Colleagues,

I was recently talking to a co-worker who used the term “SWOT” – Strengths, Weaknesses, Opportunities, and Threats. “SWOT” is used in identifying business risk and is being taught in business management. My co-worker related this term to the topic we were discussing which was risk assessment.

Risk assessment is the determination of vulnerabilities that a “product” may contain. The first step in doing a risk assessment is to determine the weaknesses of the product, what threat those weaknesses have with in the product, the opportunity for those vulnerabilities to be exploited and finally what strengths the product has to defend against the attack. When talking to management, we as security professionals can use these business terms. This way upper management may better understand what is being explained to them.

When talking to management it is best to keep the briefing short, to the point, and use business terms. Management wants to know what the problem is, how to solve the problem, how much will the solution cost, and the amount of time it will take to put the solution in place. This sounds so simple but can be very difficult to do. Many times the solution may not be cut and dry. Also the timeline to implement the solution is hard to determine due to the many variables that are in play.

So the next time you are talking to management about a security issue try using business terms and not security terms.

Cindy

The ISSA Colorado Springs Newsletter incorporates open source news articles as a training method to educate readers on security matters in compliance with USC Title 17, Section 107, Paragraph a.

The views expressed in articles obtained from public sources within this newsletter do not necessarily reflect those of ISSA, this Chapter or its leadership.
Panama Papers: A data security disaster

By Matt Jacobs, General Counsel, Black Duck Software, April 13, 2016

The Panama Papers security breach is a juicy, made-for-the-Internet scandal. It has all the elements – secret off-shore accounts; involvement by international politicians, criminals, celebrities and sports stars; 11.5 million files cyber-filched from a law firm’s files and then leaked to the media.

A Google search for Panama Papers yields more than 10 million hits. The whole world is watching.

While most of the Panama Papers attention will focus on the salacious aspects, the breach of the Panamanian law firm Mossack Fonseca’s files exposes another dirty little secret – the trouble law firms have keeping clients’ data secure.

The Mossack Fonseca breach is hardly the first. In late March the Wall Street Journal reported that that the international law firms Weil Gotshal & Manges, and Cravath, Swaine & Moore and other firms suffered data breaches, putting attention on the potential consequences for law firms with lax security. The newspaper reported that other unnamed law firms, suffered data breaches and that federal prosecutors in Manhattan are investigating whether hackers used stolen information for insider trading purposes.

Additionally, a 2015 report from Citigroup’s cyber intelligence center warned of the threat of attacks on the networks and websites of big law firms.

The report said it was reasonable to expect law firms to be targets of attacks by foreign governments and hackers because they are repositories for confidential data on corporate deals and business strategies. The report noted that digital security at many law firms generally remains below the standards for other industries.

It said law firms were at “high risk for cyber intrusions” and would “continue to be targeted by malicious actors looking to steal information on highly sensitive matters such as mergers and acquisitions and patent applications.”

What’s the solution?

A good place to start is a recent article by the FTC. It lays out 10 basic security steps that all companies should take. It also tells one cautionary tale after another of companies that failed to meet one or more of these basic steps. It’s a must read – particularly for managing partners of law firms large and small.

Analyzing the Panama Papers breach in light of some of the basic steps outlined by the FTC, it is clear to see how it happened – and could have just as easily been prevented.

Early information concerning the hack points the law firm’s client portal as the Achilles heel. That portal is reportedly built on an aged version of Drupal, the popular open source data management project. Drupal is a very successful open source project. There is nothing at all wrong with using it. After all, open source software is the way applications are built today.

The issue here is that Mossack Fonseca failed to make certain that the version they were using was, and remained, secure. In fact, the version they were reportedly using had 25 or more known security vulnerabilities. “Known” meaning that these security vulnerabilities were publicly announced going back as far as 2013. “Known” meaning that anyone paying attention, anyone using Drupal to house extremely sensitive client data, should have been aware.

And “known” meaning that hackers and bad actors also had access to this security vulnerability data. Once security vulnerabilities in a widely used program like Drupal are announced, the race is on to see if the users of the affected open source component can fix it before the hackers exploit. In any event, Mossack Fonseca’s failure to keep current the version of Drupal in use was – in a word – negligent. And avoidable.

Given the sensitive and valuable nature of the information that they were processing using Drupal, and the foreseeable damage that would result from a breach, the law firm owed their clients a much higher level of diligence around their processes and procedure.

Read the rest here:
Membership Update

We are continuing to increase our membership—up to 415 members as of the end of April. We added quite a few new Freemium members last month. Kudos to everyone who referred a student. Special shout out to Tim Gama and Mark Gonzalez who referred seven and three new Freemium members respectively. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes. We are still in need of new Freemium members so please continue reaching out to any university students you know that might be interested. This program will be one of our main focus areas for increasing our membership numbers going forward. If you have any questions feel free to drop me an email or give me a call.

I would also like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information.

Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

<table>
<thead>
<tr>
<th>New Members April</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seth Sterner</td>
</tr>
<tr>
<td>Connor Rice</td>
</tr>
<tr>
<td>Daniel Guardamondo</td>
</tr>
<tr>
<td>Benjamin Hopkins</td>
</tr>
<tr>
<td>Vanessa Solano</td>
</tr>
<tr>
<td>Jeffrey J. Maxwell</td>
</tr>
<tr>
<td>Vanessa Solano</td>
</tr>
<tr>
<td>Clarissa Mendez</td>
</tr>
<tr>
<td>Bob Stephenson</td>
</tr>
<tr>
<td>Michelle Bolitho</td>
</tr>
<tr>
<td>Joshua Greer</td>
</tr>
<tr>
<td>Randy Sirota</td>
</tr>
<tr>
<td>James Cook</td>
</tr>
<tr>
<td>Andre Williams</td>
</tr>
<tr>
<td>Mark Maluschka</td>
</tr>
<tr>
<td>Nikki Lester</td>
</tr>
</tbody>
</table>

GAO: Pentagon Has No One to Take Charge In Case of Cyber Attack

By Cathy Burke, NewsMax, April 4, 2016

The Pentagon has no clearly designated military official who'd be in charge of support in the event of a massive data breach by foreign hackers, according to Congress's watchdog agency.

