Wednesday, June 23, 2010

Introduction to Rogue Anti-Virus

If you follow the Threat Center Blog, you've heard us talk about "Rogue AV," but may not fully understand what we're referencing. This post is for those users who are not already familiar with this widespread and common threat.

In short, when we and other security researchers reference Rogue AV, we're referring to an Internet scam where an official-looking web page pops up telling the user that a virus has been detected on their computer. The web page often appears to be scanning the local computer and often reports multiple found infections. The web page, the report, and everything about this scam is a fraud.

Millions of users have been duped into installing malicious software, also known as malware onto their systems allowing cybercriminals to steal money and other personal details. Here's how the attack works:

Step One: Get the user to the malicious website

First, the group or groups behind these attacks first post large numbers of links to some new domain by spamming community forums, blog comments, and by putting the links inside hidden elements on compromised websites in a technique known as Blackhat SEO (Search Engine Optimization). In this way, they are able to get the target website high up in search results for common or recently trending search terms. Right now, for example, search results on Wimbledon and the World Cup are actively being poisoned in this manner.

The above technique is usually seen in conjunction with one or more of the following:

- Redirects from compromised websites that are otherwise legitimate
- Spam emails that are often sent via other compromised computers

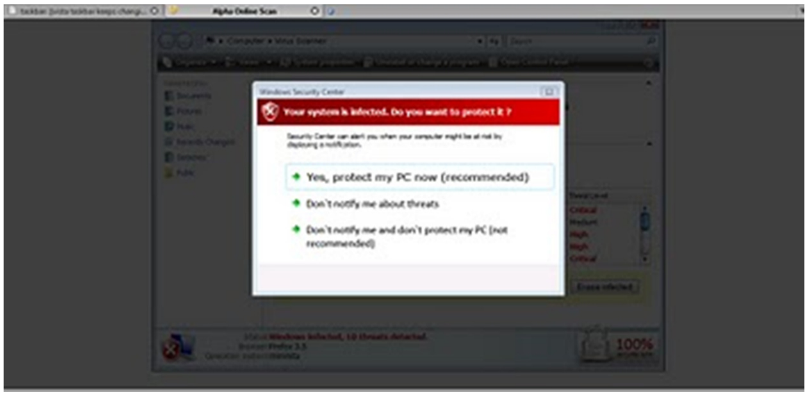
- Malvertisements where attackers pay for an ad in a legitimate ad network, but use the ad to send people to the malicious website. In the past year, reputable sites like the New York Times, White Pages, Tech Crunch and others have been caught hosting such malvertizements.

Step Two: The con game

Once on the website, social engineering tricks are invoked to convince a user to fall for this modern Internet con. Computer users are conditioned with constant reminders to keep their computer free from virus and malware by running anti-virus software and keeping their virus definitions up to date. These websites use this conditioning against the user, using visual elements to establish authority and trust and then causing a sense of danger and urgency when notifying the user that their computer is infected with viruses and that their data personal computer is under someone else's control.

Rogue anti-virus malware comes in many different forms and will take different approaches to fool a user, but at the most basic level, rogue anti-virus scams convince the user that they have a problem and that they need to download some software to fix the problem.

The screenshots below are just a few examples of fake scanners. These specially crafted pages are made with great detail to look exactly like Windows XP, Vista, or Windows 7 system alerts.



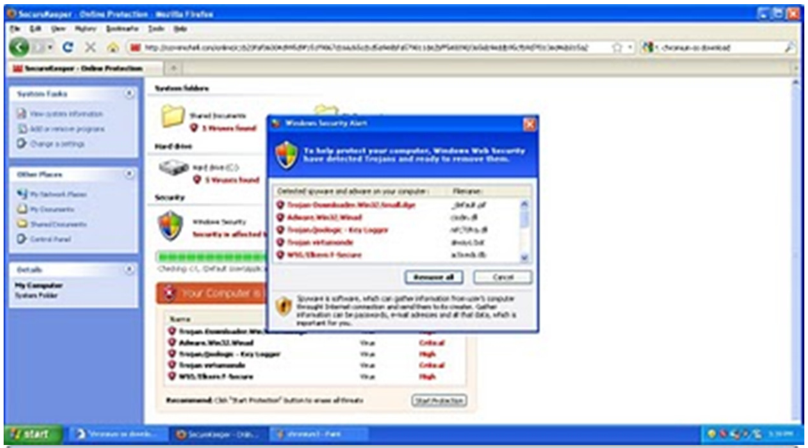
Windows Security Center

Your system is infected. Do you want to protect it ?

