

## Security and Your Business



Newsletter # 2 – August 16th, 2007

Welcome to the Archimedes Technologies, LLC 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.

### Under The Category of “You Must be Popular”

#### *E-Card scams infect PC's*

Why else would you receive 5 to 10 e-cards (Electronic Greeting Cards) in various formats a day? The messages have subjects such as “You’ve received an E-Card from \_\_\_\_\_,” ( fill in the blank: neighbor, secret admirer, friend, or roommate, etc.) This attack has been going on for about a month.

There are two variants. The older versions go to web sites that ask you to click to see your card. The newer ones contain attachments. The e-cards are coming from a variety of web sites. Most have real looking names, at least in the first part of the URL. In fact, when we traced one down, the company had changed their home page to just say, “We don’t send e-cards on the internet.” However, if you follow the whole URL, through the gobbley-gook, you’ll see it is not actually going to a greeting card company. These redirectors are loading keyloggers and backdoors. The other variant contains your e-card as an attachment packed with Trojans. A recent payload shows the following according to Trend Micro:

XML\_HACK.AO - a specially crafted XML file that exploits a vulnerability in *Apple QuickTime 7.1.3*.

JS\_DLOADER.NUF - This malicious JavaScript is downloaded by a malicious HTML script that Trend Micro detects as HTML\_IFRAME.CV from the Web site, <http://{BLOCKED}crogger.ws/flash/index.php>. It may also arrive via spammed email messages.

TROJ\_TIBS.AP – Trojan program. Trojans typically perform specific functions. This one hides in Windows\System32 as an executable.

NUCRP-3 – This can load any of 5 Worm programs.

TROJ\_AGENT.UYO - When executed, it accesses a Web site to download and execute files. Trend Micro detects the said files as TROJ\_AGENT.GUK and TSPY\_LDPINCH.AKY. As a result, routines of the downloaded Trojan and spyware are also exhibited on the affected system.

TSPY\_LDPINCH.AKY - This spyware is downloaded by another malware, specifically TROJ\_AGENT.UYO, from the Web site <http://{BLOCKED}mocrogger.ws/flash/P.EXE>.

It steals information such as user names, passwords, accounts, and installation information from certain applications. It also steals other account-related information. It sends all gathered information to the spyware author, either via email or by posting the information on the Web site <http://{BLOCKED}mocrogger.ws/pg/count.php>.

We are seeing more than one incidence of the above offenders. In fact there may be three or more to ensure survival upon scanning. Some of these appear to survive the initial scans and are categorized as “Identified – further action required”.

What can you do to protect your business? Quite simply, don’t open these mails. Delete them immediately from the inbox or junk folder.

## The Pinnacle of Success and a Target

*Phishing Scams Target Executives by Name*

Your competition is not the only ones that notice your firm as you become more successful. SecureWorks reports that over 1,400 executives have been targeted by a sophisticated phishing scheme.

An e-mail arrives, addressed to you by name from the Better Business Bureau (or the other variant is the IRS investigation) stating there has been a complaint filed against your firm. Click the link to view the complaint. What makes this scam different is the professionalism of the web site, the target is named and the e-mail looks legitimate enough to get past scanners. When you click the link you receive a very real looking web site.



Clicking the complaint details loads an information-stealing Trojan. Keyloggers grab account log-ins and at that point the doors to your business are wide open.

The BBB site has been shut down but the newer IRS investigation and faked "Invoice" variants are still out there. Various sources are reporting that the personally addressed e-mails are grammatically correct (for a change) and may contain imbedded objects such as .doc files. i.e. Complaint.Doc, Documents\_For\_Case.doc, etc.

To protect yourself and your business from such a sophisticated and targeted attack is to approach these e-mails with caution. If you receive an IRS notice and it looks real, a simple phone call will confirm if there really is any interest, or wait for the notice by U.S. Mail. The same can be said of receiving a bill or a BBB complaint.

## News

### *Microsoft*

Microsoft has published 9 new patches for August 14<sup>th</sup>. These patch a variety of issues and will require a reboot of Server 2003.

### *Dell Computers*

Dell is running a special on Optiplex business PC's. Buy 2 and receive the 3<sup>rd</sup> free. The way it works is a bit confusing as Dell shows a price for each machine on the quote. The overall savings is reflected at the bottom of the quote. Our quotes show that for an Optiplex 745, nicely configured, the three units come in about \$266 per unit below our discounted price.

Dell has a number of printers at the same "3 for 2 and 2 for 1 pricing". Please contact us for information.

### *Trend Micro for your Home*

Don't forget to protect your home PCs from malware. Many sites popular with teenagers are used to transmit spyware and other malicious programs. Once your machine is infected it can be very difficult to clean up, putting your personal information at risk. Trend Micro has powerful anti-spyware programs which Archimedes Technologies, LLC can purchase for you at discount.

## Contact us

Please contact us to discuss your security requirements. We can be reached on the web at [Info@archimedestech.com](mailto:Info@archimedestech.com) or at 973-845-6027.