Big “Blackhole” attack on UK

Overview: On Sunday, February 27th, 2011, AVG noticed a particularly large spike in detections of the Blackhole exploit kit, largely aimed at the UK. This was a large, coordinated attack, involving over 600 dedicated web servers that were use to infect innocent users. Given that it’s not called the “World Wide Web” for nothing, it’s most unusual to see one country so heavily hit by a single attack campaign in such a short time.

Background: Web-based exploit kits are commonly used to attack web surfers. Such kits are usually purchased for a few hundred dollars on the black market, and then mounted on “attack” servers, wherever they can be rented or compromised throughout the world. We think of these perpetrators as criminals, and they are, but to a large extent they are also businesses, and as such, they run organized “marketing campaigns”, just like a conventional, legitimate business.

These “campaigns” usually come in waves. The attack servers are brought online, massive amount of legitimate websites are being compromised and injected with malicious code, as a result AVG’s detection counts rise as the campaign gets under way, and then counts wane, generally as the ISP that’s providing the attack servers realizes what’s going on, and shuts them down.

An average daily detections figure from any particular exploit kit is generally between 20,000 to 30,000, with spikes from specific campaigns running into the low hundreds of thousands. When Blackhole first appeared in numbers, on January 25th, it immediately jumped to nearly 300,000 per day, which in itself is a pretty solid event, but on Feb 27th, it spiked to nearly 900,000 detections, and then dropped away over the next couple of days to just some tens of thousands. Prior to January 25th, Blackhole was not particularly popular, and we had been detecting less than a couple of hundred per day.

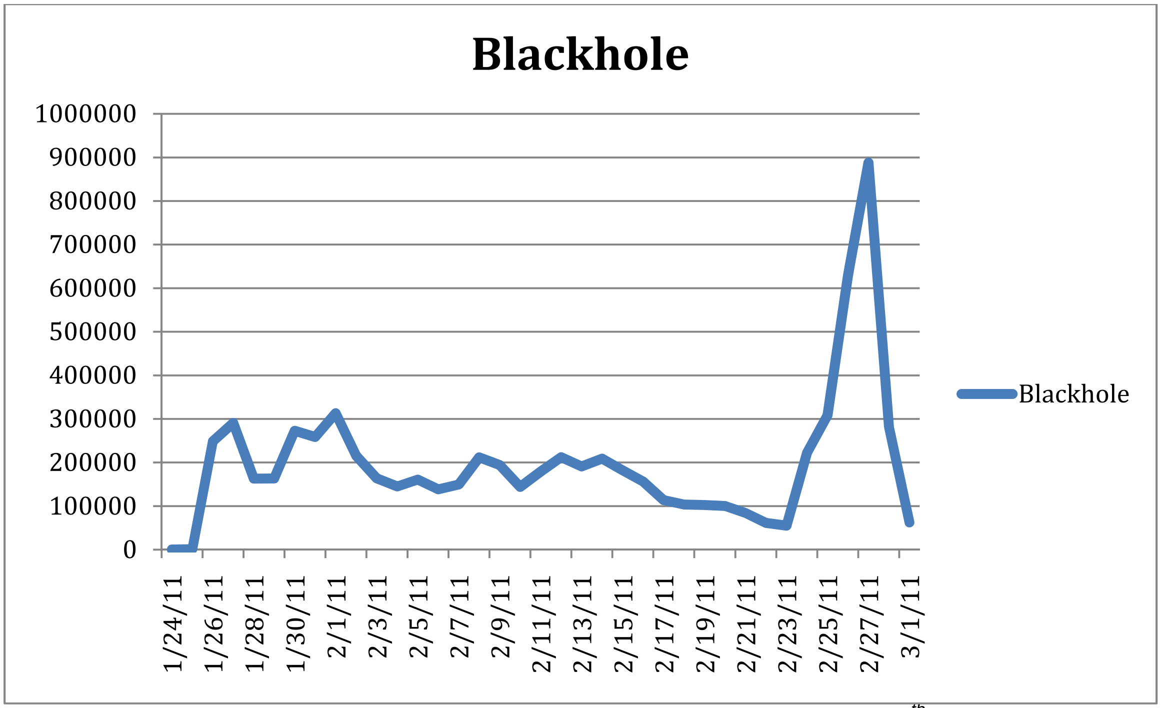
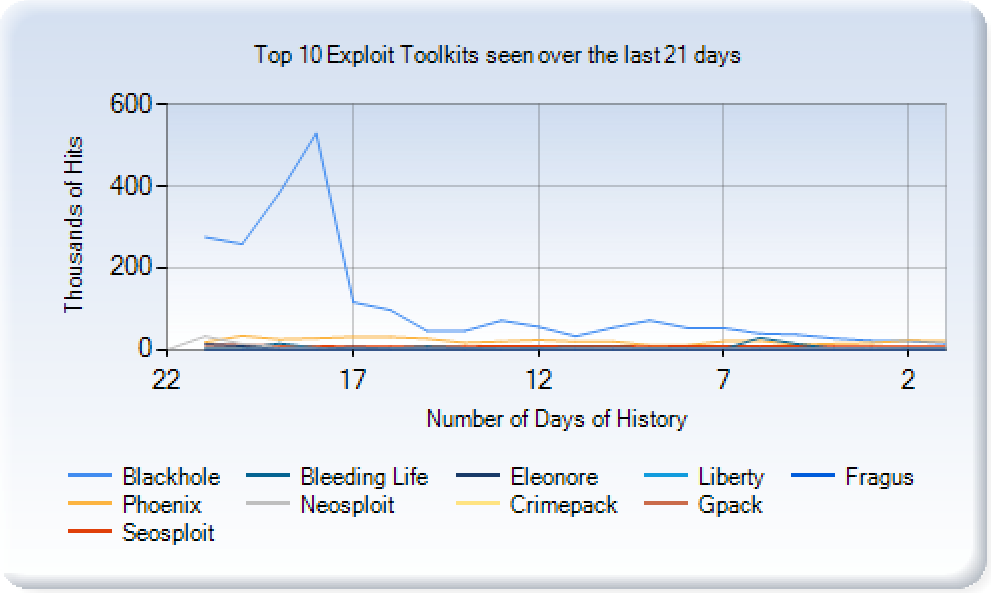


