PC & Internet Security

Hello, my name is Charles Prince and I am a spokesperson for Avast Software whose home office is in Prague, the Czech Republic.   I am not a salesman and I am not here to try to sell anyone any product.   Since Avast's main product is free of charge to home users, there is no need for me to be a salesman.

When you can see the desktop of my laptop, it is protected by Avast Free, the completely free version.   I have no problem with this since it uses the exact same engine and virus definitions as the Professional versions.

I have also been a volunteer helper on the Avast forum for about 8 years.   Lately, over the past 2 or 3 years, we have noticed an increase in users who have no idea about the dangers of using the Internet.   Most likely this is due to an increase in home users who have never used a computer before.   Rather than expensive long-distance phone calls, these days it is so much easier to keep in touch with family & friends with the use of the

Internet.   Various methods are used for this including email, instant messages, skype, Facebook, and other such programs.

Some schools, both elementry & high, offer computer classes these days but there are many schools who do not.   Then there are those people who where never offered that opportunity when they were in school because there were no such classes.   Not to mention, that just 10 years ago, there were many colleges who did not require the use of computers.   Now, computers are a requirement in even the smallest colleges.

So, this program is a little education about the risks of using the Internet.

~~~~~~~~~~~~~~~~~~

MALWARE 101

  What is   Malware?

Malware is actually the broadest category in which all such terms fall.

Malware, short for <u>mal</u>icious soft<u>ware</u>, is software designed to secretly access a computer system without the   owner's informed consent.   Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware,   scareware, crimeware, most rootkits, and other malicious and unwanted software or program.

Notice the use of words "informed consent" in above definition.   This means malware is not defined based on its functionality only.   For example, if you download and install a keylogger yourself for your own purpose, it might not classify as a malware.

~~~~~~~~~~~~

What is Spyware?

Spyware is a type of malware that can be installed on computers, and which collects small pieces of

information about users without their knowledge.   The presence of spyware is typically hidden from the user, and can be difficult to detect.   While the term spyware suggests software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring.   Spyware programs can collect various   types of personal information, such as Internet surfing habits, sites that have been visited, etc.

Going by this logic, it would mean even the cookies that websites install can fall in this category.   This is especially true for those cookies that record which websites we have visited, so that relevant ads can be shown to us.   Of course, all the websites that install such cookies have a privacy policy sneaked somewhere that supposedly warns users about such cookies.

~~~~~~~~~~~~

What is Adware?

Adware is quite specific to displaying unwanted ads.

Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer.   These advertisements can be in the form of a pop-up.

~~~~~~~~~~~~

What is a Rootkit?

Rootkits are one of the most technically advanced malware.   They are what people normally perceive as viruses.

A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.   Once   a rootkit is installed, it allows an attacker to mask the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and authorization mechanisms.

And here is the most scary part about Rootkits:

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternate, trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis.   Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel.   Reinstallation of the operating system may be the only alternative.

Of course, there are some rootkit scanners that help detect rootkits.   Check out free rootkit removers, GMER, and Trend Micro RootkitBuster.

(The rootkit scanner in Avast is a custom version of GMER)

~~~~~~~~~~~~~~

What is a Virus?

This is the most popularly used term by security

software, but probably also the least understood one. A computer virus is a computer program that can copy itself and infect a computer.   A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network, the Internet or carried it on a removable medium such as a   floppy disk, CD, DVD or USB drive.

The most important part of above definition is "can copy itself."   This is what separates a virus from other type of malware listed above.   And this is the feature that makes it most dangerous: Viruses can easily spread themselves to multiple computers. A single virus infection in a corporate network can cause havoc with the entire network. Do make sure you always have a good antivirus like Avast.

~~~~~~~~~~~~~~~~~

What is a Trojan Horse?

