

Security and Your Business



Newsletter #1 - April 30th, 2007

Welcome to the Archimedes Technologies, LLC inaugural security newsletter. As a Trend Micro Partner, Archimedes Technologies has access to analysis of the latest threats to your business. From time-to-time we will send a newsletter on security threats of concern. The purpose of our newsletter is to inform and educate you of the threats to your business. After a recent conference call with Trend Micro, we wanted to make you aware of two issues that may have an impact to your business.

From a Hacker to a Business Model

A little background – “Bots” are when a hacker loads software using an exploited security hole to gain control of your machine. These machines now become the robot for the hacker, hence Bots. Most users will notice the PC become sluggish but not know a Bot has been loaded. An infected machine can then be made to attack a web site by flooding it with traffic, email everyone on the machines contact list with spam (the quickest way to have your business blacklisted) or be used as a base to hack other machines that cannot be traced back to the hacker. The software to take over these machines has become big business. There are now tool kits available for purchase on the internet for the “wanna-be bot-herder.” But that is not the interesting information. Trend Micro has reported a blending of criminal elements for commercial gain. “Zero-Day exploit” is the term used for a discovered security hole that is reported and has not been patched as yet. The scenario is disturbing. A criminal element discovers a security hole in a popular program. They then contract with a bot-herder to check all of the machines under their control for certain registry entries that show the program on the machine and pay him to load their code exploiting the security flaw. All of this is accomplished before the security patch is sent from the software company (zero-day). For our example, let’s say that program is QuickBooks, Peachtree or Microsoft Accounting, your bank account numbers, employee social security numbers and business credit cards are now gone. These numbers are then sold as quickly as possible. Believe it or not, there are web sites that make a market in these numbers.

How to protect your business

Bots attack under-protected and unprotected machines. Of course you’re thinking, “I don’t have that problem at my office,” and you are probably right. But consider the machines from employee’s homes that connect to your office. Computers that connect through VPN and remote desktop look to be on the local LAN. All businesses require a remote computing policy. Larger and regulated businesses have these policies in place. Small and medium businesses don’t usually consider the threat. Do you have a

remote connection computer policy? Does your business provide anti-virus protection for employees' home computers?

New Blended Threats

Trend Micro has reported a new blended threat to get past security scanners. These threats work by breaking up the threat. They can come in through opening web sites. Web site hacking is on the rise. In fact, did you know the Superbowl web site last year had been hacked with the Zlob Trojan? It only needed one line of code inserted into the web site. The scenario for this threat is something you may see in your business every day. An employee goes to a web site and looks up news. They are linked to a web site that has a short video about the news item. The site looks legitimate and professional. When the employee clicks on the link for the video the web site tells you that a Codec (a piece of code required for media players to play certain file types) is required. The employee loads the Codec and is looked at by the anti-virus program but doesn't trigger the virus pattern. It does however, put a small piece of code in memory. The video plays normally. The video may refer to another video on the subject. This one will once again prompt to load a Codec. This one meets the criteria for the anti-spyware pattern but does not meet the criteria to block it. By not going through the anti-virus pattern again it is not flagged. The video plays and while the employee is happily looking at the video a second piece of code is added to the first and the machine now has a Trojan active and working in memory. Since most firewalls block incoming threats, a port opened by the Trojan going out is normally allowed. Your business is now exposed.

Blended Threat Prevention

The best method of prevention is to have an employee computer policy stating the computers are for business purposes only and enforce it. Employee security privileges can be changed that they do not have permission to load software (i.e. Codec). Both of these are unpopular with employees and the excuses as to why they need the ability to download and install for their job function are as varied as the threats themselves. Web proxy servers do not help with this type of threat because legitimate web sites (i.e. Superbowl) may have been hacked.

Trend Micro will be introducing URL filtering and reputational databases in the near future. 2007 PC-Cillin (their home internet security package) already contains URL ratings for web surfing. These products already report URL's to Trend and with their partners (Cisco Systems, etc.) they are receiving two billion DNS lookups a day. Web ratings on pages will be maintained in real-time so as a page becomes suspect it will be flagged and later-- if it is corrected -- it will be cleared.

News

Trend Micro CSM 3.6 has shipped. This new release has been modified to support Microsoft Vista operating systems.

Contact us

Please contact us to discuss your security requirements. We can be reached on the web at Info@archimedestech.com or at 973-937-0051.