



Vol. 1, No. 2, November 2009

## Flagship Solutions Group eNewsletter

### There's a Hole In Your Firewall

Firewalls provide you with many essential security features you need to protect your network, however if you want to browse the web you must keep ports 80 (HTTP) and 443 (HTTPS) open. Firewalls can help you by preventing outgoing connections to rogue web sites if the IP addresses of such sites are defined explicitly to the firewall.

However most firewalls, if not all, **do not examine outgoing and incoming encrypted packets passing through ports 80 and 443**. Firewalls also are incapable of stopping any "Distributed Hash Table" (DHT) routed packets, since DHT does not use IP addresses.

**SO YOU HAVE A HOLE IN YOUR FIREWALL. Encrypted packets generated by protocols excluding HTTP or by circumventing proxies can pass through your network firewall unchallenged.**

Protocols such as Gnutella, BitTorrent, Kazaa, LimeWire, etc., and circumventing proxies enjoy an almost virus-like popularity as an easy means of sharing music and video files with other media enthusiasts. Unfortunately, they can also share sensitive corporate and personal data with strangers around the block, the country or the world.

**Real life studies show millions of data breaches caused by the unchallenged port 80 and 443 encrypted DHT packets created by those protocols.**

Information leakage and data breaches are very expensive and embarrassing, and may lead to criminal prosecution, statutory damages, forfeiture of network equipment and victim's restitution.

Yet another major and catastrophic damage resulting from allowing unchallenged port 80 and 443 encrypted DHT packs is Malware and botnets. The originators of viruses and botnets use the hole in your firewall to embed malicious viruses and botnets in encrypted DHT packets through ports 80 and 443 because they know that you cannot stop those packets. Your network is exposed to the most dangerous risk on the Internet.

The inability to challenge encrypted DHT packets through port 80 and 443 raises another troublesome problem. DHT causes network delays and congestion for two reasons. DHT represents an overlay routing which is NOT compatible with the standard Internet routing; as a result, major network congestions may occur because of the disruption of routing caused by DHT. The second reason is the massive amount of digital data being shared through DHT if the packets are generated by a file sharing protocol.

The hole in your firewall is getting bigger each day, threatening the very survival and security of your network. There is only one security device that can stop this threat which is not controlled by other network devices, including IDS (intrusion detection systems), IPS (intrusion prevention systems), packet shapers, web scrubbers, etc. Ask Flagship about its unique and patented solution powered by SafeMedia. Contact Flagship Solutions Group at 561-289-2045 or [click here](#) to email us.

---

## Upcoming Events:



Flagship Solutions Group is an accredited IBM Infrastructure Specialty Business Partner. Join us for lunch at The Capital Grille on Wednesday, November 18<sup>th</sup>, 2009 for an informative presentation on IBM's virtualization strategy.

Date: November 18, 2009  
Time: 11:30 AM - 2:00 PM  
Location: The Capital Grille  
At The Galleria  
2430 E Sunrise Boulevard  
Fort Lauderdale

This is an exclusive invitation to a luncheon seminar on Virtualization. In almost every case, the transformation to a dynamic infrastructure will involve virtualization. Many IT professionals think of virtualization in terms of servers.

IBM, however, has a broader perspective in which virtualization is seen as a general approach to decouple logical resources from physical elements so that those resources can be allocated faster, more cost-effectively and more dynamically, wherever the business requires them in real time to ideally meet changing demand levels and business requirements. There is no cost to attend. [Click here](#) to register.



Come join Flagship Solutions Group an IBM for a discussion on Internet Security Systems and Data Protection.

DATE: November 19, 2009  
TIME: Cocktails begin at 6:00 PM  
LOCATION: University Grill  
7790 Cypress Lake Drive  
Ft. Myers, FL 33907

This is an exclusive invitation to a dinner seminar on Internet Security Systems and Data Protection. Having a clear understanding of your vulnerabilities and risks is a good first step toward securing your network, prioritizing security investments and achieving regulatory compliance.

Please join Flagship Solutions Group and IBM for a discussion on how you can prevent business interruption instead of merely planning for the recovery when a failure occurs. IBM Professional Security Services will discuss how their expertise, tools and methodology combine to deliver security expertise, staff cost savings, specialized skills and tools, and world class security intelligence.

There is no cost to attend. [Click here](#) to register.

---



## **Miami Smarter Cities Forum**

**November 12, 2009 9:00 am - 3:00 pm**  
**Hilton Miami Downtown**  
**1601 Biscayne Boulevard, Miami, FL 33132**

Join IBM on November 12, 2009 for an insightful and informative discussion about navigating the current economy and preparing for a better tomorrow. The Smarter Cities Forum is a gathering of the area's most distinguished business and government leaders who are interested in collaborating on the common goal of economic recovery.

