Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cybersecurity and Technology

ACQUISITION HOUR WEBINAR

November 29, 2017

WEBINAR ETIQUETTE

- Please
  - When logging into go-to-meeting, enter the name that you have registered with
  - Put your phone or computer on mute
  - Use the Chat option to ask your question(s): We will read them and our guest speaker will provide an answer to the group
- Thank you!

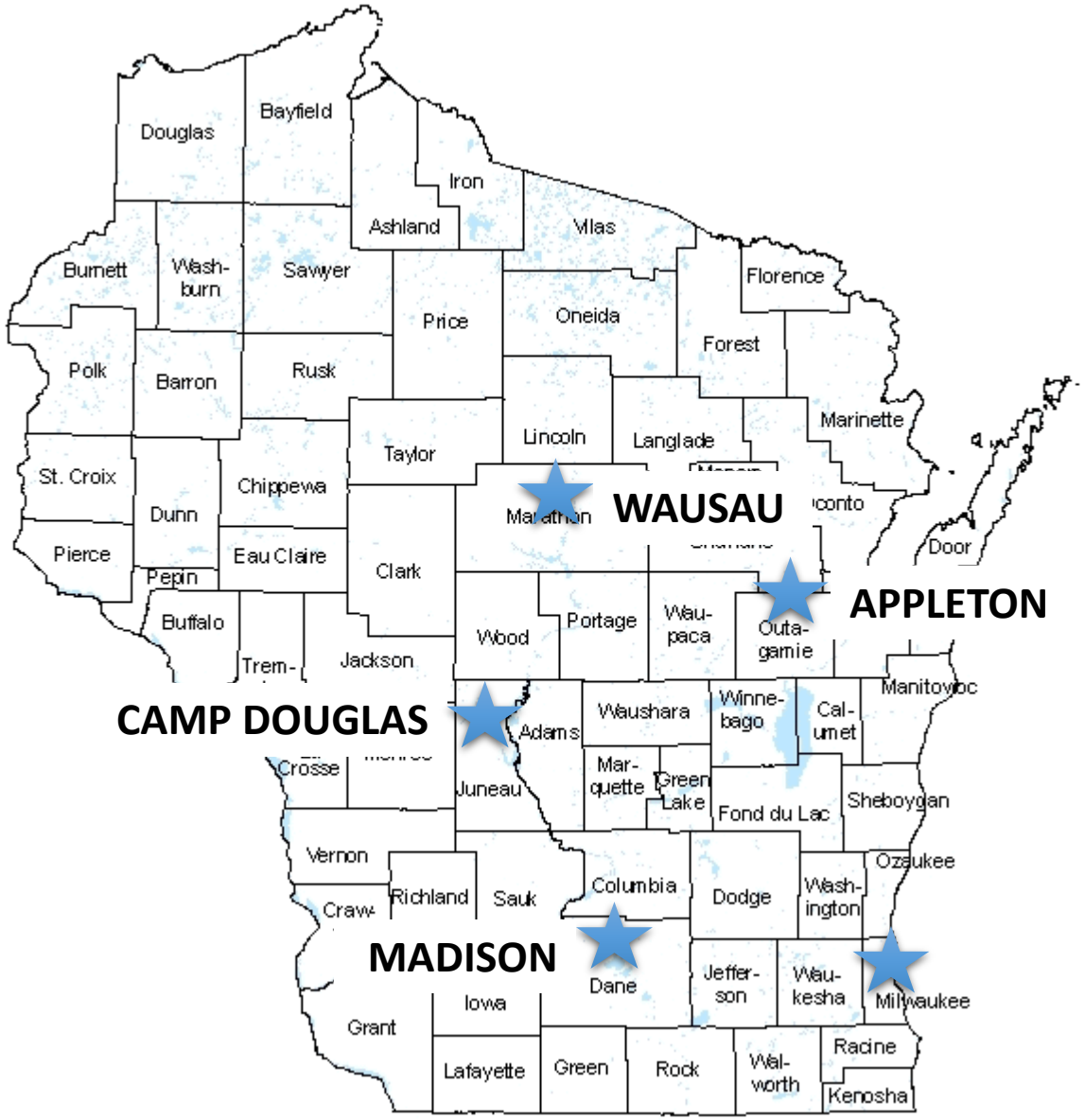
ABOUT WPI
SUPPORTING THE MISSION

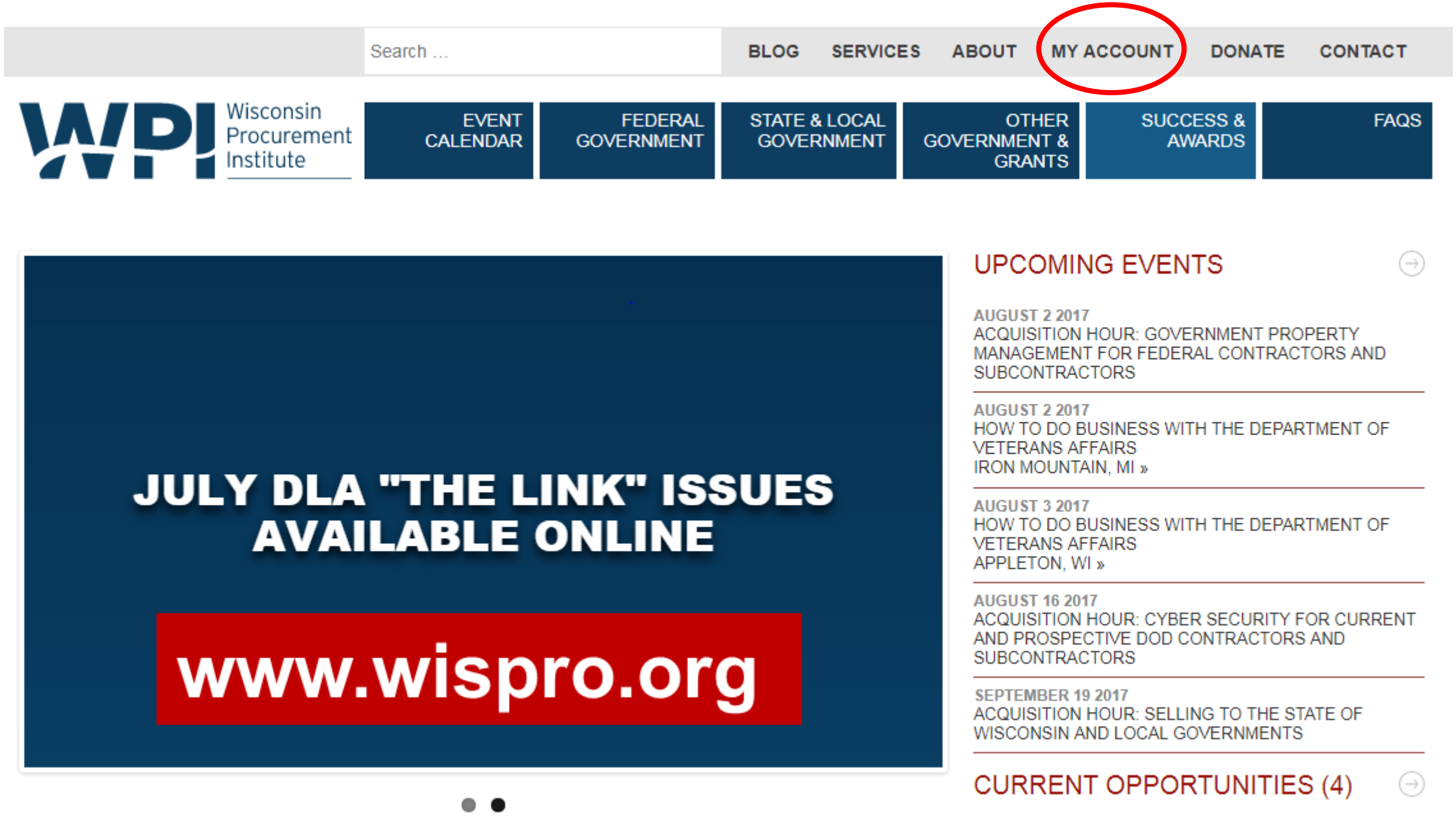
Assist businesses in creating, development and growing their sales, revenue and jobs through Federal, state and local government contracts.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