This is a less commonly used term, but the software

that it represents is equally dangerous.   A Trojan horse, or Trojan, is malware that appears to perform a desirable function for the user to run or install but instead facilitates unauthorized access of the user's computer system.   It is a harmful piece of software that looks legitimate.   Users are typically tricked into loading and executing it on their systems.

~~~~~~~~~~~~~~~~

What is a Worm?

The definition of Worm looks too similar to that of a Virus, but the definition also points out differences between both:

A computer worm is a self-replicating malware computer program.   It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer.   Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause

at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

~~~~~~~~~~~~~~~~

Polymorphic malware :

To avoid detection, polymorphic malware constantly changes it's own code, often using encryption with a varible key.   This stealthy technique poses a problem for typical scanners.

~~~~~~~~~~~~~~~~

 There is one other catagory that some consider undesirable on their computers and most antivirus services will identify them.   These programs are known as PUPS, short for **P**otentually **U**nwanted **P**rogram**s**, and include such   things as keyloggers, ad supported programs, etc.   Keyloggers are programs that record

each keystroke on a computer. PUPS are programs that can be used for good reasons or bad reasons.   Since antivirus services have no way of knowing how the PUP is being used, it detects and warns of the existing PUP.

~~~~~~~~~~~~~~~~

   I hope these definitions have left you more knowledgeable about these scary looking terms that we come across a lot nowadays.

~~~~~~~~~~~~~~~~

AVOIDING MALWARE 102

The best way to prevent malware is to not use the Internet nor external devices such as usb drives, cds, dvds, memory cards, etc.   Of course, almost no one is

going to follow that advice.   Even though hackers continue to get more cunning, you can tip the odds in your favor by practicing safe and sane computer habits. Here are a frew tips on avoidng malware.

Tip #1

If you recieve an unknown or unexpected email attachment, do not open it even if you trust the source it came from.   Some malware are able to email themselves to everyone they find in an infected user's email address book through use of an email program included in the malware itself.   Once the malware attachment is opened by you, the trouble starts.   In some cases, users do not recognise the problem until their ISP tells them they are sending out too many emails and it must be stopped or their account will be closed.

Tip #2

Computer users are just as guilty of passing along malware as hackers are of distributing them.   Do not forward email with attachments unknown to you or were

unexpected by you.

Tip #3

BitTorrent sites, Warez sites, and peer-to-peer networking clients are common ways of spreading infections.   Avoid the use of these methods when at all possible.

Tip #4

When attempting to download a legitimate program - an antivirus program, for example - use the program vender's website.   This will better assure you are getting the most recent version of the program and greatly reduce the possibility of getting a pirated version ... with malware included.

Tip #5

Pirated software is a particularly popular source of malware.   So, if your moral compass does not steer you toward the straight and narrow, the risk of malware

infection should.

Tip #6

Get into the habit of regularly checking for software updates.   Almost every software program has an update utility or button.   New exploits are being discovered almost daily in various Windows programs, QuickTime, web browsers, all Adobe programs and other common programs.   But, the user does not have to go through too many programs updating them individually. The use of Secuna PSI (Personal Security Inspector) will check the most vulnerable of these programs and the use of FileHippo Update Checker will cover almost every other software program.

~~~~~~~~~~~~

News reports of large-scale data breaches at brand name companies are more frequent than ever.   The average cost: $6.75 million.   To stay protected, you need to

know your adversary, the cybercriminal.

>From small beginnings as hackers, cybercriminals are now highly sophisticated and ambitious in their goals to take down lucrative targets.   They are also selling the tools of cybercrime like malware and botnets on underground exchanges.

Advanced Persistent Threats (APTs) can come from nation-states and terror groups.

Growth In Cyber-Crime :

The number of of malware samples per year has grown drastically.

* 2004 through 2006 - there were less than 3 million samples.

* 2009 - there were more than 11 million samples.

* 2010 - there were approximately 20 million samples.

Rate of Malware Developement :

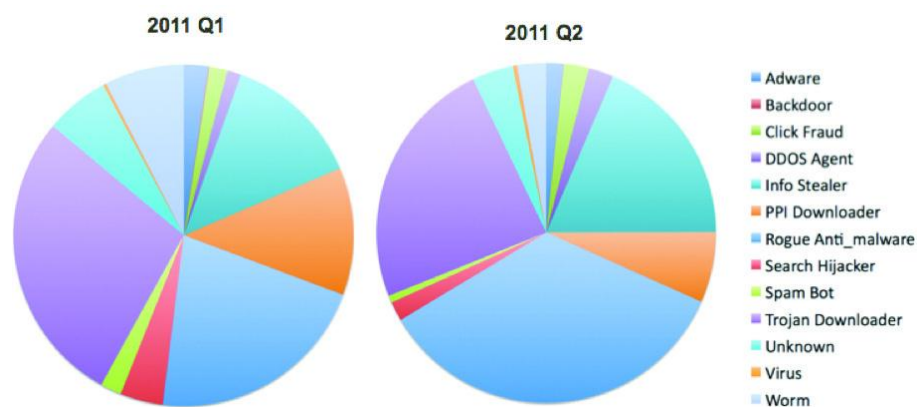* 2007 - 5 pieces of malware released online every 2

minutes.