In an analysis of the audit by the U.S. Government Accountability Office, Defense One reports the U.S. Northern Command says it’s the main Pentagon support arm in such breaches, while policies and some top brass say Cyber Command plays the lead in cyberthreats from abroad.

The Department of Defense needs to clarify its roles and responsibilities in an area of growing concern, Joseph Kirschbaum, GAO's director for defense capabilities and management, warns in the audit.

And until it does, the military “may not be positioned to effectively employ its forces and capabilities to support civil authorities in a cyberincident,” Kirschbaum says.

"[Department of Defense] officials stated that the department had not yet determined the approach it would take to support a civil authority in a cyberincident and, as of January 2016, DOD had not begun efforts to issue or update guidance and did not have an estimate on when the guidance will be finalized," Kirschbaum said.

Read the rest here:
Perhaps the biggest news in Professional Outreach in the two months revolves around the new ties between ISSA-COS and the National Cyber Intelligence Center (NCIC), the new organization that Governor Hickenlooper is promoting via the State of Colorado’s Office of Economic Development and International Trade (OEDIT). USAF Ret. Lt. Gen. Jay Lindell, who is now the Governor’s Aerospace and Defense Industry Champion working out of OEDIT, is spearheading efforts to develop the NCIC in Colorado Springs. The idea is to not merely establish a cybersecurity headquarters for Colorado, but to make Colorado Springs the national cybersecurity hub, especially given the vast resources and DoD efforts in the area. Local job creation is a leading factor in the Governor’s mission. As Jay has said, Denver has received a lot of job focus from the State, and now it is time for the Springs.

Chapter Vice President Frank Gearhart set up the meeting between ISSA-COS and Mr. Lindell, but was unable to attend due to business obligations. Dr. Pat Laverty, Past President, and myself met with Jay and learned that the planning for the NCIC is well underway, though by no means finalized. Jay released an initial document describing the NCIC planning that was created late last year. He and interim NCIC head, US Army Ret. Brigadier General Ed Anderson, want more input on the overall plans (he described the state of the plans as being like Jello) and encourage any ideas on the scope and areas of focus for NCIC that we may have. However, for now the primary effort is on securing all members of the NCIC Board. Jay has received an overwhelmingly positive response from a wide range of people, including local higher educational institutions and industry. He is also reaching out to our vast DoD resources.

Currently, the plans include using the former TRW space (including a SCIF), owned by UCCS, and transforming it into a hub of cybersecurity R&D, education development, and coordination for incubating new cybersecurity firms here in Colorado Springs. The legislature has approved the initial $8M funding, which will be used to “upgrade” the site.

Jay has been quite generous with his correspondence to me and is eager for our Chapter’s input and involvement. Since he is waiting for the Board to form, Jay welcomes comments on the overall NCIC plans, but will hold everything he receives until he can pass it to the new NCIC Board. For now, Ed and the initial Board members are overwhelmed with ideas from the very enthusiastic response. ISSA-COS is not expected to have a place on the Board.

When asked if there is an area where ISSA-COS might help, Jay suggested that we focus on the incident rapid response and information sharing division of the NCIC which will include incident response personnel. This will naturally involve Homeland Security, FBI, and so on.

Meanwhile, Pat is following up with Ed on similar efforts, and Frank is in contact with Jay on other items. We are speaking with both Jay and Ed about being speakers at upcoming meetings and/or the August conference.

Jay’s enthusiastic and immediate response to all of our queries is great news for the Chapter. Jay emphasized that the Governor wants to see real economic development in the Colorado Springs area.

Other NCIC areas include working with the Catalyst Campus to incubate startups, as well as establishing further educational advances with UCCS, CTU, Regis, and Pikes Peak Community College for both degrees and continuing education. NCIC works with Colorado Technology Association, especially with CEO Erik Mitisek, as well as STEM programs, and more.

The bottom line is that Jay would really like to see ISSA-COS involved with NCIC because of the significant and valuable role we can play, which is very encouraging.

Our focus now is to determine exactly how we can contribute to the rapid response and incident sharing areas of this exciting new organization.

Suzanne
Training Committee Update

**Mini-seminar: 14 May, at CTU, 9am-Noon:**

Our first mini-seminar on 9 April was a huge success, thanks to Art Cooper and Mark Spencer and their excellent presentations! These mini-seminars are designed to provide members an opportunity to learn something new, and earn a few CPE/CEUs, at no cost. Our next mini-seminar is scheduled for 14 May, 9am to noon, at Colorado Technical University (CTU), room 112. Topics to be covered during this mini-seminar are:

- **TBD** – Presented by TBD (details will be forthcoming!)
- **Security in Solution Architecture** – Presented by William (Bill) Blake

Want to gain knowledge on something new? Want to brush up, get a refresher, on something you may already know? Want to earn a few continuing education units (e.g. CPE/CEUs)? Come to this mini-seminar and share your knowledge, thoughts, and perspectives with your fellow ISSA members! Seats fill up quickly for these mini-seminars, so please register via Eventbrite if you plan on attending: [https://www.eventbrite.com/e/issa-cos-mini-seminar-tickets-24819743521](https://www.eventbrite.com/e/issa-cos-mini-seminar-tickets-24819743521). Can’t make the May mini-seminar? Watch for info on our June and July mini-seminars!

The idea of these "mini-seminar" is for members to give a 30 min or 1 hour (or longer) presentation on a topic of interest. Those giving the presentations would earn CPEs/CEUs for the time spent preparing their presentation, and those attending would earn CPEs/CEUs for their attendance and participation in any discussions. If you’re interested in presenting a topic, please email our Training Committee leads at: Training@issa-cos.org and let us know the topic you’d like to present and approximately how much time you’d like for your presentation. If there’s a topic you’d like us to cover during a mini-seminar, please let us know and we’ll see if someone in the Chapter is willing to develop a presentation for it.

This is a great training opportunity for those needing CPE/CEUs to maintain their existing certifications, or anyone wanting to broaden their knowledge. It’s also a great opportunity to share your knowledge and experience with other members of our Chapter, and gain experience as a speaker, by volunteering to be one of our presenters.

