

## Information at your Fingertips!

If you are our client, then you know we maintain all of your I.T. assets in our private database and we also make that available to you through our secure web portal. Need to know how many licenses of MS Office you have? How about the last time you purchased a PC or printer? Or what work we performed last time we were onsite? It's all there for you to view online through the secure portal at [www.starpointit.com](http://www.starpointit.com) – click on support then customer portal.

StarPoints Issue 12 March 2010

“As a business owner or executive, I know 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!”

David Davis, StarPoint IT Solutions – 1-800-869-0135 x101

### Latest News

#### • We're Hiring

StarPoint is looking for outstanding I.T. consultants in the San Diego area! If your referral gets hired you get \$1000! See job details at [www.starpointit.com/srclt](http://www.starpointit.com/srclt)

4379 30th Street, Suite 3  
San Diego, CA 92104  
800-869-0135  
[www.starpointit.com](http://www.starpointit.com)

**STARPOINT**  
IT SOLUTIONS

ISSUE

12

March  
2010

NEWSLETTER

# StarPoints

### Mini Meeting with Star Reach / LogMeIn Pro

With summertime around the corner, thoughts turn to fun times spent with family and friends. But for many, work travel eats up a lot of free time. Not for Eli. Eli works for an accounting firm with many small business clients around the city. In addition to reviewing their books regularly, he provides regular training to his clients, without spending time in his car. Eli uses LogMeIn Pro's Mini Meeting to show his clients the proper way to keep track of finances.

Here's how:

1. Eli sits at his LogMeIn Pro-enabled computer, right-clicks his LogMeIn icon and selects Mini Meeting.
2. He chooses "invite a guest to work with you" and sends the meeting invitation himself.
3. After filling in the meeting details, he copies the Mini Meeting link to an email he sends to his client.
4. At the arranged meeting time, his client clicks the link, Eli accepts the meeting and chooses "view only."
5. In just a few seconds, the client can see Eli's screen and Eli can walk his client through the appropriate task.



### this issue

Google Cyberattack **P.1**

Security Alert **P.2**

Top 4 Threats **P.3**

Latest StarPoint News **P.4**

## GOOGLE CYBERATTACK LINKED TO TWO CHINESE SCHOOLS

Two Chinese schools have been linked to the cyber attacks on Google and dozens of other companies last year.

Computers at Shanghai Jiaotong University and the Lanxiang Vocational School in China reportedly played a role in the attacks, according to unnamed sources cited in The New York Times.

Lanxiang Vocational School, The New York Times says, was created with funding from the Chinese military and trains computer scientists for the Chinese military. Its network is operated by a company with ties to Baidu, Google's most significant rival in China.

Evidence of the role of the two schools' computers was reportedly presented by a U.S. military contractor at a meeting of security professionals.

If true, the finding adds further weight to the views of security researchers that the attacks came from China.

While computer security experts in the U.S. suspect that the attackers have ties to the Chinese government, no conclusive evidence has been presented that the Chinese government was involved in the attacks. The Chinese government in January emphatically denied any such involvement. It has maintained that it is a frequent victim in cyber attacks.

The prevalence of illegally copied software in China ensures that many systems there are in fact poorly defended. Cybercriminals outside of China do exploit the country's vulnerable infrastructure for their operations.

Some computer security experts contend that the attacks on Google and other companies are routine and ongoing. A report on Thursday that some 2,500 businesses and government organizations had been compromised by a Zeus Trojan variant and turned into botnet zombies was met with yawns by security vendors not involved with the research.

“In the world of cyber security the 'kneber' botnet is, unfortunately, just another botnet,” said McAfee in an e-mailed statement. “With 75,000 infected machines, Kneber is not even that big, there are much larger botnets.” The company says that in the last three months of 2009, just under 4 million computers were compromised and hijacked by botnet malware.

Source: Information Week

**STARPOINT**  
IT SOLUTIONS

## What is Unified Threat Management?

Unified Threat Management (UTM) allows your organization to protect itself against the various ways cyber criminals gain unauthorized access to your computer systems by putting up “security check points” at all of the various points of entry (e.g. web, email, instant messaging, social networking applications, etc...) that you may be using. Having multiple guards in place reduces problems tenfold while protecting your data assets. UTM will also let you enforce company policies you would otherwise not be able to, backed by detailed reporting.

## Kiss Your Antivirus Bloat ware Goodbye

We asked our clients what they didn't like about their AV software. They told us they are resource hogs and slowed their computer down. They told us that scan times took way too long, and that the AV software nagged them. In short, old-style AV software takes too much Memory and CPU. Time to switch to Star Protect! It gives you malware protection that combines antivirus, antispayware, anti-root kit and other technologies into a seamless, tightly-integrated product. Even if you run “free” antivirus software, it hijacks 20% of your PC, so it's really not free at all! Find out how fast your PC can be – Email me today to make the switch ([ddavis@starpointit.com](mailto:ddavis@starpointit.com)).

## Security Alert: Hackers and Cyber Criminals Are Now Concentrating Their Attacks on Small Business

At the recent 2009 Visa Security Summit a new trend was revealed: hackers and cyber criminals are now turning their efforts to small “mom and pop” businesses instead of large enterprise corporations. Why? Because small business networks offer a much easier “lock” to pick, unlike large enterprises who invest far more man power and money into high security for their network.

“As the security becomes better at large companies, the small business begins to look more and more enticing to computer criminals,” said Charles Matthews, President of the International Council for Small Business, “It's the path of least resistance.”

Think your network is secure? Take a look at these surprising statistics:

- One-fifth of small businesses don't have up-to-date antivirus software installed.
- Sixty percent don't encrypt their wireless links.
- Two-thirds of small businesses don't have a security plan in place.
- Eighty-five percent of the fraud occurs in small and medium-sized businesses.

