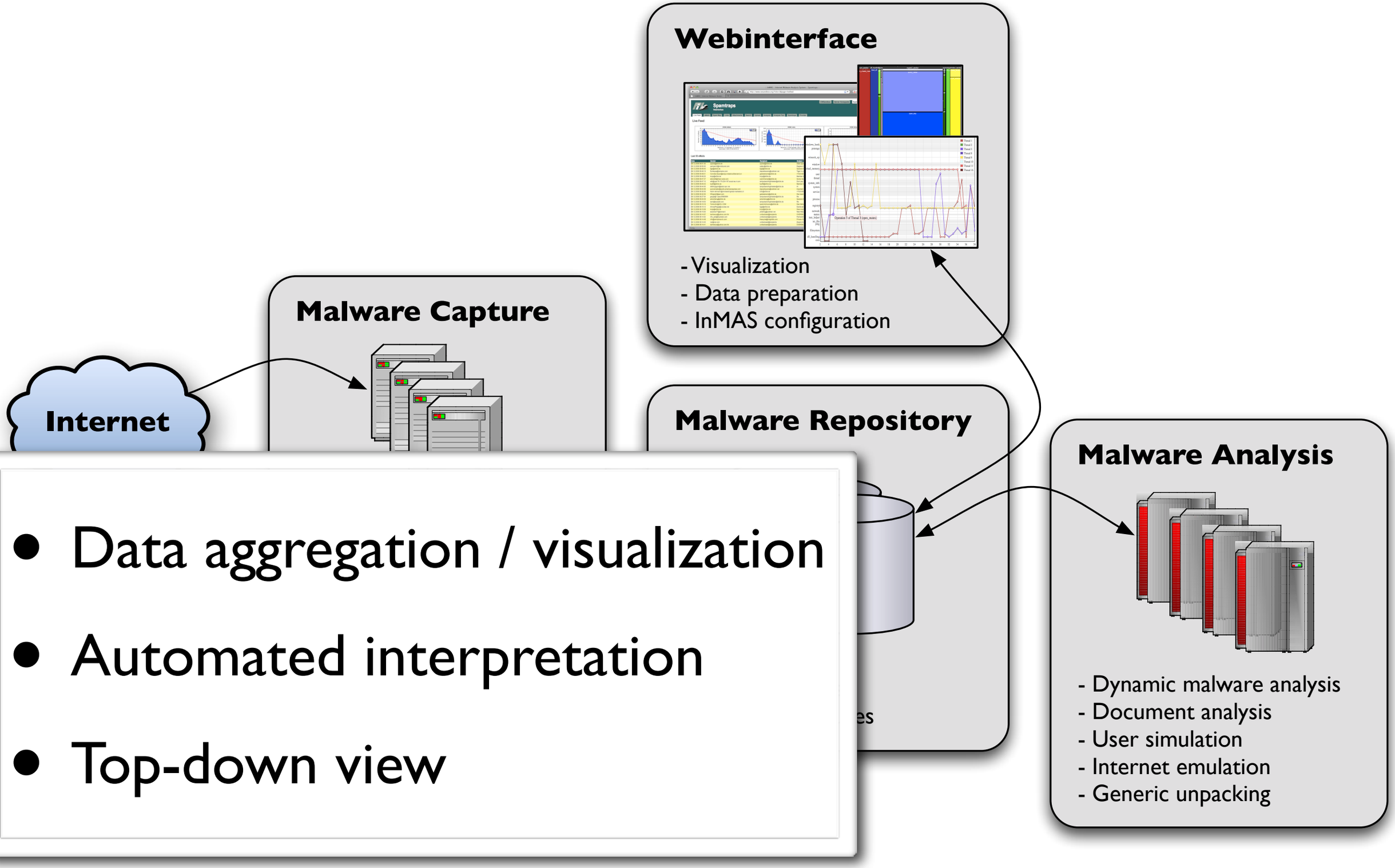


Malware - Analysis

- CWSandbox / MalOffice
- Virustotal / Packerdetection
- Generic Unpacking
- SimUser / TrumanBox



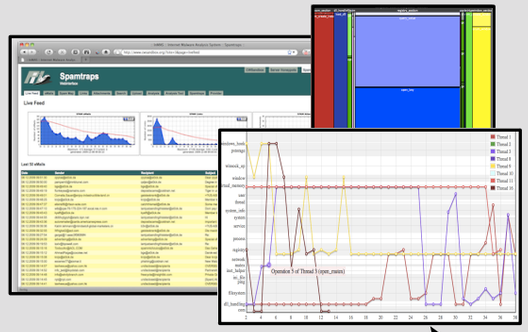
InMAS



- Data aggregation / visualization
- Automated interpretation
- Top-down view

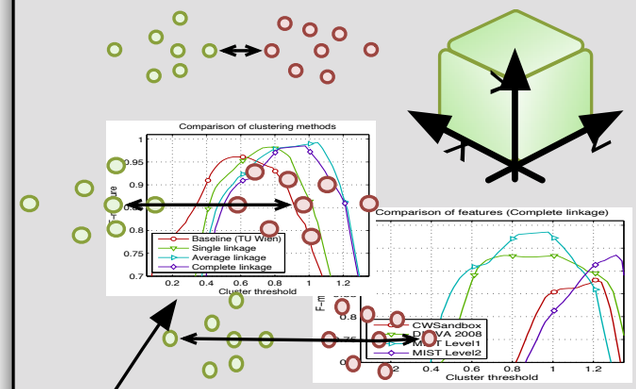
InMAS+

Webinterface



- Visualization
- Data preparation
- InMAS configuration

Malware Clustering



Malware Capture

Internet

Malware Repository

house
cedures

Malware Analysis

- Dynamic malware analysis
- Document analysis
- User simulation
- Internet emulation
- Generic unpacking

- Determine malware families
- Find *new* malware
- Behavior-signature

Webinterface

Server Honeypots
Dashboard

Dashboard:

Severity Statistics:	
High Severity	6020 Events
Medium Severity	5517 Events
Low Severity	307876 Events

Event Statistics:	
Total Events	319413 Total Events
Unique Addresses	3685 Unique Addresses
First Entry	09.06.2009 13:34:07 Entry Time
Last Entry	22.01.2010 12:10:59 Entry Time

Sensor Information:

Sensor	Hostname	Description	Type	Last Event	Event Percentage
1	[redacted]	Fast Flux Rechner (Amun)	Server Honeypot	22.01.2010 12:10:59	100 %

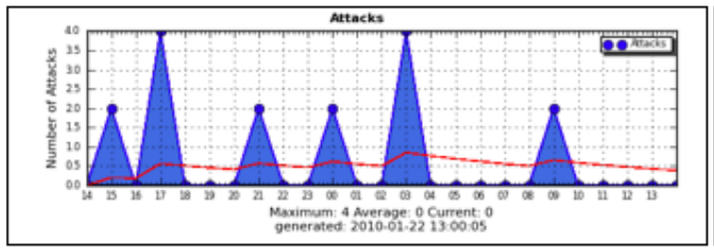
Event Information:

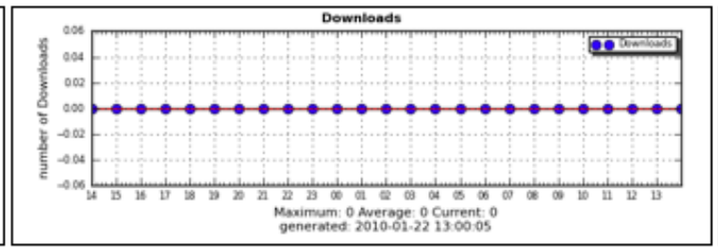
Vulnerability Name:	Vulnerability Count:	Vulnerability Percentage:
DCOM Vulnerability	1430	25.92 %
LSASS Vulnerability	1222	22.15 %
SYMANTEC Vulnerability	1058	19.17 %
PNP Vulnerability	546	9.89 %
NETBIOSNAME Vulnerability	441	7.99 %
LOTUS_DOMINO Vulnerability	182	3.3 %
MSMQ Vulnerability	165	2.99 %
MaxDB Vulnerability	122	2.21 %
MERCURY Vulnerability	106	1.92 %
ARC Vulnerability	44	0.8 %
VERITAS Vulnerability	41	0.74 %
IIS Vulnerability	38	0.69 %
HTTP Vulnerability	31	0.56 %
ASN1 Vulnerability	24	0.43 %
DAMEWARE Vulnerability	21	0.38 %
SASSERFTPD Vulnerability	19	0.34 %
WINS Vulnerability	15	0.27 %
MSDTC Vulnerability	4	0.07 %
MS08067 Vulnerability	4	0.07 %
UPNP Vulnerability	3	0.05 %
NETDDE Vulnerability	1	0.02 %

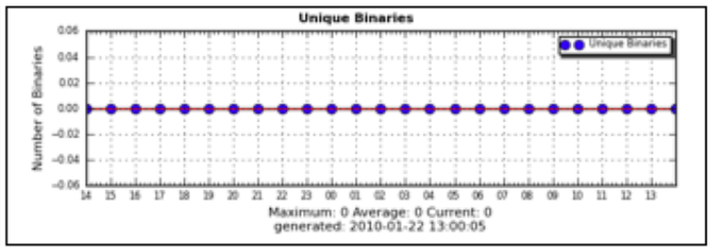
Shellcode Name:	Shellcode Count:	Shellcode Percentage:
None Shellcode	2480	44.95 %
plainurl Shellcode	1231	22.31 %
langenfeld Shellcode	989	17.93 %
plainftp Shellcode	565	10.24 %
adenau Shellcode	100	1.81 %
bielefeld Shellcode	77	1.4 %
wuerzburg Shellcode	37	0.67 %
schauenburg Shellcode	19	0.34 %
rothenburg Shellcode	6	0.11 %
bergheim Shellcode	4	0.07 %
linkbot Shellcode	3	0.05 %
schoenborn Shellcode	2	0.04 %
ulm Shellcode	2	0.04 %
mainz Shellcode	1	0.02 %
leimbach Shellcode	1	0.02 %

:: InMAS :: Internet Malware Analysis System :: Server Honeypots ::