**Security+ Seminar:**

Our next two-day Security+ Seminar is scheduled for 4 and 11 June. Registration for it may be accomplished via Eventbrite: [https://www.eventbrite.com/e/security-exam-prep-seminar-jun-2016-tickets-25000964558](https://www.eventbrite.com/e/security-exam-prep-seminar-jun-2016-tickets-25000964558). Or, you may email our Training Committee leads at: Training@ISSA-COS.org. Additional Security+ Seminars will be scheduled, as required, based on feedback.

**CISSP Seminar:**

This year’s CISSP Seminar will be held on five alternating Saturdays: 30 Jul, 13 & 27 Aug, and 10 & 24 Sep. Registration for it will start in May. Watch for details on it soon! Email the Training Committee leads at: Training@ISSA-COS.org if you have any questions.

**CISSP Study Guides**

Did you know that (ISC)² members are able to purchase the CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide, 7th Edition for a 50% retail discount? Log into (ISC)², and scroll down to the Security Central section. From there, look for the section that says: (ISC)² Textbook Discounts Get 50% off the Official CBK guides to all (ISC)² certifications. Click on the link provided.

Prefer a different CISSP study guide, or want an additional CISSP study guide? Sybex and Shon Harris both have updated their CISSP study guides, per the 2015 CISSP Common Body of Knowledge (CBK). The Sybex book is available now, and the Shon Harris book will be available for purchase in late May. Ensure you purchase the 7th edition of either book (updated per the 2015 CBK) to get the latest and most current information.

**Continuing Education (CEU/CPE) Ideas**

Do you know there are numerous free or low cost CEU and CPE options available? Check out the ISSA-COS web page (http://www.issa-cos.org), Training Classes, “On-Line Training” link for suggested sites.

**Volunteer Opportunities**

Looking for a volunteer opportunity? Looking for a way to share your knowledge/expertise? Looking for a way to earn CompTIA CEUs or (ISC)² CPEs? We’re always looking for members to teach one or more of the Security+ or CISSP domains. We provide the slides, but you can modify them as you see fit as long as your changes remain consistent with the official CompTIA or (ISC)² criteria. If you would like to volunteer to teach one of the Security+ or CISSP domains, or if you have questions, please contact our Training Committee leads at: Training@issa-cos.org.
Cyber Threats. In response to increased threats, we are strengthening cyber defenses and increasing options available in case of a cyber-attack.

The president’s budget funds $6.7 billion in FY 2017 for defensive and offensive cyberspace operations, capabilities, and cyber strategy.

Press Operations
Release No: NR-046-16
February 9, 2016

Today President Barack Obama sent Congress a proposed budget request of $582.7 billion in discretionary budget authority to fund the Department of Defense in Fiscal Year 2017 (FY 2017).

The FY 2017 budget of $582.7 billion complies with the Bipartisan Budget Act of 2015, giving the department both funding stability and protection from the damage of sequestration in FY 2016 and FY 2017. Within the confines of this negotiated amount, the budget request reflects the priorities necessary for our force today and in the future to best serve and protect our nation in a rapidly changing security environment. The base budget of $523.9 billion includes an increase of $2.2 billion over the FY 2016 enacted budget of $521.7 billion. As specified in the budget agreement, DoD’s FY 2017 overseas contingency operations budget is $58.8 billion, nearly the same as the FY 2016 enacted level of $58.6 billion. The combined request represents a total increase of $2.4 billion, or less than one percent over FY 2016 enacted levels.

The FY 2017 budget reflects recent strategic threats and changes that have taken place in Asia, the Middle East and Europe. Russian aggression, terrorism by the Islamic State of Iraq and the Levant (ISIL) and others, and China’s island building and claims of sovereignty in international waters all necessitate changes in our strategic outlook and in our operational commitments. Threats and actions originating in Iran and North Korea negatively affect our interests and our allies. These challenges have sharpened the focus of our planning and budgeting.

Addressing these challenges as part of DoD’s mission to defend the nation requires new and innovative thinking, new operational posture in strategic international challenges, we are seizing opportunities, developing new operational concepts, pioneering and dominating technology frontiers, reforming the defense enterprise, and building the force of the future.

“This budget marks a major inflection point for the Department of Defense,” Secretary of Defense Carter stated. “Even as we fight today’s fights, we must also be prepared for the fights that might come in 10, 20, or 30 years.”

The FY 2017 budget request strikes a prudent balance among the modernization of the joint force, its size, and its readiness, and continues to keep faith with service members and their families.

TA16-091A: Ransomware and Recent Variants

Department of Homeland Security

Original release date: March 31, 2016

Systems Affected

Networked Systems

Overview

In early 2016, destructive ransomware variants such as Locky and Sams were observed infecting computers belonging to individuals and businesses, which included healthcare facilities and hospitals worldwide. Ransomware is a type of malicious software that infects a computer and restricts users’ access to it until a ransom is paid to unlock it.

The United States Department of Homeland Security (DHS), in collaboration with Canadian Cyber Incident Response Centre (CCIRC), is releasing this Alert to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware.

Description

WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects computer systems, restricting users’ access to the infected systems. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user’s systems have been locked or that the user’s files have been encrypted. Users are told that unless a ransom is paid, access will not be restored. The ransom demanded from individuals varies greatly but is frequently $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user’s knowledge.

Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. For example, vulnerable Web servers have been exploited as an entry point to gain access into an organization’s network.

WHY IS IT SO EFFECTIVE?

The authors of ransomware instill fear and panic into their victims, causing them to click on a link or pay a ransom, and users systems can become infected with additional malware. Ransomware displays intimidating messages similar to those below:

(Continued on page 8)
Your computer has been infected with a virus. Click here to resolve the issue.

Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine.

All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data.

Proliferation of Variants

In 2012, Symantec, using data from a command and control (C2) server of 5,700 computers compromised in one day, estimated that approximately 2.9 percent of those compromised users paid the ransom. With an average ransom of $200, this meant malicious actors profited $33,600 per day, or $394,400 per month, from a single C2 server. These rough estimates demonstrate how profitable ransomware can be for malicious actors.

This financial success has likely led to a proliferation of ransomware variants. In 2013, more destructive and lucrative ransomware variants were introduced, including Xorist, CryptorBit, and CryptoLocker. Some variants encrypt not just the files on the infected device, but also the contents of shared or networked drives. These variants are considered destructive because they encrypt users’ and organizations’ files, and render them useless until criminals receive a ransom.

