4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381

In this issue of the FNGi Focus Newsletter, we talk about the past 19 years of being in business. The latest update on the DHCPatriot, our DHCP-based authentication solution. And then we delve into the basic evolution of computer viruses and finally we talk about The Heartbleed Bug. One of the largest security threats to happen in the wide internet in a very long time.

First Network Group, Inc is a proud member of the Ohio Telecom Association. Serving Ohio since 1895!

FOCUS

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS July —September 2014

In This Issue

19 Years and Going Strong pg 1
A Basic Evolution of the Virus pg 2
Heartbleed Bug pg 3
DHCPatriot News pg 3

19 Years and Going Strong

July 2014 marks the 19th corporate anniversary for First Network Group, Inc., and I invite you to celebrate with us this year as we evolve toward our 20 year milestone. As we contemplate our 20th anniversary in 2015, that future would not be possible without the rich history that we have – both a history of technological skill, technical and organizational agility and our relationships with you, our valued customers, nor would it exist without the excellent people who have become indispensable as part of the First Network Group family.

When FNGi was founded in 1995, as AOL and Prodigy were introducing browsers to let their customers access the World Wide Web, and the government controlled NSFNET was retired, Americans were about to add a new term to their daily vocabulary: The Internet. Many of you were in the vanguard of that moment: Com Net (in Ohio) with Bright.Net, WinBrightNet (then Access Wisconsin, now Airstream Communications) and BrightNet Oklahoma.

In 1995, Cisco Networks and Sun Microsystems were the big brands as First Network Group worked with Local Exchange Carriers to connect their DS0 and DS1 based networks to the world, and analog PSTN to their customers. First Network Group provided Technical Support (then, often called Help Desk) to end-users' and their (mostly 1200 BAUD) modems on Windows 95 PCs with a few Apple Macintosh computers thrown in. Oh how times have changed!

Today, there are more home computers and devices running Unix-based systems with Google's Android platform and Apple's iOS and OS X operating systems, than all of the computers and devices in the IT departments of old.

In the past providers recommended US Robotics modems for reliability, our Tech Support department now supports:

- 91 Specific DSL Modems from 23 different Manufacturers
- 36 Specific Cable Modems from 9 different Manufacturers
- 52 Specific Cell Phones and Cellular Modems from 15 different Manufacturers
- 10 Specific Cable/IPTV Set Top Boxes from 5 different Manufacturers
- 10 Specific Video Game Consoles from 3 different manufacturers.

When we started, we had about 10 main articles in our in-house Knowledge Base. We now have nearly 1000! We originally supported Dial-up on 3 main Operating Systems. We now support 10 distinct connection methods across 15 distinct PC operating systems and all major tablet and mobile Operating Systems.

Part of our success has been rooted in responding to your specific needs and requests. Tech Support is now available 24/7 and with live answer – and for far more than your Internet subscribers. Our expanded Customer Care Center has implemented support for your Telephone, CATV and Cellular customers along with your Internet subscribers. We also handle calls for a nationally recognized leader in providing "Safe Harbor" for the Telecommunications Industry.

Continued on Page 2

19 Years and Going Strong

... continued

Stephen C. Walter, CEO

We were recently contacted to provide customer service for a client's Home Security/Home Automation business and we were happy to develop the in-house training materials and support protocols to let their new customers have the high quality level of custom support that we provide for their Internet, Local Exchange, Cellular and CATV customers.

When it became obvious that unmanaged DHCP implementations were not compliant with USA Patriot Act and CALEA requirements, we created the DHCPatriot to provide you with a redundant, carrier class system that would give you the management and reporting capabilities to use the simplicity of DHCP and meet your compliance requirements. Earlier this year, in response to your requests, we introduced a DHCPatriot virtual machine for those of you who have high capacity virtual servers and the in-house IT teams to operate them.

My simple point is this: as your technological and business needs have changed, First Network Group has happily evolved to support you. With great thanks for your past patronage, we at First Network Group look forward to serving your needs for decades to come. Have a new project? Want to offer introduce a new product? Would you like to consolidate your current support services into one great customer oriented Customer Service Center?

To paraphrase a well-known invitation from the past "Call us, we'll tell you how it works."

Sincerely,

Stephen C. (Steve) Walter
President/CEO

A Basic Evolution of the Virus

In the early days of networking computers, viruses were little more than proof of concept bits of code. Can I write a program or exploit a function where I can remotely open a CD drive on another computer or cause some other strange behavior?