Server Honeypots
Live Feed







Last 20 Downloaded Binaries

Date	Source IP	Destination IP	Event	Details
20.01.2010 17:46:11			Malware Downloaded	>>
20.01.2010 17:20:37			Malware Downloaded	>>
20.01.2010 16:45:59			Malware Downloaded	>>
20.01.2010 16:30:34			Malware Downloaded	>>
20.01.2010 13:35:16			Malware Downloaded	>>
20.01.2010 13:11:22			Malware Downloaded	>>
19.01.2010 23:09:54			Malware Downloaded	>>
19.01.2010 22:52:28			Malware Downloaded	>>
19.01.2010 22:48:16			Malware Downloaded	>>
18.01.2010 22:28:42			Malware Downloaded	>>
18.01.2010 22:12:36			Malware Downloaded	>>
18.01.2010 22:01:43			Malware Downloaded	>>
14.01.2010 09:36:38			Malware Downloaded	>>
14.01.2010 09:09:18			Malware Downloaded	>>
14.01.2010 08:09:04			Malware Downloaded	>>
14.01.2010 07:44:33			Malware Downloaded	>>
14.01.2010 07:09:31			Malware Downloaded	>>
14.01.2010 06:47:04			Malware Downloaded	>>
14.01.2010 06:07:30			Malware Downloaded	>>
14.01.2010 05:08:30			Malware Downloaded	>>

Last 20 Offered Binaries

Date	Source IP	Destination IP	Event	Details
22.01.2010 09:57:16			Malware Offered	>>
22.01.2010 03:48:12			Malware Offered	>>
22.01.2010 03:32:53			Malware Offered	>>
22.01.2010 00:43:32			Malware Offered	>>

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware Analysis System :: Server Honeypots ::

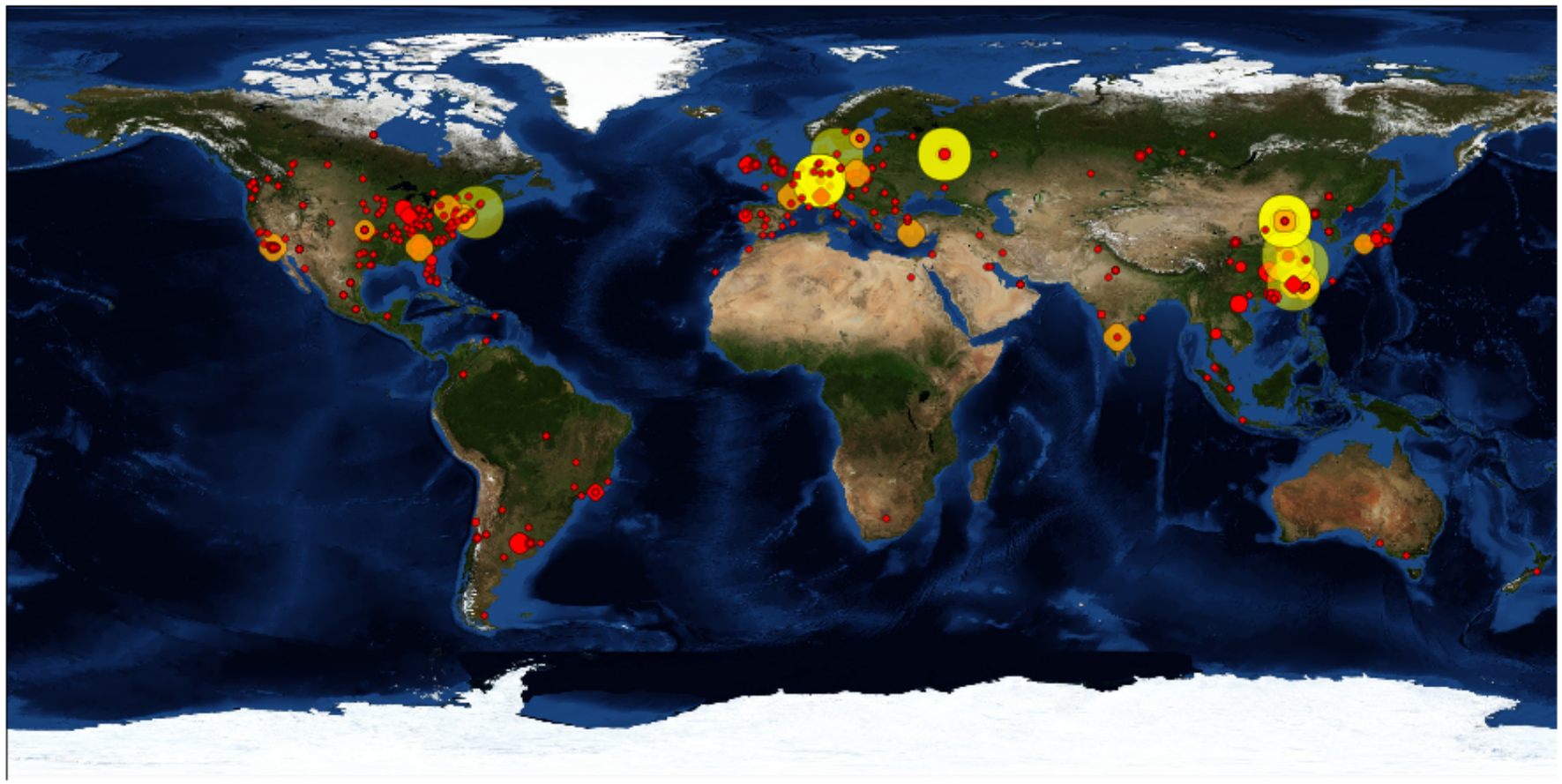
:: InMAS :: Internet Malware Analysis System :: Server Honeypots ::

:: InMAS :: Internet Malware Analysis System :: Server Honeypots ::

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Server Honeypots
Attack Map

Overview | Live Feed | Attacks | Attack Map | Binaries | Search | Analysis | Analysis Tool | Metric | Sensors



page generated in 0.01s, sql time 0.01s :: Lehrstuhl für Praktische Informatik 1, University of Mannheim

:: InMAS :: Internet Malware Analysis System :: Server Honeypots ::

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Server Honeypots
Analysis Tool

Overview | Live Feed | Attacks | Attack Map | Binaries | Search | Analysis | Analysis Tool | Metric | Sensors

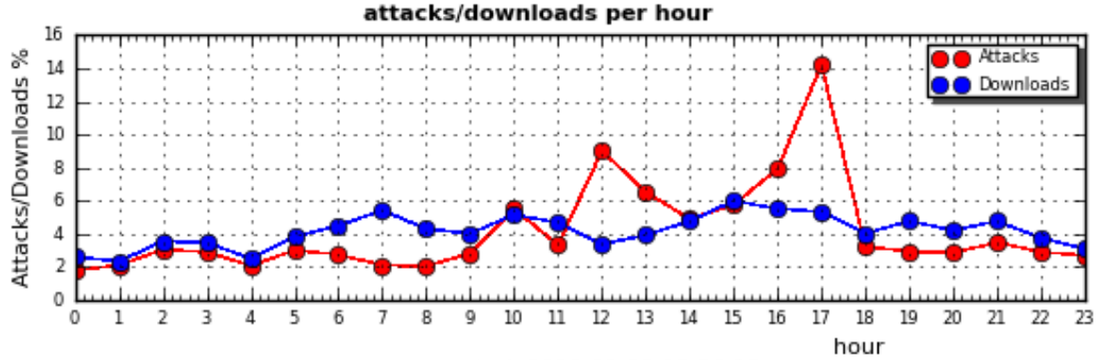
Active analysis: Attacks/Downloads per hour

Period: 2009-06-09 bis 2010-01-22

Sensor: All

Apply

attacks/downloads per hour



generated: 2010-01-22 13:26:15

This plot shows the percentage of attacks and downloads per daytime over the chosen period of time.

Client Honeypots
Dashboard

Dashboard:

Result Statistics:	
Malicious Websites	322 Websites
Benign Websites	6312 Websites
Faulty Websites	11545 Websites

Website Statistics:	
Total Websites	18179 Total Websites
Unique Addresses	7351 Unique Addresses
First Entry	21.09.2009 21:26:05 Entry Time
Last Entry	20.01.2010 17:59:47 Entry Time

Sensor Information:

Sensor	OS	VMX Path	Status	Last Event	Event Percentage
16	XP SP2	[standard] capture-ng-xp/capture-ng-xp.vmx	disabled	10.12.2009 11:26:17	19.29 %
18	XP SP2	[standard] capture-ng-xp/capture-ng-xp.vmx	disabled	22.12.2009 16:59:43	22.41 %
20	XP SP2	/home/sqrts/vmware/capture-winclient-1/capture-winclient.vmx	disabled	22.12.2009 17:00:38	21.51 %
22	XP SP2	[test] capture-ng-xp/capture-ng-xp.vmx	disabled	24.11.2009 14:50:26	4.22 %
23	XP SP2	/home/sqrts/vmware/capture-ng-xp-vm_version1/capture-ng-xp/capture-ng-xp.vmx	disabled	20.01.2010 18:02:20	32.57 %

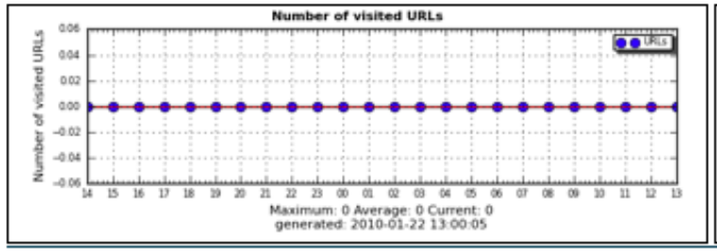
Event Information:

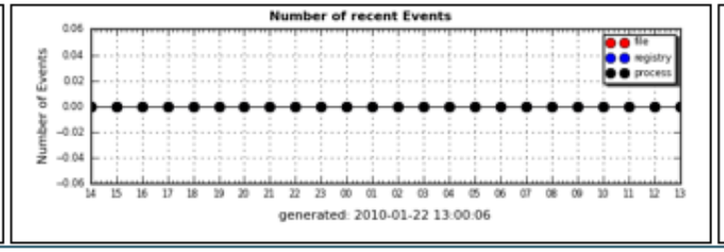
Action Name:	Action Count:	Action Percentage:
SetValueKey Action	44805	38.47 %
Write Action	26505	22.76 %
udp-connection Action	24045	20.64 %
Delete Action	13573	11.65 %
DeleteValueKey Action	4882	4.19 %
tcp-connection Action	1640	1.41 %
tcp-listening Action	538	0.46 %
created Action	400	0.34 %
terminated Action	87	0.07 %