Security Center can alert you when your computer might be at risk by displaying a notification.

- Yes, protect my PC now (recommended)
- Don't notify me about threats
- Don't notify me and don't protect my PC (not recommended)

Windows infected, 10 threats detected.

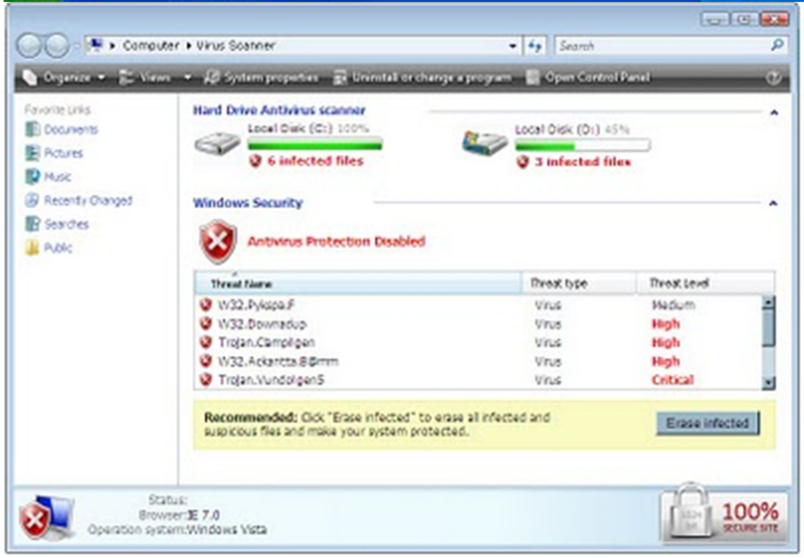


Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Trojan-Downloader.Win32.Small.dge	_default.pif
Adware.Win32.Winad	[illegible]
Trojan.Qoologic - Key Logger	[illegible]
Trojan.virtumonde	[illegible]
W95.Elkern.F-Secure	[illegible]

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gather information can be passwords, e-mail adresses and all that data, which is important for you.



Hard Drive Antivirus scanner

Local Disk (C:) 100%
6 infected files

Local Disk (D:) 45%
3 infected files

Windows Security

Antivirus Protection Disabled

Threat Name	Threat type	Threat Level
W32.Pykspa.F	Virus	Medium
W32.Downadup	Virus	High
Trojan.Campilgen	Virus	High
W32.Ackantta.B@mm	Virus	High
Trojan.Vundolgen5	Virus	Critical

Recommended: Click "Erase infected" to erase all infected and suspicious files and make your system protected.

Status:
Browser: IE 7.0
Operation system: Windows Vista

Fake scans like these are very believable for uneducated users and lead to a very high success rate for cybercriminals.

Step Three: Infection

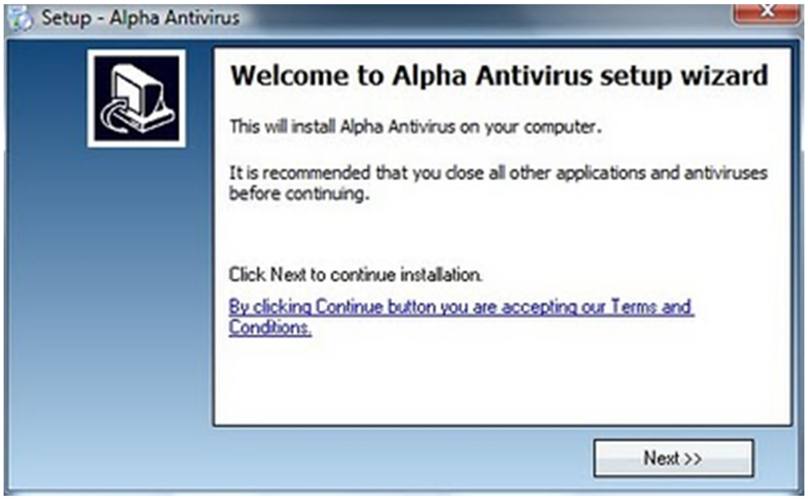
Frequently a box pops up that asks the user if they want to download the software that will fix the purported problem. In many cases, it doesn’t matter if the user agrees or cancels, the download will begin in either case. Once the downloaded file is opened, the system is infected and the user has been tricked into installing the very thing he or she sought to remove.