In early 2016, a destructive ransomware variant, Locky, was observed infecting computers belonging to healthcare facilities and hospitals in the United States, New Zealand, and Germany. It propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip). The malicious attachments contain macros or JavaScript files to download Ransomware-Locky files.

Samas, another variant of destructive ransomware, was used to compromise the networks of healthcare facilities in 2016. Unlike Locky, Samas propagates through vulnerable Web servers. After the Web server was compromised, uploaded Ransomware-Samas files were used to infect the organization’s networks.

Links to Other Types of Malware

Systems infected with ransomware are also often infected with other malware. In the case of CryptoLocker, a user typically becomes infected by opening a malicious attachment from an email. This malicious attachment contains Upatre, a downloader, which infects the user with GameOver Zeus. GameOver Zeus is a variant of the Zeus Trojan that steals banking information and is also used to steal other types of data. Once a system is infected with GameOver Zeus, Upatre will also download CryptoLocker. Finally, CryptoLocker encrypts files on the infected system, and requests that a ransom be paid.

The close ties between ransomware and other types of malware were demonstrated through the recent botnet disruption operation against GameOver Zeus, which also proved effective against CryptoLocker. In June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOver Zeus and CryptoLocker.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim’s money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

Solution

Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist.

US-CERT recommends that users and administrators take the following preventive measures to protect their computer networks from ransomware infection:

- Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of...
data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.

- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.

- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.

- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.

- Restrict users’ ability (permissions) to install and run unwanted software applications, and apply the principle of “Least Privilege” to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. For information on safely handling email attachments, see Recognizing and Avoiding Email Scams (https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf). Follow safe practices when browsing the Web. See Good Security Habits (https://www.us-cert.gov/ncas/tips/ST04-003) and Safeguarding Your Data (https://www.us-cert.gov/ncas/tips/ST06-008) or additional details.

- Do not follow unsolicited Web links in emails. Refer to the US-CERT Security Tip on Avoiding Social Engineering and Phishing Attacks (https://www.us-cert.gov/ncas/tips/ST04-014) for more information.

Individuals or organizations are discouraged from paying the ransom, as this does not guarantee files will be released. Report instances of fraud to the FBI at the Internet Crime Complaint Center (http://www.ic3.gov/).

References

Sophos / Naked Security, What’s next for ransomware? CryptoWall picks up where CryptoLocker left off https://nakedsecurity.sophos.com/2014/06/18/whats-next-for-ransomware-cryptowall-picks-up-where-cryptolocker-left-off/

Symantec, CryptoDefence, the CryptoLocker Imitator, Makes Over $34,000 in One Month http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month


Symantec, CryptoLocker Q&A: Menace of the Year http://www.symantec.com/connect/blogs/cryptolocker-qa-menace-year


SamSam: The Doctor Will See You, After He Pays The Ransom http://blog.talosintel.com/2016/03/samsam-ransomware.html
Samsung Files Patent For Augmented Reality Smart Contact Lenses

By Lauren Keating, Tech Times, April 6, 2016

Forget smart glasses, smart contact lenses will soon be the wearable of the future.

Samsung filed paperwork for a patent that reveals that it is working on smart contact lenses that are equipped with a built-in camera.

If you recall, smart contact lenses is not a new concept. Google previously filed a patent for smart contacts back in 2012 that feature a small camera sensor that could be controlled by the user by blinking. It received its patents for the product in 2014, although it's still in development.

Interestingly enough, Samsung was found to have also filed a patent for smart lenses in 2014, only it did so in South Korea. According to the patent, these smart contact lenses also feature a camera and motion detection sensors, along with an antenna and small display.

Instead of just being used to take photos and record videos (which it probably would be able to do), the lenses would provide an augmented reality experience. Images from the display would be projected directly into the eye. The user would be able to control the experience as well via blinking, but it will also need to run with a smartphone.

Just image playing a mobile game where you see and experience the virtual world while navigating the real world with nothing more than your smartphone in your pocket and contacts in your eyes.

Now that we know that Google and Samsung are both working on smart contact lenses, we can't help but wonder when we will see either company's wearables on the market. It's important to note that, while Samsung's version will aim to provide augmented reality experiences, Google's version is being designed to help diabetes patients manage their disease by detecting glucose in the bloodstream. That doesn't mean that the companies aren't quietly racing to get their product out first.

Read the rest here:

Sony Is On A Mission Impossible – Its Contact Lens Now Can Record and Play Videos Too!

By Nitin Balodi, Tech Story, April 26, 2016

On 16 Jan 2014, the whole world bowed down to Google. It unveiled the lens project which could change the lives of millions of diabetics. The lens offers a new, high-tech way to keep their glucose level in check. It also maintains hydration level in wearer's eye.

Three weeks ago, a patent application by Samsung published at Korean Patent office took the whole tech world by surprise again. The patent disclosed a contact lens which houses a tiny camera. Further, a wearer can control that with the blink of his eyes. Cool, eh?

And now this patent application by Sony couldn’t surprise me less. And believe me, it, too, is cool. Maybe uber cool!

Confused? Well, read the second claim:

“The contact lens according to claim 1, further comprising: a recording control unit configured to perform control in a manner that a captured image captured by the image pickup unit is recorded in a storage medium.”

Do you know what that means? Read the last 10 words of the claim again. Yes! Whereas Samsung’s contact lens captured images and sends them to a smartphone, the Contact Lens of Sony doesn’t only capture images but stores them, too.

Read the rest here:
http://techstory.in/sony-contact-lens/
Report: Major cyber security vulnerabilities have been found in the US visa system

By Ramkumar Iyer, Reuters, March 31, 2016

To protect the victims of the data breach from further harm, the IRS provided them with “Identity Protection PINs.” The PINs are secret codes those taxpayers now have to put on all of their tax returns, or the IRS won’t accept them. As long as they keep their PINs secret, they should be safe from fraud.

Cyber security experts have found vulnerabilities in a U.S. State Department system that could have allowed hackers to alter visa applications or steal data from the more than half-billion records on file, ABC News reported, citing sources familiar with the matter.

The department learned after an internal review several months ago that its Consular Consolidated Database (CCD) was at risk of being compromised, though no breach had been detected, the report said.