WPI OFFICE LOCATIONS

- MILWAUKEE – *Technology Innovation Center*
- MADISON –
  - *Madison Enterprise Center*
  - *FEED Kitchens*
- CAMP DOUGLAS– *Juneau County Economic Development Corporation (JCEDC)*
- WAUSAU – *Wausau Region Chamber of Commerce*
- APPLETON – *Fox Valley Technical College*




Search ...
BLOG
SERVICES
ABOUT
MY ACCOUNT
DONATE
CONTACT
Wisconsin Procurement Institute
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
OTHER GOVERNMENT & GRANTS
SUCCESS & AWARDS
FAQS
JULY DLA "THE LINK" ISSUES AVAILABLE ONLINE
www.wispro.org
UPCOMING EVENTS
AUGUST 2 2017
ACQUISITION HOUR: GOVERNMENT PROPERTY MANAGEMENT FOR FEDERAL CONTRACTORS AND SUBCONTRACTORS
AUGUST 2 2017
HOW TO DO BUSINESS WITH THE DEPARTMENT OF VETERANS AFFAIRS
IRON MOUNTAIN, MI »
AUGUST 3 2017
HOW TO DO BUSINESS WITH THE DEPARTMENT OF VETERANS AFFAIRS
APPLETON, WI »
AUGUST 16 2017
ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS
SEPTEMBER 19 2017
ACQUISITION HOUR: SELLING TO THE STATE OF WISCONSIN AND LOCAL GOVERNMENTS
CURRENT OPPORTUNITIES (4)

SERVICES OFFERED BY WPI

- FREE Bid Matching Services
- Individual Counseling and Assistance
- Locating Local, State and Federal Opportunities
- Government Market Strategy Development
- Training in use of Government websites and tools
- Assistance with System for Award Management (SAM) Registration
- Assisting in Market Research Process
- Development of Market Profile
- Small Business Subcontracting Plans Development, Outreach and Reporting
- Small Group Training
- Outreach and training with Local, State and Federal agencies
- Assist with Pre and Post Award Functions
- Assistance with Agency Specific Contracting Requirements
- Assistance with Contracting Regulations and Requirements, including FAR, DFAR, CFR
- Assistance with GSA Schedule Preparation and Administration
- Assistance with Local, State and Federal Certifications, including:
  - Service Disabled & Veteran Owned Small Business, HUBZone, Woman Owned Small Business, 8(a) Business Development Program
  - State
  - Local
  - DBE
- Bid review and Submission Assistance
- Proposal review and Submission Assistance
- Capabilities Statement and Related Government Marketing Material Development
- Assistance in Locating and Developing Teaming Partners and Subcontractors
- Updated Government Market Information

TECHNOLOGY & CRIME

Detective George Chavez

Wisconsin Procurement Institute

George A. Chavez
Retired Detective
Madison PD/ILGIA
P.O Box 85 Cottage Grove, WI. 53527
(ph) 608-215-7823
Email: wigangdet@gmail.com

George Chavez has been in Law Enforcement for 32 years with the last 26 years in the City of Madison. George has specialized in crime involving youth with an emphasis on gang related issues. George was the first Gang Detective for the City of Madison and was involved and focused on his four-pronged approach to dealing with gangs to include Prevention, Intervention, Re-Entry and Suppression.

George is currently the Midwest Representative for the International Latino Gang Investigators Association and teaches throughout the Country and Canada in developing successful strategies to dealing with gangs and gang violence. George has presented at numerous conferences for MGIA (Midwest Gang Investigators Association), GLIGIC (Great Lakes International Gang Investigators Coalition) , ILGIA (International Latino Gang Investigators Association, National Gang Summit and the Calgary Alberta Gang Crime Summit.

George has testified as an expert witness on gang related shootings and acts of violence.
George also has worked as a Detective and ERO assigned to the schools in Madison and assisted in developing strategies in schools to deal with Juvenile crime issues. George has focused on community outreach and various ways to get the community involved and starting partnership's to make communities safer.

