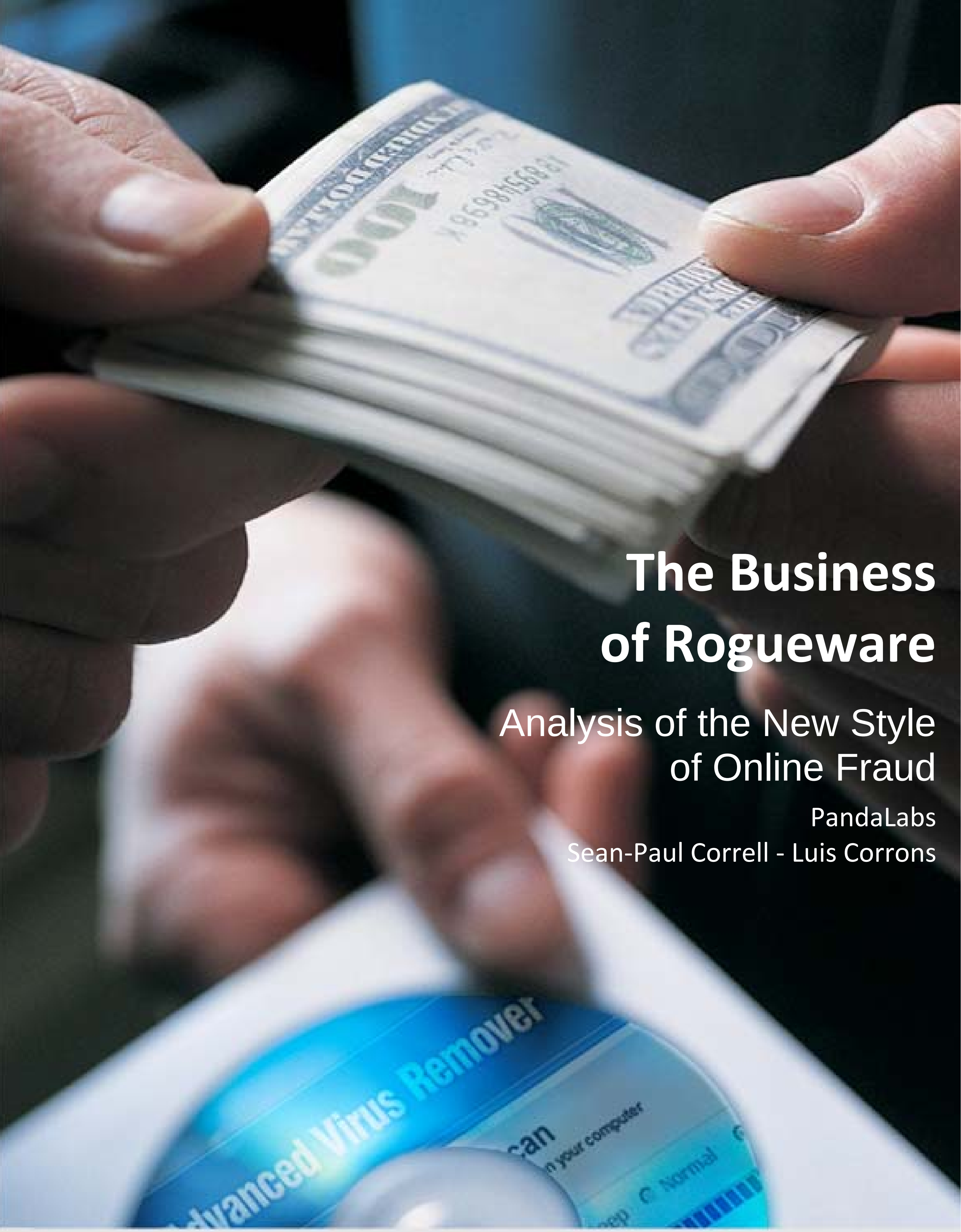


The Business of Rogueware

Analysis of the New Style of Online Fraud

PandaLabs
Sean-Paul Correll - Luis Corrons

PANDA SECURITY | 20th Anniversary 1990-2010

Executive Summary

In recent years, the proliferation of malware has been widespread and the threats have reached staggering proportions. Cybercrime has unfortunately become a part of a hidden framework of our society and behind this growing trend lies a type of malware called rogueware; a breed that is more pervasive and dangerous than threats previously seen by security researchers. Rogueware consists of any kind of fake software solution that attempts to steal money from PC users by luring them into paying to remove nonexistent threats.

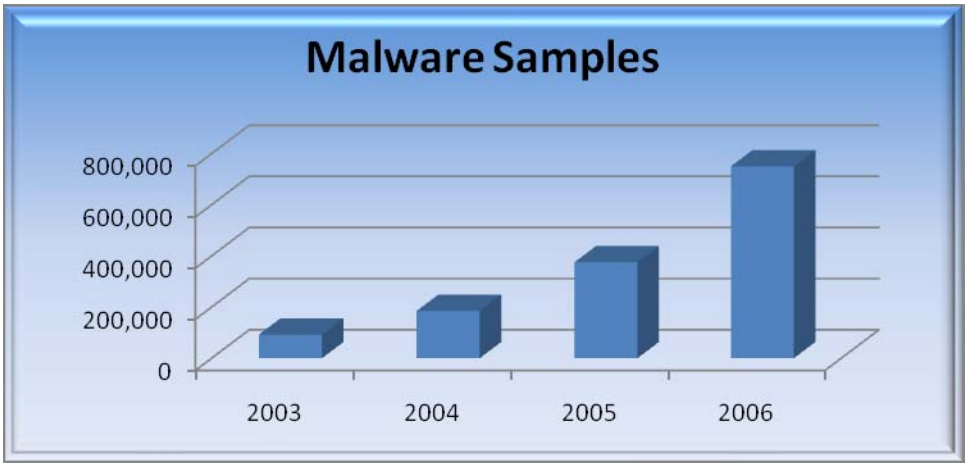
At the end of 2008, PandaLabs detected almost 55,000 rogueware samples. This study seeks to investigate the growing rogueware economy, its astounding growth and the effects it has had thus far.

The study revealed staggering results:

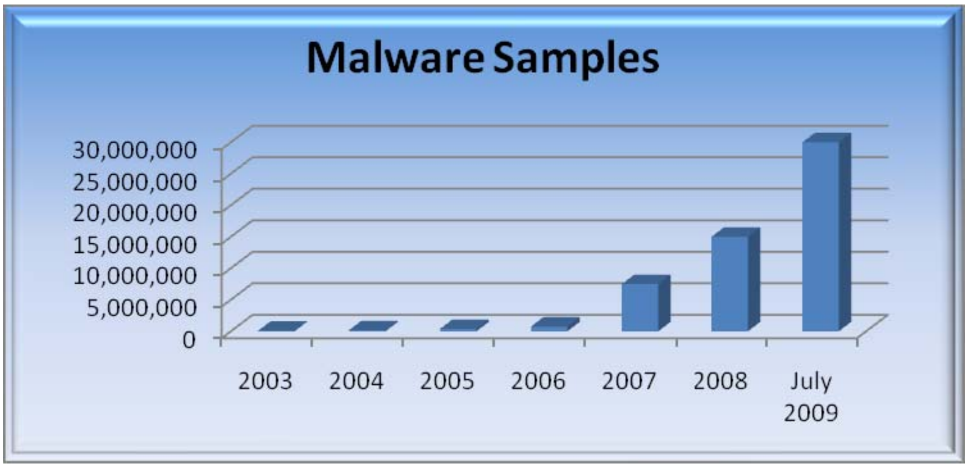
- We predict that we will record more than 637,000 new rogueware samples by the end of Q3 2009, a tenfold increase in less than a year
- Approximately 35 million computers are newly infected with rogueware each month (approximately 3.50 percent of all computers)
- Cybercriminals are earning approximately $34 million per month through rogueware attacks

Background: The History of Malware Growth

Malware has rapidly increased in volume and sophistication over in the past several years. The graph below illustrates the malware landscape from 2003 to 2006 over which the total number of malware samples doubled every year:

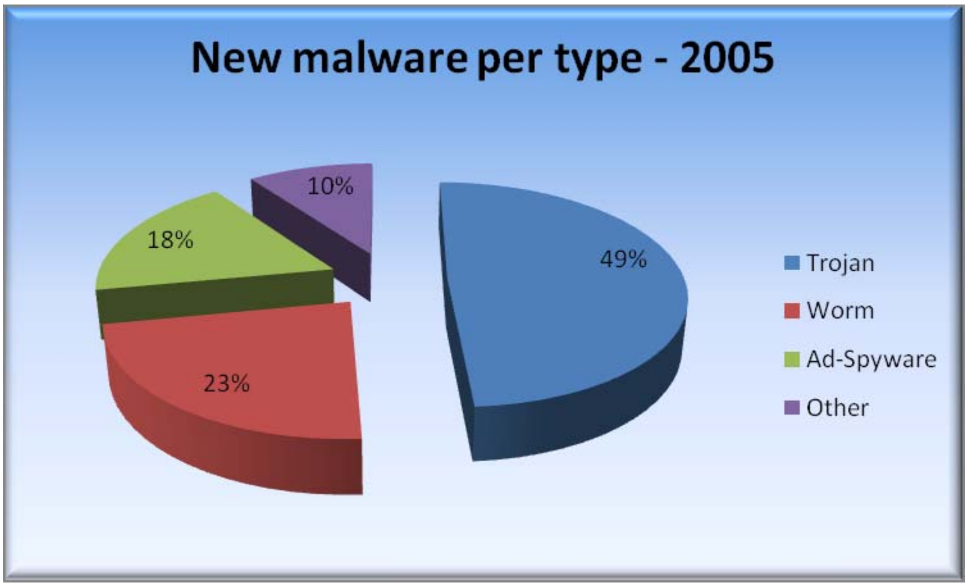


Barely five years ago, just 92,000 total malware strains existed; by the end of 2008, there were approximately 15 million. At the conclusion of this study in July 2009, PandaLabs detected more than **30 million malware samples** in existence.

