Global Cyber Security, Fraud and Nigerian Scams

Original Article Published January 2004 (Updated January 2013)

Cyber Security

Global awareness on the risks associated with conducting computer digital electronic business transactions securely and safely reached its highest level in the past 6 months in 2004 and has continued to get much higher.

Business, today demand to be conducted at the speeds at which the computer systems are able to work and businesses that lagged in the Business Technology race gets **trampled in the process**. We shall be noticing many more different kinds of businesses getting connected to the internet to take advantage of Global Connectivity for instant response and reaction to business.

The number of confirmed computer attacks and incidents was up 84 percent over those in the fourth quarter of 2002, according to a new report released by Internet Security Systems Inc. While NAT (Network Address Translation) Firewall and other kinds of Firewall protective routers/switches will keep hackers from discovering the nature and structure of your network (how many systems you have, what operating systems they're running, and so on) and help protect you from attackers trying to break in, they are good first line of defense, though they typically do not inspect connections for malicious code, then that's only half the battle. The other half is protecting your network from hackers who have already broken in or can possibly still break in--via a Trojan horse or Spyware for example--and are trying to send outgoing messages and your private information to the Internet from your systems.

The new ways that Cyber-Terrorists, Cyber-Vandals and Crackers has learned to use to get into computer systems cause for me to suspect that the real reason for the decline in viruses this year is that the serious virus writers have graduated to more sophisticated attacks, such as Trojan horses and Spyware. The occurrence of both of these threats increased in 2003. While it's now less likely you'll be infected by another LoveLetter- or Melissa-type virus, it's more likely you'll be hit by other maladies that could cause as much--if not more--damage.

While the maladies that could cause as much--if not more--damage. **Article Update October 02' 2005 :** 2 Years later in October 2005, it has become very clear that the suspected graduation to more sophisticated attacks is a new wave and form of even more dangerous security concern to combat known as Malware.

Malware programs basically get attached to HTML forms fills out on a website. It easily collects information such as users' personal and private information including name, credit card number, address, SSN, user names and passwords, and practically any type of information that will be filled in a web form.

A few years ago, such programs and data operations could not be performed without physical access to a users' computer to retrieve the collected information by the malware program now also known as ‘keylogger’. Malware program is the newest variant of the previous big family of Spyware mentioned earlier. They are generally known as **Dumaru** or **Nibu**. The malware-spyware key logger is known as **Srv.SSA-KeyLogger**. Srv.SSA-KeyLogger is a backdoor program that secretly steals data through the HTML forms from users' internet sessions, from online transaction sessions.

We have exhaustively and closely studied products and the results of extensive tests from an independent organization. The study and tests was performed on products from Major Enterprise-Class and Small Business-Class Security Software Manufacturers.

Here's what you need to know about how these pests work--and how to protect your system from them.

To refresh your memory, Trojan Horses, **open ports** on infected machines allowing malicious users to access data on those systems remotely. Mainstream use of this technology is called *Spyware*, ad-serving software that (in the best case) allows advertisers to update and target advertising on your computer or (in the worst case) allows advertisers to track your Web habits for sale to other advertisers.

The level of sophistication and the high-technology adopted in committing computer crimes, frauds and scams electronically has also become a **Global threat to Individuals, Small Businesses, Governments and Investors seeking to conduct business electronically with partners, increase their business portfolio by affiliating with other businesses and to expand globally.**

*’In **November 2011**, after 5-years of intensive tests, experiences and solutions research, Ifeanyi O. Asonye published an article titled **'Managing Risks for Global Entrepreneurial Initiatives In The New Era'** (A Solid Practical + Conceptual Review and Overview for Current, On-Going and Futuristic Solutions and Research) laying out a Comprehensive Blueprint for Solutions to issues raised in this article, from a Global Perspective.’*

One of the real stories of the early part of 2003 was the number of **worms** unleashed on the Internet. The most troublesome being the **SQL Slammer**, which attacked servers running Microsoft Corp.'s SQL Server 2000 database software that disrupted business for Financial Institutions, Governments, Small and Large Businesses. The worm exploited a vulnerability for which Microsoft had released a patch **six months** earlier infecting thousands machines in less than 10 minutes in late January.