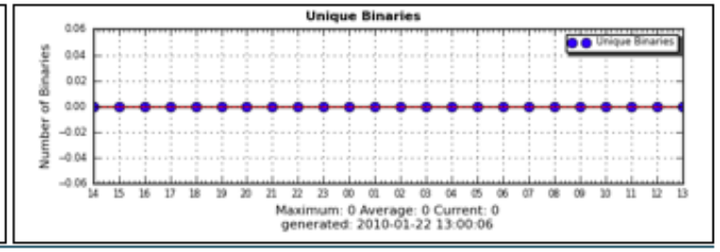
Event Name:	Event Count:	Event Percentage:
registry Event	49687	42.66 %
file Event	40078	34.41 %
connection Event	26223	22.51 %
process Event	487	0.42 %

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

Client Honeypots
Live Feed







Last 20 Malicious Websites

Last Visit	URL	Status	Import	Details
20.01.2010 18:02:20	http://cismosis.com/counter3.php	malicious	20.01.2010 17:59:47	>>
20.01.2010 18:01:20	http://cismosis.com/counter2.php	malicious	20.01.2010 17:59:42	>>
20.01.2010 18:00:03	http://cismosis.com/counter.php	malicious	20.01.2010 17:59:39	>>
20.01.2010 17:59:08	http://cismosis.com/in5.php	malicious	20.01.2010 17:57:17	>>
20.01.2010 17:58:12	http://cismosis.com/in4.php	malicious	20.01.2010 17:57:13	>>
20.01.2010 17:57:16	http://cismosis.com/in3.php	malicious	20.01.2010 17:57:03	>>
20.01.2010 17:51:32	http://cismosis.com/in2.php	malicious	20.01.2010 17:47:53	>>
20.01.2010 17:50:39	http://cismosis.com/in6.php	malicious	20.01.2010 17:47:24	>>
20.01.2010 17:49:27	http://cismosis.com/in8.php	malicious	20.01.2010 17:47:14	>>
20.01.2010 17:48:23	http://cismosis.com/in7.php	malicious	20.01.2010 17:47:01	>>
20.01.2010 17:47:29	http://cismosis.com/in9.php	malicious	20.01.2010 17:29:56	>>
22.12.2009 16:27:11	http://www.precisionplus.com/catalog/images/b	malicious	22.12.2009 14:47:38	>>
22.12.2009 12:46:14	http://24hourhiphop.com/hip+hop+Next%20In%20L	malicious	10.12.2009 22:38:30	>>
11.12.2009 14:12:50	http://www.adsnews.net/slovenias-coach-matjaz	malicious	10.12.2009 22:37:23	>>
11.12.2009 13:59:42	http://www.keegy.com/post/times-square-shooti	malicious	10.12.2009 22:37:15	>>
11.12.2009 13:38:04	http://topsy.com/twitter/gottafindjoe	malicious	10.12.2009 22:36:54	>>
11.12.2009 13:15:09	http://topsy.com/tb/twitpic.com/svioo	malicious	10.12.2009 22:36:45	>>
11.12.2009 11:51:04	http://thisismajikclick.com/site/http:/thisis	malicious	10.12.2009 22:35:35	>>
11.12.2009 10:55:15	http://www.foxnews.com/politics/2009/03/11/ob	malicious	10.12.2009 22:34:34	>>
11.12.2009 10:30:34	http://frwebgate.access.gpo.gov/cgi-bin/getdo	malicious	10.12.2009 22:34:18	>>

Last 20 Benign Websites

Last Visit	URL	Status	Import	Details
20.01.2010 17:46:33	http://twitter.com/	benign	19.01.2010 14:08:53	>>
22.12.2009 16:59:43	http://www.hottestnews.org/topic.php?term=bri	benign	22.12.2009 14:48:14	>>
22.12.2009 16:58:28	http://despardes.com/?p=11165	benign	22.12.2009 14:48:13	>>
22.12.2009 16:57:31	http://www.leapfish.com/news.aspx?q=Britney+M	benign	22.12.2009 14:48:12	>>

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

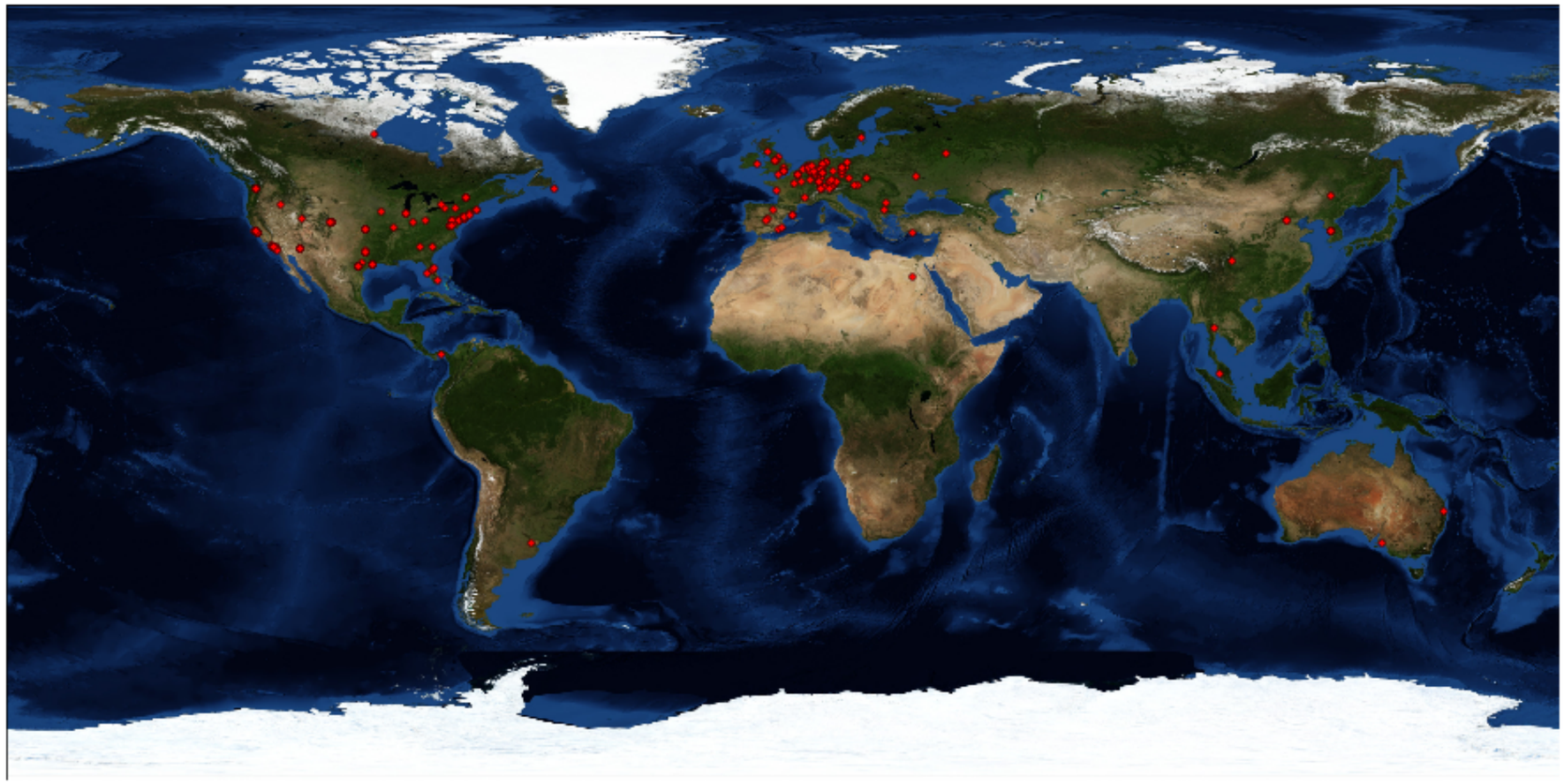
:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

Client Honeypots
URL Map

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Overview | Live Feed | Url | Url Queue | Upload | Url Map | Binaries | Search | Analysis | Analysis Tool | Sensors | Server | Exclude List | Client Handler



page generated in 0.01s, sql time 0.01s :: Lehrstuhl für Praktische Informatik 1, University of Mannheim

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

:: InMAS :: Internet Malware Analysis System :: Client Honeypots ::

Client Honeypots

CaptureHPC Exclude List

Registry Monitor

Type	Event	Process	Path	Section	Active		
+	DeleteValueKey	C:\\Program Files\\VMware\\VMware Tools\\VMwareService.exe	HKLM\\SYSTEM\\ControlSet001\\Services\\PerfDisk\\Performance\\Error Count	1	True	Disable	Delete
+	SetValueKey	C:\\WINDOWS\\system32\\svchost.exe	.*	1	True	Disable	Delete
+	DeleteValueKey	C:\\Program Files\\VMware\\VMware Tools\\VMwareService.exe	HKLM\\SYSTEM\\ControlSet001\\Services\\PerfProc\\Performance\\Error Count	1	True	Disable	Delete
+	DeleteValueKey	C:\\Program Files\\VMware\\VMware Tools\\VMwareService.exe	HKLM\\SYSTEM\\ControlSet001\\Services\\PerfOS\\Performance\\Error Count	1	True	Disable	Delete
+	DeleteValueKey	System	HKLM\\SYSTEM\\ControlSet001\\Services\\CaptureConnectionMonitor\\.*	1	True	Disable	Delete
+	SetValueKey	System	HKLM\\SYSTEM\\ControlSet001\\Services\\CaptureConnectionMonitor\\.*	1	True	Disable	Delete
+	SetValueKey	System	HKLM\\SYSTEM\\ControlSet001\\Enum\\Root\\LEGACY_CAPTUREFILEMONITOR\\.*	1	True	Disable	Delete
+	DeleteValueKey	System	HKLM\\SYSTEM\\ControlSet001\\Enum\\Root\\LEGACY_CAPTURECONNECTIONMONITOR\\.*	1	True	Disable	Delete
+	SetValueKey	C:\\Program Files\\Adobe\\Reader 8.0\\Reader\\AcroRd32.exe	.*	1	True	Disable	Delete
+	SetValueKey	C:\\Program Files\\Real\\RealPlayer\\realplay.exe	.*	1	True	Disable	Delete
+	SetValueKey	C:\\Program Files\\Internet Explorer\\iexplore.exe	.*	1	True	Disable	Delete
+	DeleteValueKey	C:\\Program Files\\Internet Explorer\\iexplore.exe	.*	1	True	Disable	Delete
+	SetValueKey	C:\\WINDOWS\\system32\\lsass.exe	HKLM\\SAM\\SAM\\Domains\\Account\\Users\\.*	1	True	Disable	Delete
+	SetValueKey	C:\\Program Files\\AOL\\AOL Toolbar 5.0\\AolTbServer.exe	.*	1	True	Disable	Delete