These prank style antics grew bigger in scope and power and quickly began to spread around the Internet. Then the environment took a more sinister turn, by bulking up the things these viruses could do. Viruses became punishing programs that would eat up CPU speed, bloat up free hard drive space, spin drives faster than they were designed for and even delete user or operating system data. They were deployed by people to punish others and destroy property and data.

Without tangible rewards creating viruses start to get a bit bland. Viruses then started evolving to an end game or reward. Viruses that previously may have taken a computer offline either by design or by unmitigated spread of the infection fell out of favor. It was becoming more and more important to not have the target go offline or notice the infection. If the target went offline, the attacker wasn't able to reap the benefits of the infection.

And what were those benefits? In that generation, most of the time it was stealing address book entries to sell to spammers. Personal information was rarely targeted, but corporate data was ripe for the picking.

This is the era of BotNet. Many viruses infect, spread and lay totally dormant. These infected computers are now slaves to the whims of the attacker. If an attacker wants to take down a large site with a DDOS attack, they can wake up 1,000's of these sleeping infections to begin slamming a site with traffic. Each computer sending out just enough traffic not to be noticed but when combined as a whole their effects can be devastating. These "Bots" can also be put to task to sneak out little bits of Spam here and there. Not enough to get flagged by the normal detection practices of a modern ISP, but combined with the sheer numbers of those infected can wreak a lot of junk mail havoc.

The virus/malware industry has gone thru a major transformation over the years. Viruses have evolved from simple pranks to a hacker's tool with which to make money, create mass damage or capture information. Viruses don't say "Happy 1999!" on your screen anymore and stop there. These new viruses like to hide, wait and use the power of their combined infection numbers to make the criminals involved a lot of money.

Find us on Facebook www.facebook.com/FirstNetworkGroup

Share this newsletter and properly recycle it.
If you'd like to receive our email based newsletter instead visit our website at **www.network1.net** and sign-up.

Heartbleed Bug

The modern internet relies a great deal on secure encrypted information. Used for bank transactions, online shopping, and any other confidential personal information, encryption is key to stop others from spying on your data. One of the more popular means of encrypting information is with OpenSSL, which is an open source version of the Secure Sockets Layer protocol, and used by a large number of web hosting servers. A bug in this software has been discovered that potentially allows a hacker to access bits of encrypted data. With millions of devices potentially affected and countless secure communications potentially compromised this issue had the potential to be one of the biggest bugs in the history of the internet.

The bug has been in a single version of the OpenSSL code since 2011, but it was just recently discovered. Fortunately, only the most recent versions of OpenSSL are affected, and many web servers were still using older versions. This greatly decreased the risk. Also, on the same day of the announcement, a patch for OpenSSL was released, which allowed people to fix their affected systems very quickly.

None of First Network Group's critical systems that house customer data were affected. Customers who were using this version of OpenSSL were patched immediately by our IT department. An issue like this highlights the importance of having an experienced IT team. First Network Group strives to be the best option to fill that need for our customers.

For more information on the Heartbleed bug check:
http://heartbleed.com

For more information about First Network Group's IT Services offerings, contact Randy Carpenter at 1-800-578-6381, x1

DHCPatriot

Work on DHCPatriot version 5.4.0 is well underway.
This revision will include enhancements to our IPv6 support on the DHCPatriot as well as enhancements to our API and finally the option to prevent a device from getting an IP address via DHCPv4.

Our IPv6 enhancements include the ability to use the web administration interface with an IPv6 address. Also, ping and traceroute to IPv6 hosts are now supported on the DHCPatriot system. This will help diagnose connectivity issues between the DHCPatriot and other IPv6 devices.

The bulk of the changes in this version are changes and additions to the API system making it even more robust and useful. When enabling a suspended device via the API, passing an additional parameter will cause the DHCPatriot to verify the user/password info via RADIUS before enabling the device.

New API calls allow the addition and removal of "sticky" IP addresses as well as listing those already assigned.

When authenticating a device with the API, a new parameter allows the device to be authenticated via its current IP address instead of requiring the MAC address, although the MAC address may still be used. The View Authenticated Users function of the DHCPatriot's web administration interface can be accessed in another API call that can perform similar searches returning XML formatted results. These changes allow more comprehensive API calls to better support the integration needs of our customers.

Another very useful addition is a "black list" for MAC addresses that prevent a specific device from getting an IP address in the first place. This can be useful for preventing certain devices from getting on the network for virus cleaning purposes or other security concerns.

We expect to release 5.4.0 of the DHCPatriot system later this summer.

— Darren Ankney, dankney@network1.net 1-800-578-6381 x3