Why is security so poor for small business? Primarily for two reasons:

Ignorance. Most small businesses believe that nothing could ever happen to them, and therefore don't take the necessary precautions to secure their network, monitor their systems, and train their staff.

They are also ignorant on HOW to get this done, which makes a strong argument for getting all of our clients on our Star Mon Unified Threat Management (UTM) Service! The second reason is that they are cutting corners in the wrong places. Some simply refuse to spend money on securing their network. That's akin to having a beautiful home full of expensive furnishings and valuables, but refusing to buy a good lock for the door because it “costs too much.”

So what should you do at a minimum to protect your organization? Here are 7 fundamentals:

1. Educate your users on security basics such as using strong passwords and not downloading “cute” screen savers and illegal music. Some companies make computer security rules part of their standard HR policies and make each employee sign that they understand the rules.
2. Install a web filtering software to police users and prevent accidental (or intentional) slip-ups on the above- mentioned usage policies.
3. Install a strong virus protection system on all computers on your network and monitor it (for our Star Protect clients, we do that for you.)
4. Replace old, outdated firewalls that are vulnerable to security breaches with newer, dynamic security appliances that are constantly monitored and updated proactively daily to guard against the constant stream of new cyber threats. When was the last time you reviewed your firewall policies or had them reviewed and explained in basic terms by your I.T. consultant?
5. Remove all unessential services and applications installed on your servers. After e-mail, this is probably the biggest security vulnerability. If a hacker gets in, this will reduce their ability to use a forgotten service or application to exploit your network.
6. Have a system in place that keeps all your servers and desktops/laptops updated with all the latest security patches. Having Windows Updates turned on is no guarantee.
7. Never keep any of the manufacturer's default settings on any of the appliances or software you install. Hackers know what these settings are and will use them to gain easy access to your network. Not doing this leaves your business as a sitting duck waiting to be exploited (most likely without your knowledge).

For those of you subscribed to our Star Advantage Services, you can rest assured we are taking good care of issues 3 through 7; however, if you would like us to conduct a training class and develop an acceptable use policy for your staff and then install a content filtering service to enforce the policies, give us a call.

This training and software is a small price to pay for the peace of mind you'll have over your network's security. And since better than 80% of all security breaches happen because of an end-user mistake, you'll also be taking a big step towards protecting your critical assets.

## Top 4 Threats Attacking Your Network and What to do About Them

I'm focusing this edition on security, mainly because I think most small organizations often overlook simple practices that can be easily implemented that would end up saving hundreds or thousands of dollars per year in computer support costs and downtime. The bad guys getting more sophisticated so giving this some attention and implementing some relatively simple practices and solutions will help to minimize this problem for your organization

### #1 Overconfidence

User overconfidence in security products is the top threat to your network. Failure to “practice safe software” results in nuisance attacks like porn storms (unstoppable rapid fire pornographic pop-ups) and more subtle key loggers that steal passwords. Surveys promising free stuff, result in theft of information like your mother's maiden name, high school, etc. used to answer common security questions leading to theft of otherwise secure data. Think before you click!

### #2 Social Networking Sites

Social networking sites like Facebook are exploding in popularity. Threats range from malware (e.g. viruses, worms, spyware) to scammers trying to steal your identity, information and money. Many businesses and government agencies are using these sites to communicate with clients and constituents, so simply blocking access is no longer reasonable. Defending your company while allowing employee access requires social

network education for your employees and the enforcement of strong acceptable use policies. We can help you develop a policy, then monitor compliance using a Unified Threat Management service that controls and reports on network access.

### #3 Attacks on Mobile Devices

Everyone is going mobile these days not just the “road warriors.” Once limited to laptop computers, mobile network devices now include PDAs, handheld computers and smart phones, with new appliances appearing in the stores every month. Mobile devices often contain sensitive data yet they are easily lost or stolen. Be sure to password protect and encrypt data on all mobile devices whenever possible. Include mobile devices in your acceptable use policy.

### #4 Cloud Computing

“The Cloud,” in its most simple form, involves using the Internet to access and store your data. When you access email using a web browser, you are working in “the cloud.” You need to be sure that any data you store and access across the Internet is secure not just where it is stored, but during the trip to and from the Internet.

## This Month's Q&A Technology Tips

**Q: I need Email on my new Smart Phone. How do I get this setup?**



**A: Since most small businesses have a server at the home office with Exchange, leverage your server's power to deliver the Email to your phone. Exchange will natively support the iPhone and all Windows Mobile handhelds – no extra software required. Using a Blackberry? RIM offers Blackberry Enterprise software with a single license for no charge. Add additional licenses for roughly \$50 each.**

## Getting Ready To Upgrade Or Refresh Your Computer Network? DON'T—Until You Read This...

Thanks to a new software technology called, “virtualization” you can now save THOUSANDS of dollars on hardware upgrades while simultaneously (and drastically) improving your ability to recover after a disaster.

Before virtualization, you could only run a single operating system and a single application on a server; but virtualization breaks that requirement by making it possible to run multiple operating systems and multiple applications on the same server hardware at the same time, reducing the need to constantly add new hardware to support your network. This technology also simplifies your infrastructure, which means less maintenance is required, and it lowers the overall operating costs of running a network.

And if the hard-to-ignore cost savings isn't enough, you'll be amazed at how quickly we can get you back up and running after a disaster.

So before you add on (yet another) server or upgrade your network, PLEASE give us a call. We'll be glad to show you exactly how much money this new technology can save your business in measurable, hard costs. After seeing the numbers, we're sure you'll agree that virtualizing your network is a far superior way to address your IT growth.