Update of March 2007

The Evolution of RootKits

What is a Rootkit, and what is the difference between a Virus, Malware and RootKit?

Rootkits were first discovered in 2005, or generally came to the public awareness with the **Sony BMG CD copy protection scandal**. While a Virus directly modifies software components of a system, **a Rootkit silently installs like regular system drivers or system kernel, so end up like legitimately running applications, systems data or files to any kind of operating system.**

Rootkits change certain areas of the Operating System while avoiding detection (**the reason Microsoft is now locking down those areas from everyone including other security software vendors with the 64 Bit Operating Systems and the Enterprise Version Software**) leaving them out to the APIs. **It has been a very hot issue in the systems security area in 2006 and 2007.**

Silent, **Unauthorized**, **Unsupported** and **Digitally Uncertified** Device Driver Installations, and Direct Access to an Operating System **Kernel** like and modifying it in the name of 'Security, Data Protection, **Software Updates, Plug-Ins** or the Driver Installations' could be likened to opening an ipod, a DVD Player, Zune or a Linksys/CISCO Networking Router with screw drivers to **HOT-SOLDER Wires**, ICs, Resistors; to add an Amplifier, a Headphone, Speakers or a PC Network Card '**Directly'** on the '**Circuit Board'** **than use the Input and Output Plugs provided by the Manufacturer.**

RootKits, originated from extremely beneficial applications, however, malware writers started using the method and technology **to avoid detection from the OS, and from any of the most effective Security Software applications**. ***RootKits currently exist for almost every known Operating system***

Unauthorized and **digitally uncertified** access and modifications to an operating system kernel, with security suite of products and firewalls installed to protect it is **similar to entering a building with security alarms**, motion detectors, security devices installed, **without triggering off the alarms**, without being captured by the video cameras, while going through the doors, and windows undetected. This is very similar to the good old movie **"The Invisible Man" (1933),** so, one could get creative and call a RootKit **"The Invisible Software" (2007)**.

As it used to be a joke, prank, game or an excitement for a harmless computer entertainment, **or just to stretch a systems to its limits**, now, its not.

Global Cyber Security, Fraud and the Nigerian Scams... Continued... Article by Ifeanyi O. Asonye

WHO'S BEHIND CRIMINAL BOT NETWORKS?

Posted: Tuesday, April 10 at 07:00 am CT by Bob Sullivan

Today, we examine who is behind these networks of infected computers.

For years, computer hackers typically were precocious, anti-social teen-agers who committed digital violence just to get attention. But computer crime has grown up, and grown into a big business. **Now it is used by highly organized gangs to steal millions of dollars.**

The top gangs, most agree, are in Russia, Eastern Europe and Brazil, **although there also are a few up-and-coming cybercrime syndicates in Asia.**

Cybercriminals tend to be talented computer programmers who can make **much more money stealing than working**, the experts agree. **There is so much money to be made in Cybercrime that some observers speculate that terrorists are using it to raise money and support their organizations.**

Computer security experts disagree on whether terrorists are involved in Cybercrime, but **there is one sure sign that computer crime has become a much more sober affair: Many experts interviewed for this story shied away from talking about the topic of who's behind botnets, pointing to concerns for family safety.**

"When I got into this, it was kind of a game," said one expert who spoke on condition of anonymity. "Now, it's very serious. **I wouldn't want my name attached (to comments about the topic)."**

That's a new sentiment in an industry that has often been criticized for using hyperbole to generate publicity. Read More

Today, all software, computer networking hardware vendors and manufacturers has been equally hit by the various flavors of adware, spyware, rootkits, worms, viruses and Trojan horses. Any operating system running on 95 % to 98% percent of the desktops and more servers will be hit most by the numbers generating more publicity.