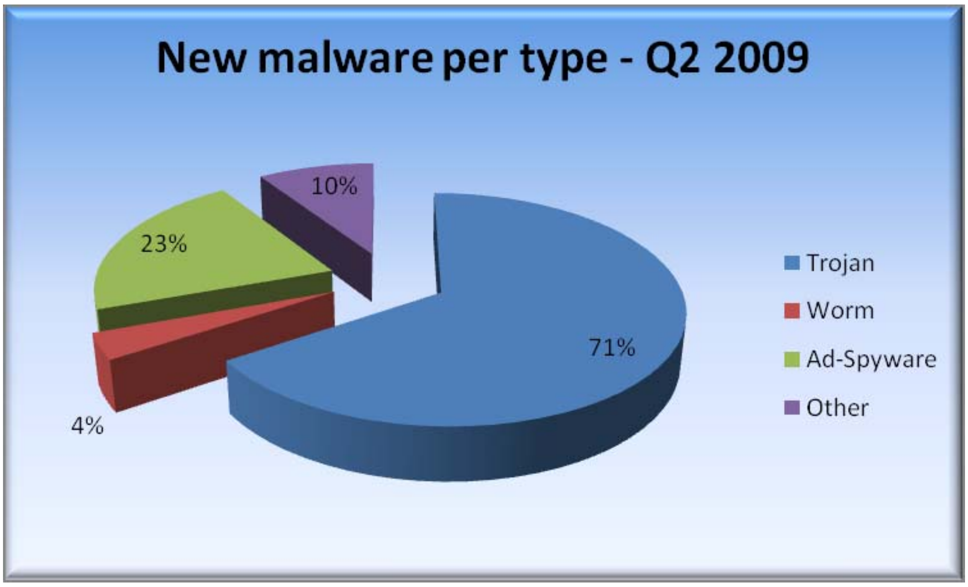


The reason behind this vast increase in malware is clear: money. In 2003, banking Trojans quietly emerged on the scene. These malicious codes, designed to steal online banking credentials, now rank among the most common forms of malware. Every day, we see new variants that have evolved technologically in order to evade the security measures banks have implemented. Organizations such as the Anti-Phishing Working Group (www.antiphishing.org) have brought industry players together to thwart the efforts of cybercriminals. Still, it's been an upward battle and it remains unclear if it’s a battle that can ever be won.

Overall, more Trojans, keyloggers and bots are created than any other type of malicious code because they are the most useful in committing identity theft. Looking back to 2005, almost half the new malicious codes that emerged were Trojans:



Now, in the second quarter of 2009, the situation is far worse and 71 percent of malware are Trojans:



As with any business, cyber-criminals look to operate as efficiently as possible. When developing a Trojan, they must decide what platform it will support and the potential number of individuals they will be to victimize. Windows is consequently targeted in more than 99 percent of cyber-criminal cases, with it being the most widely used platform to date.

The ultimate goal of cyber-criminals is to profit from the malware. While Trojans are adept at stealing information, this stolen information still must to be turned into hard cash and cyber-criminals must find innovative methods to accomplish this.

Enter fake antivirus programs. These applications pass themselves off as antivirus products, and claim to detect hundreds of threats on their victims' computers. When users try to eliminate the threats with the application, they are then asked to purchase a corresponding license. Users, naturally worried about the supposed infection, will often buy the license. Once they have handed over the money, they will no longer hear from the 'vendors' and the fake antivirus will remain on their computers.

These applications have been in circulation for several years, but it wasn't until early 2008 that cybercriminals adopted fake antivirus on a massive scale.

Rogueware

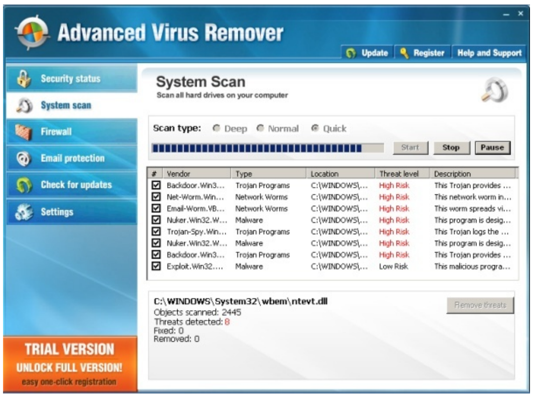
The Effects of Fake Antivirus Programs: Warning Signs of Rogueware

In addition to taking money from consumers and delivering the antithesis of security protection, many fake antivirus programs share a number of commonalities:

- They display fake pop-up warnings, launch messages in the task bar and make changes to the screensaver and desktop
- Their design is similar to that of a real antivirus
- They complete scanning of the entire system very quickly
- The 'infections' detected often refer to different files on each scan

Fake antivirus programs also make a series of alterations to the operating system in order to prevent their fake warnings from being removed. This includes hiding the Desktop and Screensaver tabs from the Display properties section. This way, users cannot restore the desktop theme or the screensaver. The purpose of these techniques is to exhaust the users' patience so that they finally register the product and pay the corresponding fee.

Below is a series of rogueware examples and the respective pay-platforms to which users are directed when they try to 'disinfect' their systems:

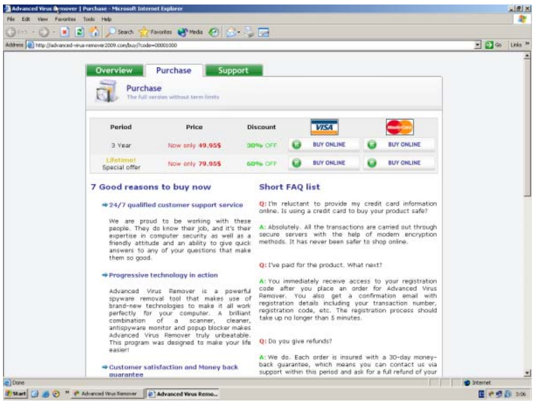


System Scan
Scan all hard drives on your computer

Scan type: ○ Deep ○ Normal ● Quick

#	Vendor	Type	Location	Threat level	Description
☑	Backdoor.Win3...	Trojan Programs	C:\WINDOWS\...	High Risk	This Trojan provides ...
☑	Net-Worm.Win...	Network Worms	C:\WINDOWS\...	High Risk	This network worm in...
☑	Email-Worm.VB...	Network Worms	C:\WINDOWS\...	High Risk	This worm spreads vi...
☑	Nuker.Win32.W...	Malware	C:\WINDOWS\...	High Risk	This program is desig...
☑	Trojan-Spy.Win...	Trojan Programs	C:\WINDOWS\...	High Risk	This Trojan logs the ...
☑	Nuker.Win32.W...	Malware	C:\WINDOWS\...	High Risk	This program is desig...
☑	Backdoor.Win3...	Trojan Programs	C:\WINDOWS\...	High Risk	This Trojan provides ...
☑	Exploit.Win32....	Malware	C:\WINDOWS\...	Low Risk	This malicious progra...

C:\WINDOWS\System32\wbem\ntevt.dll
Objects scanned: 2445
Threats detected: 8
Fixed: 0
Removed: 0



Address http://advanced-virus-remover2009.com/buy/?code=00001000

Purchase
The full version without term limits

Period	Price	Discount	VISA	MasterCard
3 Year	Now only 49.95$	30% OFF	BUY ONLINE	BUY ONLINE
Lifetime! Special offer	Now only 79.95$	60% OFF	BUY ONLINE	BUY ONLINE

7 Good reasons to buy now

➔ 24/7 qualified customer support service

We are proud to be working with these people. They do know their job, and it's their expertise in computer security as well as a friendly attitude and an ability to give quick answers to any of your questions that make them so good.

➔ Progressive technology in action

Advanced Virus Remover is a powerful spyware removal tool that makes use of brand-new technologies to make it all work perfectly for your computer. A brilliant combination of a scanner, cleaner, antispyware monitor and popup blocker makes Advanced Virus Remover truly unbeatable. This program was designed to make your life easier!

➔ Customer satisfaction and Money back guarantee

Short FAQ list

Q: I'm reluctant to provide my credit card information online. Is using a credit card to buy your product safe?

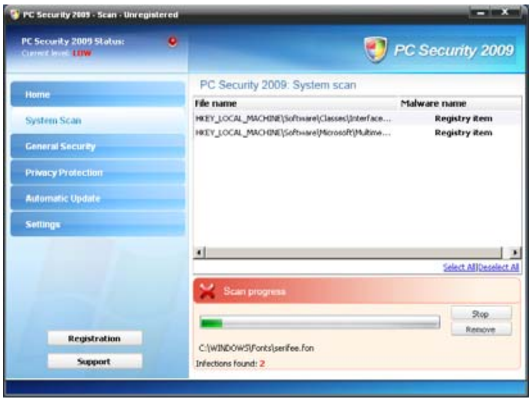
A: Absolutely. All the transactions are carried out through secure servers with the help of modern encryption methods. It has never been safer to shop online.

Q: I've paid for the product. What next?

A: You immediately receive access to your registration code after you place an order for Advanced Virus Remover. You also get a confirmation email with registration details including your transaction number, registration code, etc. The registration process should take up no longer than 5 minutes.

Q: Do you give refunds?

A: We do. Each order is insured with a 30-day money-back guarantee, which means you can contact us via support within this period and ask for a full refund of your

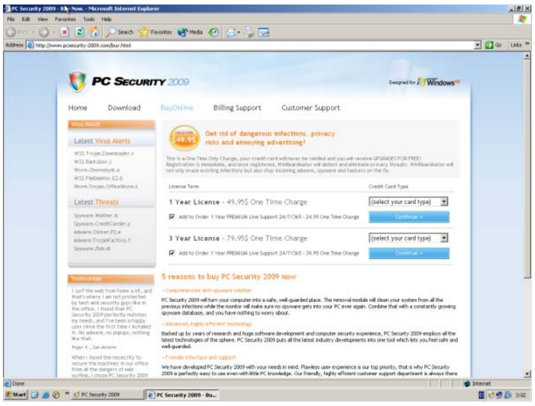


PC Security 2009 Status:
Current level: LOW

PC Security 2009: System scan

File name	Malware name
HKEY_LOCAL_MACHINE\Software\Classes\Interface...	Registry item
HKEY_LOCAL_MACHINE\Software\Microsoft\Multime...	Registry item

C:\WINDOWS\Fonts\serifee.fon
Infections found: 2



Address http://www.pcsecurity-2009.com/buy.html

Latest Virus Alerts
W32.Trojan.Downloader.i
W32.Backdoor.j
Worm.Chernobyl6.a
W32.FileDeleter.E2.b
Worm.Trojan.OfficeWorm.k

Latest Threats
Spyware.Wather.ic
Spyware.CreditCarder.y
Adware.Clicker.P2.e
Adware.TrojanFactory.f
Spyware.Zlob.dl

Get rid of dangerous infections, privacy risks and annoying advertising!

