



Capraro Technologies, Inc.

IN THIS ISSUE

WHAT IS CLOUD COMPUTING?

MALWARE AND THE MAC

A GREAT PHILOSOPHY

Compiled by Michelle Manning

QUICK LINKS

CNY BUSINESS INFORMATION TECHNOLOGY

Capraro Technologies, Inc

2118 Beechgrove Place

Utica NY 13501

315.733.0854

Dear Colleague,

Summer is right around the corner. Get away from the Internet and enjoy the good weather. Your real friends are only a beer away.

Sincerely,

Gerard T. Capraro, Ph.D.
President

WHAT IS CLOUD COMPUTING?

It's the new IT terminology being "thrown around" today, **Cloud Computing**. We've all heard or seen it in the news or on TV in commercials or in advertising on the Internet.

According to **NIST** (National Institute of Standards and Technology); *Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

The terms "cloud computing" and "working in the cloud" refer to performing computer tasks using services delivered entirely over the Internet. Cloud computing is a movement away from applications needing to be installed on an individual's computer towards the applications being hosted online. (The "cloud" refers to the Internet and was inspired by technical flow charts and diagrams, which tend to use a cloud symbol to represent the Internet.)

Examples of Cloud Computing Services

Web-based email services like Gmail and Hotmail deliver a cloud computing service: users can access their email "in the cloud" from any computer with a browser and Internet connection, regardless of what kind of hardware is on that particular computer. The emails are hosted on Google's and Microsoft's servers, rather than being stored locally on the client computer.

Over the last few years we've seen tremendous growth in cloud computing, as witnessed by the many popular Web apps used today, including: VoIP (e.g., Skype, Google Voice), social applications (e.g., Facebook, Twitter, LinkedIn), media services (e.g., Picasa, YouTube, Flickr), content distribution (e.g., BitTorrent), financial apps (e.g., Mint), and many more. Even traditional desktop software, such as Microsoft Office, has moved in part to the Web, starting with its Office 2010 Web Apps.

Types of Cloud Computing

The applications mentioned above refer to software solutions provided over the Internet, or Software-as-a-Service (SaaS). Other cloud computing services include virtual server storage (Infrastructure-as-a-Service or IaaS), such as Amazon Web Services, and software and product development tools (Platform-as-a-Service or PaaS), such as Google Apps.

Cloud Computing Benefits

Cloud services free businesses and consumers from having to invest in hardware or install software on their devices. They reduce maintenance and hardware upgrading needs; because the solutions are all Web-based, even older computers can be used to access cloud services.

For mobile workers especially, cloud computing provides incredible flexibility: professionals can work from any computing device anywhere as long as they have access to the Web. It also makes collaboration easier, since distributed teams (or a combination of mobile workers and in-office staff) can work on shared information stored centrally in the cloud via, for example, online groupware applications.

MALWARE AND THE MAC

It seems as though it was too good to be true. While I haven't heard a lot about viruses attacking Macs, the new malware "Fake Security Alert" is now showing up on Mac.

Here is a timeline of the evolution of this threat: (<http://nakedsecurity.sophos.com/2011/05/26/apple-malware-evolved-no-password-required>)

May 2, 2011: The first widely distributed (<http://nakedsecurity.sophos.com/2011/05/02/mac-users-hit-with-fake-av-when-using-google-image-search/>) fake security tool for OS X is being spread through poisoned Google Image Search results, seemingly targeting random keywords and the death of Osama bin Laden. It displays a fake JavaScript popup pretending to be a Windows XP anti-virus scanner telling you that your computer is infected.