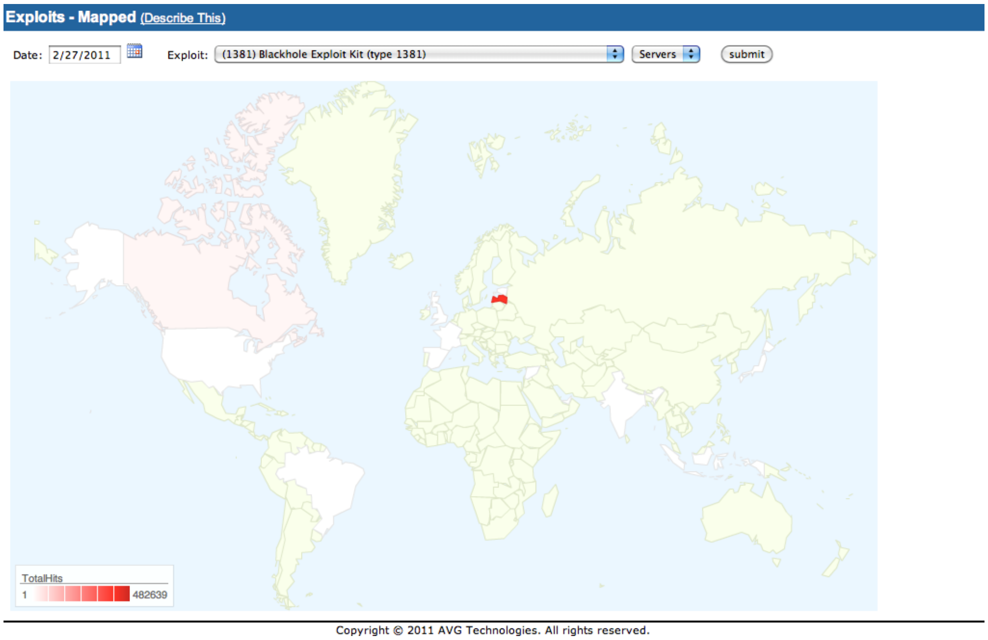
Fig 1. – Blackhole attack "campaign" as spotted on February 27th 2011

What is particularly interesting is that nearly 750,000 of these events were directed at the UK, with nearly 500,000 coming from Latvia, and 250,000 coming from the USA.

Just for a benchmark, here is how the Blackhole attack compares to other toolkits we are seeing on an average day



This first map shows that Latvia was the origin point of the major spike for the day.



Exploits - Mapped (Describe This)

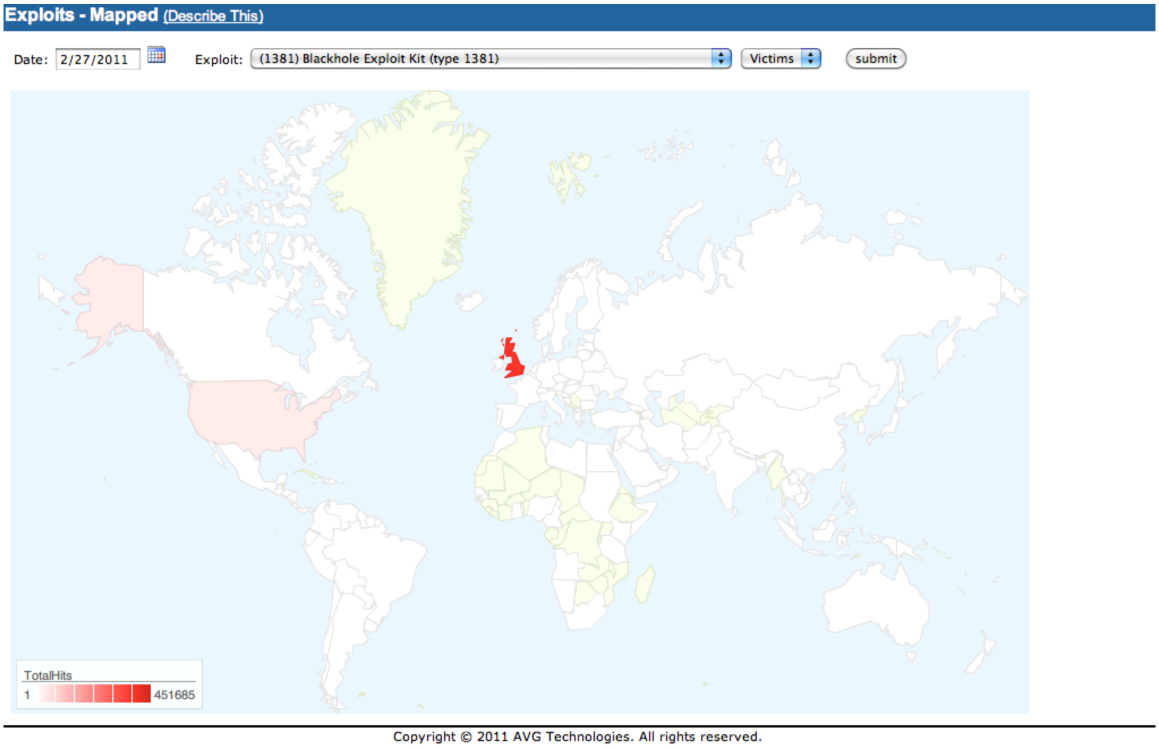
Date: 2/27/2011

Exploit: (1381) Blackhole Exploit Kit (type 1381)

Servers

Fig 2.: Geo location of origin of the attacks as recorded on AVG server

This map shows that the principal victim of most of the Latvian attacks was the UK.