This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE! Registration is immediate, and once registered, WinReanimator will detect and eliminate privacy threats. WinReanimator will not only erase existing infections but also stop incoming adware, spyware and hackers on the fly.

License Term	Credit Card Type
1 Year License - 49.95$ One Time Charge	(select your card type)
☑ Add to Order 1 Year PREMIUM Live Support 24/7/365 - 24.95 One Time Charge	Continue »
3 Year License - 79.95$ One Time Charge	(select your card type)
☑ Add to Order 1 Year PREMIUM Live Support 24/7/365 - 39.95 One Time Charge	Continue »

5 reasons to buy PC Security 2009 now:

- Comprehensive anti-spyware solution

PC Security 2009 will turn your computer into a safe, well-guarded place. The removal module will clean your system from all the previous infections while the monitor will make sure no spyware gets into your PC ever again. Combine that with a constantly growing spyware database, and you have nothing to worry about.

- Advanced, highly efficient technology

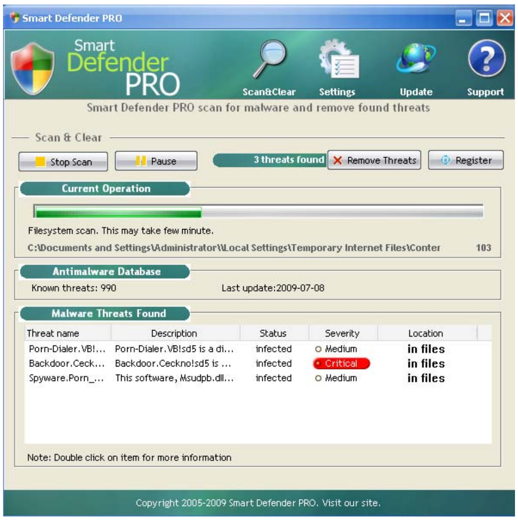
Backed up by years of research and huge software development and computer security experience, PC Security 2009 employs all the latest technologies of the sphere. PC Security 2009 puts all the latest industry developments into one tool which lets you feel safe and well-guarded.

- Friendly interface and support

We have developed PC Security 2009 with your needs in mind. Flawless user experience is our top priority, that is why PC Security 2009 is perfectly easy to use even with little PC knowledge. Our friendly, highly efficient customer support department is always there

I surf the web from home a lot, and that's where I am not protected by tech and security guys like in the office. I found that PC Security 2009 perfectly matches my needs, and I've been a happy user since the first time I installed it. No adware, no popups, nothing like that.
Roger K., San-Antonio

When I faced the necessity to secure the machines in our office from all the dangers of web surfing, I chose PC Security 2009



Smart Defender PRO scan for malware and remove found threats

Scan & Clear

Stop Scan | Pause | 3 threats found | Remove Threats | Register

Current Operation

Filesystem scan. This may take few minute.

C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Conter 103

Antimalware Database

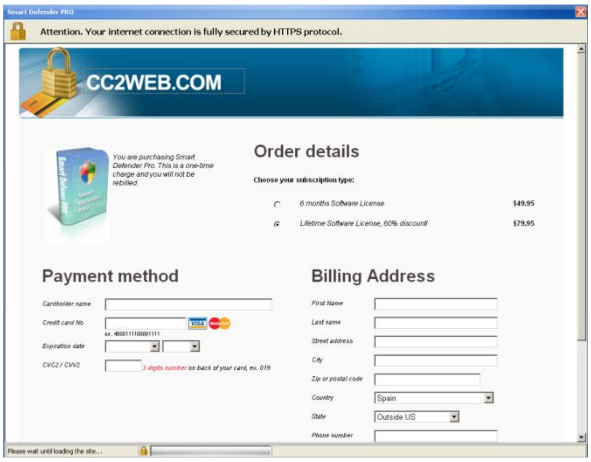
Known threats: 990 Last update:2009-07-08

Malware Threats Found

Threat name	Description	Status	Severity	Location
Porn-Dialer.VB!...	Porn-Dialer.VB!sd5 is a di...	infected	○ Medium	in files
Backdoor.Ceck...	Backdoor.Ceckno!sd5 is ...	infected	● Critical	in files
Spyware.Porn_...	This software, Msudpb.dll...	infected	○ Medium	in files

Note: Double click on item for more information

Copyright 2005-2009 Smart Defender PRO. Visit our site.



Attention. Your internet connection is fully secured by HTTPS protocol.

CC2WEB.COM

You are purchasing Smart Defender Pro. This is a one-time charge and you will not be rebilled.

Order details

Choose your subscription type:

○	6 months Software License	$49.95
●	Lifetime Software License, 60% discount!	$79.95

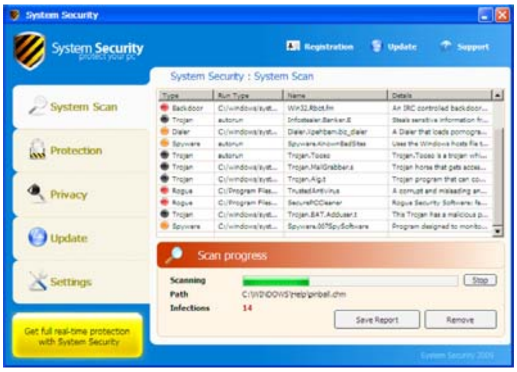
Payment method

Cardholder name
Credit card No
ex. 4000111100001111
Expiration date
CVC2 / CVV2 — 3 digits number on back of your card, ex. 019

Billing Address

First Name
Last name
Street address
City
Zip or postal code
Country: Spain
State: Outside US
Phone number

Please wait until loading the site...

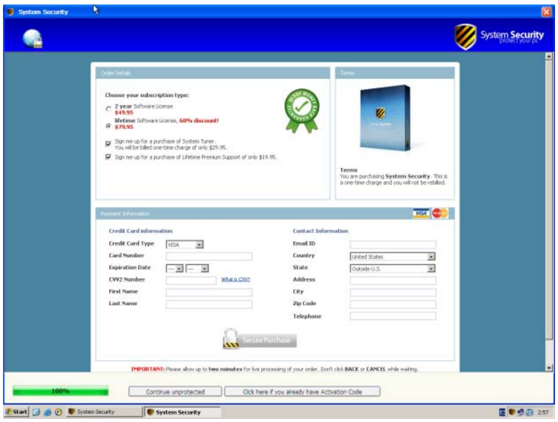


System Security : System Scan

Type	Run Type	Name	Details
Backdoor	C:/windows/syst...	Win32.Rbot.fm	An IRC controlled backdoor...
Trojan	autorun	Infostealer.Banker.E	Steals sensitive information fr...
Dialer	C:/windows/syst...	Dialer.Xpehbam.biz_dialer	A Dialer that loads pornogra...
Spyware	autorun	Spyware.KnownBadSites	Uses the Windows hosts file t...
Trojan	autorun	Trojan.Tooso	Trojan.Tooso is a trojan whi...
Trojan	C:/windows/syst...	Trojan.MailGrabber.s	Trojan horse that gets acces...
Trojan	C:/windows/syst...	Trojan.Alg.t	Trojan program that can co...
Rogue	C:/Program Files...	TrustedAntivirus	A corrupt and misleading an...
Rogue	C:/Program Files...	SecurePCCleaner	Rogue Security Software: fa...
Trojan	C:/windows/syst...	Trojan.BAT.Adduser.t	This Trojan has a malicious p...
Spyware	C:/windows/syst...	Spyware.007SpySoftware	Program designed to monito...

Scan progress

Scanning
Path C:\WINDOWS\Help\pinball.chm
Infections 14



Order Details

Choose your subscription type:

○ 2 year Software License $49.95
● lifetime Software License, 60% discount! $79.95

☑ Sign me up for a purchase of System Tuner. You will be billed one-time charge of only $29.95.
☑ Sign me up for a purchase of Lifetime Premium Support of only $19.95.

Terms

Terms
You are purchasing System Security. This is a one-time charge and you will not be rebilled.

Payment Information

Credit Card information
Credit Card Type: VISA
Card Number
Expiration Date: -- --
CVV2 Number — What is CVV?
First Name
Last Name

Contact Information
Email ID
Country: United States
State: Outside U.S.
Address
City
Zip Code
Telephone

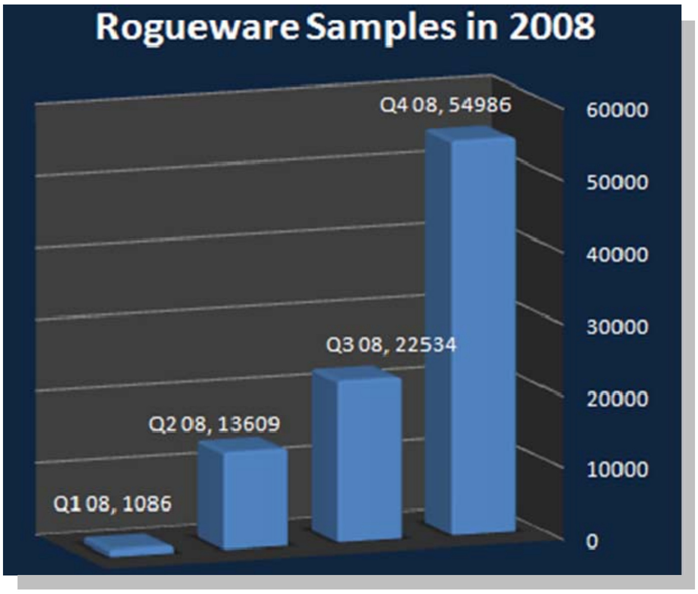
IMPORTANT: Please allow up to two minutes for live processing of your order. Don't click BACK or CANCEL while waiting.