The CCD holds current and archived visa records and data, including names, photos, addresses, biometric data and identification numbers from the Bureau of Consular Affairs and is key to processing passport applications for visa applicants and travelers.

The State Department did not immediately respond to a request for comment.

The vulnerabilities stemmed from aging “legacy” computer systems that comprise the CCD, the report said.

An official associated with the department’s efforts to address the security concerns said a mitigation plan had already fixed the visa-related vulnerabilities, and further steps were being taken, ABC News said.

Read the rest here:

Hacking Lottery Machines

By Bruce Schneier, Schneier on Security, April 12, 2016

Interesting article about how a former security director of the US Multi-State Lottery Association hacked the random-number generator in lottery software so he could predict the winning numbers.

For several years, Eddie Tipton, the former security director of the US Multi-State Lottery Association, installed software code that allowed him to predict winning numbers on specific days of the year, investigators allege. The random-number generators had been erased, but new forensic evidence has revealed how the hack was apparently done.

[...]

The number generator had apparently been hacked to produce predictable numbers on three days of the year, after the machine had gone through a security audit.

Note that last bit. The software would only produce the non-random results after the software security audit was completed.

Read the rest here:
By Cory Bennet, The Hill, April 22, 2016

A tech sector initiative to secure internet browsing for the entire web now covers millions of websites.

The campaign, Let's Encrypt, offers encryption certificates to websites, free of charge. As of Thursday, Let's Encrypt had issued two million certificates. Each certificate protects multiple websites.

That's “millions and millions of sites” now securing internet traffic, said the Electronic Frontier Foundation (EFF), a digital rights advocate behind Let's Encrypt.

“This rapid adoption has already made Let's Encrypt one of the world's largest public certificate authorities by number of certificates issued,” EFF said in a blog post.

A cross-section of the tech industry is backing the effort.

The EFF, Firefox manufacturer Mozilla and researchers at the University of Michigan co-founded the project. Tech giant Cisco Systems and cloud services company Akamai then came on as founding co-sponsors. After the launch, Silicon Valley bigwigs such as Google and Facebook also joined as sponsors.

Since former NSA contractor Edward Snowden exposed a variety of U.S. surveillance programs, internet companies have worked to boost their security by implementing HTTPS, an encrypted version of basic HTTP, which is how all data moves around the internet.

While several prominent services, including major social networks and banking websites, now encrypt their traffic by default, the vast majority of websites do not.

The EFF said “almost all” of Let's Encrypt certificates are going to these websites that had “never supported” HTTPS.

“Let's Encrypt is steadily helping to make HTTPS encryption more and more conveniently available to everyone, across the entire web,” the EFF said.

The spread of encryption has caused tension between the tech community and the government.

While digital companies insist that widespread encryption is essential to global digital security and online privacy, federal officials warn that the technology is impeding legitimate law enforcement investigations.

UW team stores digital images in DNA — and retrieves them perfectly

By Jennifer Langston, UW Today, April 7, 2016

As brazen heists go, it was a quiet one. Over a single weekend in February, hackers managed to extract tens of millions of dollars from Bangladesh's central bank before anyone noticed. Now the bank is in turmoil, its governor has resigned and much of the cash is missing. It's one of the biggest holdups in history -- and other central banks should be on notice.

Technology companies routinely build sprawling data centers to store all the baby pictures, financial transactions, funny cat videos and email messages its users hoard.

But a new technique developed by University of Washington and Microsoft researchers could shrink the space needed to store digital data that today would fill a Walmart supercenter down to the size of a sugar cube.

For more information, visit the Molecular Information Systems Lab.

In a paper presented in April at the ACM International Conference on Architectural Support for Programming Languages and Operating Systems, the team of computer scientists and electrical engineers has detailed one of the first complete systems to encode, store and retrieve digital data using DNA molecules, which can store information millions of times more compactly than current archival technologies.

Authors of the paper are UW computer science and engineering doctoral student James Bornholt, UW bioengineering doctoral student Randolph Lopez, UW associate professor of computer science and engineering Luis Ceze, UW associate professor of electrical engineering and of computer science and engineering Georg Seelig, and Microsoft researchers and UW CSE affiliate faculty Doug Carmean and Karin Strauss.

In one experiment outlined in the paper, the team successfully encoded digital data from four image files into the nucleotide sequences of synthetic DNA snippets. More significantly, they were also able to reverse that process — retrieving the correct sequences from a larger pool of DNA and reconstructing the images without losing a single byte of information.

The digital data is chopped into pieces and stored by synthesizing a massive number of tiny DNA molecules, which can be dehydrated or otherwise preserved for long-term storage.

That's a tenfold increase compared to 2013, and will represent enough data to fill more than six stacks of computer tablets stretching to the moon. While not all of that information needs to be saved, the world is producing data faster than the capacity to store it. DNA molecules can store information many millions of times more densely than existing technologies for digital storage — flash drives, hard drives, magnetic and optical media. Those systems also degrade after a few years or decades, while DNA can reliably preserve information for centuries. DNA is best suited for archival applications, rather than instances where files need to be accessed immediately.

The team from the Molecular Information Systems Lab housed in the UW Electrical Engineering Building, in close collaboration with Microsoft Research, is developing a DNA-based storage system that it expects could address the world's needs for archival storage.

First, the researchers developed a novel approach to convert the long strings of ones and zeroes in digital data into the four basic building blocks of DNA sequences — adenine, guanine, cytosine and thymine.

"How you go from ones and zeroes to As, Gs, Cs and Ts really matters because if you use a smart approach, you can make it very dense and you don't get a lot of errors," said co-author Georg Seelig, a UW associate professor of electrical engineering and of computer science and engineering. "If you do it wrong, you get a lot of mistakes."

The digital data is chopped into pieces and stored by synthesizing a massive number of tiny DNA molecules, which can be dehydrated or otherwise preserved for long-term storage.

Read the rest here:
7 potential security concerns for wearables

By Michelle Drolet, NetworkWorld, April 11, 2016A

Wearables are rapidly invading the workplace in much the same way that smartphones did. Fitness trackers, smartwatches, head-mounted displays and other new form factors are beginning to capture the public imagination. Sales of wearable electronic devices topped 232 million in 2015, and Gartner forecasts they'll rise 18.4% this year, when another 274.6 million devices are sold.

