TECHNOLOGY TIMES

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

By Computer Networks of Roanoke, Inc.

Serving Roanoke and surrounding areas since 2006

Volume 8, Issue 5 **May 2015**

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Hank Wagner, Owner/Founder
Computer Networks of Roanoke.

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

Crooks and Miscreants

Malware Takes Bold Steps to Avoid Analysis (May 4, 2015) Malware known as Rombertik goes to great lengths to evade analysis.

Rombertik employs a number of methods to prevent researchers from examining its workings, including a component that self-destructs if it detects it is being examined, and when it does, it attempts to

See Rombertik Page 2

INSIDE THIS ISSUE

Culture of Security

This month, let's talk more about developing a "Culture of Security".

It seems that everywhere you look, there are companies out there losing the personal information of their clients, Patients and customers.

Have you stopped to ponder what would happen to your business if you lost your customer's personal information and had to report it in the news?

Are all of your Patients and clients so understanding that they will forgive you? How about your potential clients? Do you think that someone who was thinking about doing business with your firm would have second thoughts if they saw you had lost all of your existing customer information to a hacker?

If companies do not start thinking about how to appropriately protect their information from getting into the public domain, then you can bet that the government is going to step in and require that you install adequate protections.

A good example of that is HIPAA which applies in the medical world. A Physician's office is required to perform a Security Risk Analysis, document the results, fix the problems found, develop Policies and Procedures for staff to follow, implement employee training, and to install appropriate controls on their computer network to prevent the leakage of data.

Network security generally involves layering protection and then managing that protection from a central computer. You want a high-end Unified Threat Management firewall with it's own anti-virus, Intrusion protection, Content

See Culture Page 3

Rombertik continued from Page 1

delete hard drive data and render the infected machine useless until the operating system is reinstalled.

Rombertik spreads through spam and phishing emails and is designed to harvest all plain text entered in the browser window.
http://arstechnica.com/security/2015/05/04/super-secretive-malware-wipes-hard-drive-to-prevent-analysis/

What is the takeaway? Educate the staff!

- Do not open emails from people you do not know to keep from getting infected
- Do not click on links in emails
- Stay off of sketchy websites

Tip:
If you hover the mouse over a link in an email, it will tell you where the link is going to send you. So, if you receive a link that purports to be your credit card company, and you hover over the link with your mouse, and the link that show up is some place in a foreign country not associated with the credit card company, then you know that the email is a phishing email designed to trick you into giving up your personal information.

Constant reminders from management will go a long way to keeping the staff in line.❖

Predictable Results For a Predictable Fee

We do it all…HIPAA Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, IT Consulting.

And, we do that for businesses with as few as 10 PCs.

We are looking for a select number of new clients in the medical and professional services fields.

If you are dissatisfied with the level of service you are getting from your current IT Vendor, pick up the phone, call me, Hank Wagner, at 757-333-3299 x232, or email me: hank.wagner@computernetworksinc.com and let's chat a bit about your needs. ❖

SANS Security News

www.sans.org

--US Justice Department to Review Cell Site Simulator Use (May 3 & 4, 2015) The US Justice Department (DoJ) will review the policies involved in the use of cell phone-site simulators, also known as IMSI catchers, or by the brand name Stingray. The technology tricks cell phones by making them trust the technology as a cellphone tower, while collecting data about the communications including device locations, metadata, and even content of communications. One of the American Civil Liberties Union's (ACLU's) concerns is that the device collects data from phones that are not being targeted in an investigation.
http://www.computerworld.com/article/2917803/data-privacy/us-reviews-use-of-cellphone-spying-technology.html

--Ryanair Investigating EURO 4.6 Million Electronic Bank Theft (April 29 & 30, 2015) Ireland-based, low fare airline Ryanair was the target of an attack last week in which thieves stole EURO 4.6 million (US $5.15 million) from a company bank account. The money was sent to a bank account in China, and the funds have reportedly been frozen.
http://www.theregister.co.uk/2015/04/30/ryanair_online_heist ❖

Culture continued from Page 1

2015 Verizon Data Breach Investigations Report

The Verizon Data Breach Investigations Report (DBIR) is an annual publication that provides data from and analysis of information security incidents, with a specific focus on data breaches.

Some selected findings:

- Phishing (targeting the human) was one of the top ways bad guys are accessing networks. The median time was 1 minute 22 seconds across all campaigns.

Comment-there is a growing need to educate the end users who are being targeted in these types of attacks. The end user has to be aware that clicking on a phishing link can lead to a compromise of the computer network and subsequent loss of data. This year, Verizon noted that some of these stats went higher, with 23% of recipients now opening phishing messages and *****11% clicking on attachments*****. *The numbers again show that a campaign of just10 e-mails yields a greater than 90% chance that at least one person will become the criminal's prey, and it's bag it, tag it, sell it to the butcher (or phishmonger) in the store.*

Lance Spitzner, Training Director for the SANS Securing The Human program, notes that "one of the most effective ways you can minimize the phishing threat is through effective awareness and training. Not only can you reduce the number of people that fall victim to (potentially) less than 5%, you create a network of human sensors that are more effective at detecting phishing attacks than almost any technology."

