



Threat Landscape

Mark Harris

VP of SophosLabs

Agenda

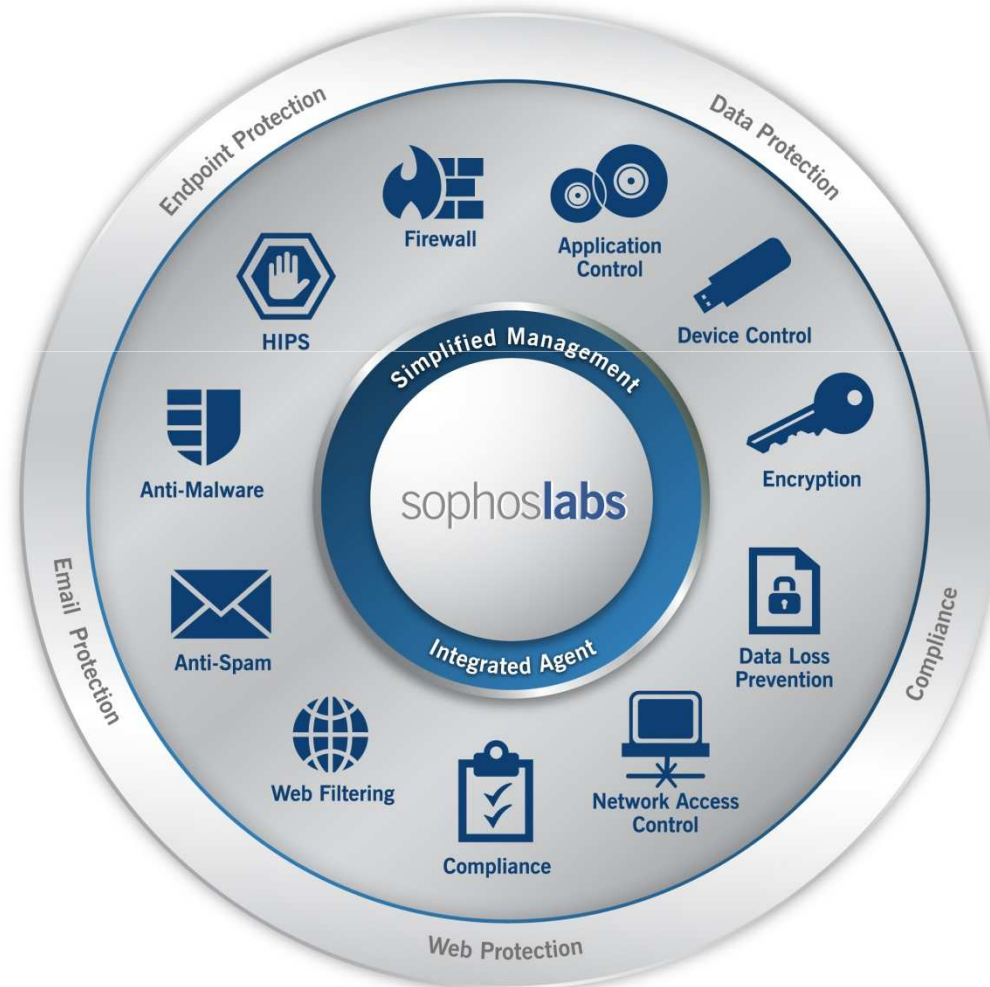
- About SophosLabs
- LatestThreats
 - Email – Web
 - Search Engine Poisoning
 - The Italian Connection
- Protection

SophosLabs Overview

- Global team of 80
- 24-7
- Mixture of skillsets
- Wide array of responsibilities
 - Analysis, IDEs
 - Spam rules
 - HIPs rules
 - Vulnerabilities, exploits
 - DLP



SophosLabs at the core



SophosLabs

- Detect and block the spam
- Block the spam website
- Detect and block the Malicious Javascript
- Detect and block the Exploit
- Detect and block the Trojan