Exploits - Mapped (Describe This)

Date: 2/27/2011

Exploit: (1381) Blackhole Exploit Kit (type 1381)

Victims

Fig 3: The Geo location of users targeted by the attacks

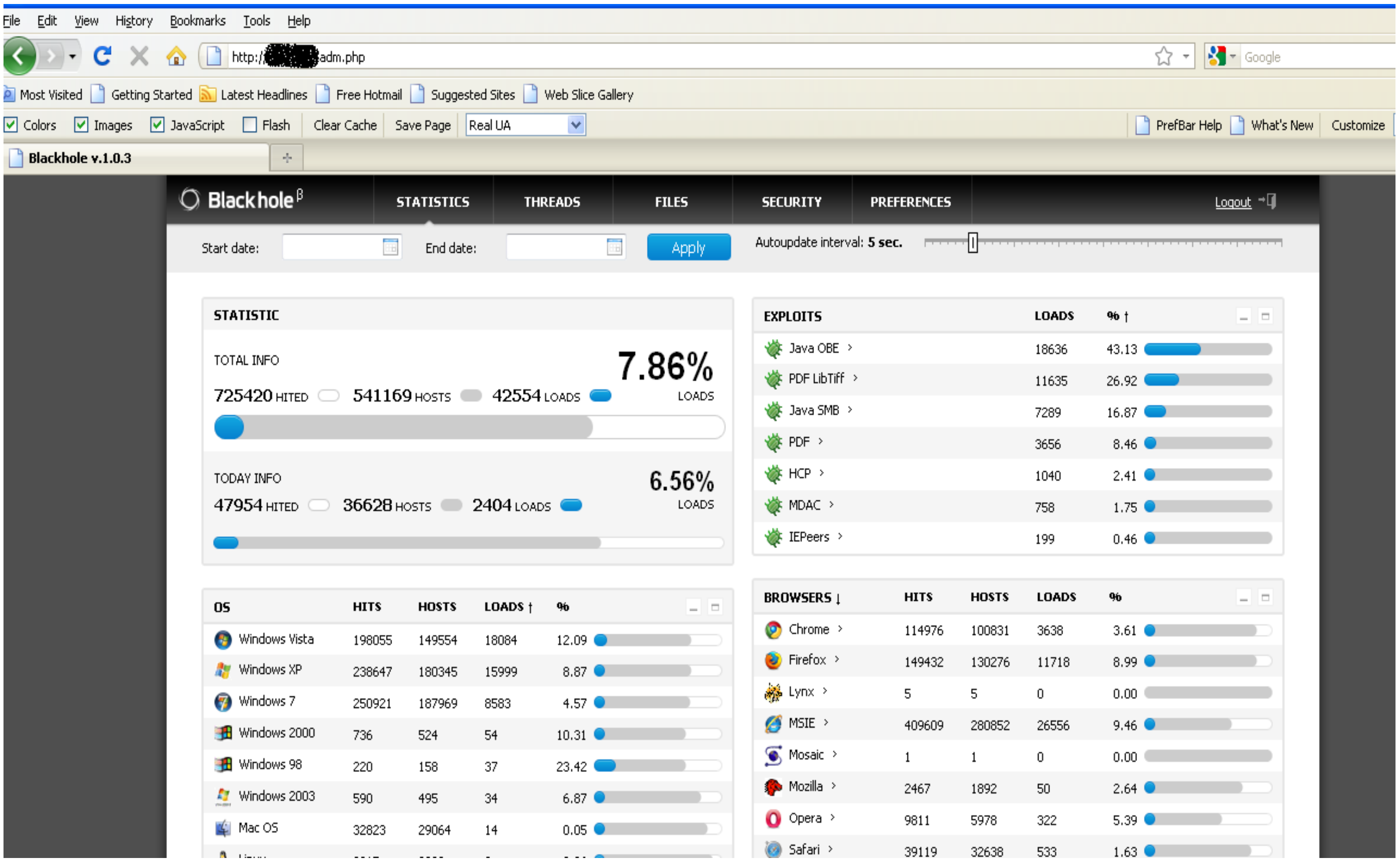
Background about the Blackhole Exploit Kit:

Blackhole is fairly new kit, having been first noticed late in 2010. The kit itself contains the following exploits:

CVE-2010-1885	- Microsoft Help Center exploit
CVE-2010-1423	- Argument injection vulnerability in the URI handler in Java
CVE-2010-0886	- Unspecified vulnerability in the Java Deployment Toolkit
CVE-2010-0842	- Unspecified vulnerability in the Sound component in Java
CVE-2010-0840	- Unspecified vulnerability in the Java Runtime Environment
CVE-2009-1671	- Multiple buffer overflows in Java Deployment Toolkit ActiveX
CVE-2009-0927	- Stack-based buffer overflow in Adobe Reader
CVE-2007-5659	- Multiple buffer overflows in Adobe Reader
CVE-2006-0003	- MDAC

There is nothing particularly new in this list, and MDAC is over four years old. It’s usually included because it’s so easy to use and reliable. If someone isn’t patched, it works every time.

This is the admin panel for one of the attack servers.