System Security
System Security protect your pc
30 DAY MONEY BACK GUARANTEE
Secure Purchase
100%
Continue unprotected
Click here if you already have Activation Code
Start
System Security
System Security
2:57

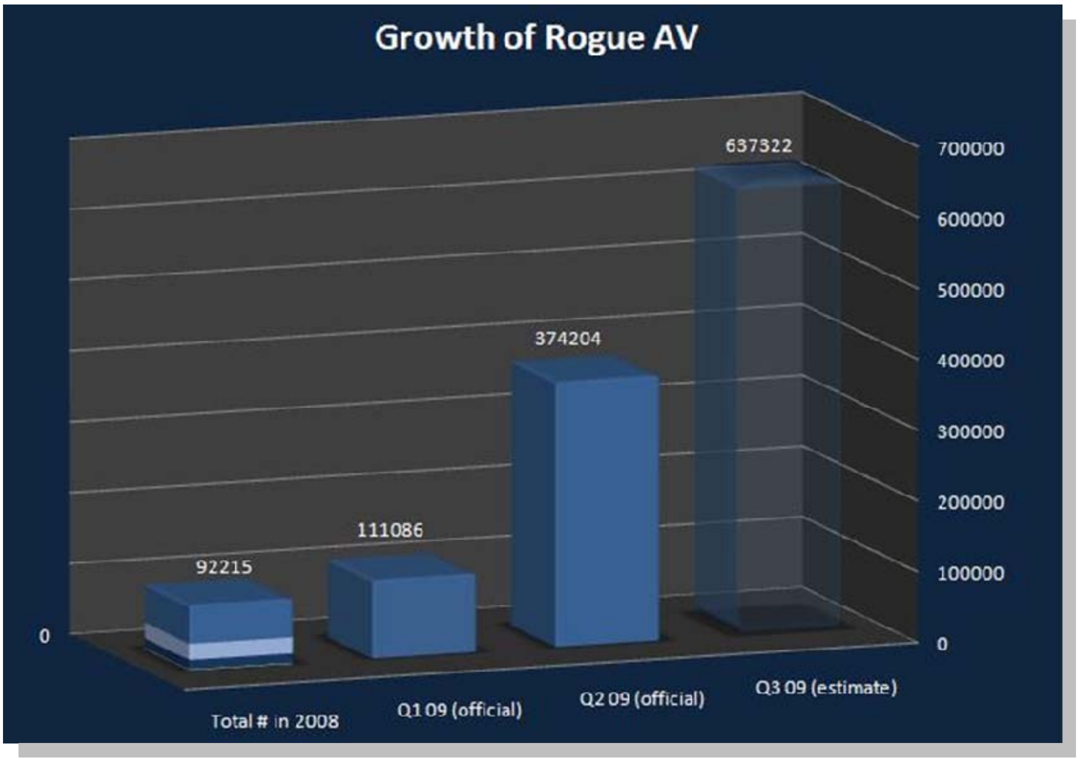
Cyber-criminals no longer need to steal users' information in order to make their money; instead, they simply need to find ways to get users to part with their cash voluntarily. As shown above, rogue antivirus programs' interfaces are carefully crafted and extremely convincing, indicating that cyber-criminals are spending enormous amounts of time and effort developing and distributing these programs. They also employ aggressive techniques, aiming to frighten users into buying the license.

Evolution of Rogue AV from 2008 to Q2 2009, and Predictions for the Future

Fake antivirus is experiencing an exponential growth. In the second quarter of 2008, PandaLabs created a specialized team to detect and eliminate this type of malware. The following graph illustrates the growth of fake antivirus programs over the course of 2008:



The number of samples grew exponentially, and the progression through 2009, as evidenced below demonstrates an even greater growth curve:

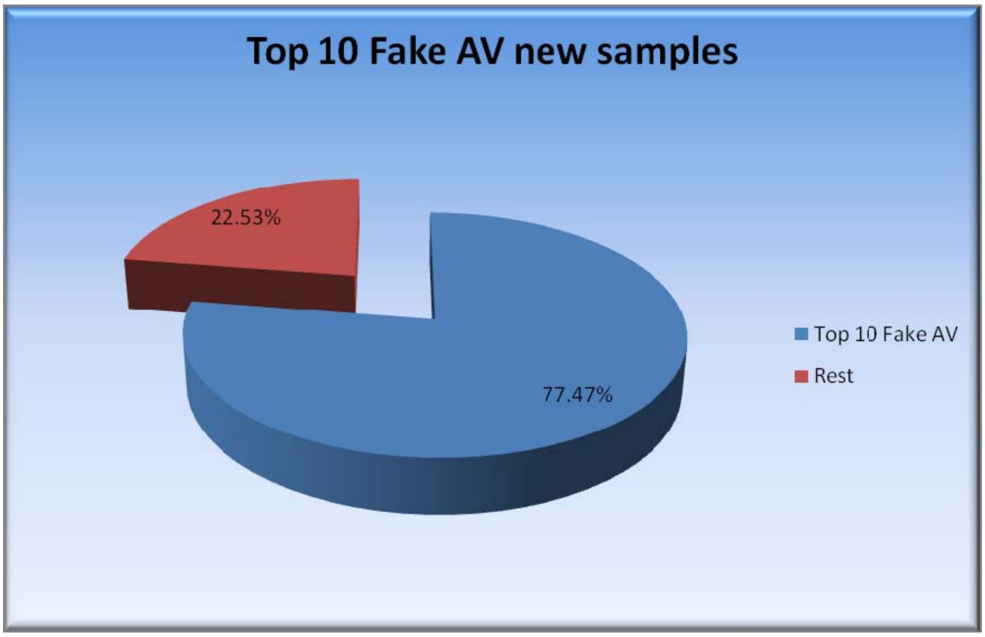


In the first quarter of 2009 alone, more new strains were created than in all of 2008. The second quarter painted an even bleaker picture, with the emergence of four times as many samples as in all of 2008. In the third quarter, PandaLabs estimates a malware total greater than the previous eighteen months combined.

The primary reason for the creation of so many variants is to avoid signature-based detection by (legitimate) antivirus programs. The use of behavioral analysis, which works well with worms and Trojans, is of limited use in this type of malware because the programs themselves do not act maliciously on computers, other than displaying false information.

Several methods are being used to create the many variants. One of the most widespread techniques is known as server-side polymorphism, which means every time the fake antivirus is downloaded it is a different binary file.

Although there are approximately 200 different families of rogueware, extrapolating the data from Q2 2009 found that 10 of these families are responsible for 77.47 percent of the variants:



Taking a look at the Top 20 families in the past six months, the number amounts to approximately 90 percent of all malware samples:

Fake Antivirus	Number of samples	%
SystemSecurity	70883	18.94%
SystemGuard2009	38927	10.40%
Xpantivirus2008	33233	8.88%
WinPcDefender	32749	8.75%
Antivirus2009	29666	7.93%
SpywareGuard2008	24323	6.50%
XPPolice	20151	5.39%
AntivirusXPPro	19536	5.22%
SystemSecurity2009	10265	2.74%
MSAntiSpyware2009	10191	2.72%
SecuritySystem	9512	2.54%
ProAntispyware2009	8628	2.31%
RogueAntimalware2009	7382	1.97%
MalwareDefender2009	6120	1.64%
PCProtectionCenter2008	4949	1.32%
VirusResponseLab2009	4409	1.18%
VirusShield2009	4218	1.13%
WinDefender2009	4038	1.08%
VirusRemover2008	3242	0.87%
AdvancedVirusRemover	2931	0.78%

Rogue infections in H1 2009

The number of variants does not necessarily correspond to the proportion of computers infected by fake antivirus programs. To verify exactly how widespread they are, PandaLabs generated infection ratios from its statistics servers and found that from the global infection data for 2009 approximately 98 percent of all computers scanned were infected.

PandaLabs then proceeded to take details from all computers infected by fake antivirus programs and found that 3.50 percent of all the computers scanned each month were infected with this rogueware. As explained earlier, the massive creation of new variants is made to avoid antivirus detection, so the most infectious families do not necessarily have to be the more prolific.

The following chart represents the Top 20 fake antivirus families in the last six months that comprised 81.67 percent of all rogueware related infections detected by PandaLabs. Those highlighted in red are also in the Top 20 with the most samples:

1	**Antivirus2009**	**15.89%**
2	**VirusRemover2008**	**9.90%**
3	**Xpantivirus2008**	**8.52%**
4	**XPAntiSpyware2009**	**6.13%**
5	**SystemGuard2009**	**5.26%**
6	**SpywareRemover2009**	**4.34%**
7	**Antivirus360**	**3.88%**
8	**RealAntivirus**	**3.57%**
9	**RogueAntimalware2008**	**3.45%**
10	**SystemSecurity**	**3.42%**
11	**SpywareGuard2008**	**2.67%**
12	**AntivirusPro2009**	**2.39%**
13	**AntivirusXP2008**	**2.04%**
14	**MSAntiSpyware2009**	**1.87%**
15	**RogueAntimalware2009**	**1.69%**
16	**AntivirusXPPro**	**1.67%**
17	**ProAntispyware2009**	**1.57%**
18	**SecurityCenter**	**1.38%**
19	**AntiMalwareSuite**	**1.02%**
20	**Antispy2008**	**1.00%**

The Financial Ramifications

Given the rapid growth of rogueware and its sole purpose of financial gain, PandaLabs sought to quantify the economic effect of this type of malware on the global economy. Using existing industry estimates, PandaLabs extrapolated information and estimated the following figures to demonstrate the financial consequences of rogueware. According to analyst firm, Forrester Research, there are approximately 1 billion computers worldwide. Based on this figure, PandaLabs estimates that approximately 35 million, or 3.5 percent of all computers, are infected with rogueware each month. We shouldn't translate this into 35 million people being infected, since there are people that manage a different computer at home and at work. Given this variable, let's assume half of this amount are actual users: 17,500,000.

Another industry research analyst firm, Gartner Group, has projected that 3.30 percent of people are losing money due to phishing, where victims are sending their banking information to phishers. Rogueware is much more aggressive and deceptive than phishing, and there have been no studies to date that investigate how many people are being fooled into purchasing fake antivirus "software" to eliminate infections that do not actually exist. Since there is no hard evidence available, PandaLabs estimated that based on the Gartner figure of 3.30 percent of users paying for phishing, 557,500 users are buying rogueware each month. It is important to note that the techniques used by rogueware are much more aggressive, so it is likely that Gartner's forecast is higher.