Add Registry Rule

Type	Event	Process	Path	Section	
+	OpenKey			Clean Windows XP SP2 System	Add Rule

Filesystem Monitor

Type	Operation	Process	Path	Section	Active		
+	Delete	C:\\WINDOWS\\system32\\wbem\\wmiadap.exe	.*	1	True	Disable	Delete

Spamtraps
Dashboard

Dashboard:

eMail Statistics:	
Attachments	4417 Attachments
Links	6982782 Links

General Statistics:	
Total eMails	304477 Total eMails
Recipient Addresses	304477 Recipient Addresses
Sender Addresses	304478 Sender Addresses
First Entry	02.07.2009 14:53:33 Entry Time
Last Entry	22.01.2010 13:07:52 Entry Time

Sensor Information:

Sensor	Provider	Mail Address	Status	Last Event	Event Percentage
1	Core Networks		active	22.01.2010 13:07:52	82.58%
7	GMX		active	22.01.2010 08:36:31	0.03%
9	GMX		active	22.01.2010 03:51:57	0.02%
10	GMX		active	22.01.2010 08:14:20	0.03%
4	GMX		active	22.01.2010 08:37:11	0.03%
8	Web.de		active	22.01.2010 11:19:08	0.28%
11	Catchall Link		active	22.01.2010 12:46:51	11.98%
12	Spamtrap Link		active	22.01.2010 07:48:21	0.11%
14	Upload		active	10.11.2009 09:30:59	0.08%

Event Information:

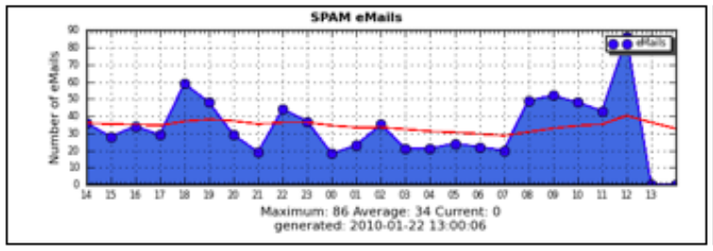
Mime-Type Name:	Mime-Type Count:	Mime-Type Percentage:
image/jpeg Mime-Type	3684 %	83.41
application/zip Mime-Type	310	7.02 %
image/gif Mime-Type	194	4.39 %
text/html Mime-Type	66	1.49 %
text/plain Mime-Type	47	1.06 %
application/msword Mime-Type	39	0.88 %

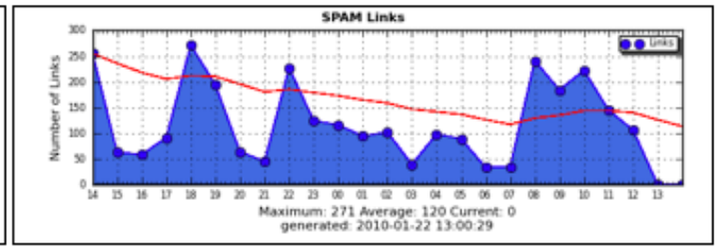
SA Score:	SA Count:	SA Percentage:
<10 SA Score	87553	28.76 %
>20 SA Score	76420	25.1 %
<20 SA Score	63899	20.99 %
<15 SA Score	49979	16.41 %
<5 SA Score	26626	8.74 %

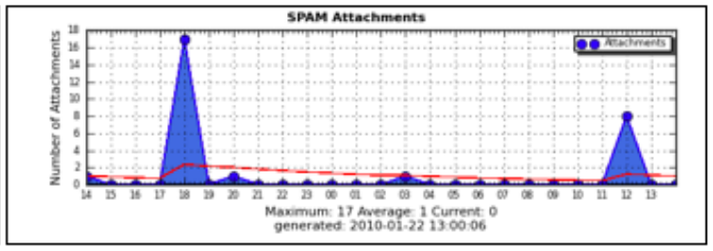
:: InMAS :: Internet Malware Analysis System :: Spamtraps ::

:: InMAS :: Internet Malware Analysis System :: Spamtraps ::

Spamtraps
Live Feed







Last 50 eMails

Date	Sender	Recipient	Subject	SA Score	Details
22.01.2010 13:07:52			You will be satisfied with all those envy eyes staring at you. Feel yourself freely and self-confident in any society.	13	>>
22.01.2010 13:07:44			Special 80% discount for customer spammichzuicq on all Pfizer	21.1	>>
22.01.2010 13:02:36			RE: UK MensHealth Discount ID510071	29.1	>>
22.01.2010 13:02:28			Frohe Weihnachten!	18.7	>>
22.01.2010 12:57:16			Hi remember me?	12	>>
22.01.2010 12:52:16			Bestellen Sie Software, Aber Nur Legal	15.8	>>
22.01.2010 12:52:09			The latest fashion and prices	25.5	>>
22.01.2010 12:52:00			Special 80% discount for customer qzkn on all Pfizer	23.3	>>
22.01.2010 12:46:59			Shopping Guru tips	25.5	>>
22.01.2010 12:46:51			Special 80% discount for customer qsljev on all Pfizer	33	>>
22.01.2010 12:46:44			Turbo' mode for your rod	13.8	>>
22.01.2010 12:41:35			You need more blood to make your penis bigger?	26.3	>>
22.01.2010 12:41:31			Meet her carnal needs	16.5	>>
22.01.2010 12:41:22			Special 80% discount for customer petgord34truew on all Pfizer	30.7	>>
22.01.2010 12:39:28			Plaetze frei	17.6	>>
22.01.2010 12:36:08			Drill her regardless of your age	8.7	>>
22.01.2010 12:36:03			=?iso-8859-1?Q?1_Stunde=2C_um_soviel_Geld_wie_m=F6glich_zu_gewinnen?=	15.7	>>
22.01.2010 12:30:58			Your Submariner SS watch will overshadow all the other watches. Your wrist was made for the diamonds.	14.1	>>
22.01.2010 12:30:50			=?iso-8859-1?Q?1_Stunde=2C_um_soviel_Geld_wie_m=F6glich_zu_gewinnen?=	15.7	>>
22.01.2010 12:25:44			Nur ein Klick und Ihrem Konto wird gutgeschrieben.	19.5	>>
22.01.2010 12:25:39			Nur ein Klick und Ihrem Konto wird gutgeschrieben.	15.7	>>
22.01.2010 12:25:18			B uy watch online	19.5	>>
22.01.2010 12:23:36			Fwd: Beneficiary	6.6	>>
22.01.2010 12:20:40			Diese Seite ist genial.	15.7	>>
22.01.2010 12:20:36			=?iso-8859-1?Q?Ihnen_wurde_eine_Goldm=FCnze_gutgeschrieben?=	15.7	>>
22.01.2010 12:20:30			=?iso-8859-1?Q?Spielen_Sie_jetzt_und_machen_Sie_einen_gro=DFen_Gewinn!?=	18.8	>>

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware Analysis System :: Spamtraps ::

:: InMAS :: Internet Malware Analysis System :: Spamtraps ::

:: InMAS :: Internet Malware Analysis System :: Spamtraps ::

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Spamtraps
Analysis Tool

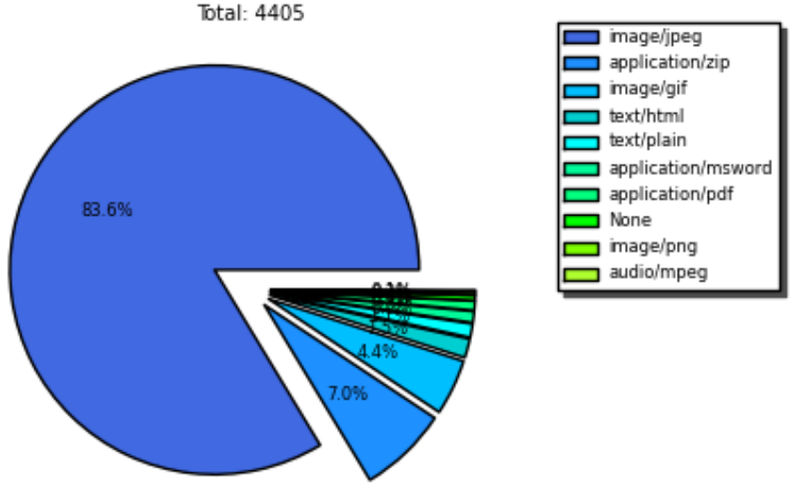
Overview | Live Feed | eMails | Spam Map | Links | Attachments | Search | Upload | Analysis | Analysis Tool | Spamtraps | Provider

Active analysis: Top Mime Types

Period: 2009-07-02 bis 2010-01-22

Apply

Top 10 Mime Types

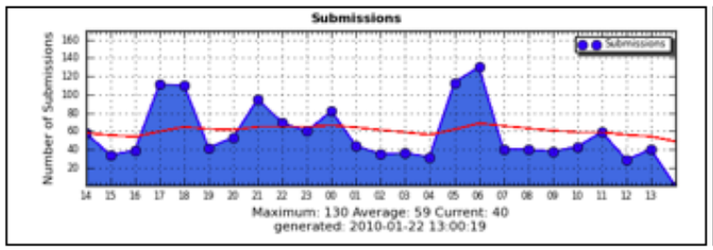


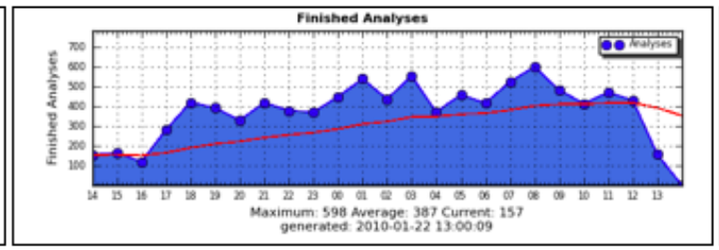
This plot shows the most found mime types on attachments