File Edit View History Bookmarks Tools Help
http://[redacted]adm.php
Google
Most Visited Getting Started Latest Headlines Free Hotmail Suggested Sites Web Slice Gallery
☑ Colors ☑ Images ☑ JavaScript □ Flash Clear Cache Save Page Real UA
PrefBar Help What's New Customize
Blackhole v.1.0.3
Blackhole β
STATISTICS THREADS FILES SECURITY PREFERENCES
Logout
Start date: End date: Apply
Autoupdate interval: 5 sec.

STATISTIC

TOTAL INFO

725420 HITED 541169 HOSTS 42554 LOADS — 7.86% LOADS

TODAY INFO

47954 HITED 36628 HOSTS 2404 LOADS — 6.56% LOADS

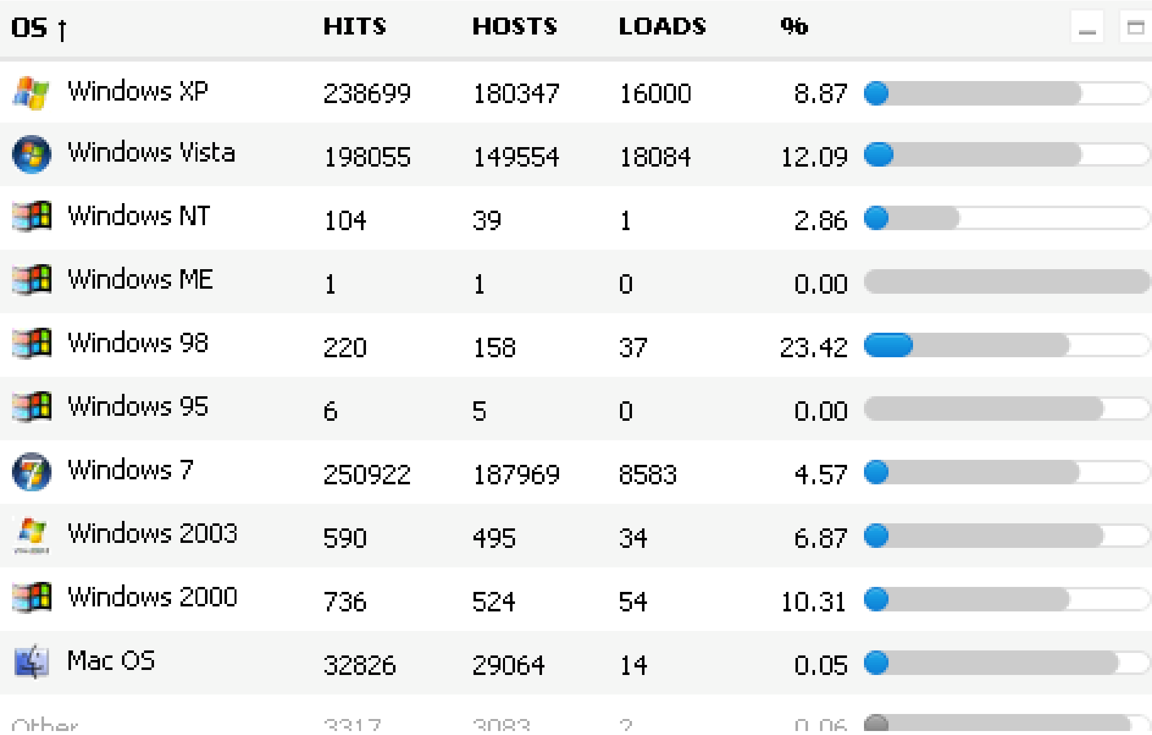
EXPLOITS	LOADS	% ↑
Java OBE ›	18636	43.13
PDF LibTiff ›	11635	26.92
Java SMB ›	7289	16.87
PDF ›	3656	8.46
HCP ›	1040	2.41
MDAC ›	758	1.75
IEPeers ›	199	0.46

OS	HITS	HOSTS	LOADS ↑	%
Windows Vista	198055	149554	18084	12.09
Windows XP	238647	180345	15999	8.87
Windows 7	250921	187969	8583	4.57
Windows 2000	736	524	54	10.31
Windows 98	220	158	37	23.42
Windows 2003	590	495	34	6.87
Mac OS	32823	29064	14	0.05

BROWSERS ↓	HITS	HOSTS	LOADS	%
Chrome ›	114976	100831	3638	3.61
Firefox ›	149432	130276	11718	8.99
Lynx ›	5	5	0	0.00
MSIE ›	409609	280852	26556	9.46
Mosaic ›	1	1	0	0.00
Mozilla ›	2467	1892	50	2.64
Opera ›	9811	5978	322	5.39
Safari ›	39119	32638	533	1.63

Fig 4: Blackhole Administration panel

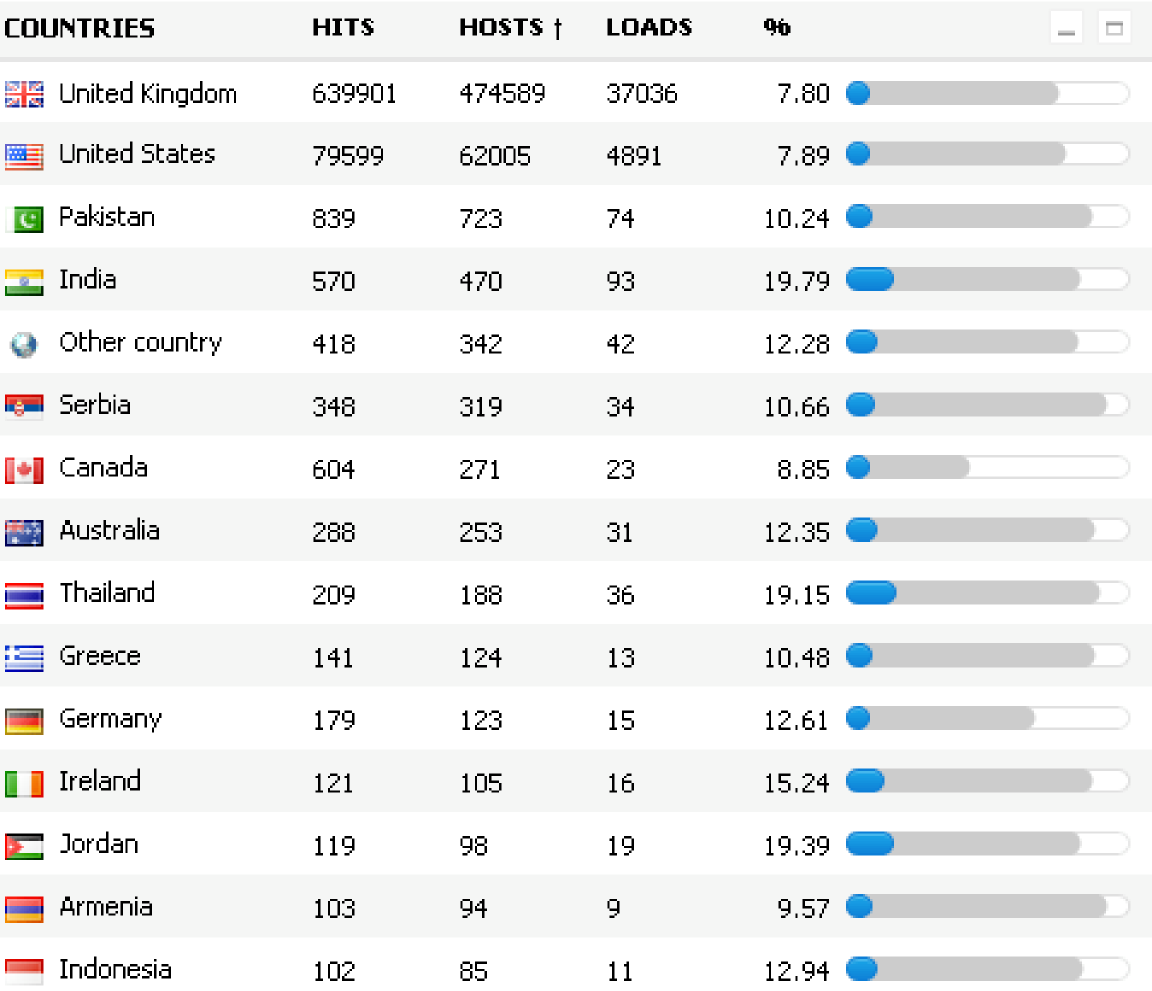
Interestingly, if we zero in on the target OSs, we see that they are claiming loads on Mac OS. Not very many load, but loads none the less. The implication of this is that the kit developers are at least thinking about Apple.



OS ↑	HITS	HOSTS	LOADS	%
Windows XP	238699	180347	16000	8.87
Windows Vista	198055	149554	18084	12.09
Windows NT	104	39	1	2.86
Windows ME	1	1	0	0.00
Windows 98	220	158	37	23.42
Windows 95	6	5	0	0.00
Windows 7	250922	187969	8583	4.57
Windows 2003	590	495	34	6.87
Windows 2000	736	524	54	10.31
Mac OS	32826	29064	14	0.05
Other	3317	3083	2	0.06

Fig 5: Blackhole Analytics – infected OS types

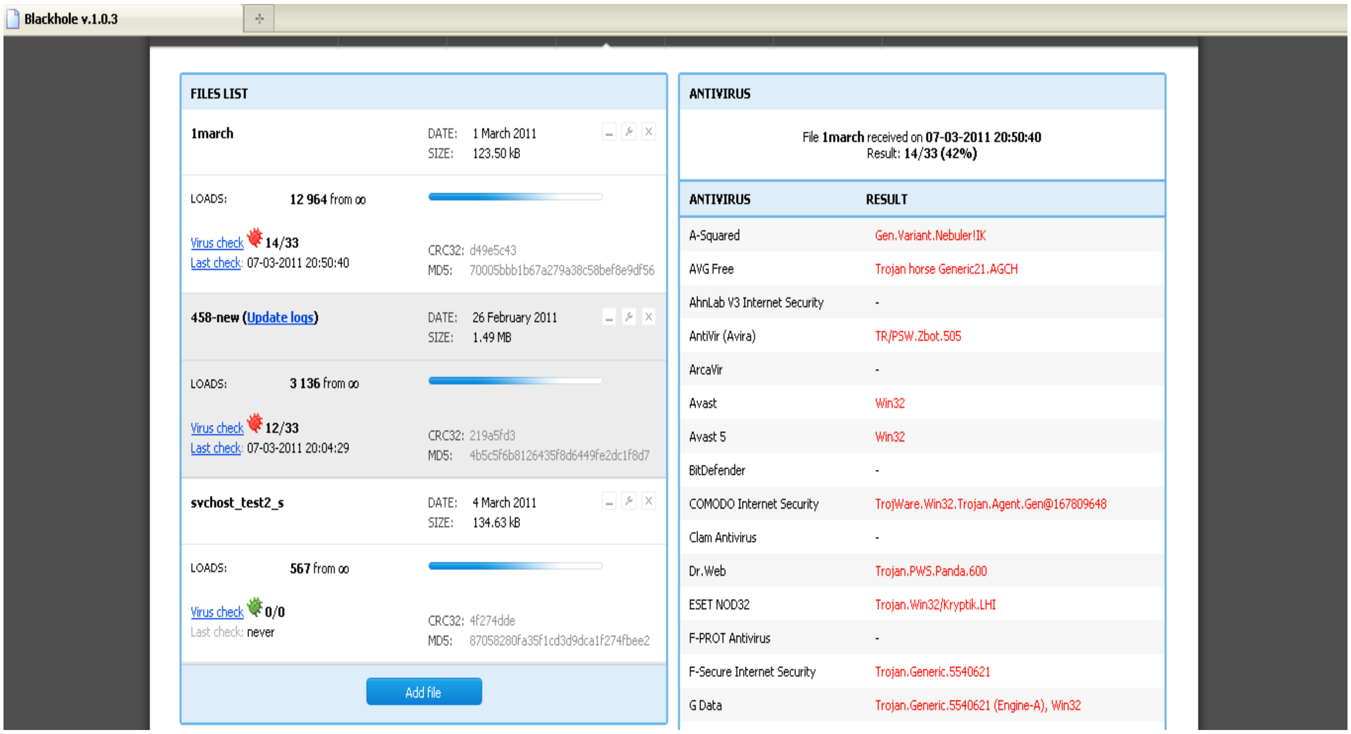
If we zero in on the countries, we see that, from this server, UK was indeed the top target, although from the point of view of percentage of successful loads, India, Thailand and Jordan were actually more successfully attacked. This probably indicates a less-protected population.