These wearable devices represent some appealing opportunities for businesses to increase efficiency and gather data, but in the rush to win market share, security concerns are taking a backseat for many manufacturers and app developers. The potential ramifications of unchecked wearable device usage within the enterprise are alarming.

1. Easy Physical Access to Data
The fact that many wearables store data on the local device without encryption is a real issue. There’s often no PIN or password protection, no biometric security and no user authentication required to access data on a wearable. If it falls into the wrong hands, there’s a risk that sensitive data could be accessed very easily.

2. Ability to Capture Photos, Videos and Audio
The kinds of discreet abilities that many modern wearable devices have in terms of video and audio surveillance surpass high-end spy gear from just a few years ago. It's easy for someone to surreptitiously take photographs or record video or audio files using something like a smartwatch or smart glasses. Covert capture of confidential information, and videos and images of sensitive areas, is a very real possibility.

3. Insecure Wireless Connectivity
The fact that wearable devices tend to connect to our smartphones or tablets wirelessly using protocols such as Bluetooth, NFC and Wi-Fi creates another potential point of entry. We may have Bluetooth on our smartphones turned on all the time now so they can sync with the wearable, but what else could be connecting? Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack. The first step for securing networks is simply to get visibility on how many connected devices there are. One-third of the organizations surveyed by AT&T recently revealed they have more than 5,000 connected devices.

4. Lack of Encryption
We already mentioned the lack of encryption on many wearable devices, but there are also serious issues with data in transit when it’s being synced and with data being stored on manufacturer’s or service provider’s cloud servers. Some third-party apps neglect basic security standards and send or store information that’s not encrypted. The kind of data that’s automatically being collected by wearables is very valuable to the right people.

5. No Regulation or Compliance
Because many of the security issues around wearables really have to be addressed by the manufacturers, the issue of whether they’ll self-regulate or be bound by government regulations is an important one. In either case, companies suffering a data breach that breaks compliance or regulatory requirements for their specific industry will not be able to shift the blame onto wearables. They’ll still be held fully accountable. Ignorance of wearable device security and manufacturer or third-party app policy is no defense.

6. Patching and Vulnerabilities
Many wearables run their own operating system and applications. As wearable devices become more common, they’ll also become bigger targets for hackers. The same principles that apply to keeping the software on your desktops, laptops, smartphones and tablets fully patched and up to date to avoid the latest vulnerabilities also apply to wearables. But there’s a lack of insight and policy to cater for this issue right now.

7. Current MDM Policies Don’t Cover Wearables
We can’t assume that MDM (mobile device management) systems developed to deal with the BYOD trend can also cater to this influx of wearables. For the sake of convenience, mobile platforms generally make it easy to share data between apps and devices. Because wearables work differently from smartphones, there are many unforeseen circumstances where they pose new security risks. Banning or restricting features is not a sound long-term strategy, so companies need to rethink policies, draft new plans and employ new services to deal with mobile device management.

Read the rest here:
http://www.networkworld.com/article/3054584/security/7-potential-security-concerns-for-wearables.html
You Lost More Than Your Office March Madness Pool with the CBS App

By Autumn Foster, SecureWorld Media, April 13, 2016

March Madness has come and gone, you've licked your wounds and conceded that Amy in accounting knew what she was doing when she picked Villanova to win it all. While the NCAA Tournament was good for the Wildcats, it may have been really bad for you.

Wandera released a threat advisory that a CBS Sports app left personal information of millions of users unencrypted. Security researchers say the app exposed first and last names, dates of birth, email addresses, login passwords (this is why you never use the same password across multiple platforms!), and zip codes. The researchers also found that the mobile website didn't encrypt user data during the login process either. That means your email address and password information was sent in clear text.

CBS Sports Digital won't comment on why the app even needed that kind of personal information in the first place, but says the vulnerability is fixed.

SC Magazine obtained a statement from CBS Sports Digital which read:

"There was no data breach on either the CBS Sports app or mobile site. Our internal teams are rigorous about monitoring our platforms for any potential security issues. We take issue with outside companies publicizing the security operations of other firms for their own purposes rather than user protection."

Oh, really? Because someone else exposed a security flaw that you're responsible for, you "take issue" with it? We know you'd rather sweep this under the rug and pretend it didn't happen, CBS Sports Digital. But to publicly decry a security team for exposing a vulnerability to millions of people is just bad form.

Security researchers reported the issue to CBS Sports Digital on March 18. Which, you'll recall, was at the height of the first round of the NCAA Men's Basketball Tournament.

Read the rest here:

Who's Winning the Race to Secure Connected Cars?

By Autumn Foster, SecureWorld Media, April 7, 2016

After the "Great Jeep Hack of 2015," the average consumer likely turned his nose up in the air and swore off connected cars. But the automotive industry is confident it will win over those Nervous Nellys and is moving full-speed ahead to bring us the most technologically advanced vehicles imaginable.

And that means cybersecurity companies are racing to win over automakers and consumers alike with advanced security solutions.

Today, startup Karamba Security entered the race, announcing it's ready to launch its approach to in-car security. The company has created an Electronic Control Units (ECU) endpoint solution it says will protect a car's externally connected components. How? Karamba says its solution identifies attack attempts and blocks exploits from infiltrating the car's network.

Karamba's product embeds directly on the ECU to ensure only approved code and applications can be loaded and run on the controller. The solution blocks any foreign code, regardless of whether it's entered through the internet, USB drive, or service port. The company claims there are no false alarms.

Karamba's approach appears to be getting attention. The Connected Vehicle Trade Association gives it a big thumbs up.

"Early detection of cyberattack attempts and prevention of malware without false positive risks are essential to immunize cars against malicious software," explained Scott J. McCormick, President of the CVTA. "We are impressed with Karamba Security's unique approach, which can be used to provide early warnings of attack attempts and prevent malware from infiltrating the safety controllers of both new and existing cars."

Read the rest here:
Almost half of dropped USB sticks will get plugged in

By Lisa Vaas, Naked Security, April 8, 2016

Bad bots are used by fraudsters and are the key culprits behind web scraping, brute force attacks, competitive data mining, online fraud, account hijacking, data theft, unauthorized vulnerability scans, spam, man-in-the-middle attacks, digital ad fraud, and downtime.

