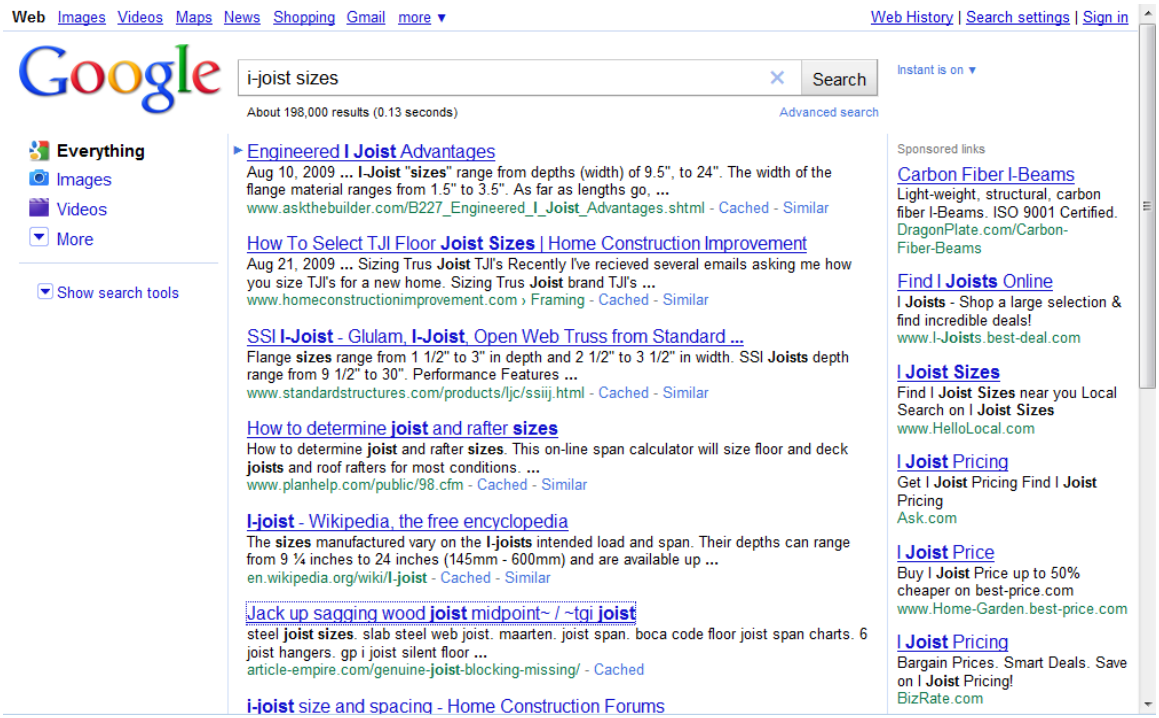
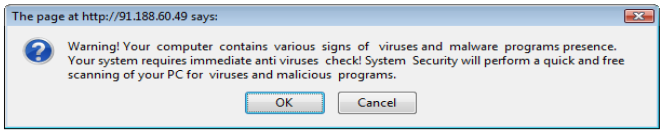
KIND TECHNOLOGIES, LLC
Product & Service Solutions... with a human touch!
www.kindtechnologies.com (360) 225-8723