COUNTRIES	HITS	HOSTS ↑	LOADS	%
United Kingdom	639901	474589	37036	7.80
United States	79599	62005	4891	7.89
Pakistan	839	723	74	10.24
India	570	470	93	19.79
Other country	418	342	42	12.28
Serbia	348	319	34	10.66
Canada	604	271	23	8.85
Australia	288	253	31	12.35
Thailand	209	188	36	19.15
Greece	141	124	13	10.48
Germany	179	123	15	12.61
Ireland	121	105	16	15.24
Jordan	119	98	19	19.39
Armenia	103	94	9	9.57
Indonesia	102	85	11	12.94

Fig 6: Blackhole Analytics – Geo distribution of infections

Finally, it is interesting to note that this screen shows that the attacker is able to use online virus scanning services to check how well his or her malware is currently being detected. This allows them to switch out their binaries when they start to get well detected.



FILES LIST

1march
DATE: 1 March 2011
SIZE: 123.50 kB
LOADS: **12 964** from ∞
Virus check **14/33**
Last check: 07-03-2011 20:50:40
CRC32: d49e5c43
MD5: 70005bbb1b67a279a38c58bef8e9df56

458-new (Update logs)
DATE: 26 February 2011
SIZE: 1.49 MB
LOADS: **3 136** from ∞
Virus check **12/33**
Last check: 07-03-2011 20:04:29
CRC32: 219a5fd3
MD5: 4b5c5f6b8126435f8d6449fe2dc1f8d7

svchost_test2_s
DATE: 4 March 2011
SIZE: 134.63 kB
LOADS: **567** from ∞
Virus check **0/0**
Last check: never
CRC32: 4f274dde
MD5: 87058280fa35f1cd3d9dca1f274fbee2

ANTIVIRUS

File **1march** received on **07-03-2011 20:50:40**
Result: **14/33 (42%)**

ANTIVIRUS	RESULT
A-Squared	Gen.Variant.Nebuler!IK
AVG Free	Trojan horse Generic21.AGCH
AhnLab V3 Internet Security	-
AntiVir (Avira)	TR/PSW.Zbot.505
ArcaVir	-
Avast	Win32
Avast 5	Win32
BitDefender	-
COMODO Internet Security	TrojWare.Win32.Trojan.Agent.Gen@167809648
Clam Antivirus	-
Dr.Web	Trojan.PWS.Panda.600
ESET NOD32	Trojan.Win32/Kryptik.LHI
F-PROT Antivirus	-
F-Secure Internet Security	Trojan.Generic.5540621
G Data	Trojan.Generic.5540621 (Engine-A), Win32

Fig 7: Blackhole administration panel – detection rate by Av vendors

What’s new about this attack?

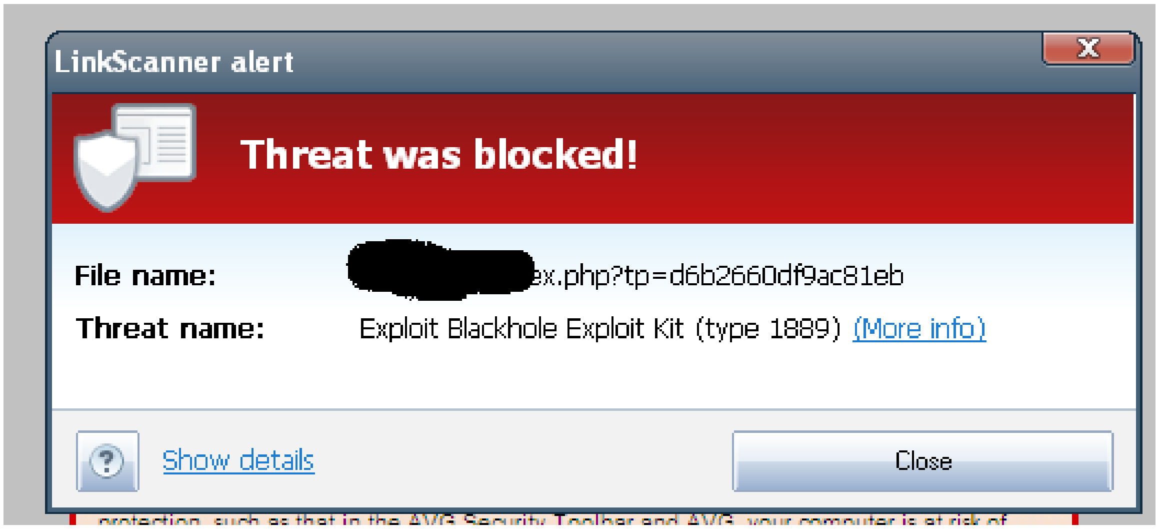
Although the Blackhole exploit kit itself is fairly new, most of the exploits contained in it are pretty run of the mill, and simply copied from other kits. The thing that’s new about this is the size of the attack, and the seemingly targeted nature of it that we have not seen for a while.