Slammer was only the beginning. Several others less successful but equally annoying worms also made their debuts during the first quarter. Deloder and a new version of Lovgate both hit the Web in March, as did Code Red.F. In addition to generating a tremendous amount of network traffic as they propagate and slowing down the entire internet traffic, both Deloder and Code Red.F **install back doors on infected machines**, **leaving machines vulnerable to future manipulation by attackers.**

Suddenly, it became the full time job of someone to monitor systems security and install patches. In most cases, it is important to ensure that the patch being applied do not affect the other business and proprietary software in the production environment.

ISS (Internet Security Systems Inc.) compiles its quarterly statistics, known as the Internet Risk Impact Summary Report, by culling data from more than 400 intrusion detection sensors installed at customer sites.

Frauds and Scams

Cyber-attacks also have been complicated with the Frauds and Scams emanating especially from countries like Nigeria though it has been known to be worst the Global Financial Indutry by 2012, though ***for whatever reason***; Nigeria (**now, they come from - and are all over the world**) seems to appear on the records and at the heart of some of the biggest money scams.

Many flavors of the popular **'419 Scam'** emails popularly known as **"the Nigerian Princes Letters".** '419' is the decree in Nigeria against 419. Another popular term for it in Nigeria is **OBT (Obtaining By Trick).** Nonetheless, t**he letters and emails most of the time appear obviously as scams or not from a legitimate business. To view some such letters click here to read more**, the comments that come in suggest that this scam hurt the reputation of legitimate African businessmen among people who have no other knowledge of, e.g., West African society. **As if business was not tough enough.**

The relatively few scam artists cast an unearned shadow of suspicion over many legitimate global business dealings. Africa is truly a country rich in resources with a tremendous history and is quite attractive to many aggressive 'business people.' Many of the scams actually play on the victims' greed, though many play on victim's financial neediness, altruism or religious feelings. The specifically business-related scams entice small to mid-sized business people or faith-based organizations to pay advance fees to bid on non-existent contracts, or to give money to pay fees associated with moving money to their bank account. The religious scams, sprinkled with a lot of references to God and church work prey especially on faith-based organizations.

There are many concerned individuals and organizations from the many different parts of the world that have published articles and also shown great concern in many different ways as one of the seasoned, Canadian and World-Class Veteran **Dr. Joel A. Freeman stated: 'Perhaps (let us hope) a future Nigeria, tranquil and prosperous, will see fewer of these frustrated novelists-in-crime -- their literary talents will have found other legitimate avenues by which to profit. The 419 scams are truly sad, because there are so many wonderful people in Africa. Many people truly love Africa and love Africans.'**

Nothing about this issue is taken as a criticism of any nation or people, nor do we suggest that there are no scam artists in other countries'. You can find more about him and read his writings at http://www.freemaninstitute.com/JAFbio.htm

On the **Internet Fraud Complaint Center (IFCC) report** released in April 2003, ("IFCC is a program of the FBI and the National White Collar Crime Center, and its mission is "to address fraud committed over the Internet") statistics, about 75,063 complaints were filed in 2002 and the "total dollar loss from all referred cases of fraud was $54 million, up from $17 million in 2001, with a median dollar loss of $299 per complaint.'

Ifeanyi's Final Commentary.. on Global Security

Final Commentary.. We've asked, how do you know that an email is really **who it says it is**? How would you tell if a phone call is the voice of the person you think that it is, and if that voice **can be trusted**?

With **experience**, concentration and focus many times we can tell anyway, right?. **Yes- Let's face it. The REALITY is that we could all get very smart and highly intelligent**, we've **also seen how a 'phishing' email worked right back on the smartest people in IT and in the security areas, and back on the scam artist themselves and just wondered why and how they fell for it themselves.**.

What "if" one was just fairly tired and mistakenly clicked on a link that downloads a Malicious Code? What if a Legitimate Account and Identity is hijacked? What if..., happens? We can go on and on.

This is not about getting paranoid and scared of using computers on the internet, doing global business, or taking reasonable and strategic business risks. **It's just about the awareness and safety, playing safe on the internet, for work, play and for your global business.**

Follow Us On: