Fake Antivirus Extortion Set to Grow in 2009

Submitted by: Marylebone Media Relations
Monday, 29 December 2008

And 10 things users can do to protect themselves in 2009

Bournemouth, UK (29th December 2008) - Amongst the top threats that (http://www.eset.co.uk) ESET predicts for 2009 is the increasing volume and sophistication of hackers' attempts to extort money from end users in return for fake anti-malware. ESET says that the trend developed from fake antivirus and antispyware programs and sites to spoofing real vendor sites in 2008, and is set to grow next year as cyber criminals increase the level of sophistication in their social engineering techniques that sometimes persuade even savvy users into buying fake software.

"Some of the major antivirus companies have seen their websites spoofed over the last couple of months," comments David Harley, Director of Malware Intelligence, ESET. "Although currently users are often conned out of their money in exchange for fake antivirus which performs no useful function at all, in the near future we expect that more extortionists will take the opportunity to add to the range of ways in which they exploit others. Even now, when these gangs find an opportunity to install fake security software, it's possible and even likely that spyware and adware are installed at the same time. In addition, when a victim is tricked into giving out confidential information such as credit card details, that information may be used subsequently in many different ways, apart from the original "sting". "

"Make no mistake: there are many con-men out there trying to pass themselves off as legitimate security vendors, and using any means they can to blur the distinction between what they do and what we do. For instance, some are claiming falsely to have industry standard certifications for their "products", introducing rudimentary "real" detection into the product, blackening vendor reputations in public forums, and threatening legal action against real security vendors and others who might expose them for what they are. In many respects, this is as much an attack on the security community as it is on end users," Harley continues

ESET Senior Analyst Pierre-Marc Bureau notes that in recent months fake anti-malware programs are being found in very high volumes. Currently ESET amasses more than a gigabyte of new fake antivirus samples a day on ThreatSense.Net, which collects data from more than 10 million systems worldwide.

ESET also believes that 2009 will bring an increase in VM (virtual machine) aware malware, which either stays dormant when it recognises that it is in a virtual environment, or actively searches for exploitable vulnerabilities. In addition, ESET anticipates an increase in threats to mobile devices, including proof-of-concept attacks and mobile browser exploits such as attacks against WebKit-based browsers found in iPhone and Google Android-powered phones.

10 things users can do to protect themselves in 2009

1) Disable Autorun in Windows: this facility is consistently exploited by the class of malware ESET detects as INF/AUTORUN, among other threats.

2) Keep applications and Operating System components up-to-date with automatedupdates and patches, and by regularly reviewing the vendors' product update sections on their web sites.

3) Log on to your computer with an account that doesn't have "Administrator" privileges, to reduce the likelihood and severity of damage from self-installing malware.

4) Use different passwords for your computer and on-line services. Also practice changing passwords on a regular basis and avoid simple passwords, especially those that are easily guessed.

5) Don't trust unsolicited files or embedded links, even from friends. It's easy to spoof email addresses, for instance, or to disguise a harmful link so that it looks like something quite different, whether it's in email, chat or whatever.

6) Don't disclose sensitive information on public websites like FaceBook or LinkedIn. Even information that in itself is innocuous can be combined with other harmless information and used in social engineering attacks.

7) If sensitive information is stored on your hard drive, protect it with encryption and by regularly backing up your data to a separate disk and, where possible, a remote site or facility.

8) Don't expect antivirus alone to protect you. Use additional measures such as a personal firewall, antispam and anti-phishing toolbars, but be aware that there is a lot of fake security software out there, and sometimes even the best protection might not protect you as well as common sense and caution.

9) Don't connect to just any "free Wi-Fi" access point: it might alter your DNS queries or be the "evil twin" of a legitimate access point, set up to intercept your logins and online transactions.

10) Don't use cracked/pirated software! These are easy avenues for introducing malware into, or exploiting weaknesses in, a system. This also includes the illegal P2P (peer-to-peer) distribution of copyrighted audio and video files: some of these are counterfeited or modified so that they can be used directly in the malware distribution process.

About ESET

ESET develops software solutions that deliver comprehensive protection against evolving computer security threats. ESET pioneered and continues to lead the industry in proactive threat detection. ESET NOD32 Antivirus, its flagship product, consistently achieves the highest accolades in all types of comparative testing and is the foundational product that extends the ESET product line to include ESET Smart Security. Both products have an extremely efficient code base that avoids the unnecessary large footprint found in some solutions. This means faster scanning that doesn't slow down computers or networks.

Sold in more than 110 countries, ESET has worldwide production headquarters in Bratislava, SK and worldwide distribution headquarters in San Diego, U.S. ESET also has offices in UK, Argentina and Czech Republic and is globally represented by an extensive partner network. For more information, visit www.eset.co.uk or call 0845 838 0832.

Contact:

Sara Claridge
Marylebone Media Relations
sara@marylebone.co.uk
+44 (0) 20 8133 5572
+44 (0) 7968 626838 (mobile)
(www.marylebone.co.uk)