The price of each rogueware application varies, but in general there are two types of licenses:

- The least expensive is $49.95
- The most expensive is $79.95

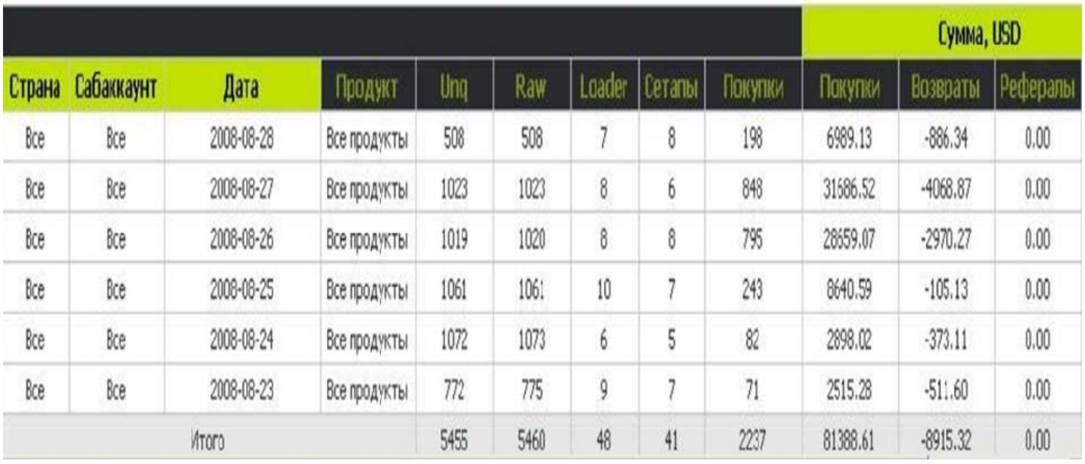
Using these figures and assuming that 2/3 of the people will buy the $49.95 option, the average price is $59.95, PandaLabs estimated that cybercriminals are profiting more than $34 million per month from rogueware campaigns.

$59.95 * 557,000 = $34,621,125 ← PER MONTH

$34 million per month translates into more than $415 million in economic loss per year.

A Look Inside of the Rogueware Business

In September of 2008, a hacker going by the handle “NeoN” was able to infiltrate Bakasoftware (a major Rogueware manufacturer) by exploiting SQL injection vulnerabilities on their website. The hacker was able to reveal key information about the way Bakasoftware conducted its business, and for the first time, we were able to see the real damage the Rogueware business was causing.

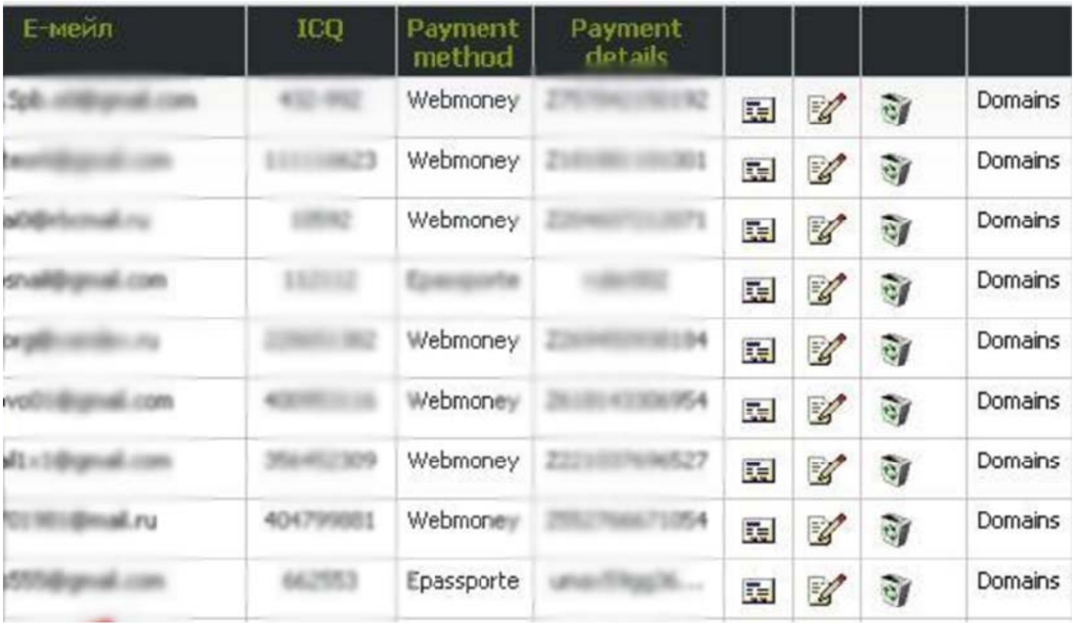


									Сумма, USD		
Страна	Сабаккаунт	Дата	Продукт	Unq	Raw	Loader	Сетапы	Покупки	Покупки	Возвраты	Рефералы
Все	Все	2008-08-28	Все продукты	508	508	7	8	198	6989.13	-886.34	0.00
Все	Все	2008-08-27	Все продукты	1023	1023	8	6	848	31686.52	-4068.87	0.00
Все	Все	2008-08-26	Все продукты	1019	1020	8	8	795	28659.07	-2970.27	0.00
Все	Все	2008-08-25	Все продукты	1061	1061	10	7	243	8640.59	-105.13	0.00
Все	Все	2008-08-24	Все продукты	1072	1073	6	5	82	2898.02	-373.11	0.00
Все	Все	2008-08-23	Все продукты	772	775	9	7	71	2515.28	-511.60	0.00
Итого				5455	5460	48	41	2237	81388.61	-8915.32	0.00

A six-day sales capture of a top selling affiliate for Baka revealed an $81,388.61 USD earning period, which means that if the sales were sustained over several weeks, the earnings for this one individual would be close to $400,000 USD per month. That’s almost $5,000,000 per year and it’s an astronomical number considering that this projection is just for one of many affiliates in Baka’s roster, not to mention that the rogueware business has grown about four times the size it was in 2008 (in terms of sample volume).

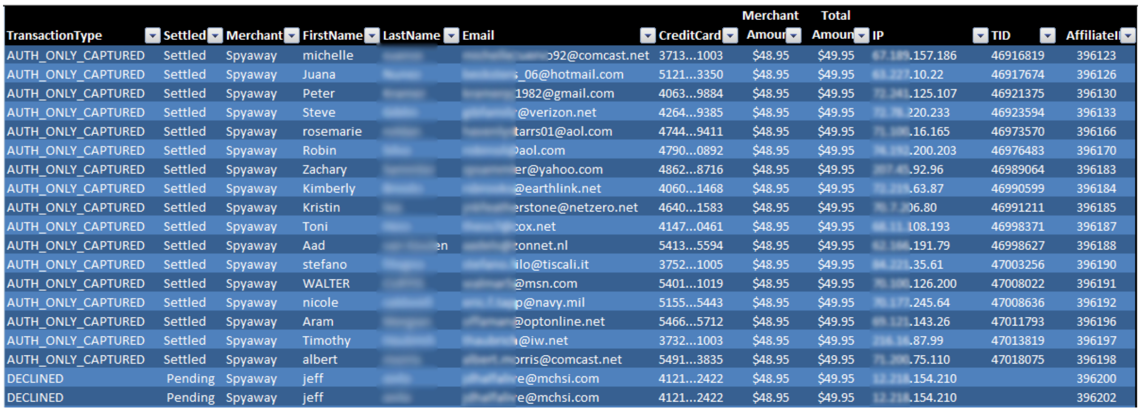
The Affiliate System

The Rogueware business model consists of two major parts: program creators and distributors. The creators are in charge of making the rogue applications, providing the distribution platforms, payment gateways, and other back office services. The affiliates are in charge of distributing the scareware to as many people and as quickly as possible.



E-мейл	ICQ	Payment method	Payment details				
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	[redacted]	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Webmoney	[redacted]	▤	✎	🗑	Domains
[redacted]	[redacted]	Epassporte	[redacted]	▤	✎	🗑	Domains

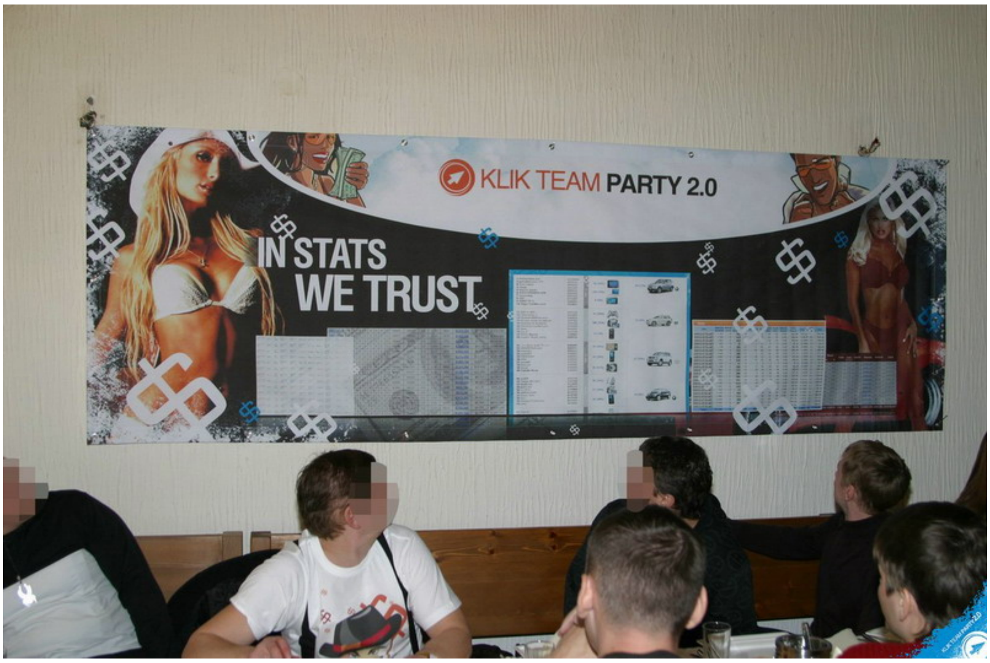
The affiliates are mostly comprised of eastern Europeans recruited from underground hacking forums. They earn a variable amount per each install and between 50-90 percent commissions for completed sales. Webmoney seems to be the payment collection method of choice, but Epassporte is used as well. After recruitment, the affiliate provides their payment method of choice and contact details, such as e-mail and ICQ number to stay in contact. Once the affiliate is entered into the system, they are assigned a unique identifier to be appended to the end of each malware distribution domain, which allows for the sales to be tracked. (E.g. http://www.rogueware.com/index.php?aid=1200)