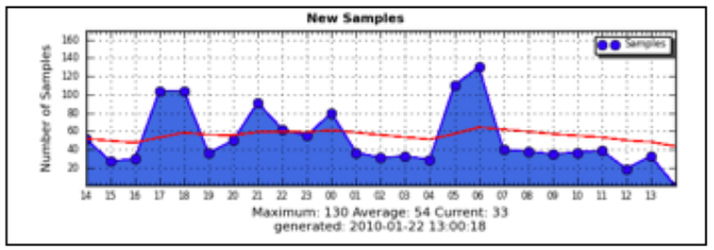
page generated in 0.02s, sql time 0.01s :: Lehrstuhl für Praktische Informatik 1, University of Mannheim

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

CWSandbox
Live Feed







The view may be filtered by clicking on the IP address, the e-mail address or the filesize

Date	Uploader IP	Uploader E-Mail	Sample	MD5	Size	Tag	Details
22.01.2010 13:44:39			1101592	52173bd84926cc066a2609f5ad137625	142848	autosubmit	>>
22.01.2010 13:44:33			1101591	bc9122a9d1d76d82f25094af3e9f5732	142848	autosubmit	>>
22.01.2010 13:44:05			1101590	c58d890e06fa056adc852bdbb0570272	142848	autosubmit	>>
22.01.2010 13:42:49			1101589	e95b79477adc6cdb346d7082a70274d9	142848	autosubmit	>>
22.01.2010 13:42:41			1101588	730e719b8f0ac455c5bc8fea52732f5f	142848	autosubmit	>>
22.01.2010 13:38:51			1860	e269d0462eb2b0b70d5e64dcd7c676cd	154624	default	>>
22.01.2010 13:38:51			1860	e269d0462eb2b0b70d5e64dcd7c676cd	154624	autosubmit	>>
22.01.2010 13:38:27			270	1f8a826b2ae94daa78f6542ad4ef173b	155648	default	>>
22.01.2010 13:38:27			270	1f8a826b2ae94daa78f6542ad4ef173b	155648	autosubmit	>>
22.01.2010 13:38:25			1101587	05015e7027ea37870cebe15c0a63efcf	142848	autosubmit	>>
22.01.2010 13:37:12			1101586	5637de4978fd401765eee4bafd177c88	134320	autosubmit	>>
22.01.2010 13:36:37			1101585	3cda29e279728eb48960d1d0f0c9cfa1	142848	autosubmit	>>
22.01.2010 13:36:23			1099720	524fa2b8bb070816efecc2c6fa52f446	131072	autosubmit	>>
22.01.2010 13:36:15			1101584	a66d6b37b5d94037a107c66e68428a56	131072	autosubmit	>>
22.01.2010 13:35:59			1101583	cc0538cf565bac08b838f4362eedd5e1	142848	autosubmit	>>
22.01.2010 13:35:23			1101581	f05ff61a331b9e6b4ddd201414acc0c7	142848	autosubmit	>>
22.01.2010 13:35:23			1101582	3264cd024fb976d986a5abed7b80ecaa	142848	autosubmit	>>
22.01.2010 13:35:11			1101580	e9c284847afe22305a03d0afeb0d62ea	142848	autosubmit	>>
22.01.2010 13:34:37			1101579	7c73fd67267a6c187319073041c7d40f	142848	autosubmit	>>
22.01.2010 13:34:37			1101578	56f59c7ae223641ec7aff16fd145ea39	440320	default	>>
22.01.2010 13:31:45			1101577	93b47a8f56f144efd04127e7190a5b91	142848	autosubmit	>>
22.01.2010 13:30:37			1101576	74c047d98c35ac4d90ff9e76d392b8be	142848	autosubmit	>>
22.01.2010 13:21:09			1101575	d62e9fa40a467a86db57ee8321c5d70d	142848	autosubmit	>>
22.01.2010 13:18:56			1095104	7f25f9de92f1204da399aaa30c8059cd	130048	autosubmit	>>
22.01.2010 13:17:05			1101574	8c3e3591d36b66dde647c3cc3c0fd529	142848	autosubmit	>>
22.01.2010 13:12:45			802655	3aff8601a8a6fc1dccb836ae3e971e3e	158967	autosubmit	>>
22.01.2010 13:12:06			17388	f8815cdca238ad5ab566f05f5a6335a4	162816	default	>>
22.01.2010 13:12:06			17388	f8815cdca238ad5ab566f05f5a6335a4	162816	autosubmit	>>

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

CWSandbox
Sample Details

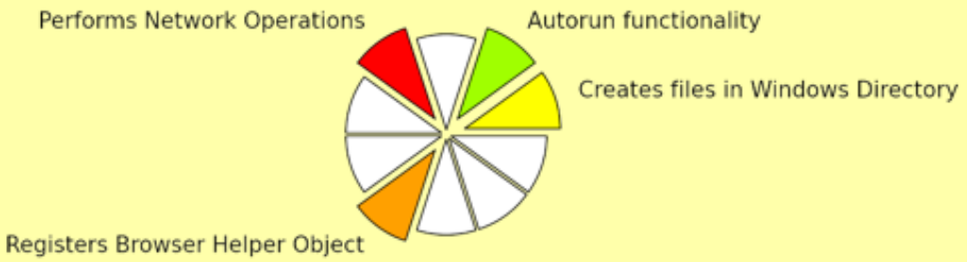
CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Live Feed | Malware Browser | Search | Clustering | Submit | Sandbox Status

General Information

Filename	76aaa3b03a183fe8a8cb9978e54fb49c (download file [analyze with Ether])
Filesize	954135
MD5 hash	76aaa3b03a183fe8a8cb9978e54fb49c
SHA1 hash	ef598c7ed01b708bdfccd5af0e8330d780164c3c
MIME Type	application/x-dosexec
Tags	autosubmit
Priority	**0** 1 2 3 4 5 6 7 8 9 10

Summary of sample execution (AnalysisID: 2599175)



Clustering/Classification (AnalysisID: 2599175)

Cluster	C001-0010
Date	21.01.2010
Prototype	2417161
Distance	

Analyses of this sample

analyzer	start	end	
CWSandbox 2.1.22	21.01.2010 13:33:45	21.01.2010 13:37:15	2599175 (PCAP / CAB (browse))
VirusTotal Scan 1.0.0	18.12.2009 07:47:22	18.12.2009 07:47:22	1898810
re-analyze			

Submissions

date	submitter	filename	comment
18.11.2009 17:41:34		76aaa3b03a183fe8a8cb9978e54fb49c	

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware A

:: InMAS :: Internet Malv

load_image load_dll open_file **open_key**
query_value find_file create_process
check_for_debugger get_system_directory create_mutex
set_windows_hook create_window create_thread vm_protect
download_file kill_process **enum_window** winsock_section
connections_unknown connection plain_communication_data recv
dump_line send gethostbyname connections_udp
recv_datagram open_mutex get_computer_name impersonate_user
get_file_attributes open_scmanager create_open_file open_service
enum_values connections_outgoing http_data http_cmd header_data
header stored_created_files_section stored_created_file
com_create_instance enum_keys sleep open_process
set_value create_key get_username delete_key
find_winc
read_value get_system
resulting_addr downlc
create_file create_serv