ANATOMY OF A ROGUE ANTISPYWARE WEB ATTACK

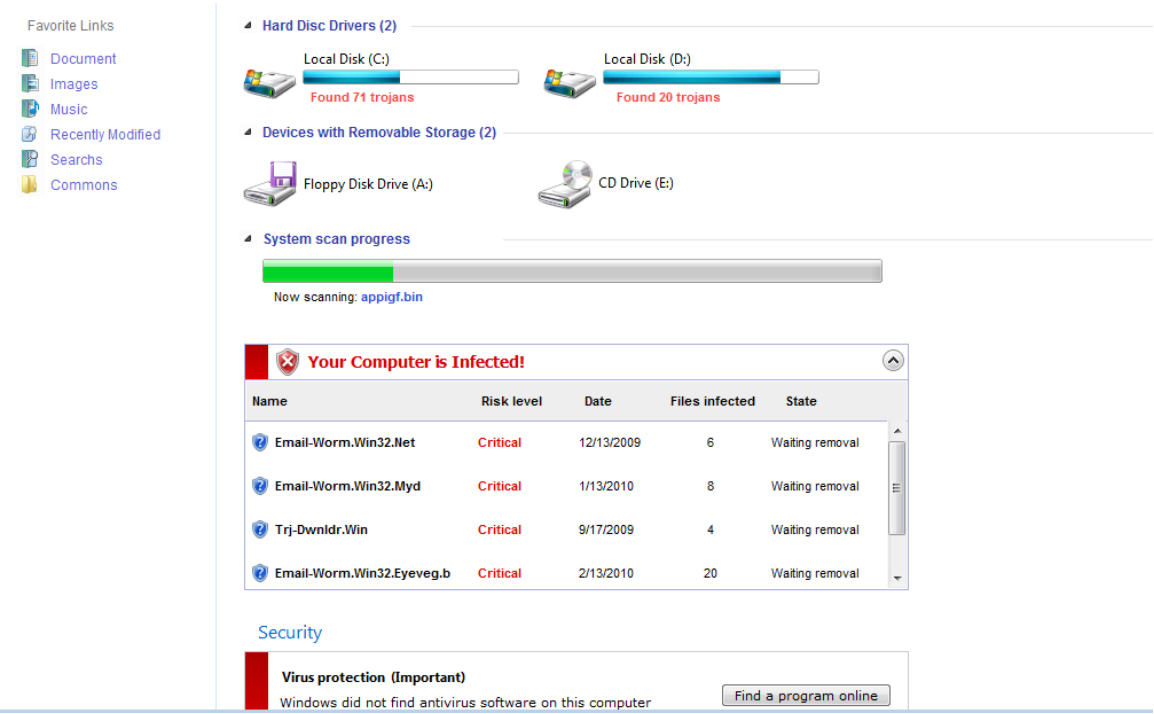
The attack begins with an innocent, unsuspecting Web search. In this real example, the link selected is outlined with a dotted-line border. There is nothing to indicate the link does not refer to a legitimate website:



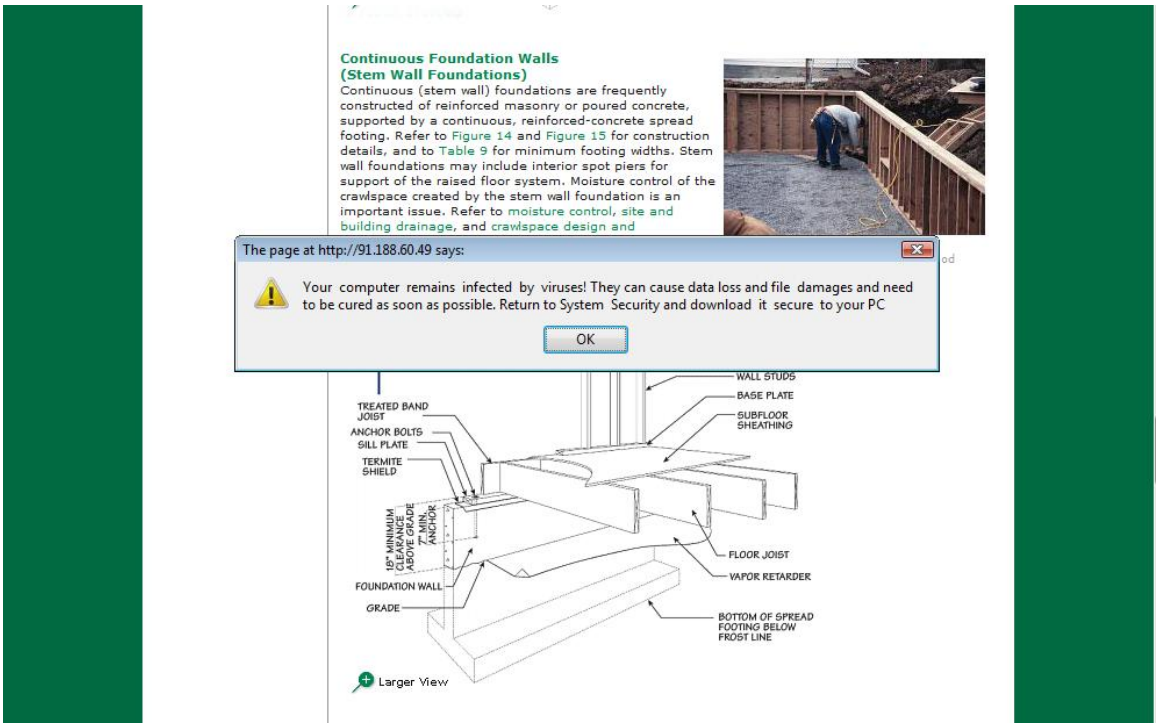
The immediate result of clicking the link is the warning below. Pressing either button within the box will result in the download and running of malware on the computer and the consequent successful attack. Since this is a popup window, the browser tab cannot be closed until the popup window is closed. The red “X” in the upper right-hand corner is the *only* standard Windows control that can safely be clicked:



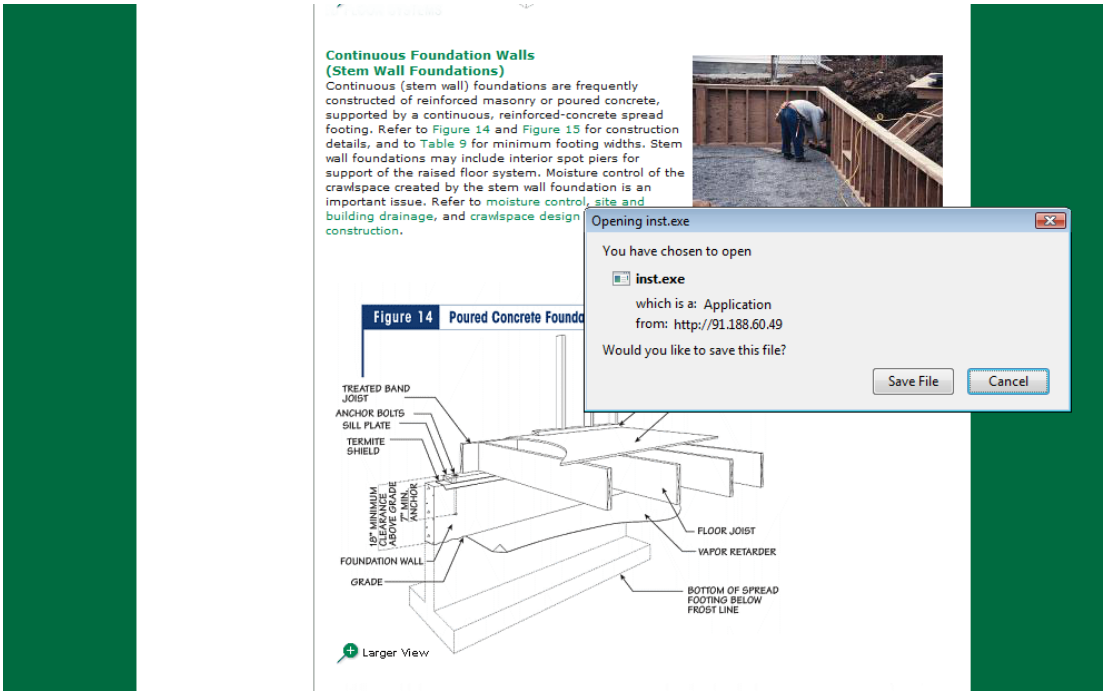
After clicking the “X” to close the first popup window, the screen below immediately follows. It is designed to resemble a Windows notification dialog and thereby appear legitimate. It is actually a rogue AntiSpyware web page completely bogus in its warning notification. Clicking any control within the page will download malware and successfully hack the system, regardless of installed protection(s). Again, the only safe action is to close the Web page by clicking the red “X” in its upper right-hand corner or the red “X” associated with the open tab (neither control is visible in webshot below):