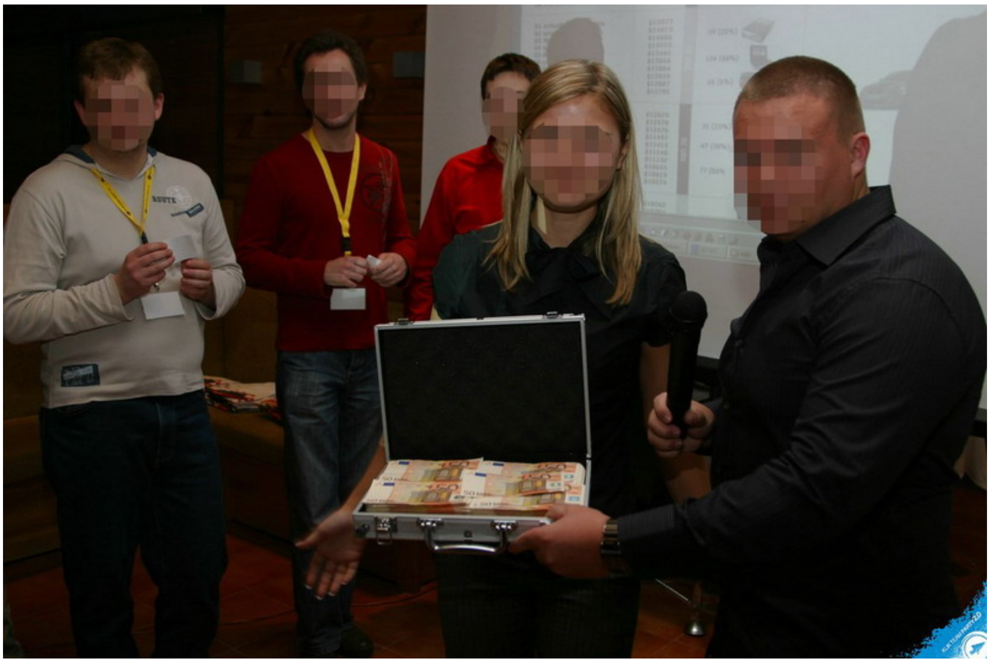


TransactionType	Settled	Merchant	FirstName	LastName	Email	CreditCard	Merchant Amoun	Total Amoun	IP	TID	AffiliateI
AUTH_ONLY_CAPTURED	Settled	Spyaway	michelle	[redacted]	[redacted]92@comcast.net	3713...1003	$48.95	$49.95	[redacted].157.186	46916819	396123
AUTH_ONLY_CAPTURED	Settled	Spyaway	Juana	[redacted]	[redacted]_06@hotmail.com	5121...3350	$48.95	$49.95	[redacted].10.22	46917674	396126
AUTH_ONLY_CAPTURED	Settled	Spyaway	Peter	[redacted]	[redacted]1982@gmail.com	4063...9884	$48.95	$49.95	[redacted].125.107	46921375	396130
AUTH_ONLY_CAPTURED	Settled	Spyaway	Steve	[redacted]	[redacted]@verizon.net	4264...9385	$48.95	$49.95	[redacted]220.233	46923594	396133
AUTH_ONLY_CAPTURED	Settled	Spyaway	rosemarie	[redacted]	[redacted]tarrs01@aol.com	4744...9411	$48.95	$49.95	[redacted].16.165	46973570	396166
AUTH_ONLY_CAPTURED	Settled	Spyaway	Robin	[redacted]	[redacted]aol.com	4790...0892	$48.95	$49.95	[redacted].200.203	46976483	396170
AUTH_ONLY_CAPTURED	Settled	Spyaway	Zachary	[redacted]	[redacted]er@yahoo.com	4862...8716	$48.95	$49.95	[redacted].92.96	46989064	396183
AUTH_ONLY_CAPTURED	Settled	Spyaway	Kimberly	[redacted]	[redacted]@earthlink.net	4060...1468	$48.95	$49.95	[redacted].63.87	46990599	396184
AUTH_ONLY_CAPTURED	Settled	Spyaway	Kristin	[redacted]	[redacted]erstone@netzero.net	4640...1583	$48.95	$49.95	[redacted]06.80	46991211	396185
AUTH_ONLY_CAPTURED	Settled	Spyaway	Toni	[redacted]	[redacted]cox.net	4147...0461	$48.95	$49.95	[redacted]108.193	46998371	396187
AUTH_ONLY_CAPTURED	Settled	Spyaway	Aad	[redacted]en	[redacted]zonnet.nl	5413...5594	$48.95	$49.95	[redacted].191.79	46998627	396188
AUTH_ONLY_CAPTURED	Settled	Spyaway	stefano	[redacted]	[redacted]ilo@tiscali.it	3752...1005	$48.95	$49.95	[redacted].35.61	47003256	396190
AUTH_ONLY_CAPTURED	Settled	Spyaway	WALTER	[redacted]	[redacted]@msn.com	5401...1019	$48.95	$49.95	[redacted].126.200	47008022	396191
AUTH_ONLY_CAPTURED	Settled	Spyaway	nicole	[redacted]	[redacted]p@navy.mil	5155...5443	$48.95	$49.95	[redacted].245.64	47008636	396192
AUTH_ONLY_CAPTURED	Settled	Spyaway	Aram	[redacted]	[redacted]@optonline.net	5466...5712	$48.95	$49.95	[redacted].143.26	47011793	396196
AUTH_ONLY_CAPTURED	Settled	Spyaway	Timothy	[redacted]	[redacted]@iw.net	3732...1003	$48.95	$49.95	[redacted].87.99	47013819	396197
AUTH_ONLY_CAPTURED	Settled	Spyaway	albert	[redacted]	[redacted]rris@comcast.net	5491...3835	$48.95	$49.95	[redacted].75.110	47018075	396198
DECLINED	Pending	Spyaway	jeff	[redacted]	[redacted]e@mchsi.com	4121...2422	$48.95	$49.95	[redacted].154.210		396200
DECLINED	Pending	Spyaway	jeff	[redacted]	[redacted]e@mchsi.com	4121...2422	$48.95	$49.95	[redacted].154.210		396202

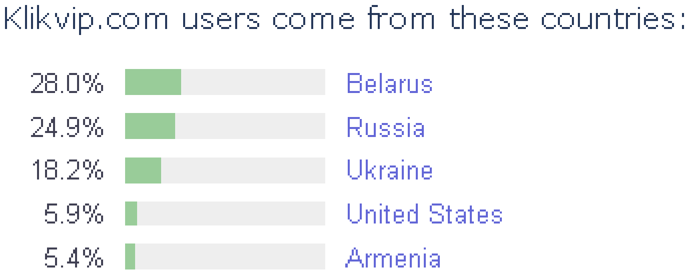
Additionaly, PandaLabs was able to uncover sales logs which contained personal data of victims duped by rogueware. Details such as full names, financial data, e-mail addresses, and IP addresses were obtained from the payment gateway servers. It's obvious that not only do the cyber criminals want to take the money generated from the sale, but also generate additional revenues by reselling the extracted data logs from the payments.

Ultimately, these affiliate programs work as a normal business. One of the most known affiliate system is run by KlikVIP, who are giving commissions to anyone installing their rogueware applications, and from time to time they organize parties with their "distributors". These pictures are from the last party they had in Montenegro, back in March 2008:

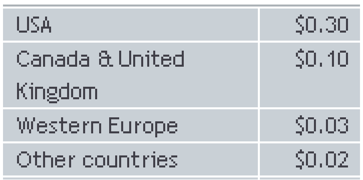




Taking a look at the Alexa statistics from KlikVIP for the last three months, we were able to identify the distributors' origin:



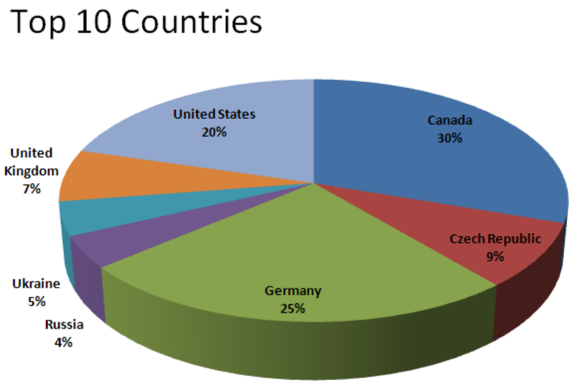
These distributors usually use a pay-per-install system. Following is a price range from one of the affiliate sites:

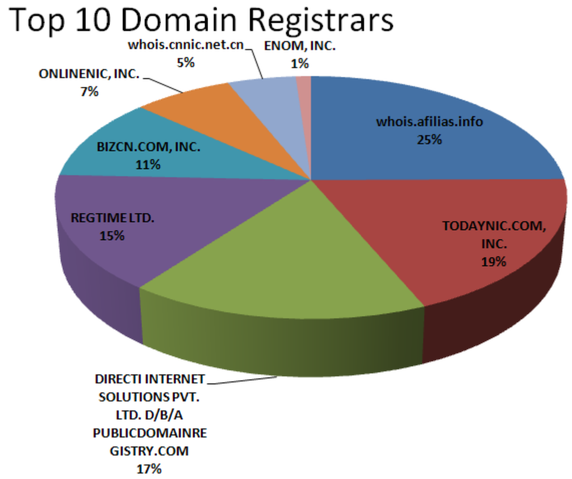


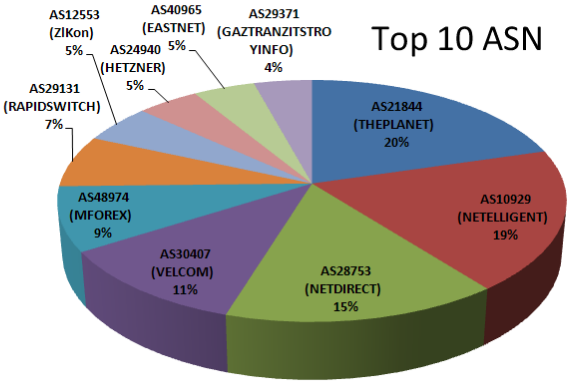
USA	$0.30
Canada & United Kingdom	$0.10
Western Europe	$0.03
Other countries	$0.02

Where is it all coming from?