May 6, 2011: At this point, we're seeing new variants almost daily. Some of the new samples display random pornographic web pages (<http://nakedsecurity.sophos.com/2011/05/06/mac-fake-anti-virus-attack-dirty/>) to scare you and better convince you that your Mac is infected. We also sometimes see the name change from MacDefender to Mac Security (<http://nakedsecurity.sophos.com/2011/05/06/mac-fake-anti-virus-attack-adopts-new-disguise/>)

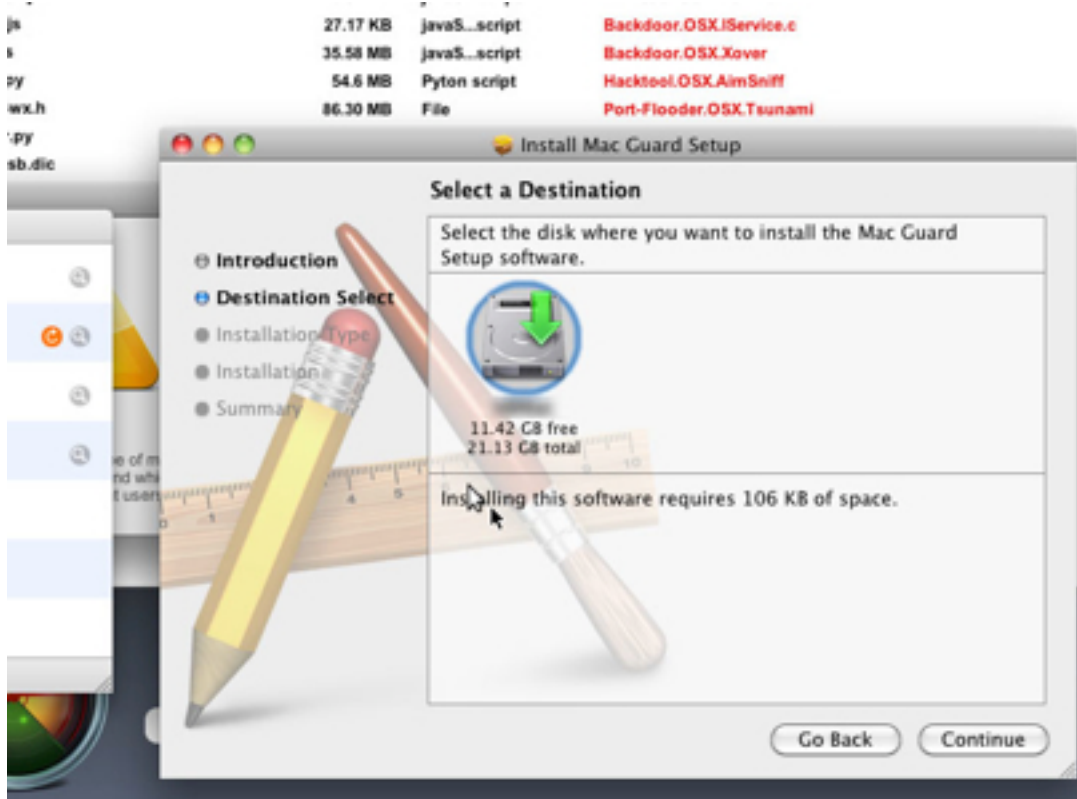
May 7, 2011: A massive uptick in the success of SEO poisoning related to Mother's Day Google searches (<http://nakedsecurity.sophos.com/2011/05/07/mothers-day-search-terms-lead-to-mac-rogue-security-software/>) results in a large increase in the infection rate. This version ditches the Windows XP fake JavaScript screen and substitutes a very professional looking fake Finder that "detects" malware on your Mac.

May 15, 2011: We begin seeing the first attempts to obfuscate the content inside the malware to disguise its functionality. Early versions had the registration codes embedded in plain text, but now the registration codes are encoded so they are more difficult to discover.