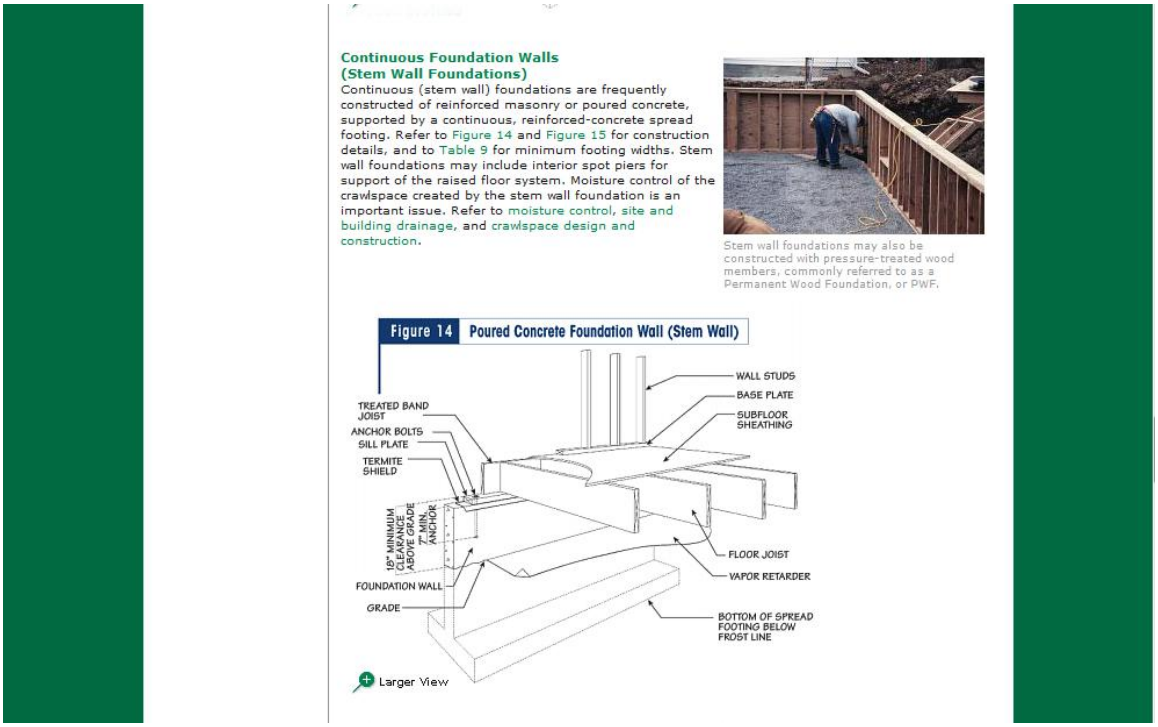
After closing the previous Web page by clicking the red “X,” the following popup warning appears, again tempting the user to allow malware to be downloaded by the system by clicking the “OK” control inside the window. Once more the only safe control to click is the red “X” in the window’s upper right-hand corner, which closes the popup:



This leads to the last popup window in the sequence. This window is designed to fool even the savvy surfer since it appears that, despite all previous proper actions, a malware program is still in the process of being loaded. Actually this is also a bogus popup identical to the previous and, again, clicking the red "X" is the only safe means of preventing a successful system hack. The cancel button is programmed exactly the same as the "Save File" button and both will download and run malware on the system:



After closing the prior popup, the Web page/tab is finally shut down and the threat averted. By attentive and educated response to a Web threat *that no antivirus or antispyware countermeasure could prevent*, significant time and money has been saved and an Internet hacker has been denied the reward of a successful attack!



Continuous Foundation Walls (Stem Wall Foundations)

Continuous (stem wall) foundations are frequently constructed of reinforced masonry or poured concrete, supported by a continuous, reinforced-concrete spread footing. Refer to Figure 14 and Figure 15 for construction details, and to Table 9 for minimum footing widths. Stem wall foundations may include interior spot piers for support of the raised floor system. Moisture control of the crawlspace created by the stem wall foundation is an important issue. Refer to moisture control, site and building drainage, and crawlspace design and construction.

Stem wall foundations may also be constructed with pressure-treated wood members, commonly referred to as a Permanent Wood Foundation, or PWF.

Figure 14 Poured Concrete Foundation Wall (Stem Wall)

Larger View

While the knowledge of these threats is your best defense, Kind Technologies now offers an affordable computer system upgrade for any Windows operating system that will allow you to easily and quickly reverse the effects of a successful attack.

Take back your <u>real</u> security by calling us today!

KIND TECHNOLOGIES, LLC

Product & Service Solutions... *with a human touch!*

(800) 852-8723 www.kindtechnologies.com

Big Profits in the Rogue Anti-Spyware Business

Dec 15 2009, 07:04 PM

On December 11th, 2009 the FBI released a press release titled *Pop-Up Security Warnings Pose Threats*. In this press release they state:

"The FBI warned consumers today about an ongoing threat involving pop-up security messages that appear while they are on the Internet. The messages may contain a virus that could harm your computer, cause costly repairs or, even worse, lead to identity theft. The messages contain scareware, fake or rogue anti-virus software that looks authentic."