There is no doubt that the major Rogueware distributors are physically located in Eastern Europe, but another interesting point is the location of the domains, servers, and countries used to distribute the attacks:







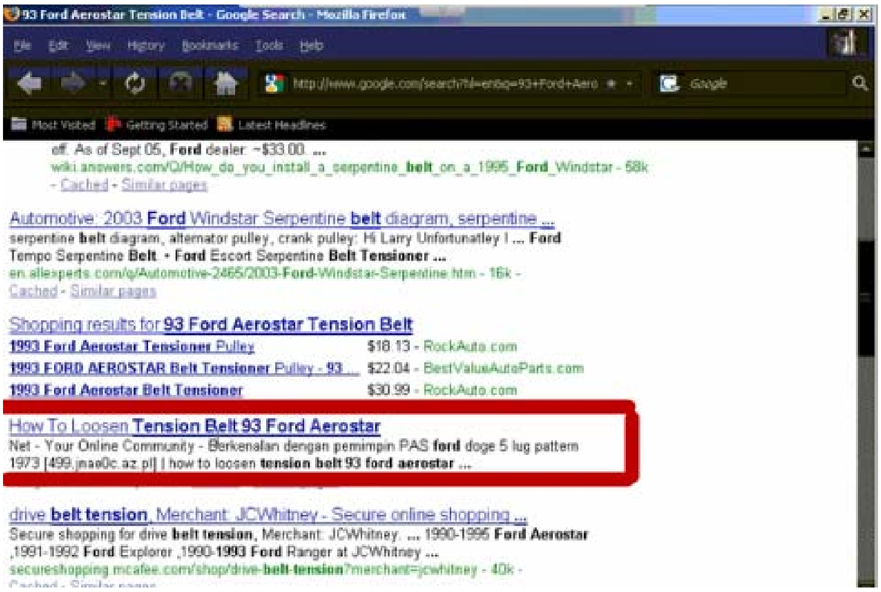
Rogueware Distribution

The highly lucrative nature of the rogueware business fuelled a firestorm of distribution efforts in the latter part of 2008 and throughout 2009. For the first time social media sites, such as Facebook, MySpace, Twitter, and Digg, became large targets for distributors. But despite the plunge into social media, the single largest distribution effort came in the form of a Blackhat SEO attack in April 2009 against the Ford Motor Company. Over three million search terms were hijacked, which turned almost any top search result for Ford cars, parts, or services into rogueware distribution sites. After Ford acknowledged the situation publically, the cyber criminals quickly moved the targeted search campaigns to Nissan and Volkswagen.

Top 5 Attacks in Social Media

Following are the top five rogueware attacks in social media.

1. SEO attack against Ford Motor Company


93 Ford Aerostar Tension Belt - Google Search - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://www.google.com/search?hl=en&q=93+Ford+Aero
Google
Most Visited
Getting Started
Latest Headlines

off. As of Sept 05, **Ford** dealer: ~$33.00. ...
wiki.answers.com/Q/How_do_you_install_a_serpentine_**belt**_on_a_1995_**Ford**_Windstar - 58k
- Cached - Similar pages

Automotive: 2003 **Ford** Windstar Serpentine **belt** diagram, serpentine ...
serpentine **belt** diagram, alternator pulley, crank pulley: Hi Larry Unfortunatley I ... **Ford**
Tempo Serpentine **Belt**. • **Ford** Escort Serpentine **Belt Tensioner** ...
en.allexperts.com/q/Automotive-2465/2003-**Ford**-Windstar-Serpentine.htm - 16k -
Cached - Similar pages

Shopping results for **93 Ford Aerostar Tension Belt**
1993 Ford Aerostar Tensioner Pulley — $18.13 - RockAuto.com
1993 FORD AEROSTAR Belt Tensioner Pulley - 93 ... — $22.04 - BestValueAutoParts.com
1993 Ford Aerostar Belt Tensioner — $30.99 - RockAuto.com

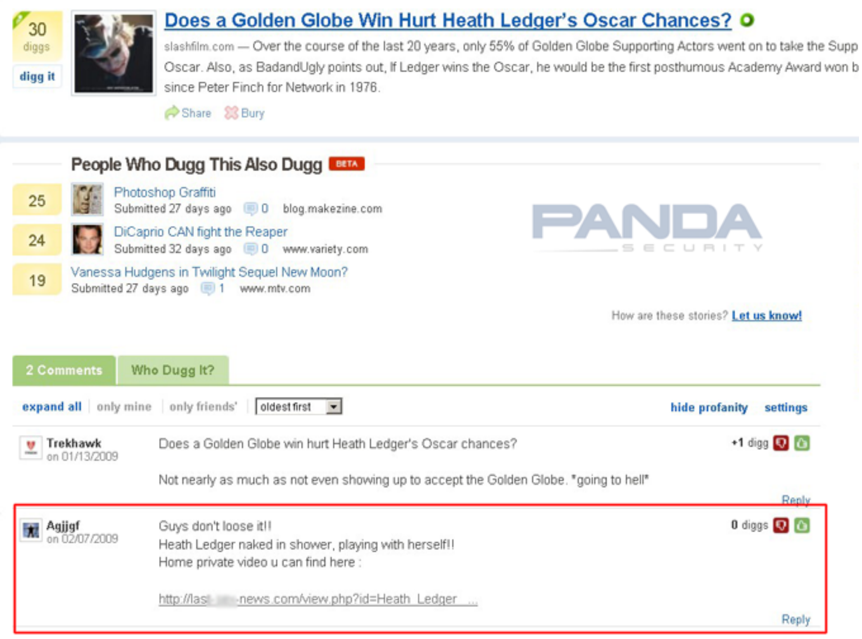
How To Loosen **Tension Belt 93 Ford Aerostar**
Net - Your Online Community - Berkenalan dengan pemimpin PAS **ford** doge 5 lug pattern
1973 [499.jnae0c.az.pl] | how to loosen **tension belt** 93 **ford aerostar** ...

drive **belt tension**, Merchant: JCWhitney - Secure online shopping ...
Secure shopping for drive **belt tension**, Merchant: JCWhitney. ... 1990-1996 **Ford Aerostar**
,1991-1992 **Ford** Explorer ,1990-**1993 Ford** Ranger at JCWhitney ...
secureshopping.mcafee.com/shop/drive-**belt-tension**?merchant=jcwhitney - 40k -
Cached - Similar pages

The Attack:

- 1,000,000 malicious links indexed by Google
- 3,000,000 legitamate search terms hijacked
- Targeted users looking for instructions (E.g. How to loosen a tension belt)
- Served 100 new MSAntiSpyware2009 binaries in 24 hours

2. Comments on Digg.com leading to Rogueware



30 diggs

digg it

Does a Golden Globe Win Hurt Heath Ledger's Oscar Chances?

slashfilm.com — Over the course of the last 20 years, only 55% of Golden Globe Supporting Actors went on to take the Supp Oscar. Also, as BadandUgly points out, If Ledger wins the Oscar, he would be the first posthumous Academy Award won b since Peter Finch for Network in 1976.

Share Bury

People Who Dugg This Also Dugg BETA

25 Photoshop Graffiti
Submitted 27 days ago 0 blog.makezine.com

24 DiCaprio CAN fight the Reaper
Submitted 32 days ago 0 www.variety.com

19 Vanessa Hudgens in Twilight Sequel New Moon?
Submitted 27 days ago 1 www.mtv.com

How are these stories? Let us know!

2 Comments | Who Dugg It?

expand all | only mine | only friends' | oldest first | hide profanity | settings

Trekhawk
on 01/13/2009

Does a Golden Globe win hurt Heath Ledger's Oscar chances?

Not nearly as much as not even showing up to accept the Golden Globe. "going to hell"

+1 digg

Reply

Agjjgf
on 02/07/2009

Guys don't loose it!!
Heath Ledger naked in shower, playing with herself!!
Home private video u can find here :

http://las[redacted]-news.com/view.php?id=Heath_Ledger ...

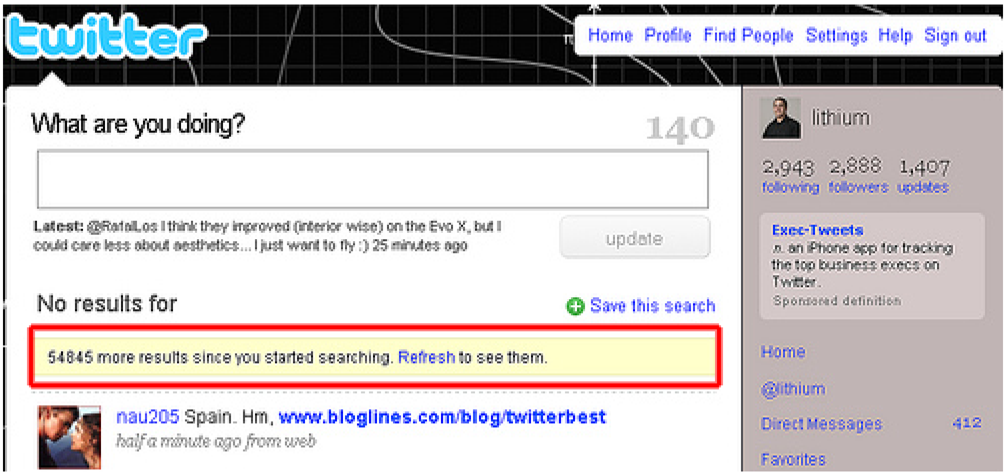
0 diggs

Reply

The Attack:

- 500,000+ comments leading to Rogueware
- Comments targeted news submission title and content

3. Twitter trending topics lead to Rogueware



twitter

Home Profile Find People Settings Help Sign out

What are you doing? 140

Latest: @RafalLos I think they improved (interior wise) on the Evo X, but I could care less about aesthetics... I just want to fly :) 25 minutes ago

update

No results for

Save this search

54845 more results since you started searching. Refresh to see them.

nau205 Spain. Hm, www.bloglines.com/blog/twitterbest
half a minute ago from web

lithium

2,943 following | 2,888 followers | 1,407 updates

Exec-Tweets
n. an iPhone app for tracking the top business execs on Twitter.
Sponsored definition