Some Numbers

50000

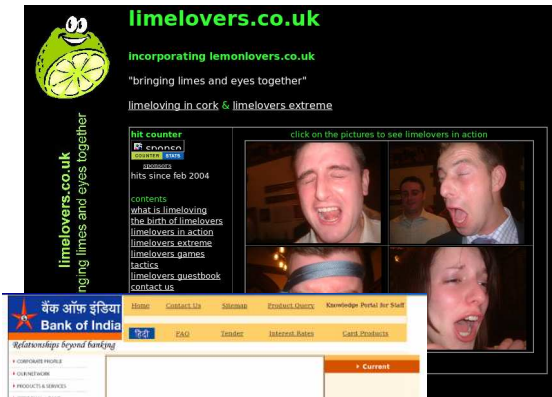
5 Minutes

5 Seconds

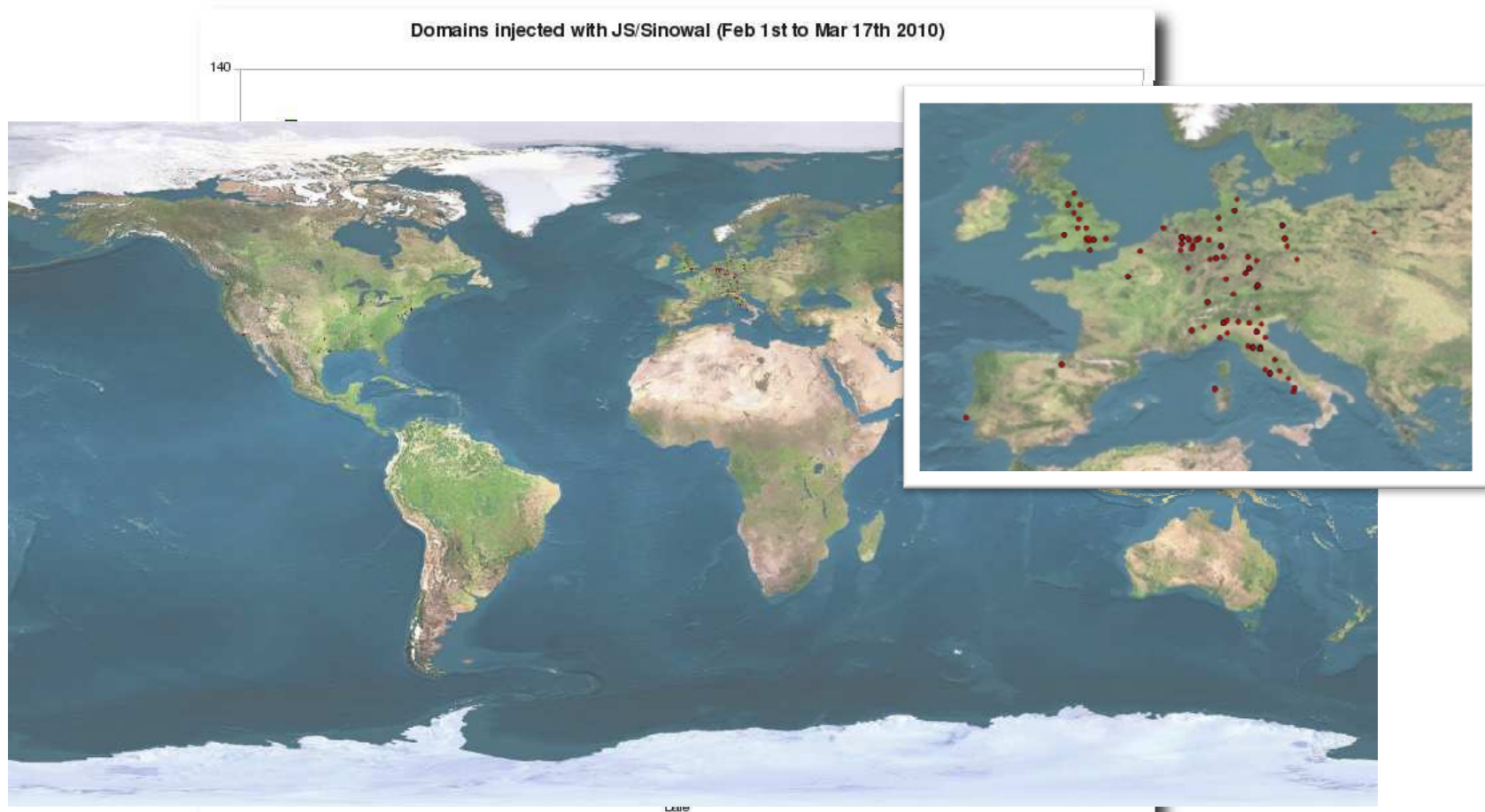
5 Million

Web threats

- Over 90% are compromised websites
 - Legitimate organisations
 - “Hacked”
- Can be Anything!



Sinowal – Install MBR Rootkit



From to

Country: **Italy** Name: **JS/Sinowal-Gen2**

Note: Click the name to search the malware queue for that domain

Domain	% of total	Total URIs
kromolab.it	5.87	185
sceglierbio.com	5.23	165
pureitems.com	4.50	142
motorcar2.it	4.03	127
alejandroherrero.com	3.52	111
lineaquotidiano.net	3.27	103
beatfly.net	2.98	94
riotmaker.net	2.82	89
basketforum.it	2.31	73
kaly.it	2.06	65
blog83.net	1.87	59
prolocoarzignano.it	1.78	56
monza-news.it	1.74	55
fertilita.org	1.68	53
esnpisa.it	1.49	47
fi.it	1.46	46
dallelucche.com	1.24	39
elmotor.net	1.20	38
camilagiorgi.it	1.11	35
giratempoweb.net	1.05	33
gdrzine.com	0.98	31
giapox.it	0.92	29
giovannidaddabbo.com	0.89	28
elita.it	0.86	27
emanuelenonni.com	0.86	27
anrieti.it	0.70	22
styleforstyle.it	0.67	21
todotusoft.com	0.67	21

Dynamic redirection: Sinowal

- Malicious script injected into legitimate sites
 - Dynamic, date-driven generation of domains
 - Query *Twitter* trends JSON data
 - Use character in algorithm for domain generation



- *Italian focus* - hosting providers hit
- Heavily obfuscated JavaScript
- Payload: **Sinowal** (aka Mebroot)
 - MBR rootkit
- Subtle, “sub-radar” attacks

Protection technology

Content

- 'Signatures'
- Characteristics

Behaviour

- What is it going to do
- What is doing

Reputation

- Where did it come from
- Have we seen it before

Content - Detection signatures

Conventional Detection

@Streams ("PE")

```
; CMD: mkid3 -g -r 1000,6000 dwnl-hkw.unp
; File Format: Win32 PE
; Entry Point: 0x0434b
; File Name : dwnl-hkw.unp
```

```
55 8b ec 53 8b 5d 08 56 8b 75 0c 57 8b 7d 10 85
f6 75 09 83 3d 28 32 01 10 00 eb 26 83 fe 01 74
05 83 fe 02 75 22 a1 a4 3a 01 10 85 c0 74 09 57
56 53 ff d0 85 c0 74 0c 57 56 53 e8 15 ff ff ff
85 c0 75 04 33 c0 eb 4e 57 56 53 e8 75 fd ff ff
83 fe 01 89 45 0c 75 0c 85 c0 75 37 57 50 53 e8
f1 fe ff ff 85 f6 74 05 83 fe 03 75 26 57 56 53
e8 e0 fe ff ff 85 c0 75 03 21 45 0c 83 7d 0c 00
74 11 a1 a4 3a 01 10 85 c0 74 08 57 56 53 ff d0
89 45 0c 8b 45 0c 5f 5e 5b 5d c2 0c 00 ff 25 9c
50 00 10 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
!F !434b - s0
!1000 + Lf ; 0x01000
8b 0d 58 60 00 10 89 4c 24 38 89 74 24 3c 8b 15
94 32 01 10 df 6c 24 38 25 ff ff 00 00 50 52 d9
ff dd 1d b0 32 01 10 ff 15 34 50 00 10 8b 0d 98
37 01 10 89 01 e9 5b 06 00 00 68 00 00 0a 1c 68
```

Content - Proactive malware detection

Conventional Detection

@Streams ("PE")

```
; CMD: mkid3 -g -r 1000,6000 dwnl-hkw.unp
; File Format: Win32 PE
; Entry Point: 0x0434b
; File Name : dwnl-hkw.unp
```

```
55 8b ec 53 8b 5d 08 56 8b 75 0c 57 8b 7d 10 85
f6 75 09 83 3d 28 32 01 10 00 eb 26 83 fe 01 74
05 83 fe 02 75 22 a1 a4 3a 01 10 85 c0 74 09 57
56 53 ff d0 85 c0 74 0c 57 56 53 e8 15 ff ff ff
85 c0 75 04 33 c0 eb 4e 57 56 53 e8 75 fd ff ff
83 fe 01 89 45 0c 75 0c 85 c0 75 37 57 50 53 e8
f1 fe ff ff 85 f6 74 05 83 fe 03 75 26 57 56 53
e8 e0 fe ff ff 85 c0 75 03 21 45 0c 83 7d 0c 00
74 11 a1 a4 3a 01 10 85 c0 74 08 57 56 53 ff d0
89 45 0c 8b 45 0c 5f 5e 5b 5d c2 0c 00 ff 25 9c
50 00 10 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
!F !434b - s0
!1000 + Lf ; 0x01000
8b 0d 58 60 00 10 89 4c 24 38 89 74 24 3c 8b 15
94 32 01 10 df 6c 24 38 25 ff ff 00 00 50 52 d9
ff dd 1d b0 32 01 10 ff 15 34 50 00 10 8b 0d 98
37 01 10 89 01 e9 5b 06 00 00 68 00 00 0a 1c 68
```

Proactive Detection

@Streams ("Gene")

```
Gene("Total,MSVC9DLL") D!:=0 s0
```

```
Gene("Total,CodeSize-A")
```

```
D<2000 far fail
```

```
D>6000 far fail
```

```
r0 !100 EmLm
```

```
[20
```

```
[20 Gene("AND,ConfickPk,DllNoExp,VProtect,NoRsrc") D!:=0
```

```
[20 Gene("OR,FalsePos") D==0
```

```
!ns Ri
```

```
!3 !1 !1
```

```
!3 GCall W32/Confick-A
```

```
!800
```

```
GCall G/FreqVar-A
```

```
D>20 fail
```

```
SetPackGene
```

```
!1 SetGeneEx("Pack,ConfickPk")
```

```
!1 SetGeneEx("Gene,Packed")
```

```
:fail tu
```

```
!
```

Runtime behavioral protection

- Complementary to Behavioral Genotype
- Inspects process behaviour **exhibited** on the system
- Inspects all running processes for sign of malicious modifications of system objects
 - Files
 - Registry entries
 - Processes
 - Network connections
 - Loaded drivers

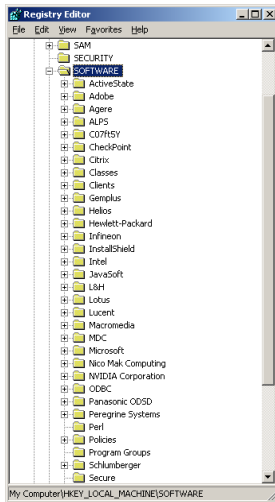
Simplified runtime arch

Register in run key

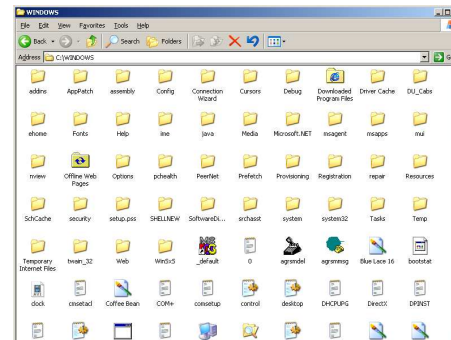


Privileged – kernel mode

Non-privileged – user mode



Virus.exe

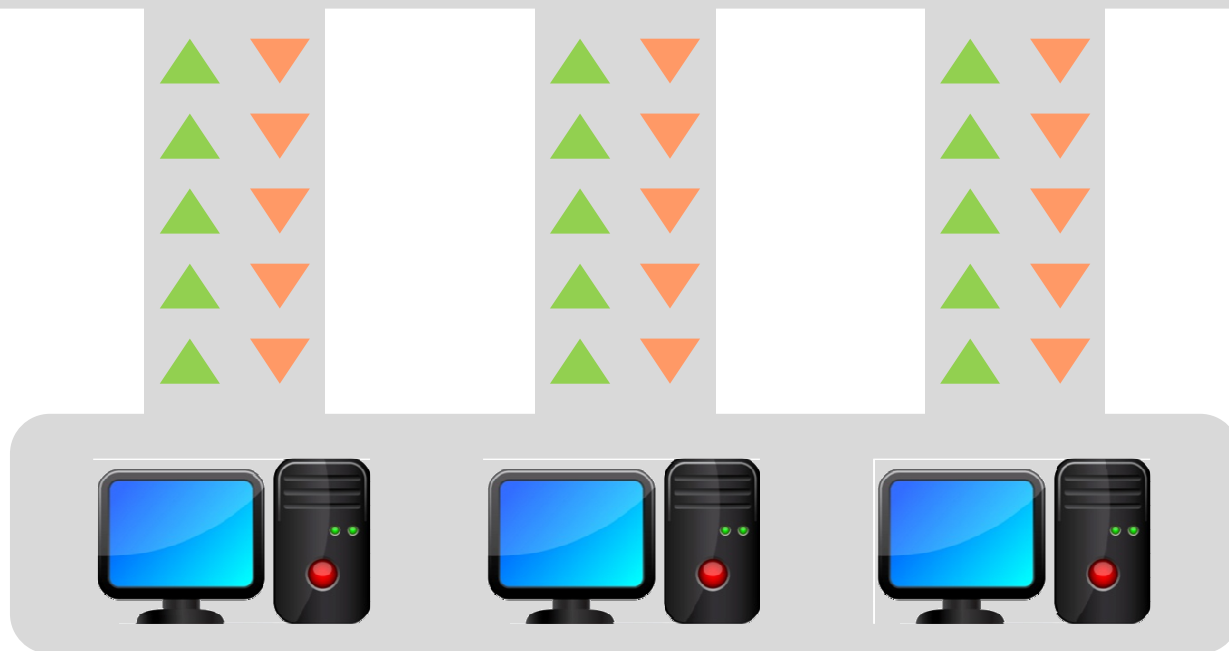


- Process virus.exe starting...
- Oh, OK, scanning for viruses...
- Nothing found.
- Virus.exe is opening registry run key...
- Interesting. Tell me more about it.
- Virus.exe registers itself to run key...
- Oh, no not OK, block operation!!!
- Operation blocked.
- Thank you kernel!
- Reporting behaviour.



Reputation

sophos**labs**



Reputation

sophoslabs [DASHBOARD](#) [LAB INFO](#) [REPORTS](#) [TOOLS](#) [MESSAGES](#)

Active Users [anna.szalay](#), [fraser.howard](#), [james.wyke](#), [michael.s](#), [stephen.edwards](#) [Login](#)

SavCloud - Identity Browser

[Navigation](#) | [Dashboard](#) | [Identity Browser](#) | [Identity Manager](#) | [Checksum Browser](#) | [Checksum Manager](#) | [Checksum Log](#)

Time Range:

Identity Prefix:

Columns —

Identity	Status	E	L	S	P	Lookups	N.XSums	N.Cust	N.E.P.	Path	Filename	First Seen	Last Seen
8aec8b0d632b63ed						9958416	148433	105	449	UNKNOWN_DIR	LKXKLUI.DLL	2010-03-16 18:12	2010-04-06 21:42
5f887d053c80299a						363687	189300	3	1	UNKNOWN_DIR	8d8a61dcd07f91c5c7e1	2010-03-16 19:02	2010-03-31 11:14
Mal/Generic-A	detected	E	L			334162	195353	15	12	UNKNOWN_DIR	hd1.exe	2010-03-17 11:02	2010-04-06 12:52
Mal/Hrup-B	detected	E	L			62475	34443	1	1	UNKNOWN_DIR	dca71364821d52fc	2010-03-19 06:46	2010-03-29 08:30
Troj/DwnLdr-HQY	detected		L			40545	34263	2	1	UNKNOWN_DIR	dldr-hqy.unp	2010-03-19 06:48	2010-03-31 07:27
Mal/Packer						35540	21713	5	3	UNKNOWN_DIR	fsgtest.exe	2010-03-17 00:11	2010-04-01 13:19
Mal/WinTrim-F						35021	33001	1	1	UNKNOWN_DIR	dca64a8c21ace83f	2010-03-24 18:08	2010-03-29 08:32
W32/Allaple-F						33395	28091	2	1	UNKNOWN_DIR	blah-d.000	2010-03-19 06:42	2010-03-31 05:42
Mal/Generic-E	detected			P		28017	17873	2	1	UNKNOWN_DIR	1032fee.unp	2010-03-19 06:44	2010-03-31 07:28
Mal/Swizzor-K						24478	17313	2	1	UNKNOWN_DIR	swizzo-k.004	2010-03-19 06:44	2010-03-31 06:05
App/InstantA-C						23634	13748	2	1	UNKNOWN_DIR	instac-c.pee	2010-03-19 06:46	2010-03-30 17:40
Mal/FakeAV-AD	detected			S	P	22659	20014	2	1	UNKNOWN_DIR	encpk-bb.001	2010-03-19 06:48	2010-03-31 05:47
Troj/Virtum-Gen						21197	13114	4	4	UNKNOWN_DIR	A0176864.exe	2010-03-19 07:58	2010-04-06 05:31
Mal/AutoRun-J						19312	15249	2	1	UNKNOWN_DIR	mautor-j.pee	2010-03-19 06:43	2010-03-31 05:42
Mal/Koutodoor-A						18881	16896	2	1	UNKNOWN_DIR	koutod-a.000	2010-03-19 08:02	2010-03-31 05:52
Mal/Sality-B						18084	11770	2	1	UNKNOWN_DIR	msal-b.pe6	2010-03-16 20:02	2010-03-31 06:32
Troj/DwnLdr-HYE						17581	8329	2	1	UNKNOWN_DIR	dwnl-hye.pe2	2010-03-19 06:46	2010-03-31 05:43
W32/Scribble-B						16958	11981	2	1	UNKNOWN_DIR	scribb-b.p59	2010-03-19 06:42	2010-03-31 06:36
W32/Mofkys-B						14877	14414	2	1	UNKNOWN_DIR	mdropckh.pee	2010-03-19 09:06	2010-03-31 05:55
Mal/Wintrim-E						14647	10979	1	1	UNKNOWN_DIR	d16120a90080c84b	2010-03-19 06:44	2010-03-29 08:30
Mal/VBNam-A						14270	11104	2	1	UNKNOWN_DIR	vbnam-a.00c	2010-03-19 09:04	2010-03-31 05:51
W32/Small-C	unknown			P		14139	5560	2	1	UNKNOWN_DIR	SMALL-C.PE3	2010-03-19 06:42	2010-03-30 20:39
Mal/Kates-A						13036	6612	2	1	UNKNOWN_DIR	kates-a.003	2010-03-19 06:46	2010-03-31 06:03
Mal/Sality-D						11916	8916	2	2	UNKNOWN_DIR	d9ee6ce717bd7653	2010-03-18 23:03	2010-03-29 08:31
Sus/UnkPack-C						11735	7480	6	4	UNKNOWN_DIR	mask-a.un1	2010-03-17 11:02	2010-03-31 07:22

Showing 1 to 25 of 500 entries

[First](#) [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [Next](#) [Last](#)

Conclusions

- Rapidly changing threat landscape
- Focus on making money
- Professional Malware development
- Web is the focus
- Traditional AV signatures not enough