How to tell if you were attacked and/or infected.

Our research indicates that the compromised websites these criminals are using to infect users include a large variety of hacked, innocent lures, mixed with some adult websites, and possibly an ad network. The range of innocent lures involved seems to indicate a pretty large hack operation.

What this means is that while some victims were visiting “adult” websites, which is obviously always a risky idea, most victims were simply surfing the web, as many innocent websites have been hacked, and malicious banner ads can come up on any major web property at any time. The ad networks do their best to screen all ads for maliciousness, but the attackers are highly skilled at disguising their intentions until the ad is running.

If you were unlucky enough to encounter this attack, and you were running AVG, you would have seen a popup that showed the attack being blocked.



LinkScanner alert

Threat was blocked!

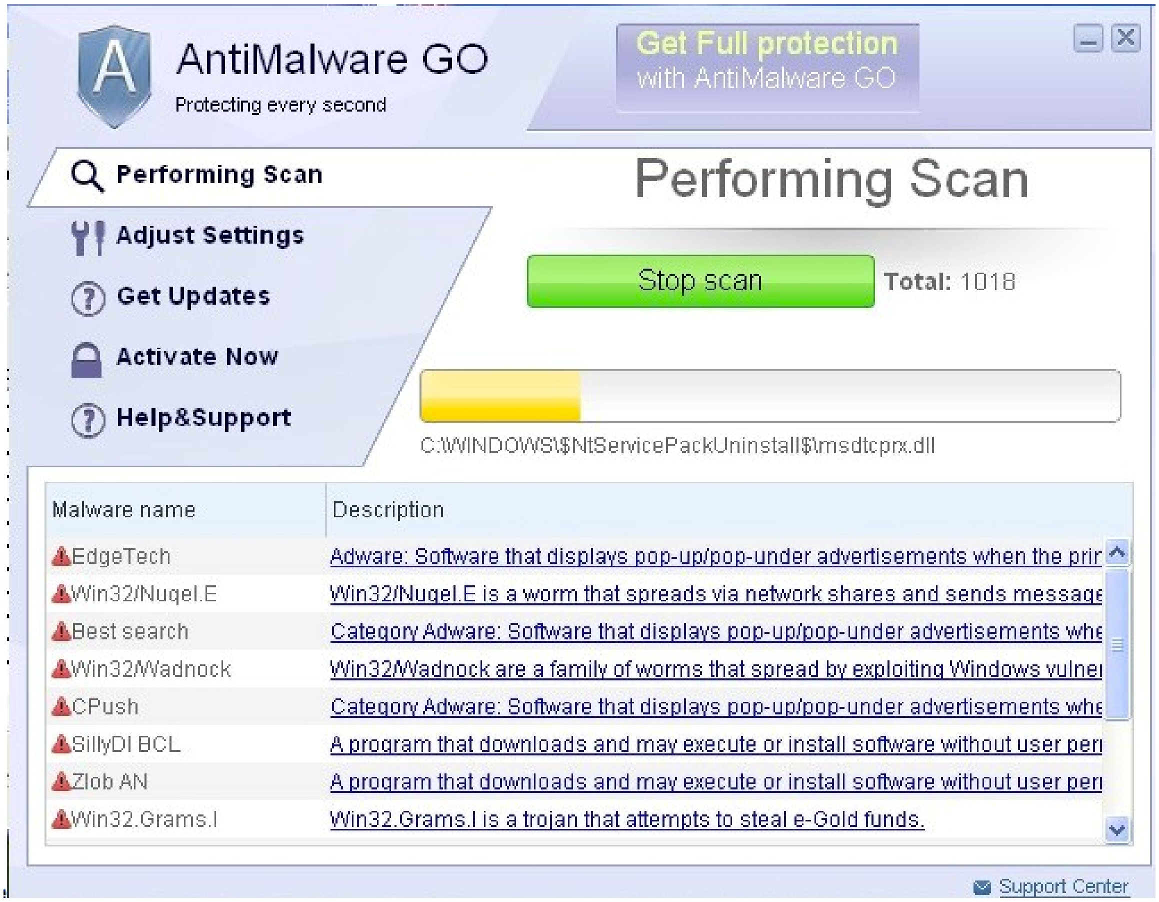
File name: [redacted]x.php?tp=d6b2660df9ac81eb

Threat name: Exploit Blackhole Exploit Kit (type 1889) (More info)

protection, such as that in the AVG Security Toolbar and AVG, your computer is at risk of

Fig 8: AVG Linkscanner detection dialog

If your antivirus wasn’t able to block the attack, then what you saw was something similar to the following screenshot.



