IT Strategy Brief

ISSUE 5 | VOL 3 | May 2017

INTEGRATE SEAMLESSLY

SWK TECHNOLOGIES

"Useful Technology Ideas for Your Business"

What's Inside:

Over 75% of ransomware attacks occur in just four industries. Is yours one?

According to a new global threat intelligence report (www.securitysales.com/article/more_than_75_of_ransomware_attacks_globally_occur_in_four_industries_report) by NTT Security 77% of all detected ransomware from October 1, 2015 to Sept. 31, 2016 attacks occurred in four business sectors. Professional services had 28%, government had 19%, healthcare was at 15%, and retail came in at 15% as well.

The report highlighted not only ransomware, but also phishing and distributed denial of service (DDoS) attacks too. These are the type of attacks that are most common in today's world as threats to businesses.

While the numbers for ransomware are certainly interesting another key point to note is that phishing attacks were responsible for 73% of all malware delivered to organizations. In case you forgot phishing is where a hacker uses a fake email to appear like a reputable business in order to steal information. Phishing has become such a threat to businesses you may have seen things like what SWK offers for security awareness training for employees (the color insert we've had the past couple months), because no matter how secure your network is if an employee's information gets stolen a hacker can find their way in.

DDoS attacks like the one where hackers used internet connected devices to shut down parts of the internet not that long ago only represented about 6% of attacks globally.

Some other interesting facts that were uncovered in the report:

- When broken down into more specific industries finance, government, and manufacturing were the top three most commonly attacked.
- Only 32% of the organizations had an incident response plan (which sadly was up from 23% in previous years)
- Over half the incidents that occurred in the finance industry were related to malware
- Half of incidents in the healthcare industry were related to ransomware

What our clients are saying: EAM Land Services

"We have always found SWK's support to be professional, courteous and quick. Matt, Dave, Ben and the rest of the staff have exceeded our expectations and EAM would certainly recommend your company if a client needed a referral."

Kate Sparacino-Taylor
Executive Vice President
EAM Land Services

eam land services inc.

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:

Jill Geary
Micro Format, Inc.

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

1. What do you like most about our services?

2. Tell us about a specific experience with us that you were happy with.

3. What are the biggest benefits you've received or experienced since hiring us?

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form: http://bit.ly/nwsnews-survey before **June 5th** to get your name in the hat.

You could win a $25 Gift Card!

Sly phishing attack catching users off guard

You pay close enough attention to the links you click to avoid clicking on something like goolge.com or evrenote.com…right? Because if you're not, you could end up exposing your computer or smartphone to a host of malware. The newest phishing attack strategy is the worst of all, and can catch even the most astute users off guard.

What are homographs?

There are a lot of ways to disguise a hyperlink, but one strategy has survived for decades — and it's enjoying a spike in popularity. Referred to as "homographs" by cybersecurity professionals, this phishing strategy revolves around how browsers interpret URLs written in other languages.

Take Russian for example, even though several Cyrillic letters look identical to English characters, computers see them as totally different. Browsers use basic translation tools to account for this so users can type in non-English URLs and arrive at legitimate websites. In practice, that means anyone can enter a 10-letter Cyrillic web address into their browser and the translation tools will convert that address into a series of English letters and numbers.

How does this lead to phishing attacks?

Malicious homographs utilize letters that look identical to their English counterparts to trick users into clicking on them. It's an old trick, and most browsers have built-in fail-safes to prevent the issue. However, a security professional recently proved that the fail-safes in Chrome, Firefox, Opera and a few other less popular browsers can be easily tricked.

Without protection from your browser, there's basically no way to know that you're clicking on a Cyrillic URL. It looks like English, and no matter how skeptical you are, there's no way to "ask" your browser what language it is. So you may think you're clicking on apple.com, but you're actually clicking on the Russian spelling of apple.com — which gets redirected to xn—80ak6aa92e.com. If that translated URL contains malware, you're in trouble the second you click the link.

The solution

Avoiding any kind of cybersecurity attack begins with awareness, and when it comes to phishing, that means treating every link you want to click with skepticism. If you receive an email from someone you don't know, or a suspicious message from someone you do, always check where it leads. Sometimes that's as simple as hovering your mouse over hyperlink text to see what the address is, but when it comes to homographs that's not enough.

In the case of homographs, the solution is unbelievably simple: Manually type in the web address. If you get an email from someone you haven't heard from in 20 years that says "Have you checked out youtube.com??", until your browser announces a fix, typing that URL into your browser's address bar is the only way to be totally sure you're safe.