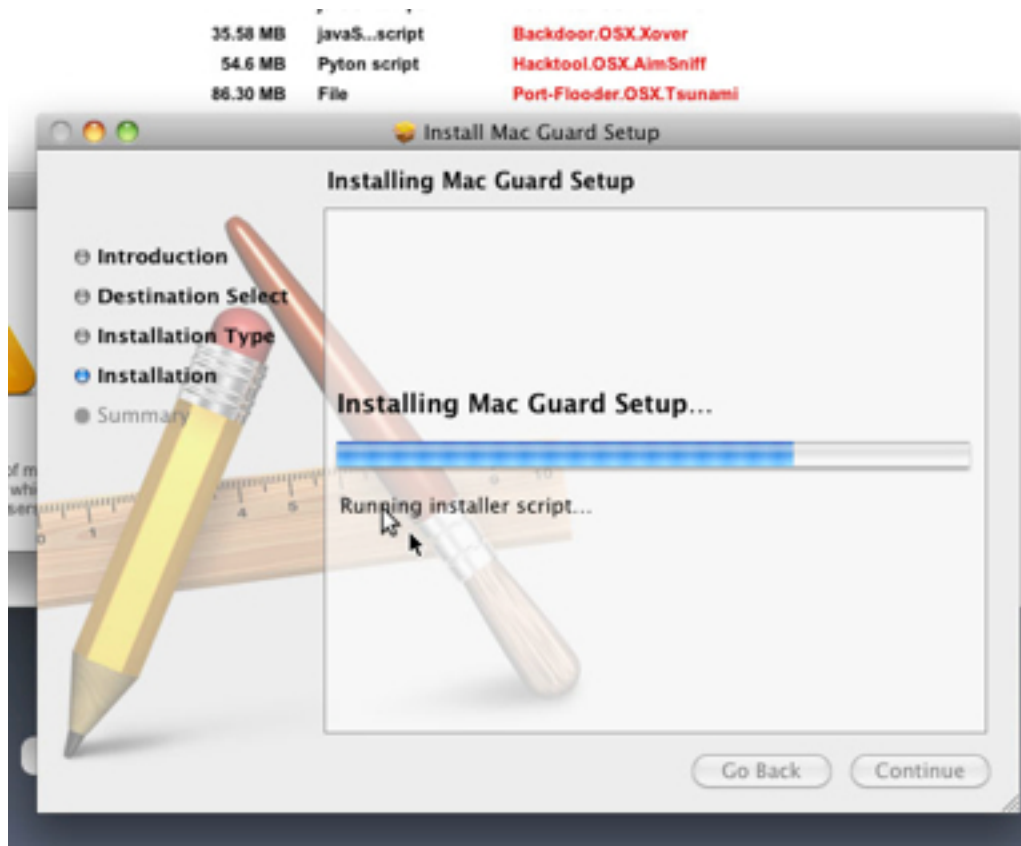
All of these original variants still prompted the user for their Administrator password to install the malware. As Apple advises (<http://support.apple.com/kb/HT4650>) in their knowledge base article on the topic, this is a warning sign and an excellent opportunity to abort the installation.

May 25, 2011: Just like in the Windows versions, the latest variants seen today (OSX/FakeAvDI-A) (<http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/OSX~FakeAvDI-A.aspx>) no longer require administrative credentials. They now install into areas of the system that only require standard user privileges. In other words, the attacks **no longer ask for an admin password**. On Windows the criminals did this to avoid UAC (User Account Control) warnings, and have copied this trick to their Mac OS X releases.

It looks like a regular install process, but doesn't require you to enter your username and password:



With the destination drive chosen, the install of the fake anti-virus software begins:

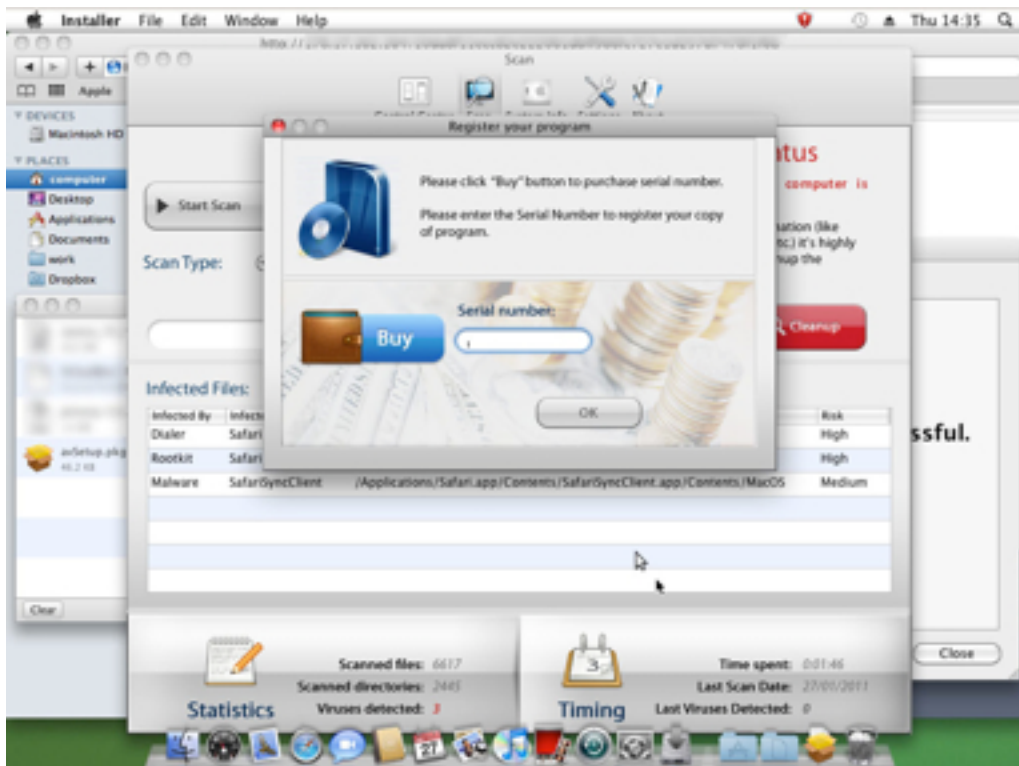


MALWARE AND THE MAC (CONTINUED)

Once installed, the software claims to have found lots of malware threats on your Mac, but advises that you need to register your copy to remove the infections:

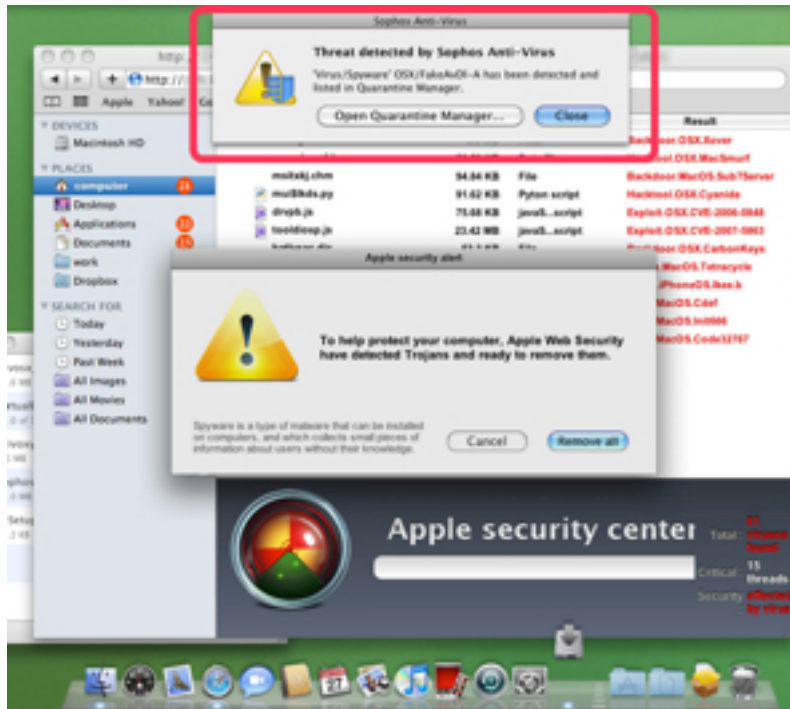


What's that? You don't have a registration number? Not to worry, the criminals have thought of that and urge you to enter your credit card details to buy the required serial number. Unfortunately, you can't tell what they plan to do with your credit card information - but you can be sure they're up to no good.