Thought leaders and subject matter experts will discuss the ways to promote greater public-private sector collaboration. You will also learn more about the role your organization can play in helping Miami take its rightful place in the global economy of the 21st Century.

**Don't miss this opportunity to participate in building a smarter planet, city by city.**

For more information and to register, [click here](#).

---

## **Universities in Hot Water Over Students' Peer-To-Peer Sharing**

Universities are now suffering as a result of students taking advantage of the high speeds and seemingly free access to all network resources. Many universities are forced to withdraw access to students' IT accounts and require the students to confer with IT department officials who then explain to the student that what they are doing is against the law.

There are dozens of reports a year from campus to campus from organizations such as Paramount, Columbia, the RIAA and Tristar as a result of students' copyright infringement. But because students are downloading music, films, software and

other copyrighted media from their campus housing or the university library, those monitoring the downloading see the originating IP address dedicated to that university. Unless the university can pin the blame on a student – who they probably cannot identify - then the university could be sued as a result.

Even if you do not use Peer to Peer (P2P) networking to share files, and have best-of-breed fire-walls, packet shapers, web blockers and web-sensing devices, your network and your company are still at risk. Unauthorized file access and sharing through P2P networks is presenting management with a new security challenge, which routinely outwits current security devices. There's little to no legal compliance, liability is high, bandwidth routinely gets maxed out and confidential information is routinely disclosed.

**Flagship's P2P Navigator is a sure bet to keep your organization remaining healthy and fit.** For more information about this revolutionary technology that stops P2P file sharing in its tracks, contact Flagship Solutions Group at **(561) 289-2045** or visit [www.flagshipsg.com](http://www.flagshipsg.com).

---

## **Amazon Virtual Private Cloud (VPC) Opens the Door To Citrix Customers**



The Amazon Web Services announcement of the Virtual Private Cloud (VPC) offering has just made Cloud computing more attractive to the enterprise.

Amazon is offering VPC, a dedicated secure network extending from a company data center into the Amazon Cloud with isolated virtual machines available on demand. This could be particularly attractive for Citrix customers.

For Citrix Customers, this is particularly attractive for expanding XenApp farms or centralizing new applications on XenApp without large facility and capital costs. Customers can bring their own XenApp licenses to VPC or point back to existing Citrix license servers on premise. [Citrix C3 Blueprints](#) with tested deployment techniques are now available to assist companies that want to evaluate these new offerings.

This announcement represents another progressive move for Citrix as a leader and enabler of Cloud Computing. Contact Flagship Solutions Group at **(561) 289-2045** or visit [www.flagshipsg.com](http://www.flagshipsg.com) for more information on how to leverage the power of VPC for your organization.

---

## **ChoicePoint To Pay \$275,000 In Latest Data Breach**

ChoicePoint, one of the nation's largest data brokers, has been fined \$275,000 by the U.S. Federal Trade Commission for a data breach that exposed the personal information of 13,750 people last year.

In April 2008, ChoicePoint turned off a key electronic security tool that it used to monitor access to one of its databases and failed to notice the problem for four months, according to an FTC statement.

During that period, unauthorized searches were conducted for 30 days on a ChoicePoint database that contained Social Security numbers and other sensitive information, the FTC said. The FTC alleged that ChoicePoint's conduct violated a 2006 court order requiring the company to institute a comprehensive information security program following a 2005 breach that compromised the personal information of more than 163,000 people and resulted in at least 800 cases of identity fraud. The company was ordered to pay \$10 million in civil penalties and \$5 million to consumers in that case.

To settle the recent charges, ChoicePoint agreed to pay the fine and provide reports on its data protection practices to the FTC every two months for two years. Meanwhile, payroll processor PayChoice has had two data breaches in less than a month. On October 1, the company said it was investigating a breach in which targeted e-mails were sent to customers that attempted to trick them into downloading malware.

Then last week, PayChoice told customers it was again shutting down its online portal after clients started noticing fake employees being added to their payroll in what is likely the second stage of a broader attack, according to the Security Fix blog.

***YOUR business could be next to face public humiliation and headache. Adding additional layers of network protection against emergent threats is MUCH less expensive than the fines and bad publicity associated with data breaches.*** For more information a solution that adds another layer of protection to your network, contact Flagship Solutions Group at 561-289-2045 or [click here](#) to email us.

---

**Flagship Solutions Group**  
**3701 FAU Blvd, Suite 210 • Boca Raton FL 33431 • (P) 561-289-2045**  
**[www.flagshipsg.com](http://www.flagshipsg.com)**  
**<mailto:sales@flagshipsg.com>**