George worked with the Dane County Narcotics and Gangs Task Force as well as the Badgerland Fugitive Felon Apprehension Squad with the US Marshals Service. George worked in an undercover capacity with the narcotics unit and also conducted investigations in the drug unit as an Officer and Detective.
George been involved in numerous overdose death investigations and has conducted investigations at RAVE events and Pharmacy Robberies involving collaborative efforts between local LE and Federal agencies. George has presented on these topics to numerous Law Enforcement and Community groups

George has focused on utilizing the social media, computer applications as well as phone applications to gain intelligence on various crimes to assist with prosecution and investigations. George has done numerous presentations for Law Enforcement Officers around the country on social media and assisted with investigations involving social media platforms. George has been building a network for Officers, Detectives and Investigators to share information and knowledge on dealing with Social Media cases.

George also received his certification as an Ethical Hacker from the International Council of E-Commerce Consultants and Training Camp.

The Guardian view on internet security: complexity is vulnerable

Editorial

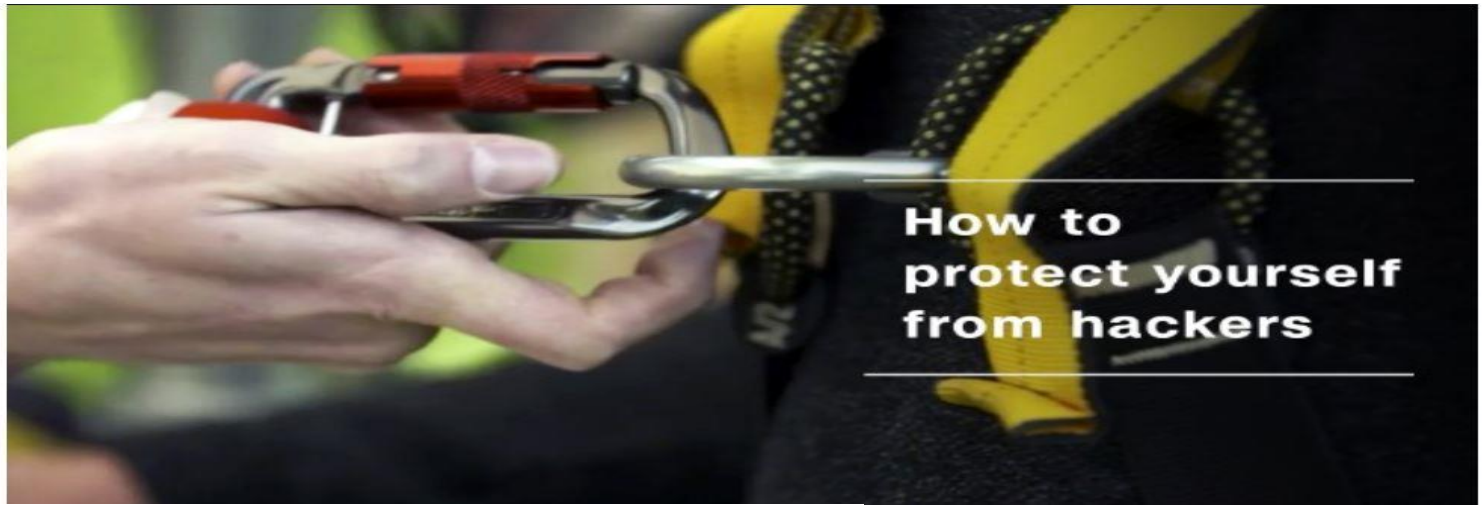
A huge weakness in wifi security erodes online privacy. But the real challenge is designing with human shortcomings in mind

