PANDA
CLOUDINTERNETPROTECTION

Simply... ***Evolution***

FAKE ANTI-VIRUS: A GROWING THREAT

PANDA CLOUD
OFFICE PROTECTION

PANDA CLOUD
EMAIL PROTECTION

PANDA CLOUD
INTERNET PROTECTION

PANDA
SECURITY

Index

1. Fake Anti-virus: A Growing Threat 2

2. The Panda Cloud Internet Protection (PCIP) Solution 3

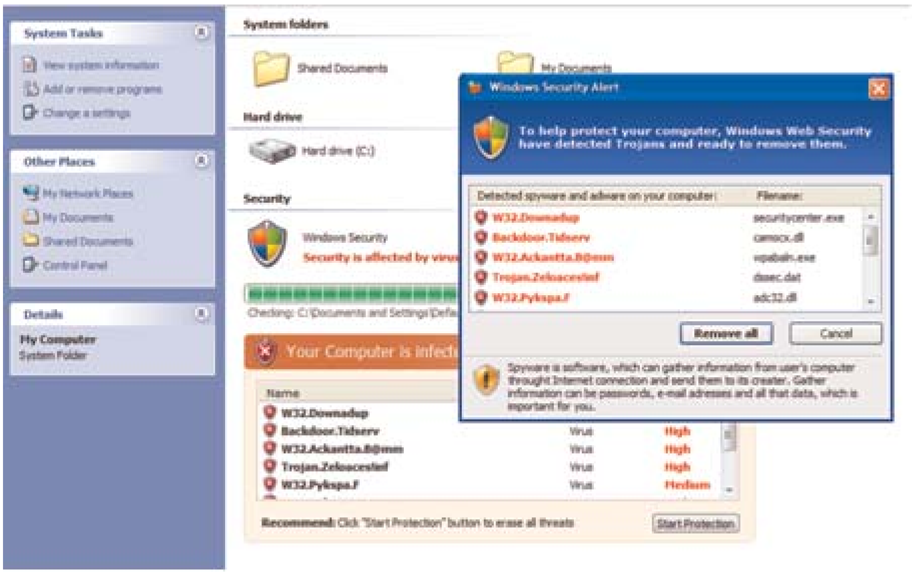
6. Panda Cloud Protection Suite 3

1. Fake Anti-virus: A Growing Threat

Google announced that fake anti-virus (AV) pages represent discovered on domains that include popular search terms. The Panda Security research team has shown that some popular searches, as illustrated in , can contain up to 90% of malicious links to fake AV pages in the first 100 results. Even more alarming is the fact that attackers are becoming adept at having their links displayed as the first result for very popular searches.

Malicious fake anti-virus malware hides behind legitimate sites that have been hacked. New pages targeting popular searches are added to the hacked sites. Using Blackhat Search Engine Optimization (SEO) techniques, attackers are able to achieve a high ranking on search engines for these pages. When users click on a malicious search result link, they are redirected to a fake AV page on a different domain. The malicious page appears very realistic (figure 1); it looks like a desktop AV tool is scanning the user's computer. The malware warns that the computer is infected, and prompts the user to download a free AV client to clean up the computer.

Even though fake anti-virus is a growing threat and represents more than 60% of the malware coming from Google searches, it is not well detected. Google can take several days to clean up some of the malicious links. Five days later, popular searches still contain malicious links on the first 10 pages. Since attackers are hiding behind multiple legitimate sites and use new domains every day to host the fake AV pages, diagnostic tools including Google Safe Browsing do not offer comprehensive protection. The malicious pages are added too late and many are missing. Similarly, anti-virus tools do not do a great job either; on average only popular tools detect the executable as a virus (Kapersky, AVG, McAfee, Fortinet, etc. miss them). Lastly, offline security tools are not the answer either as redirection to a fake AV page only occurs by performing an online Google/Yahoo/Bing search.



Checking: C:\Documents and Settings\Defa

Your Computer is infect

Name		
W32.Downadup		
Backdoor.Tidserv	Virus	High
W32.Ackantta.B@mm	Virus	High
Trojan.Zeloacestef	Virus	High
W32.Pykspa.F	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

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

Detected spyware and adware on your computer:	Filename:
W32.Downadup	securitycenter.exe
Backdoor.Tidserv	camocx.dll
W32.Ackantta.B@mm	wpabaln.exe
Trojan.Zeloacestef	dssec.dat
W32.Pykspa.F	adc32.dll

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

Figure 1: Fake AV Page

2. The Panda Cloud Internet Protection (PCIP) Solution

Dynamic threats such as fake anti-virus require in-line inspection of every file – HTML, Javascript, etc. In order to be effective, a security solution must inspect the content in real-time. By examining every transaction in-line, PCIP´s Advanced Threat service is able to detect and block fake AV pages that have not been blacklisted by third party feeds such as Google Safe Browsing (part of Firefox), malwaredomainlist.com, etc. The deep inspection technology helps to continually protect organizations as new fake AV pages and domains appear.

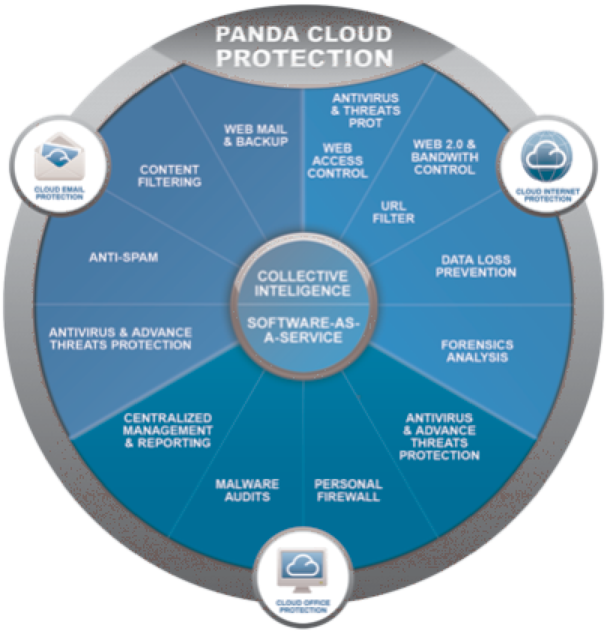
6. Panda Cloud Protection suite

Panda Cloud Internet Protection is part of the Panda Cloud Protection suite which is a complete SaaS security solution that protects all the main threat entry points: endpoint, email and Web traffic, against malware, spam, phishing, cross-site scripting and other advanced Web 2.0 attacks, through a light, secure and simple solution.

As the security suite is based in the cloud it offers maximum protection, while optimizing costs and productivity. Deployment takes just minutes, and day-to-day management is handled easily using Panda’s unique and intuitive Cloud Management Console.

The Panda Cloud Protection suite harnesses the power of Collective Intelligence. Panda's cloud-based Collective Intelligence leverages 21 terabytes of knowledge and experience drawn directly from millions of users to deliver comprehensive, instantaneous, non-intrusive real-world protection against known and unknown malware to all users.

Panda Cloud Protection leverages the power of the cloud to not only provide up-to-the-minute protection against known and unknown threats but also to streamline the delivery of that protection through the anytime, anywhere power of the Cloud Management Console.



PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos. Madrid. SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P.O. Box 10578. Glendale, CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com

PANDA
SECURITY