Of course, if you were running an anti-virus product on your Mac (<http://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx>**) then you would have been protected and the bad guys wouldn't have been able to scare you into entering your credit card details.

**Sophos did write this article - but I have downloaded and am trying Sophos out and while I haven't been infected, Sophos isn't a burden on my system either.



In this case, Sophos detects the threat as OSX/FakeAvDI-A.

Apple has stated:

"In the coming days, Apple will deliver a Mac OS X software update that will automatically find and remove Mac Defender malware and its known variants."

This is good news for OS X users who have been affected, but with new variants arriving daily, how will this work?

When Apple introduced XProtect with OS X 10.6 Snow Leopard, they added rudimentary detection of malware (<http://nakedsecurity.sophos.com/2009/08/28/snow-leopard-malware-protection/>). In the nearly two years since its introduction, they have only updated it a few times. (<http://nakedsecurity.sophos.com/2010/06/18/apple-secretly-updates-mac-malware-protection/>)

Are they going to develop their own anti-virus software? The fast pace with which new variants arrive requires a very different style of software development and updating than Apple is accustomed to.

Even though this article pertains to Mac - the same holds true for Windows machines and how they are getting infected with these 'Fake Alerts' - it's ridiculous that you only need to mouse over an infected image to get your computer bombarded with these alerts and dire predictions.

When things in your life seem almost too much to handle, when 24 hours in a day are not enough, remember the mayonnaise jar and the two pints of beer.

A professor stood before his philosophy class and had some items in front of him. When the class began, wordlessly, he picked up a very large and empty mayonnaise jar and proceeded to fill it with golf balls.

He then asked the students if the jar was full. They agreed that it was.

The professor then picked up a box of pebbles and poured them into the jar. He shook the jar lightly, and the pebbles rolled into the open areas between the golf balls. He then asked the students again if the jar was full. They agreed again that it was.

The professor next picked up a box of sand and poured it into the jar. Of course, the sand filled up the rest of the space. He asked once more if the jar was full, and his students responded with a unanimous "yes."

The professor then produced two pint glasses of beer from under the table and poured the contents of both into the jar, effectively filling the empty space between the grains of sand. The students laughed.

"Now," said the professor, as the laughter subsided, "I want you to recognize that this jar represents your life. The golf balls are the important things - your family, children, health, friends and your favourite passions; things that, if everything else was lost and only they remained, would still make your life full."

The pebbles are the other things that matter like your job, your house and your car. The sand is everything else - the small stuff.

"If you put the sand into the jar first," he continued, "There is no room for the pebbles or the golf balls. The same goes for life. If you spend all your time and energy on the small stuff, you will never have room for the things that are important to you."

"Pay attention to the things that are critical to your happiness. Play with your children, take time to get medical checkups, take your partner out to dinner and play another 18 holes. There will always be time to clean the house and fix the leaky tap. Take care of the golf balls first - the things that really matter. Set your priorities, because the rest is just sand."

One of the students raised her hand and inquired what the beer represented.

The professor smiled. "I'm glad you asked. It goes to show you that no matter how full your life may seem to be, that there's always room for a couple of beers with a friend."

-author unknown

You can now find Capraro Technologies, Inc on  Facebook (<http://www.facebook.com/pages/Utica-NY/Capraro-Technologies-Inc/138676162813774?ref=ts>) and  Twitter (<https://twitter.com/CapraroTech>)

Please share this newsletter with your friends and colleagues. For archives of our previous newsletters you can find them online at <http://www.cnybit.com/newsletter>.

If you have any comments or suggestions, please email newsletter@caprarotechnologies.com.

Gerard T. Capraro, Ph.D.
President
Capraro Technologies, Inc.
2118 Beechgrove Place, Utica NY 13502