Cyber-Safe

Hackers are targeting schools, U.S. Department of Education warns

by Selena Larson @selenalarson

October 18, 2017: 10:51 PM ET



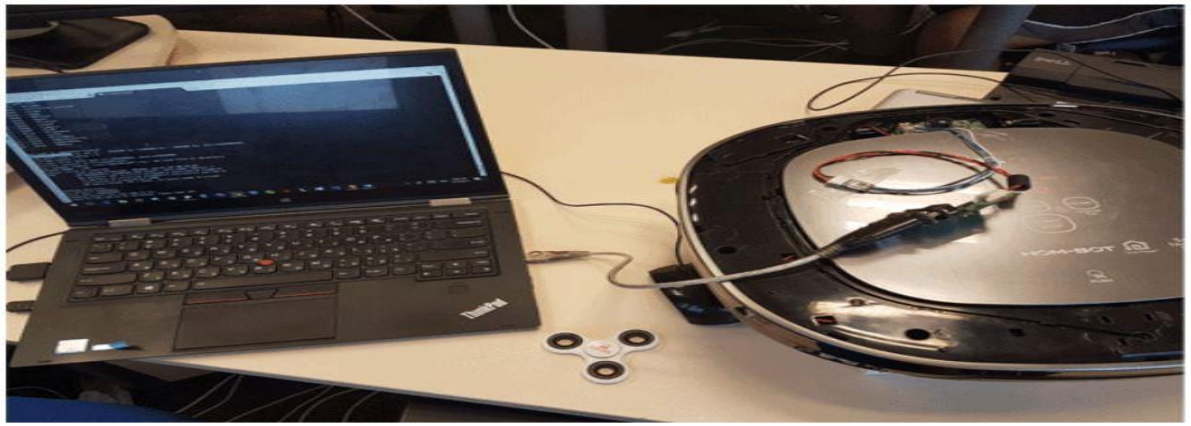
Recommend 8

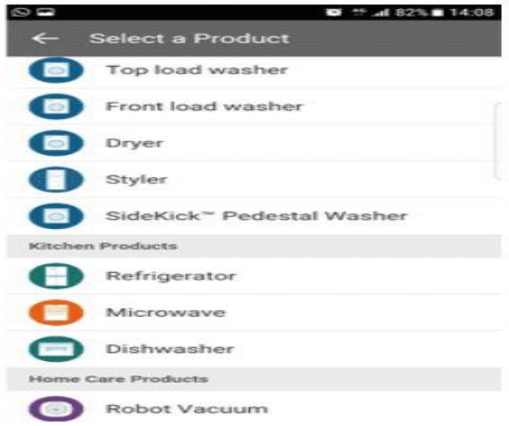
Social Su

sexual ha

Hackers Could Turn LG Smart Appliances Into Remote-Controlled Spy Robot

Thursday, October 26, 2017 Swati Khandelwal





If your smart devices are smart enough to make your life easier, then their smart behaviour could also be exploited by hackers to invade your privacy or spy on you, if not secured properly.

Paul Gordon, Contributor
Paul Gordon is a entrepreneur.

Rise Of The Cyber Criminals

Whilst financial crime threats are growing, companies are still lagging behind when it comes security.

08/25/2016 07:50 am ET | **Updated** Mar 28, 2017

I STOCK

If 2015 was the year cybercrime came of age, 2016 is already proving to be the year criminals refined their approach to a level of sophistication that has never previously been seen.

CYBER CRIMES

Cyber Crime Statistics and Trends

Businesses risk financial loss, damage to reputation, compromised brand perception, and fear repercussions from breaches to customers' private and sensitive information. Cybersecurity is no longer something only CEOs manage and IT professionals take responsibility for, it's something every level of business operations needs to prioritize.

The technology trends for 2017 will be dominated by artificial intelligence (AI) and cyber-crime, say several industry sources.

With the adoption of machine learning gathering pace, and the internet of things creating a fully connected world, technologists predict that we will see rapid development of intelligent devices and apps this year.

The current flagship product for adoption of machine learning devices is Amazon's Echo, powered by the Alexa conversational user interface. The Echo, with more than five million sold in two years, is a smart device that connects users to information and services via the voice interface of Alexa.
Volkswagen has signed a deal with Amazon for Alexa to be built into its cars, with other manufacturers likely to follow suit. Retailers, restaurants, internet services and other companies are also developing smart links for Alexa.

Every connected device is at risk from hackers and thieves, so cyber security will continue to be a recurring theme in headlines throughout 2017. Furthermore, some experts are turning the spotlight on banks who they say face dire consequences if cyber criminals continue to prevail.