Distance

Analyses of this sample

analyzer

CWSandbox 2.1.22

VirusTotal Scan 1.0.0

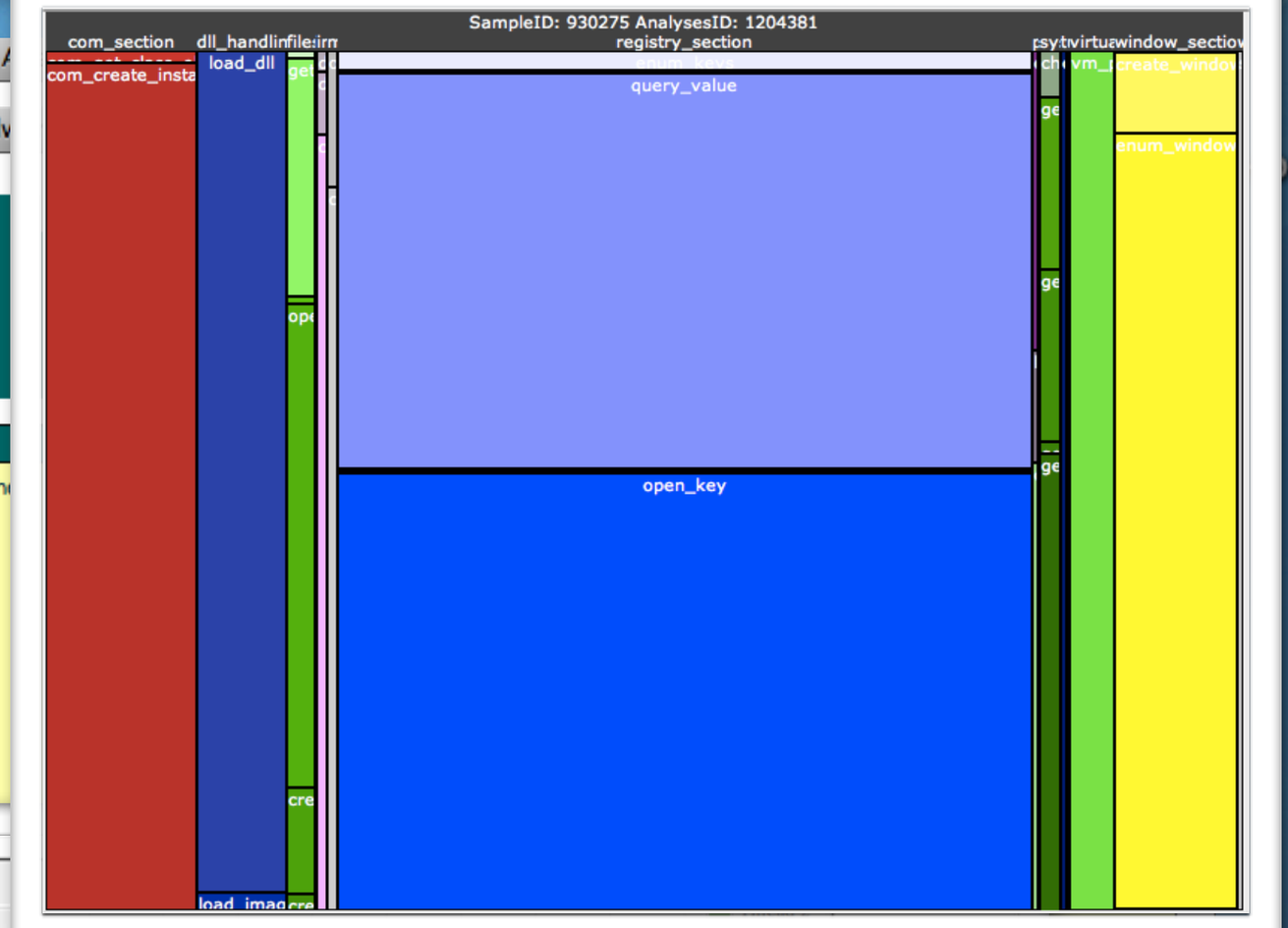
re-analyze

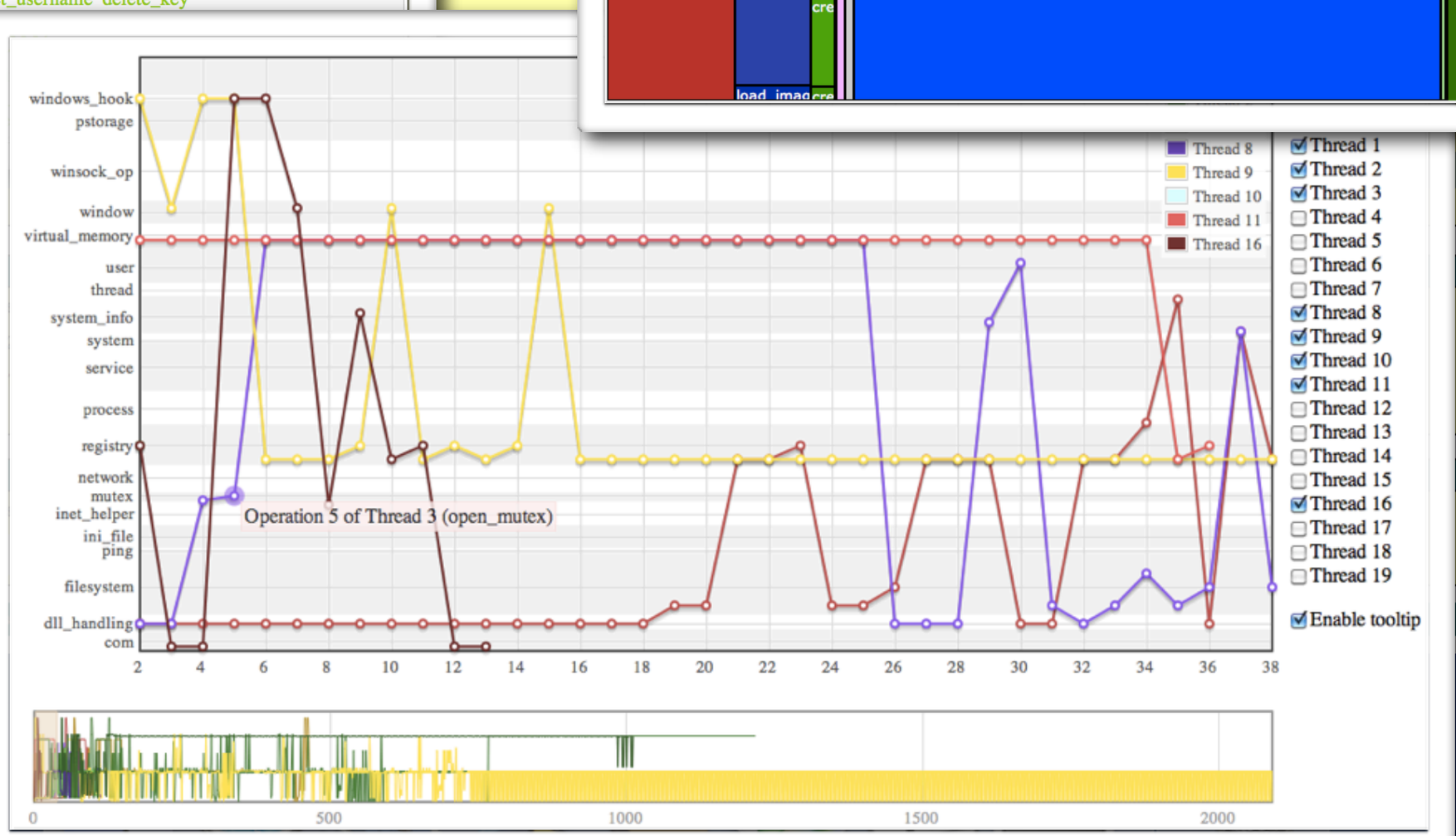
Submissions

date

18.11.2009 17:41:34

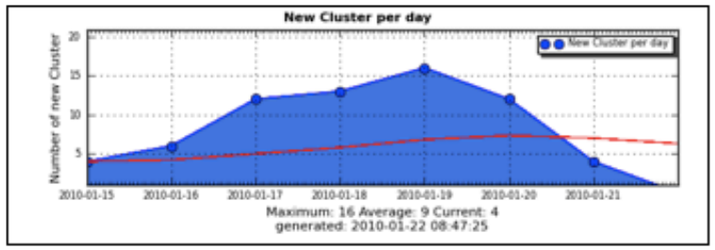
page generated in 0.44s, sql time 0.

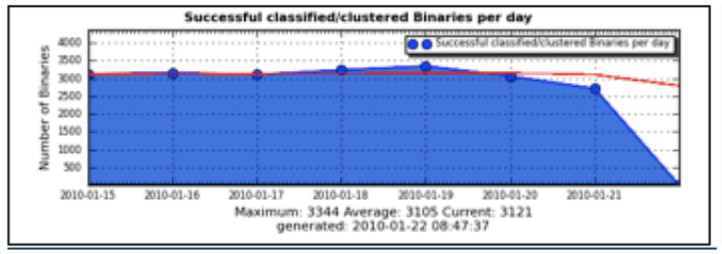


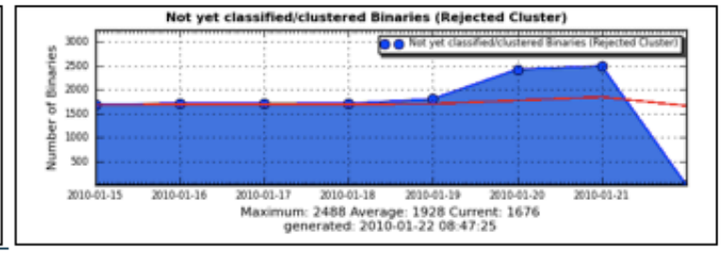


:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

CWSandbox
Clustering







Periode	Clusterruns	# Cluster	Clustered Samples	Rejected Samples	Avg Sample per Cluster	Avg Prototypes per Cluster	Min/Max Distance	Avg Distance	Avg Median	Avg Std Deviation
06.12.2009 - 21.01.2010	47	402	139664	2668	341	5	0/0.679985	0.336741	0.397853	0.193544

Directly jump to cluster run:

1 go

Cluser	Run (Date)	# Analyses	# Prototypes	Min Distance	Max Distance	Average Distance	Median	Std Deviation	Density	Details
C001-0001	1 (01.01.2010)	11606	1	0	0.000366211	0.0003645	0.000366211	4.08826e-06	0.00108243	>>
C001-0006	1 (01.01.2010)	36049	6	0	0.556843	0.418642	0.494156	0.129087	1.24322	>>
C001-0007	1 (01.01.2010)	1078	2	0	0.62158	0.290316	0.165952	0.200925	0.862134	>>
C001-0010	1 (01.01.2010)	4941	6	0	0.679718	0.328648	0.321905	0.127628	0.975968	>>
C001-0016	1 (01.01.2010)	844	4	0	0.672435	0.428953	0.486178	0.162387	1.27384	>>
C001-0017	1 (01.01.2010)	523	1	0	0.605704	0.458069	0.515308	0.0937636	1.3603	>>
C001-0020	1 (01.01.2010)	8983	3	0	0.206281	0.132347	0.131217	0.00628713	0.393024	>>
C001-0021	1 (01.01.2010)	658	3	0	0.672138	0.418038	0.397311	0.158978	1.24142	>>
C001-0037	1 (01.01.2010)	217	6	0	0.676953	0.46965	0.493101	0.144884	1.39469	>>
C001-0051	1 (01.01.2010)	269	3	0	0.676734	0.506652	0.58076	0.125822	1.50458	>>
C001-0053	1 (01.01.2010)	3495	2	0	0.658674	0.0977279	0.0966804	0.03548	0.290217	>>
C001-0061	1 (01.01.2010)	606	3	0	0.678292	0.446526	0.570273	0.191795	1.32602	>>
C001-0062	1 (01.01.2010)	569	2	0	0.67823	0.427967	0.429091	0.14216	1.27091	>>
C001-0078	1 (01.01.2010)	2240	3	0	0.673816	0.442757	0.420853	0.0591102	1.31483	>>
C001-0079	1 (01.01.2010)	1335	7	0	0.678951	0.547244	0.550821	0.0773938	1.62512	>>
C001-0082	1 (01.01.2010)	1204	11	0	0.679943	0.521149	0.56466	0.135433	1.54763	>>
C001-0093	1 (01.01.2010)	478	3	0	0.679725	0.35323	0.187097	0.197926	1.04897	>>
C001-0098	1 (01.01.2010)	843	7	0	0.678767	0.430014	0.466908	0.166959	1.27699	>>
C001-0099	1 (01.01.2010)	240	2	0	0.679701	0.404609	0.401674	0.136328	1.20155	>>
C001-0105	1 (01.01.2010)	8384	3	0	0.509982	0.427833	0.423588	0.0261433	1.27051	>>
C001-0113	1 (01.01.2010)	359	3	0	0.664479	0.386381	0.336059	0.129392	1.14741	>>
C001-0119	1 (01.01.2010)	848	2	0	0.668238	0.317366	0.328989	0.0734662	0.942463	>>
C001-0120	1 (01.01.2010)	499	3	0	0.650086	0.23845	0.217426	0.0894744	0.708111	>>