As new rogues are released almost daily, and we stay on top with them with the guides, this is not news to us. Rogues have become an epidemic in the malware scene and they do not seem to be slowing down. In fact the Wini family of rogues releases a new one almost every other day. This is further illustrated in a Kaspersky an article by Vyacheslav Zakorzhevsky called *Rogue antivirus: a growing problem* that states "Such programs are extremely widespread and are increasingly used by cybercriminals. Whereas Kaspersky Lab detected about 3,000 rogue antivirus programs in the first half of 2008, more than 20,000 samples were identified in the first half of 2009.". Unfortunately, the developers of Rogue software are typically located in countries that do not have a strong policy on cyber crime and thus there is little that can be done about it.

The reason these rogues are created in the first place is because they generate huge amounts of revenue. These rogues are promoted through affiliate programs where affiliates get paid a certain amount of dollars, some as high as $30, every time the rogue is installed on a computer. As most of these rogue companies do not care how the affiliates get the program installed, many of the affiliates will use any means at their disposal to get these programs installed on a computer. This includes using malware to silently install them or fake online anti-malware scanners to trick a user into thinking they are infected.

These huge profits are shown in the FBI press release where it states "The FBI estimates scareware has cost victims more than $150 million.". This is further corroborated in an article written by Brian Krebs titled *Massive Profits Fueling Rogue Antivirus Market* where we learn that some of the top rogue affiliate earners have made over 200 thousand dollars in 15 days. With profits such as this, it make perfect sense why these types of malware are so prolific and why they are here to stay.

Hackers make 57,000 booby-trapped websites weekly: experts

AFP/File – About 57,000 seemingly legitimate websites booby-trapped by hackers spring up on the Internet each week, ...

– Thu Sep 9, 8:33 pm ET

SAN FRANCISCO (AFP) – About 57,000 seemingly legitimate websites booby-trapped by hackers spring up on the Internet each week, computer security researchers at PandaLabs said.

The online traps are often made to look like versions of legitimate bank, auction, or shopping websites, according to the team at Spain-based Panda Security.

"The problem is that when you visit a website through email or search engines, it can be difficult for users to know whether it is genuine or not," said PandaLabs technical director Luis Corrons.

"Although search engines are making an effort to mitigate the situation by changing indexing algorithms, they have so far been unable to offset the avalanche of new websites being created by hackers every day."

Cyber crooks try to pass their rigged websites off as legitimate, putting links in emails or posts at social networks and getting them listed in query results at search engines.

Bogus websites are typically designed to slip viruses onto visitors' computers and trick people into typing in valuable information such as account names or passwords.

Online auction house eBay and money transfer service Western Union were top choices for hackers, each being subjects of fake websites in more than 20 percent of the cases found by a PandaLabs study that spanned three months.

The PandaLabs list of the top 10 companies impersonated included Visa, Amazon.com, PayPal, HSBC, and the US Internal Revenue Service.

Nearly two-thirds of the trick websites had to do with banks, according to PandaLabs.

"Given the proliferation of this technique, we advise consumers to visit banking sites or online stores by typing in the address in the browser directly rather than using search engines or links in an email," Corrons said.

Procedure for Shutting Down Rogue Internet Browser

Strategy for Avoiding the Internet Hack Attack

Use this procedure when an Internet browser window or popup will not remain closed after clicking on "X" in upper right-hand corner of the window. *Do not click on any controls inside of window* but instead utilize the procedure below to shut down the browser without activating any malicious code:

1) While holding down "Ctrl" & "Alt" keys, press "Delete" key;
2) Left click "Task Manager" button;
3) Left click "Applications" tab;
4) Locate the problem browser in the application list;
5) Left click to highlight & select;
6) Left click "End Task" button to shut down browser window(s);
7) Confirm request to shut down browser window(s);
8) Close Task Manager by clicking on "X" in upper right-hand corner.

Note: If the above procedure cannot be accomplished or does not appear to work as described it is advisable to simply shut down the computer by use of the power button or switch. If necessary hold the power button down for several seconds to shut off the system. As long as no web page controls were activated by the computer operator during the hack attack it is likely the system will reboot without any negative repercussions. To be safe, when asked the first time, do not permit the browser to re-activate a web page and/or tab(s) open at time of system shutdown.