* 2010 - 1 piece of malware released online every 2 seconds.

Many times the attitude of people seems to be that of ... "Well, they do not know me." "My computer has no information that would be of interest to anyone but me." ... and many others. The approach to computers by too many is one of naivity. They also seem to often think on a personal level instead of on a global level which one must do when using the Internet. The Internet is not a personal experience no matter how secure some application says you might be. Hackers/info gatherers could care less who you are on a personal level. What they care about is what can be used out of the information gained. Usually, this information is used for monetary gain. So, the thinking should be ... "Each time I log-on to the Internet, it is possible for me to be connected to any other person or computer globally and that all my information on my computer or information about me on the Internet is monetarily valuable to someone, somewhere."

The fastest growing malware categories are Fake-AV programs and Info-stealer executables.

  For example, Fraud software makes money by creating automated HTTP transactions to particular websites in the interest of distorting (driving up) payments to advertisers. Fake-AV software is sold on the pretense that it has found non-existent malware on consumer computers and then offering to "clean" out the infection if consumers buy the full version.
The figure below shows the distribution of these primary malware purposes across our sample in the first two quarters of 2011.
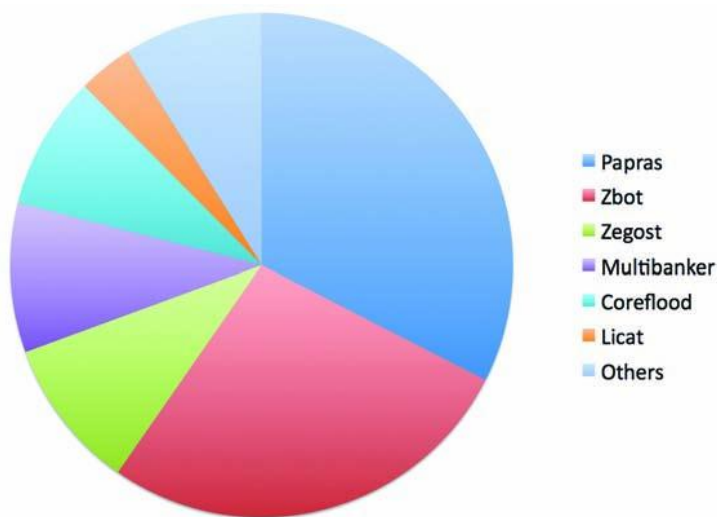

Several things stand out. The three largest categories of

malware in Q2 are Fake-AV (listed as Rogue Anti_malware), Downloader Trojans (whose primary function is to download other pieces of malware), and information stealers of various forms. Comparing to Q1, we can see a striking growth in Fake-AV (Rogue Anti_malware) and information stealing malware most likely due to a successful monetization model.

Within the category of Information Stealers, the figure below shows the most widespread types of malware. You are are cautioned that, particularly for information theft, the most widespread and the most serious may be very different.

• **Zbot (Zeus)** Primarily a banking Trojan, Zbot has become extremely famous for fraud against online banking for both consumers and small and medium enterprises and likely represents a high priority threat even to large enterprises in the form of fraud against senior executives.

• **Papras (aka Snifula)** has received far less publicity, but in our sample it appears to have become just as widespread as Zbot.   Papras is less specialized: it steals account credentials for various online services and also logs information entered in web forms.
As such, it's probably a basic tool in a number of different kinds of manually directed
intrusions and information thefts.

• **Zegost** is also primarily a keylogger.

• **Multibanker** are specialized banking trojans.

• **Coreflood** is a botnet that operated in many versions for ten years until taken down by the Department of Justice in April of 2011.

• **Licat** is believed to be associated with Zbot.

~~~~~~~~~~~~~~~~~~~~~

Information compiled by

Charles Prince

~~~~~~~~~~~~~~~~~~~~~