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

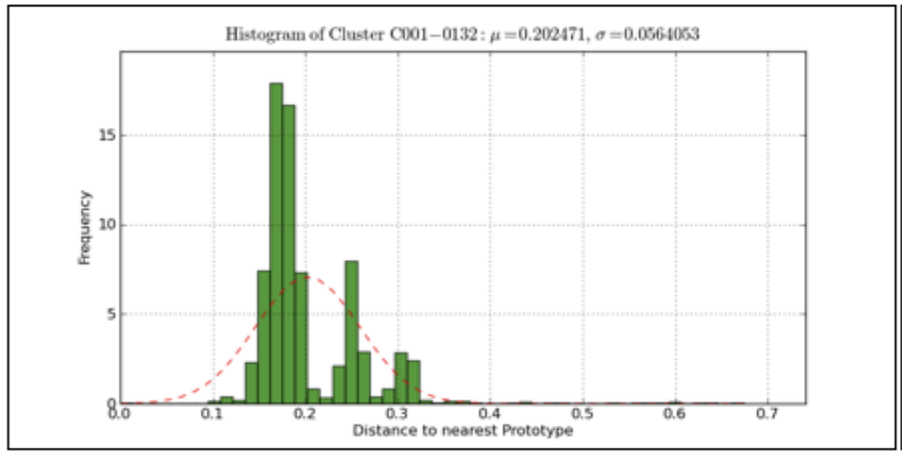
:: InMAS :: Internet Malware Analysis System :: CWSandbox ::

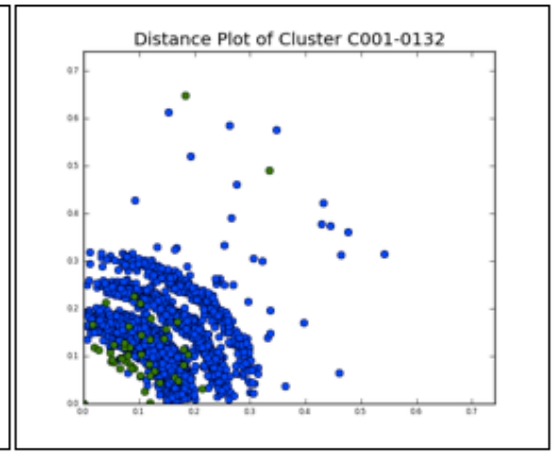
CWSandbox
Clustering

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

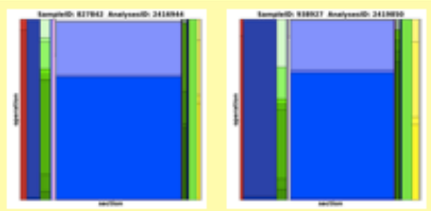
Live Feed | Malware Browser | Search | Clustering | Submit | Sandbox Status

Cluster	
Cluster	C001-0132
Run (Date)	1 (01.01.2010)
Analyses in Cluster	2922
Prototypes of Cluster	2
Mininal Distance to Prototypes	0
Maximal Distance to Prototypes	0.673547
Average Distance to Prototypes	0.202471
Median of Distance to Prototypes	0.181815
Standard Deviation	0.0564053
Density	0.601266



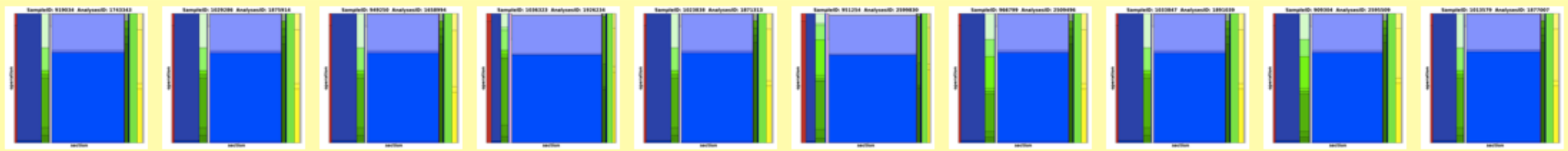


Prototypes (represented samples)



98.66 % 1.34 %

Top 10 Inlier (distance)



0.0981367 0.102198 0.102198 0.102213 0.106 0.111977 0.113319 0.113319 0.11673 0.11673

:: InMAS :: Internet Malware Analysis System :: MalOffice ::

MalOffice

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Live Feed | Overview | Submit Document | Embedded Objects | Statistics | Search

Filename	Document type	SHA1	Total result	
waledac-ec2nd09.pdf	Portable File Format	e6f67a8fa8f04b23a12279f544f71e5a5e177599		>>
uebung09.pdf	Portable File Format	344fcea61005ee2af19917f0d863e46c5bc3678f		>>
uebung10.pdf	Portable File Format	c5a390b145f5ba568d1aaa384667c06ac9756254		>>
Hello.doc	Microsoft Word document	6cac6c2d046d95b7dfa8d2e31b417d2dfbc64ebb		>>
Hello.doc	Microsoft Word document	fb356b7cb81139d54c6ca50a2145201e3ec9dd28		>>
testdoc.doc	Microsoft Word document	e7edba3fbb9b73274c7f2f1a6913d1229fab8ec1		>>
testdoc.doc	Microsoft Word document	6ba319b76381ca9efe15c6db046af262ee1e5072		>>
fe4cc608e9bfc1ad19c4652d911c1b1c.doc	Microsoft Word document	88e0c04e1ec5c5bc02bc2555c055fad6e486b7fe		>>
f9f782c10f7a415b8b5d82a4466ec848.doc	Microsoft Word document	75e7299eb436268f54635e254b91bf85b0c0ffb8		>>
f926414961e278303c4fe6b7a0dae651.doc	Microsoft Word document	bd7b64307a2ec0e0cc28c29aebad5e65a19a1e00		>>
b9b3f41a85f1d716b348a806506fc045.doc	Microsoft Word document	b12b98756f503374f907153c5038b5f882b05c19		>>
5d8a9531e7f2a802da8305e762e45316.doc	Microsoft Word document	cd302ec622895ab6ba1fcac3eee1199d33c27c78		>>
545c5843ca66cd6847b82df42f5c8ba3.doc	Microsoft Word document	8833f8627a2211258a7d3652883779f40cece2cb		>>
2bbae69228a792f10055de438c370a91.doc	Microsoft Word document	f36dcbb6bc9bb6e015a8fda037280c7a1086b02b		>>
039f67b8ad46de7790f8270a3880c3d0.doc	Microsoft Word document	bf07910bb72a76dea326a74c693cabff37dd9bb1		>>
zuerich99.ppt	Microsoft PowerPoint presentation	50ce1ea4d8821f9b5306dc68f9245590d48b3027		>>
zagreb.ppt	Microsoft PowerPoint presentation	2ba3d8327aab36a5e6c9017c6d4d1d367d1a906d		>>
YouthWorkcurriculumslides.ppt	Microsoft PowerPoint presentation	e0097f7bf2bd7c585a7e338328732b2fc6b5913d		>>
youth_2004_sasada_final.ppt	Microsoft PowerPoint presentation	1f7443ce7ed8e2ccc72d7ec0dd2e3340cfec6128		>>
Yearendauditissuewebinarfinal.ppt	Microsoft PowerPoint presentation	95bcb23e6a8512fe11302e0bf49a6538d93419f4		>>
yakushev.ppt	Microsoft PowerPoint presentation	bb8555e2db84a1bd648592c1e1d8d7d1cb1e64ce		>>
Xyratex_Corporate_Presentation_09V...ppt	Microsoft PowerPoint presentation	06ec025e371762f39b7b141001d85f98d26a6743		>>
xxxatcmlecture.ppt	Microsoft PowerPoint presentation	413d65cc193a20649b4847f2b84f246bc20c1d03		>>
ww112_uebergabe_hohlstrahlrohre.ppt	Microsoft PowerPoint presentation	6af664b9816a4f788ec01c76812f2e25d43e2d3d		>>
WVDEISHearingpresentationDKZ071706.ppt	Microsoft PowerPoint presentation	18fd21598d927cf4162206010ad8139350ceb2da		>>
WS_Dauphin_Metzler.ppt	Microsoft PowerPoint presentation	5aaef1222f8d9487015c616fc6eceb3545a8edc8		>>
World_Internet_Project_Media.ppt	Microsoft PowerPoint presentation	0d0c17c3adecc7f10fae4b8742d36a47bd4c1086		>>
World_Health_Day_2008_14_Air_quality.ppt	Microsoft PowerPoint presentation	2c073f85f20a486bf679a876c4fb8923c9d3a79a		>>
wlx_powerpoint.ppt	Microsoft PowerPoint presentation	951b89e9e6df23ac58019db31f18c5da9a254aae		>>
wi_specialty_share_of_cheese_produ...ppt	Microsoft PowerPoint presentation	707daa74acb18c112017fa36720831de3270faa6		>>
WiFi_Gen_0806.ppt	Microsoft PowerPoint presentation	135692f807e9478c744f344192c3c9e6e4cf3a95		>>
What_is_211.ppt	Microsoft PowerPoint presentation	99b89e08477f8c504f3b5b94bfe094e56620a4fd		>>
WGCPI_report_Vienna.ppt	Microsoft PowerPoint presentation	ff7c9234a2ebddfcf7ded20e31561d346f7bfe2a		>>
Weygman.ppt	Microsoft PowerPoint presentation	2f55c00b8ee82dcbc2a6c6afbf51cfd101d5240e		>>
Weinper.ppt	Microsoft PowerPoint presentation	ba91a504256a338c09606041c692762787278b54		>>
week07samenwerking.ppt	Microsoft PowerPoint presentation	fa68efdf98c7461bd44027a82504b951e7031c0a		>>
WCTE_Benefits_New_T.ppt	Microsoft PowerPoint presentation	7c66d05dd4cfc0892e097cadd6aa0e4799ca4ae6		>>
WatkinsCreekCase.ppt	Microsoft PowerPoint presentation	70abc9205b396d569602076e3c912f68cbfdbddb		>>
warner.ppt	Microsoft PowerPoint presentation	4ad882a629d060690235b22f5bc1970758836aab		>>
WAPI_diaporama_projet_promo_manuel.ppt	Microsoft PowerPoint presentation	7f767f0d280e8da03194c158e0ca414902988a4f		>>