People are still plugging in USB sticks scattered around parking lots, a new study has confirmed.

This time, the researchers hail from the University of Illinois. They decided to test what they call the “anecdotal belief” that people pick these things up and plug them in, so they dropped 297 drives on the school’s Urbana-Champaign campus last year.

Sure enough, they found that if there were real malware on these drives, it would have been successful at infecting those users who plug them in. The success rate fell between 45% and 98%, as they describe in a paper titled “Users Really Do Plug in USB Drives They Find”.

They also found that a USB drive-inflicted infection would take root very quickly: the first drive phoned home to the researchers in less than 6 minutes after it was placed.

Multiple security researchers have already determined that people do this, of course.

One of the more recent experiments was done by CompTIA, which littered four US cities – Chicago, Cleveland, San Francisco and Washington, D.C. – with 200 unbranded, rigged drives, leaving them in high-traffic, public locations to find out how many people would do something risky.

The nearly one out of five users who plugged in the drives in CompTIA’s study proceeded to engage in several potentially risky behaviors: opening text files, clicking on unfamiliar web links or sending messages to a listed email address.

The numbers get even worse in the University of Illinois study: at least 48% of the boobytrapped drives were picked up and plugged into a device before somebody then opened the files stored on the drive.

While slightly less than half of the drives were plugged in, nearly all of them – 98% – were moved from their original drop location.

The researchers don’t actually know if the 155 drives that were moved but didn’t have their files opened were plugged in or not. Somebody might have picked up a drive, plugged it in and refrained from opening a file, or they might not have connected it at all.

That big “don’t know” shadow is how they pegged the attack’s success rate at between 45–98%.

The university students and staff who connected the drives weren’t rated as being particularly risk-prone, with the exception of recreational risk (because college students, one assumes?) and, well, the tendency to plug in mysterious flash drives.

Still, the majority of them – 68% – took no precautions with the sticks.

The researchers know this because they presented their subjects with a short survey after they opened files on the drives. The subjects who at least tried to protect themselves took these steps, though the researchers said they did so ineffectually:

- 16% scanned the drive with their anti-virus software.
- 8% believed that their operating system security features would protect them, e.g., “I trust my MacBook to be a good defense against viruses”.
- 8% sacrificed a personal computer or used university resources to protect their personal equipment.

In 2011, Sophos studied 50 USB keys bought at a major transit authority’s Lost Property auction, finding that 66% of them – 33 – were infected.

Obviously, lost flash drives carry risk both to the finder and to employers: somebody who picks up a rigged drive can spread infection onto not only their own devices, but also onto his or her company’s systems in these days of bring your own device (BYOD).

Those that aren’t placed by security researchers or miscreants trying to plant malware also carry the risk of compromised data, of course – most particularly given that flash drives are rarely encrypted.

Sophos found that in studying those 50 USB keys: not one of the batch was encrypted. Nor were their files password-protected.

How do you keep your data safe and your systems uninfected when dealing with these matchbox-sized threat vectors? Here are a few tips:

1. Encrypt personal and business data before you store it on a USB key so it can’t be accessed if you drop the drive.
2. Use security software, and keep it up to date. An infection rate of 66% means there are a lot of malware-spreaders out there.

Read the rest here: https://nakedsecurity.sophos.com/2016/04/08/almost-half-of-dropped-usb-sticks-will-get-plugged-in/
Lawmakers fear insider threats in DOD network consolidation

By Billy Mitchell, FedScoop, April 20, 2016

Insider threats continue to remain a high risk for today's companies, and a recent study by SailPoint proves exactly why management doesn't trust their own personnel.

The Defense Department has planned for security in its Joint Information Environment to protect from outside cyber attackers, but lawmakers worry the departmentwide network consolidation might not do enough to protect against threats from within.

In a proposal for its portion of the National Defense Authorization Act of 2017 released Tuesday, the House Armed Services Committee's Subcommittee for Emerging Threats and Capabilities put forward a number of policy and spending proposals, including hardening JIE, reigning in the Defense Department's Silicon Valley innovation outpost and boosting the use of commercial cloud computing.

The Defense Information Systems Agency-led JIE is intended to standardize, simplify, centralize, secure and automate the DODwide IT infrastructure under one network. Officials have said the new network would provide less surface area for outside cyberattacks, but the subcommittee proposal frets not enough is being done to police activity inside the network.

"Historically, the tools used to monitor ... exterior threats do not provide good defenses against insiders or lateral movements within a network" by attackers who've already penetrated the system, the proposal says. "Where the Department has been focused on insider threats, the committee is concerned that those recommendations have been focused on procedural changes that are not connected to the capabilities, or the capability needs, for network tools and digital rights management."

The proposal — which still faces mark up from the subcommittee, as well as the full committee as part of the 2017 NDAA — would require DOD CIO Terry Halvorsen to brief the House Armed Services Committee by the year's end on his plan to integrate insider threat defenses into the JIE.

"This briefing should address those tools currently planned for incorporation, like digital rights management, as well as identification of any gaps in the architecture where commercial tools for insider threat monitoring might be included into JIE, or into upgrades to key enabling capabilities like the Joint Regional Security Stacks or the Host Based Security System," the proposal says.

The subcommittee targeted an array of defense IT issues in its proposal, such as updating the DOD cloud access point strategy to enable greater adoption of commercial cloud; assessing DOD's efforts to secure the Internet of Things; countering terrorists groups' spread of messaging on social media; and funding the DOD-led development of security clearance systems to replace those housed by the Office of Personnel Management that resulted in stolen information on tens of millions of Americans who applied for federal background checks.

Read the rest here:

Google Patents Electronic Device That Would Be Injected Onto Your Freaking Eyeball

By Darren Orf, Gizmodo, April 29, 2016

Merging biology with electronics isn’t a question of if, but when. Some enterprising biohackers have even decided that the time is now. Google-parent Alphabet appears to be preparing for our cybernetic future with a new patent for electronics that can be injected onto your eye.

The company has been interested in eyeball tech for awhile, most notably with its longtime development of smart contact lenses for monitoring diabetes. However, this cringe-inducing tech (I do apologize for that GIF above) would actually work to help focus light onto the retina.