- 99.9% of the exploited vulnerabilities were compromised more than a year after being identified

Comment-this indicates that regular patching of software is a huge deterrent to being compromised. Installing bugs fixes and security patches regularly reduces your expose to 00.1%, according to the Verizon study.

- The common denominator across the top 4 patterns (accounting for nearly 90% of breach incidents) is people

Comment-train your staff to be cautious. Suspect everything, especially as it relates to the Internet. These cyber crooks are not coming by your office and breaking in during the middle of the night; they are getting your staff to install their malicious software for them.

- Malware is reduced with proper network hardware and software

Comment- Our analyses of the data showed that half the organizations experienced 35 or fewer days of caught malware events during an entire calendar year. Keep in mind, by the time it hits appliances, controls like firewalls, intrusion detection systems (IDS)/intrusion prevention systems (IPS), spam filters, etc., will have already reduced the raw stream of malware.

So, what am I trying to tell you?

It's a new day and a new way of doing business. The security measures that worked a couple of years ago, are no longer relevant today. Your business needs to step up its game to protect your customers, Patients, and clients. ❖

Filtering (to keep the staff from going willy-nilly all over the Internet), a company wide anti-virus/anti-spyware that is managed from a single server, regular patch updates to all of the software installed on your network to fix bugs and security issues, a backup of your data to some secure offsite location, and some monitoring of all that to insure that it is really taking place.

From an employee standpoint, you want some regular reminder training that the Internet has bad stuff as well as good, you want to restrict staff Internet browsing to business related sites (there is always one in the crowd who thinks the company computers are there for their personal use) insure that the anti-virus is updated hourly on every machine and that all the machines are scanned every night.

Your staff training should emphasize that Security of the company's clients, Patients and customers is foremost and that it must be protected from escaping onto the Internet.

Your employees are going to be the weakest link in the security process. If you tighten up all of the computer controls, then educate staff, you have gone a long way to making your network safe.

Let us know if you want to chat more about how to protect your business. Heck, we might even take you to lunch on our dime. ❖

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

Sad, but, true…

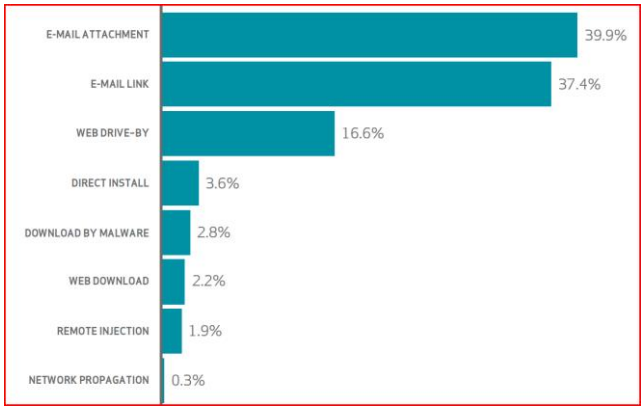
The Lighter Side:

The First Computer Bug Was Actually A Moth?

- The first actual computer "bug" was a dead moth stuck in a Harvard Mark II computer in 1947.
- Big banks don't process checks and debit card charges to your account in the order they're received, but instead use a computer program that selects the biggest amounts first and charges them against your account, emptying your account faster and resulting in more overdraft fees (profit).
- In September 1956, IBM launched the 305 RAMAC, the first "SUPER" computer with a hard disk drive (HDD). The HDD weighed over a ton and stored 5 MB of data.
- A computer as powerful as the human brain would be able to perform about 38 thousand trillion operations per second and hold about 3,584 terabytes of memory.
- The first entirely computer-generated movie sequence in cinema history was the Genesis Device demonstration video in *Star Trek II: The Wrath of Khan*. The studio that made the scene would later become Pixar.
- CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."
- MIT has developed computer software that can identify and distinguish a real smile from a smile of frustration.

Primary Ways Computers Are Compromised

Verizon Data Breach Investigations Report 2015

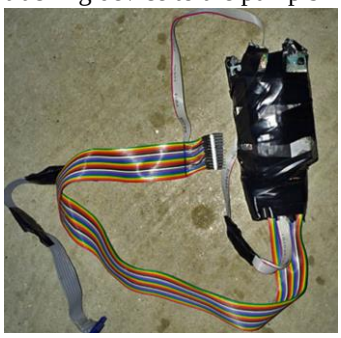


2 common factors-

- The Internet
- Your staff

One For The Good Guys

One morning last year the Redlands, Calif. police department received a call about a skimming device that was found attached to a local gas pump. This wasn't the first call of the day about such a discovery, but Redlands police didn't exactly have time to stake out the compromised pumps. Instead, they attached a specially-made GPS tracking device to the pump skimmer.



At around 5 a.m. the next morning, a computer screen at the Redlands Police Department indicated that the compromised skimming device was on the move. The GPS device that the cops had hidden inside the skimmer was beaconing its location every six seconds, and the police were quickly able to determine that the skimmer was heading down a highway adjacent to the gas station and traveling at more than 50 MPH. Using handheld radios to pinpoint the exact location of the tracker, the police were able to locate the suspects, who were caught with several other devices implicating them in an organized crime ring.❖