Cybercriminals make it very difficult to click away from the page, so that in some cases, the user relents out of a sense of frustration and not knowing how else to move forward. In many cases the malicious file is downloaded with no user interaction at all.

The actual file that is downloaded changes often with different names and characteristics. eSoft rarely sees more than two or three legitimate anti-virus software (of over 40 checked) detecting the file as a virus at the time of the attack. The perpetrators of this attack spit out new variations on the download at a very high rate in an attempt to stay ahead of signature-based anti-virus software.

Step Four: Asking for payment

Once a user has clicked to open the malicious file and install the software, the problem only gets worse. The cybercriminals do well in masking their malicious intentions throughout the install process. In many cases the installation is a *silent* install – one which requires no user interaction – or a standard install wizard which raises no red flags to the user.



Setup - Alpha Antivirus

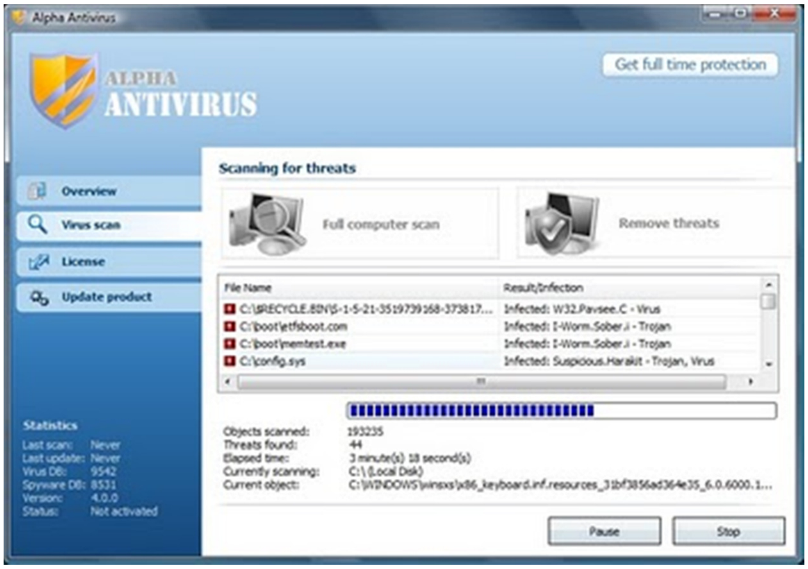
Welcome to Alpha Antivirus setup wizard

This will install Alpha Antivirus on your computer.

It is recommended that you close all other applications and antiviruses before continuing.

Click Next to continue installation.

By clicking Continue button you are accepting our Terms and Conditions.



Scanning for threats

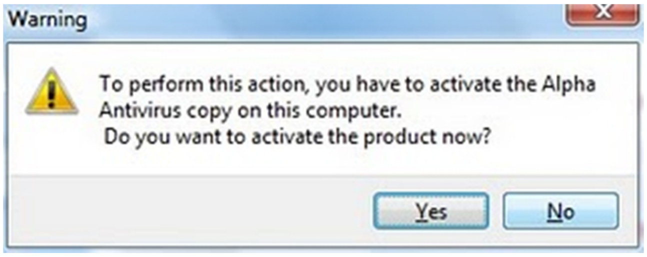
File Name	Result/Infection
C:\$RECYCLE.BIN\S-1-5-21-3519739168-373817...	Infected: W32.Pavsee.C - Virus
C:\boot\etfsboot.com	Infected: I-Worm.Sober.i - Trojan
C:\boot\memtest.exe	Infected: I-Worm.Sober.i - Trojan
C:\config.sys	Infected: Suspicious.Harakit - Trojan, Virus

```
Objects scanned:     193235
Threats found:       44
Elapsed time:        3 minute(s) 18 second(s)
Currently scanning:  C:\ (Local Disk)
Current object:      C:\WINDOWS\winsxs\x86_keyboard.inf.resources_31bf3856ad364e35_6.0.6000.1...
```