Home

@lithium

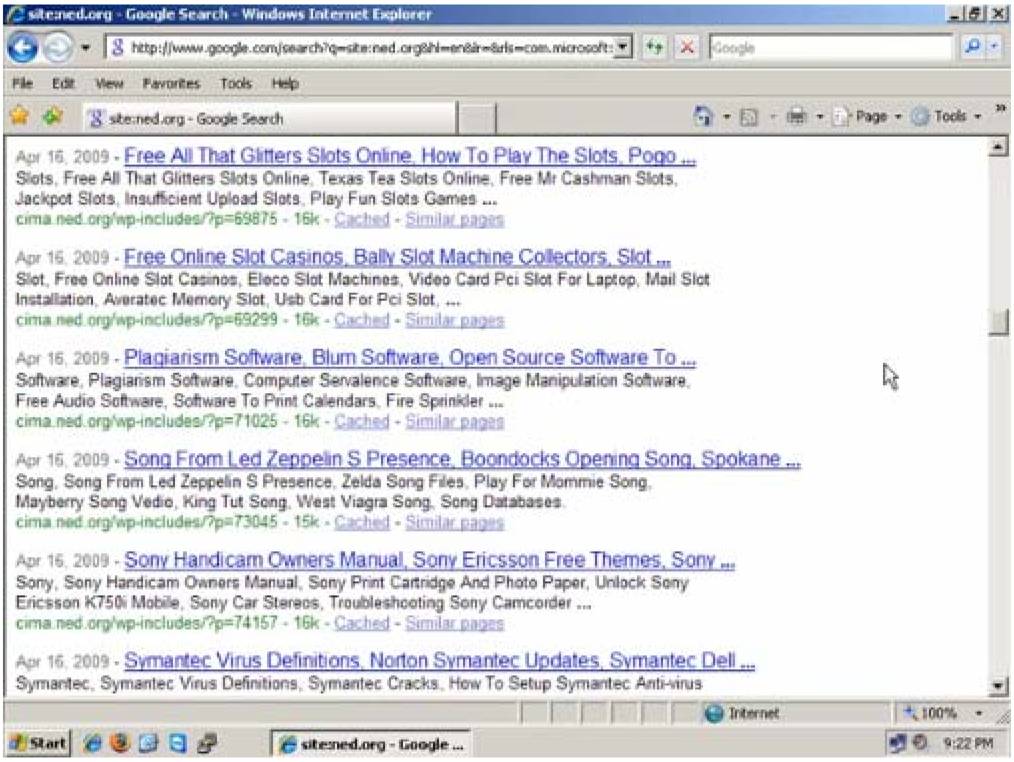
Direct Messages 412

Favorites

The Attack:

- Messages (tweets) targeting trending topics on Twitter.com
- 27,000 tweets per 24 hours
- 60 unique samples detected over 72 hour period

4. Rogueware exploits Wordpress vulnerability to facilitate Blackhat SEO attack


site:ned.org - Google Search - Windows Internet Explorer
http://www.google.com/search?q=site:ned.org&hl=en&lr=&rls=com.microsoft:
Google
File
Edit
View
Favorites
Tools
Help
site:ned.org - Google Search
Page
Tools
Internet
100%
Start
site:ned.org - Google ...
9:22 PM

Apr 16, 2009 - Free All That Glitters Slots Online, How To Play The Slots, Pogo ...
Slots, Free All That Glitters Slots Online, Texas Tea Slots Online, Free Mr Cashman Slots, Jackpot Slots, Insufficient Upload Slots, Play Fun Slots Games ...
cima.ned.org/wp-includes/?p=69875 - 16k - Cached - Similar pages

Apr 16, 2009 - Free Online Slot Casinos, Bally Slot Machine Collectors, Slot ...
Slot, Free Online Slot Casinos, Eleco Slot Machines, Video Card Pci Slot For Laptop, Mail Slot Installation, Averatec Memory Slot, Usb Card For Pci Slot, ...
cima.ned.org/wp-includes/?p=69299 - 16k - Cached - Similar pages

Apr 16, 2009 - Plagiarism Software, Blum Software, Open Source Software To ...
Software, Plagiarism Software, Computer Servalence Software, Image Manipulation Software, Free Audio Software, Software To Print Calendars, Fire Sprinkler ...
cima.ned.org/wp-includes/?p=71025 - 16k - Cached - Similar pages

Apr 16, 2009 - Song From Led Zeppelin S Presence, Boondocks Opening Song, Spokane ...
Song, Song From Led Zeppelin S Presence, Zelda Song Files, Play For Mommie Song, Mayberry Song Vedio, King Tut Song, West Viagra Song, Song Databases.
cima.ned.org/wp-includes/?p=73045 - 15k - Cached - Similar pages

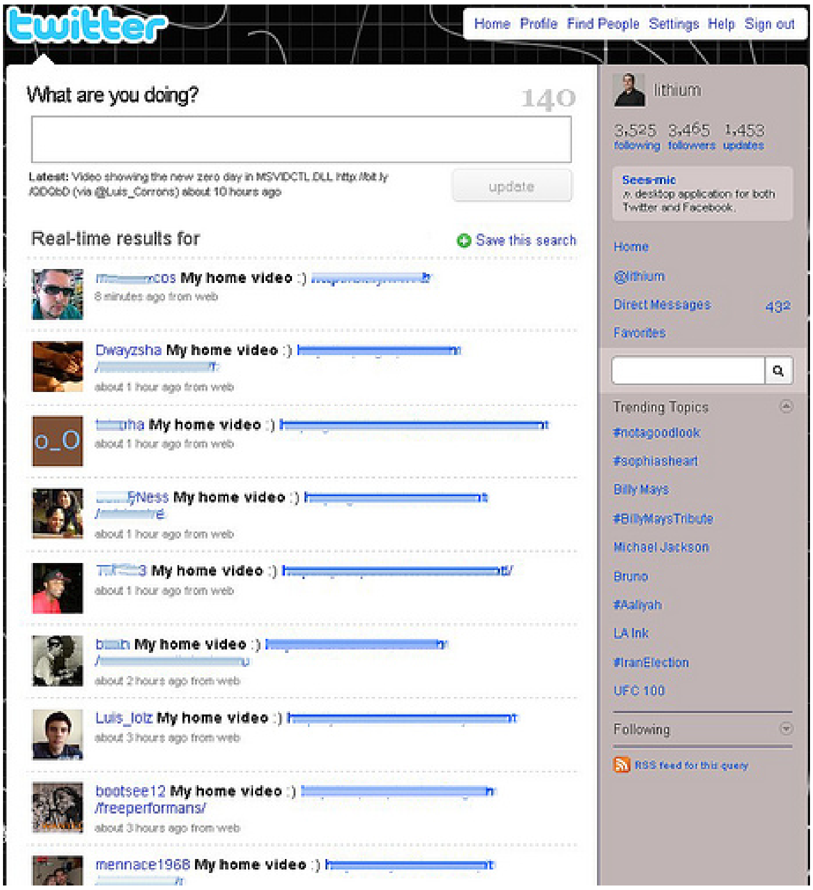
Apr 16, 2009 - Sony Handicam Owners Manual, Sony Ericsson Free Themes, Sony ...
Sony, Sony Handicam Owners Manual, Sony Print Cartridge And Photo Paper, Unlock Sony Ericsson K750i Mobile, Sony Car Stereos, Troubleshooting Sony Camcorder ...
cima.ned.org/wp-includes/?p=74157 - 16k - Cached - Similar pages

Apr 16, 2009 - Symantec Virus Definitions, Norton Symantec Updates, Symantec Dell ...
Symantec, Symantec Virus Definitions, Symantec Cracks, How To Setup Symantec Anti-virus

The Attack:

- Affected Ned.org and TheWorkBuzz.com
- Targeted a security vulnerability in an old version of Wordpress
- Redirected all links to point to Rogueware servers
- Facillitated a Blackhat SEO attack against 13,000 search terms

5. Koobface moves to Twitter



What are you doing?

140

Latest: Video showing the new zero day in MSVIDCTL.DLL http://bit.ly/QDGbD (via @Luis_Corrons) about 10 hours ago

update

Real-time results for

Save this search

[redacted]cos My home video :) [redacted]
8 minutes ago from web

Dwayzsha My home video :) [redacted]
about 1 hour ago from web

[redacted]pha My home video :) [redacted]
about 1 hour ago from web

[redacted]ﾂNess My home video :) [redacted]
about 1 hour ago from web

T[redacted]3 My home video :) [redacted]
about 1 hour ago from web

b[redacted]h My home video :) [redacted]
about 2 hours ago from web

Luis_lolz My home video :) [redacted]
about 3 hours ago from web

bootsee12 My home video :) [redacted]
/freeperformans/
about 3 hours ago from web

mennace1968 My home video :) [redacted]

lithium

3,525 following 3,465 followers 1,453 updates

Sees-mic
A desktop application for both Twitter and Facebook.

Home
@lithium
Direct Messages 432
Favorites

Trending Topics
#notagoodlook
#sophiasheart
Billy Mays
#BillyMaysTribute
Michael Jackson
Bruno
#Aaliyah
LA Ink
#IranElection
UFC 100

Following

RSS feed for this query

The Attack:

- Messages (tweets) pointing to 20 Rogueware sites.
- The worm further propagated on Twitter upon infection
- Malicious site presented a realistic looking Flash update popup

Conclusion

As we have demonstrated throughout this report, the rogueware situation is very serious and growing as cybercriminals continue to create new methods for developing and distributing malware. It is a very lucrative business for the cybercriminals, so the name of the game is to infect as many people as possible. As a result, social networks have proven to be an effective channel to infect users. Based on PandaLabs' extensive research, the situation is most likely to escalate even further.

Furthermore, cybercriminals know how to avoid antivirus detection; on one hand, most of them don't show suspicious behaviors, so antivirus companies have to focus on signatures (specific or generic) to deal with those programs. This is the main reason why cyber criminals are creating so many new samples. On the other hand, PandaLabs has started to identify more advanced malware variants that are using typical Trojan features, as well as Rootkits and other techniques to subvert virus protection technologies.

For many years consumers and businesses alike have been faced with new threats, ranging from viruses and spam to phishing. In order to fight the war against cybercrime, grassroots awareness, advocacy and individual user education will continue to be important. Antivirus companies must play a fundamental role in exposing the problem in near real-time and presenting solutions along the way.

Finally, antivirus companies must admit that the industry is not even close to winning this battle. This is precisely why Panda started to develop Cloud based technologies in 2006. The company needed to be able to quickly analyze every new sample against its 20 years of accumulated malware data in real time to deliver protection in minutes instead of days. Fortunately, other vendors are now following this trend, but cybercriminals will soon look to new channels for malware monetization.

Authors

Sean-Paul Correll

Sean-Paul started at Panda Security back in 2005 in our technical support area. Since that time, he has worn many hats throughout the organization all while staying true to his true passion--Security. He specializes in threat surveillance with an emphasis on emerging threats. He is an active member of the security community and frequently volunteers his time to helping individuals with malware infections.

Luis Corrons

Luis has been working for Panda Security since 1999. He started in the technical support department, helping home and corporative users with virus incidents. A year later, he joined the international technical support team assisting Panda's technical support belonging to their partners distributed over 50 countries around the world. In 2002, he became PandaLabs' director as well as malware alerts coordinator in worldwide infection situations, dealing with worm such as Klez, SQLSlammer, Sobig, Blaster. Sasser, Mydoom, etc. During this time, he has coordinated several automated projects related with malware, such as the automatic analisys and response system, and the malware automatic information system.

His first contact with computers was at the age of 4, with a Sharp MZ-80K, which he started Basic language programming with. His main hobbies are his wife Nerea, his dog Robin and his work as well as chess and videogames.