Finder File Edit View Go Window Help demo

:: InMAS :: Internet Malware Analysis System :: MalOffice ::

:: InMAS :: Internet Malware Analysis System :: MalOffice ::

MalOffice

CWSandbox | Server Honeypots | Spamtraps | Client Honeypots | MalOffice | General

Live Feed | Overview | Submit Document | Embedded Objects | Statistics | Search

General Information

Filename	how_to_get_there.pdf download
Filesize	126423
MD5 hash	8b85aea1920bc99157c27efc60397e21
SHA1 hash	124946c349bebde6c9d5ce6dace5cf1d5bc878fa
Document type	Portable File Format
Total result	

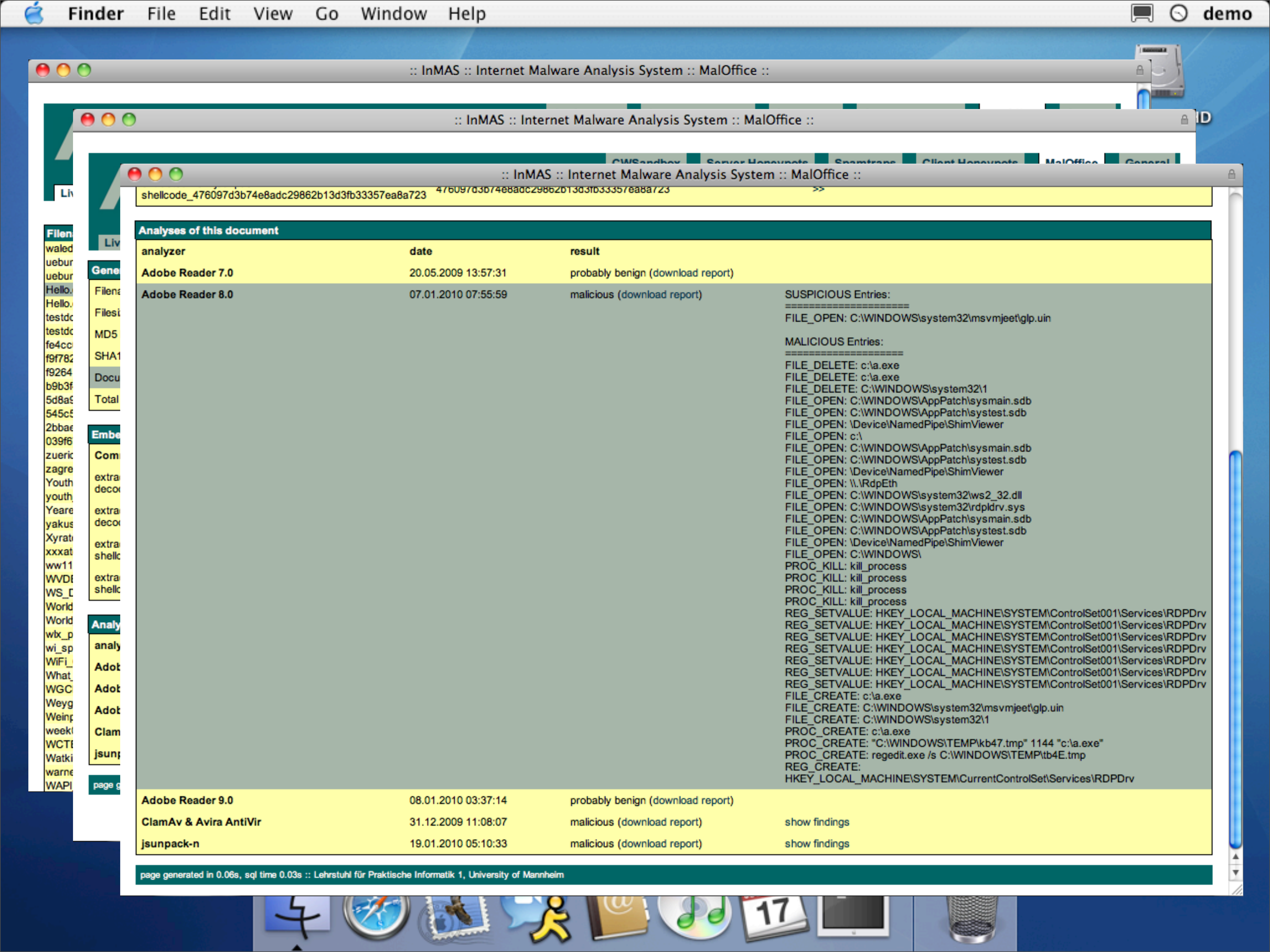
Embedded Objects

Comment	SHA1 hash	Download
extracted from jsunpack-n: decoding_6f8ca5f2d575ffac9d69b71cb5ca6115b612e876	6f8ca5f2d575ffac9d69b71cb5ca6115b612e876	>>
extracted from jsunpack-n: decoding_90845849f5cd7e9a10d7038ecb46e7fb62dd867d	90845849f5cd7e9a10d7038ecb46e7fb62dd867d	>>
extracted from jsunpack-n: shellcode_c77410f78ab7acfbef279aa76c97adce081e0597	c77410f78ab7acfbef279aa76c97adce081e0597	>>
extracted from jsunpack-n: shellcode_476097d3b74e8adc29862b13d3fb33357ea8a723	476097d3b74e8adc29862b13d3fb33357ea8a723	>>

Analyses of this document

analyzer	date	result	
Adobe Reader 7.0	20.05.2009 13:57:31	probably benign (download report)	
Adobe Reader 8.0	07.01.2010 07:55:59	malicious (download report)	show findings
Adobe Reader 9.0	08.01.2010 03:37:14	probably benign (download report)	
ClamAv & Avira AntiVir	31.12.2009 11:08:07	malicious (download report)	show findings
jsunpack-n	19.01.2010 05:10:33	malicious (download report)	show findings

page generated in 0.06s, sql time 0.02s :: Lehrstuhl für Praktische Informatik 1, University of Mannheim


Finder File Edit View Go Window Help
demo
:: InMAS :: Internet Malware Analysis System :: MalOffice ::
shellcode_476097d3b74e8adc29862b13d3fb33357ea8a723
Analyses of this document
analyzer
date
result
Adobe Reader 7.0
20.05.2009 13:57:31
probably benign (download report)
Adobe Reader 8.0
07.01.2010 07:55:59
malicious (download report)
SUSPICIOUS Entries:
====================
FILE_OPEN: C:\WINDOWS\system32\msvmjeet\glp.uin
MALICIOUS Entries:
====================
FILE_DELETE: c:\a.exe
FILE_DELETE: c:\a.exe
FILE_DELETE: C:\WINDOWS\system32\1
FILE_OPEN: C:\WINDOWS\AppPatch\sysmain.sdb
FILE_OPEN: C:\WINDOWS\AppPatch\systest.sdb
FILE_OPEN: \Device\NamedPipe\ShimViewer
FILE_OPEN: c:\
FILE_OPEN: C:\WINDOWS\AppPatch\sysmain.sdb
FILE_OPEN: C:\WINDOWS\AppPatch\systest.sdb
FILE_OPEN: \Device\NamedPipe\ShimViewer
FILE_OPEN: \\.\RdpEth
FILE_OPEN: C:\WINDOWS\system32\ws2_32.dll
FILE_OPEN: C:\WINDOWS\system32\rdpldrv.sys
FILE_OPEN: C:\WINDOWS\AppPatch\sysmain.sdb
FILE_OPEN: C:\WINDOWS\AppPatch\systest.sdb
FILE_OPEN: \Device\NamedPipe\ShimViewer
FILE_OPEN: C:\WINDOWS\
PROC_KILL: kill_process
PROC_KILL: kill_process
PROC_KILL: kill_process
PROC_KILL: kill_process
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
REG_SETVALUE: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\RDPDrv
FILE_CREATE: c:\a.exe
FILE_CREATE: C:\WINDOWS\system32\msvmjeet\glp.uin
FILE_CREATE: C:\WINDOWS\system32\1
PROC_CREATE: c:\a.exe
PROC_CREATE: "C:\WINDOWS\TEMP\kb47.tmp" 1144 "c:\a.exe"
PROC_CREATE: regedit.exe /s C:\WINDOWS\TEMP\tb4E.tmp
REG_CREATE:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDPDrv
Adobe Reader 9.0
08.01.2010 03:37:14
probably benign (download report)
ClamAv & Avira AntiVir
31.12.2009 11:08:07
malicious (download report)
show findings
jsunpack-n
19.01.2010 05:10:33
malicious (download report)
show findings
page generated in 0.06s, sql time 0.03s :: Lehrstuhl für Praktische Informatik 1, University of Mannheim

Results

Server honeypots

- ~ 7 month
- 1 Amun instance

Statistics

attacks	unique IPs	downloads
307.791	3.670	6.019

Top vulnerabilities

dcom	lsass	symantec
25.92%	22.15%	19.16%

Client honeypots

- ~ 4 month
- 5 Capture clients

Statistics

websites	webserver IPs	malicious	faulty
18.179	7.351	322	11.545

Suspicious events

registry	filesystem	network
42.66%	34.41%	22.51%

Spamtraps

- ~ 6 month
- 8 spamtraps + web-upload

Statistics

emails	attachments	urls
304.222	4.413	6.982.146

Attachments

image	zip	pdf
83.39%	7.02%	0.73%

CWSandbox

- Free service online for 3 years
- 15 native sandbox systems / 2.5 minutes per run

Statistics

submissions	unique samples	user
1.059.780	999.005	11.895

Analyses

overall	CWSandbox	Virustotal
2.560.575	992.757	1.378.650

Clustering

- ~ 1 1/2 month
- 52 incremental cluster runs

Statistics

clustered reports	rejected	cluster
155.722	2.931 (~1.88%)	432

Cluster

avg/min/max member	avg. # prototypes	avg. distance
353/10/38.505	5	0.335011

Conclusion

Conclusion

- The InMAS approach for malware capture and analysis
- System online since 2007
- Sandbox service is used by many security research teams
- Continuously enhanced

Philipp Trinius

http://pi1.informatik.uni-mannheim.de/
trinius@uni-mannheim.de

Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITY OF MANNHEIM