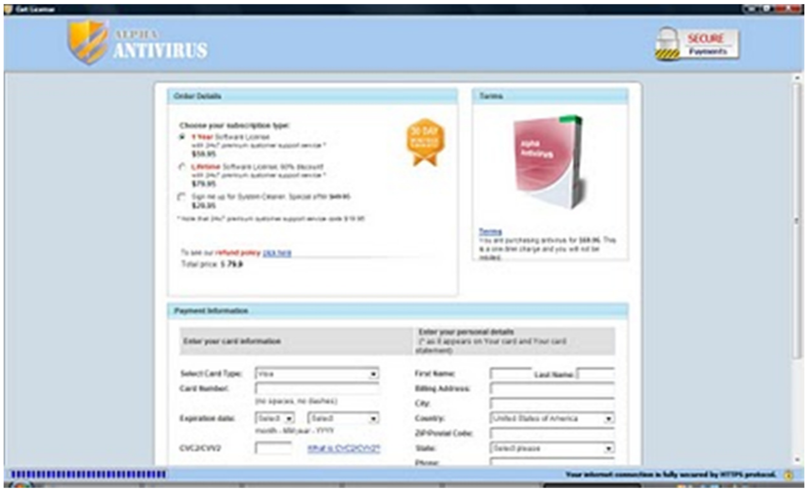
Statistics

```
Last scan:     Never
Last update:   Never
Virus DB:      9542
Spyware DB:    8531
Version:       4.0.0
Status:        Not activated
```

Once installed, the rogue anti-virus program will inundate the user with notifications that the system is infected and that they still need to take action. In order to remove the supposed infections (not the real problem) the user is asked to pay a license or subscription fee that typically runs between $50 and $100 USD.



To perform this action, you have to activate the Alpha Antivirus copy on this computer.
Do you want to activate the product now?



Order Details

Choose your subscription type:

● 1 Year Software License with 24x7 premium customer support service * $59.95

○ Lifetime Software License, 60% discount with 24x7 premium customer support service * $79.95

□ Sign me up for System Cleaner. Special offer $49.95 $29.95

* Note that 24x7 premium customer support service costs $19.95

To see our refund policy click here

Total price: $ 79.9

Terms

Terms

You are purchasing antivirus for $59.95. This is a one-time charge and you will not be rebilled.

Payment Information

Enter your card information		Enter your personal details (* as it appears on Your card and Your card statement)	
Select Card Type:	Visa	First Name:	Last Name:
Card Number:	(no spaces, no dashes)	Billing Address:	
		City:	
Expiration date:	Select / Select month - MM year - YYYY	Country:	United States of America
		ZIP/Postal Code:	
CVC2/CVV2	What is CVC2/CVV2?	State:	Select please
		Phone:	

Your internet connection is fully secured by HTTPS protocol.

Though the branding changes – these screenshots show the Rogue AV "Alpha AntiVirus" – the checkout pages remain as convincing as the rest of the scam, frequently with badges showing secure payments and other "trust me" icons. Pricing is comparable to legitimate anti-virus products and comes with a money back guarantee to further convince the user who may be wavering that the risk to giving up their credit card and personal information is low. In reality, submitting credit card info does not clean their system, but instead sends name, address, and credit card info directly to the perpetrators of the attack.

Users infected with this might just assume this is an annoyance, but the scam goes much deeper than this. These programs have been created by large underground crime rings that now have the users' personal information and credit card number. In addition, these programs are often packaged with downloader Trojans which are capable of downloading any type of malware the attacker chooses. Because many of these criminal enterprises are also heavily involved in banking malware this is just one of the many additional types of malware that can be installed. As a result, an infected computer should have a computer professional remove the virus, which can cost small businesses thousands of dollars per year.

Prevention

Cybercriminals go a long way to making sure they can infect a machine and to get around classic signature-based virus scanning. If a user gets a web browser window that says their computer is infected with malware, they should immediately attempt to close the window. If that is not possible, then quitting and restarting the web browser is the next best thing. This, of course, requires that users are trained in spotting and avoiding this attack, but in practice, training unsavvy users alone is not always fruitful.