The patent specifically covers a method for "injecting a fluid into a lens capsule of an eye, wherein a natural lens of the eye has been removed from the lens capsule." (EW!) An “intra-ocular” floats in the fluid and conforms to the surface of the eye. (GROSS!) It’s powered by "radio frequency energy" received by a small antenna inside. This teeny eyeball gadget even has its own data storage.

Read the rest here:
http://gizmodo.com/a-new-google-patent-injects-vision-correcting-electronic-1773789578
Short URLs plus cloud services equal bad security

By Zeljka Zorz, Help Net Security, April 15, 2016

Short URLs are great when they lead to public websites, and documents and files that aren’t meant to remain private, but you should think twice about using them to lead collaborators to content that’s meant only for their eyes.

“URLs created by many URL shortening services are so short that the entire space of possible URLs can be scanned or at least sampled on a large scale,” researchers Martin Georgiev and Vitaly Shmatikov pointed out in their research paper.

They proved this claim by checking out URLs created through the integrated URL shortening services in the Microsoft OneDrive cloud storage service and Google Maps.

“We did not perform a comprehensive scan of all short URLs (as our analysis shows, such a scan would have been within the capabilities of a more powerful adversary), but we sampled enough to discover interesting information and draw important conclusions,” Shmatikov shared in a blog post.

In the case of OneDrive, they found files (ethical concerns prevented them from analyzing their content) and a way to get to other files in the accounts. They also found that 7% of the OneDrive accounts exposed in this fashion allow anyone to write into them, making it possible for attackers to upload malware.

“Since cloud-stored files are automatically copied into users’ personal computers and devices, this is a vector for large-scale, automated malware injection,” they explained.

In the case of Google Maps, they found directions that users shared with each other, and which could be used to discover information about the users, including their identities, home addresses, and potentially sensitive locations they visited (e.g. specialized medical institutions).

Their findings were disclosed to Microsoft and Google. The latter responded promptly and made newly created short URLs to Google Maps consist of 11 or 12-character tokens.

Microsoft, on the other hand, did not immediately admit that there was a problem. Still, they recently removed the “shorten link” option from OneDrive, and changed the API that allowed the researchers to root through accounts once they found their way in.

Read the rest here:
Cybercriminals are adopting corporate best practices

By Staff, Help Net Security, April 12, 2016

Cybercriminals are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This new class of professional cybercriminal spans the entire ecosystem of attackers, extending the reach of enterprise and consumer threats and fueling the growth of online crime.

“Advanced criminal attack groups now echo the skill sets of nation-state attackers. They have extensive resources and a highly-skilled technical staff that operate with such efficiency that they maintain normal business hours and even take the weekends and holidays off,” said Kevin Haley, director, Symantec Security Response. “We are even seeing low-level criminal attackers create call center operations to increase the impact of their scams.”

Advanced professional attack groups

Advanced professional attack groups are the first to leverage zero-day vulnerabilities, using them for their own advantage or selling them to lower-level criminals on the open market where they are quickly commoditized. In 2015, the number of zero-day vulnerabilities discovered more than doubled to a record-breaking 54, a 125 percent increase from the year before, reaffirming the critical role they play in lucrative targeted attacks, according to Symantec’s Internet Security Threat Report.

Meanwhile, malware increased at a staggering rate with 430 million new malware variants discovered in 2015. The sheer volume of malware proves that professional cybercriminals are leveraging their vast resources in attempt to overwhelm defenses and enter corporate networks.

Over half a billion personal records stolen or lost in 2015

Data breaches continue to impact the enterprise. In fact, large businesses that are targeted for attack will on average be targeted three more times within the year. Additionally, we saw the largest data breach ever publicly reported last year with 191 million records compromised in a single incident. There were also a record-setting total of nine reported mega-breaches. While 429 million identities were exposed, the number of companies that chose not to report the number of records lost jumped by 85 percent. A conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.

“The increasing number of companies choosing to hold back critical details after a breach is a disturbing trend,” said Haley. “Transparency is critical to security. By hiding the full impact of an attack, it becomes more difficult to assess the risk and improve your security posture to prevent future attacks.”

Encryption used as a weapon to hold critical data hostage

Ransomware also continued to evolve in 2015, with the more damaging style of crypto-ransomware attacks growing by 35 percent. This more aggressive crypto-ransomware attack encrypts all of a victim’s digital content and holds it hostage until a ransom is paid. This year, ransomware spread beyond PCs to smartphones, Mac and Linux systems, with attackers increasingly seeking any network-connected device that could be held hostage for profit, indicating that the enterprise is the next target.

Scammers make you call them to hand over your cash

As people conduct more of their lives online, attackers are increasingly focused on using the intersection of the physical and digital world to their advantage. In 2015, Symantec saw a resurgence of many tried-and-true scams.

Cybercriminals revisited fake technical support scams, which saw a 200 percent increase last year. The difference now is that scammers send fake warning messages to devices like smartphones, driving users to attacker-run call centers in order to dupe them into buying useless services.

Read the rest here:
https://www.helpnetsecurity.com/2016/04/12/professional-attack-groups/
The Information Systems Security Association (ISSA®) is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at: doncream-issa@q.com

Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

This Ancient Laptop Is The Only Key To The Most Valuable Supercars On The Planet
By Máté Petrány, Jalopnik, April 29, 2016

This is a Compaq LTE 5280 laptop from the early 1990s, running a bespoke CA card. In 2016, McLaren Automotive—one of the most high-tech car and technology companies on the planet—still uses it and its DOS-based software to service the remaining hundred McLaren F1s out there, each valued at $10 million or more.

McLaren Special Operations is a workshop like no other. It’s located in an industrial complex a few minutes from their well-known Technology- and Production Center in Woking, England, in a building where McLaren used to work on its Formula One racing efforts before deciding to give it a go against Ferrari on the streets as well. I’ll have more detailed story on MSO later, but for now, let’s focus on the most challenging part of their job: the maintenance of McLaren F1s.

Read the rest here:
http://jalopnik.com/this-ancient-laptop-is-the-only-key-to-the-most-valuabl-1773662267

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing™, Woodland Park, Colorado