For most, this trend feels like yet another development that justifies giving up on cybersecurity altogether. But for small- and medium-sized businesses that have outsourced their technology support and management to a competent and trustworthy IT provider, it's just another reason to be thankful they decided against going it alone. If you're ready to make the same decision, call us today.

Shiny gadget of the month:
Sunscreenr – make sure you're protected from the sun this summer

sunscreenr.com

The weather is finally starting to warm up and summer is approaching. That means we all get to spend more time outside and enjoy the nice weather. The more time you spend outside means the more you are to be exposed to the sun, especially if you are going to be at the beach or by a pool. It is common knowledge now that getting sun burn can lead to an increased risk of skin cancer, so with that in mind a device called the Sunscreenr was created. The idea is to be able to make sure you have not missed spots applying sunscreen. According to the creators most people only apply about 25 to 50% of the sunscreen they should.

The Sunscreenr is a little rugged camera that detects sunscreens with a SPF of 15 or higher. The difference between this and a smart phone is that it uses a special lens and filter along with an algorithm and works with the UV light that a normal camera will not show.

For example, this photo shows the same shot, but with the Suncreenr to the left that depicts a stencil showing up from applying sunscreen over it and then a normal photo.

The device itself is built with the beach in mind, making it waterproof, dust/sand proof, compact, lightweight, and easy to use. It even has a video feature if you are alone so you can record 30 seconds and replay it for inspection. The gadget is said to start shipping this summer on their website (sunscreenr.com) and sells for $119.00.

I'm sure most of us have had an experience where either they, or someone else, completely missed a spot and they got burnt. The idea for Sunscreenr came from the founder's experience with a family member and their struggle with skin cancer. They hope to eliminate inadequate sunscreen coverage and help you live a happy healthy life outside.

5-year-old malware still targeting EMRs

A piece of malware known as Stegoloader continues to wreak havoc on healthcare companies that inadvertently download it under the guise of product keys. The malware steals information from infected machines and spreads itself through the compromised network. Keep reading to find out how this infection can affect your business data and what you can do about it.

What is Stegoloader?
The trojan known as Stegoloader infects machines through product key generators packaged with downloads of pirated software. Small companies have been targeted by the malware, particularly those in the healthcare industry — and to a lesser extent, the insurance and technology sector.

Steganography is a cyber attacker term for hiding malware inside an image file. Once the image is opened on a vulnerable machine, the program gathers information and crawls through the network looking for weaknesses. Although Stegoloader doesn't appear to be a particularly sophisticated program, it can devastate your business by stealing electronic medical records as well as installing a secondary piece of malware to pilfer banking information.

Anthem and Premera Blue Cross are two big-name victims of the widespread malware. Symantec believes that Stegoloader's creators plan to sell healthcare data because they're more lucrative than other information types. Symantec also believes the cyber attackers are opportunistic, taking advantage of companies that download pirated versions of popular software.

How to Avoid becoming infected by Stegloader
Because the Stegoloader trojan often lurks in illegal product key generators and illegitimate software, the best way to avoid infection is to stay away from sites that offer pirated software. Other than that, we recommend educating your employees on safe practices, avoiding unknown image files and quarantined backups, and updating operating system and antivirus software as often as possible.

When business owners download pirated software, they're trying to cut corners to save money on business applications and technology consultants. But not only are they getting themselves in trouble with cyber attackers, they're also messing with the law. We promise that partnering with us will end up saving you more money and hassle than the alternatives. If you're looking for a better way to protect your company and keep your information safe, contact us today.

Gift Card Trivia!

This month's question is:

What was responsible for delivering 73% of all malware to organizations according to the NTT Security report? *(Hint: The answer is in this newsletter.)*

a. DDoS
b. Phishing
c. Ransomware
d. Zip Files

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **June 5th**, in order to be placed in the running for this month's gift card prize!

We can help you with:

- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.

South Jersey
650 Grove Road, Suite 106
West Deptford, NJ 08066

North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at
www.swktech.com

SWK TECHNOLOGIES

The South Jersey Office Has Moved!

We Moved!

For those of you who may not have heard the SWK Networking team that previously resided in the South Jersey Westville, NJ office has moved to a new location at 650 Grove Road, Suite 106, West Deptford, NJ 08066.

As we have grown over the years the old location became a little too small for us. We are very excited about the new building and all of the space we have to continue to grow and best serve our clients.

If you have any questions regarding this, please feel free to reach out to us at (856) 956-5800.