Total: 1018

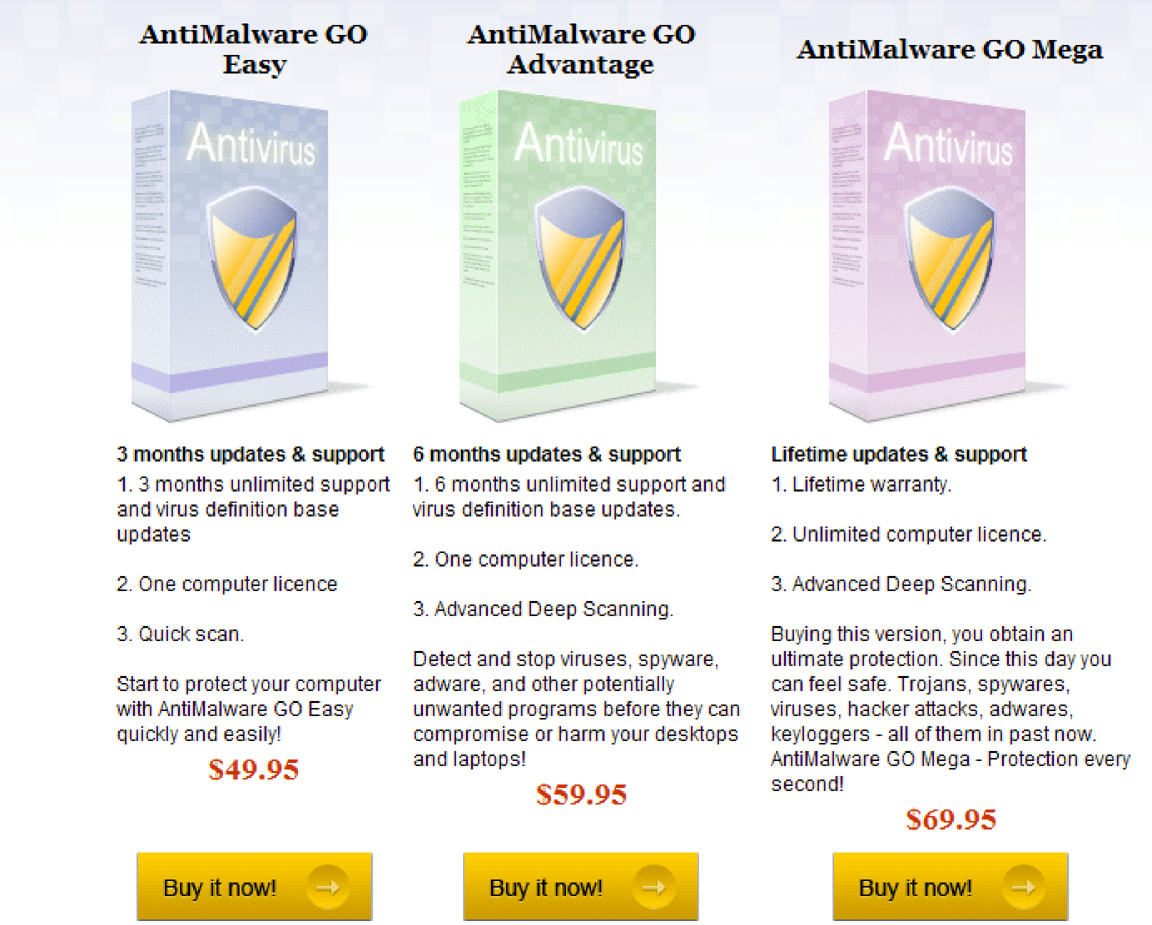
C:\WINDOWS\$NtServicePackUninstall$\msdtcprx.dll

Malware name	Description
EdgeTech	Adware: Software that displays pop-up/pop-under advertisements when the prir
Win32/Nugel.E	Win32/Nugel.E is a worm that spreads via network shares and sends message
Best search	Category Adware: Software that displays pop-up/pop-under advertisements whe
Win32/Wadnock	Win32/Wadnock are a family of worms that spread by exploiting Windows vulner
CPush	Category Adware: Software that displays pop-up/pop-under advertisements whe
SillyDI BCL	A program that downloads and may execute or install software without user peri
Zlob AN	A program that downloads and may execute or install software without user peri
Win32.Grams.I	Win32.Grams.I is a trojan that attempts to steal e-Gold funds.

Fig 9: The rogue antivirus offered by the Blackhole cmapain

This is a typical rogue antivirus attack. It tells you that it’s finding a large number of viruses (that don’t exist) on your computer, and that you need to register (pay) for the software, in order to clean it up.

When you click the Activate Now button, you are taken to a merchant website, where you get to make a choice of three products.



AntiMalware GO Easy

3 months updates & support

1. 3 months unlimited support and virus definition base updates

2. One computer licence

3. Quick scan.

Start to protect your computer with AntiMalware GO Easy quickly and easily!

$49.95

AntiMalware GO Advantage

6 months updates & support

1. 6 months unlimited support and virus definition base updates.

2. One computer licence.

3. Advanced Deep Scanning.

Detect and stop viruses, spyware, adware, and other potentially unwanted programs before they can compromise or harm your desktops and laptops!

$59.95

AntiMalware GO Mega

Lifetime updates & support

1. Lifetime warranty.

2. Unlimited computer licence.

3. Advanced Deep Scanning.

Buying this version, you obtain an ultimate protection. Since this day you can feel safe. Trojans, spywares, viruses, hacker attacks, adwares, keyloggers - all of them in past now. AntiMalware GO Mega - Protection every second!

$69.95

Fig 10: Blackhole rogue AV merchant website

Obviously not everyone who sees this screen will buy, but if you have launched 900,000 attacks, you don't need a terribly high percentage of successes to make some pretty good money. Even a 1% success rate equates to at least $450,000. Not bad for a single day.

What to do if you have been infected

If you do have one of these rogues running on your system, the first thing to is to *not* pay their registration fee / ransom. Instead, back up any data that’s critical to you, install an AVG anti virus product, and let it remove the rogue AV.

After you have cleaned your computer, you should change all your passwords, keep your system patched, and your antivirus up to date.