ATM

New types of ATM thefts have started to emerge. These are happening particularly because many ATM networks don't use updated software, thus don't receive the latest security updates, which makes them extremely vulnerable when faced with digital frauds.

1) **The new scheme no longer relies on cyber criminals physically standing in front of an ATM and using skimming devices, but attacking the ATM from inside, through their network.**

2) **One of the easiest ways to infiltrate the ATM network is by sending phishing e-mails to bank employees; once they introduce a malicious code into the e-mail system, they capture valuable information about the employees' daily tasks and they can also trace vulnerabilities of the ATM network.**

3) **The next and final step is to install malware on the ATM server. Mainly, the hackers use a code that generates a secret-key for each session. When a bank customer uses the same key, the code allows the hacker to empty the ATM.**

4) **The attackers establish which ATMs they should infect depending on geographical location, public visibility and other criteria. This way, their partners know exactly which ATM they should collect the cash from and simply wait to pick up the money.**

There are two downsides to the ATM infection:

- **the customer won't realize this is happening because the ATM either works normally or looks like it is out of service**

- **it's hard to find the real hackers because they often resell the malware they use for this fraud.**

Self driving cars can be hacked by just putting stickers on street signs.

Car Hacking is a hot topic, though it's not new for researchers to hack cars. Previously they had demonstrated how to hijack a car remotely, how to disable car's crucial functions like airbags, and even how to steal cars.

All it takes is a simple sticker onto a sign board to confuse any self-driving car and cause accident.

A team of researchers from the University of Washington demonstrated how anyone could print stickers off at home and put them on a few road signs to convince "most" autonomous cars into misidentifying road signs and cause accidents.

According to the researchers, image recognition system used by most autonomous cars fails to read road sign boards if they are altered by placing stickers or posters over part or the whole road sign board.

By simply adding "Love" and "Hate" graphics onto a "STOP" sign (as shown in the figure), the researchers were able to trick the autonomous car’s image-detecting algorithms into thinking it was just a Speed Limit 45 sign in 100 percent of test cases.

The researchers also performed the same exact test on a RIGHT TURN sign and found that the cars wrongly classified it as a STOP sign two-thirds of the time.

A US freeway may get self-driving car lanes thanks to Foxconn

The I-94 highway connects to the Apple supplier's upcoming facility in the Midwest.

Saqib Shah, @eightiethmnt
11.14.17 in Transportation

17
Comments

874
Shares

Wisconsin highway planners are studying the possibility of placing driverless vehicle lanes on I-94 to serve Foxconn's mega factory in Racine County. The Taiwanese company -- supplier to tech firms including Apple, Microsoft, and Nintendo -- reportedly made the suggestion at a meeting with regional officials, according to *USA Today*'s *Journal Sentinel.*

While companies like Uber and Waymo are trialing self-driving vehicles on roads across the US, there's also been talk of dedicated lanes for robocars

How Google Is Teaching Robot Cars To Respond To Emergency Vehicles

In order for driverless cars to work, they'll need to be able to do tackle a bevy of ordinary tasks that motorists perform each day: navigate roadways, stay within a lane, stop for pedestrians who unexpectedly cross their path and successfully pull over for police cruisers or fire trucks needing to speed by. Google, through its self-driving car subsidiary Waymo, has been working on the latter task, and recently teamed up with a local Arizona fire and police department to conduct its "first emergency vehicle testing day" with the company's fleet of self-driving Chrysler Pacificas.

In a blog post on Monday, Waymo said it spent a day last month with the fire and police departments in Chandler, Arizona, conducting test runs with police cars, motorcycles, firetrucks, and ambulances around the city. The goal, Waymo says, was to have the sensors collect an extensive amount of data to build "up a library of sights and sounds to help teach our self-driving cars to respond safely to emergency vehicles on the road."

The cars come equipped with an audio detection system designed in-house by Waymo. Coupled with a suite of self-driving sensors, the vehicles can "see emergency vehicles and their flashing lights even further and clearer with our custom vision system, radars, and LiDARs," Waymo said.

SELF-DRIVING CARS WILL KILL PEOPLE. WHO DECIDES WHO DIES?

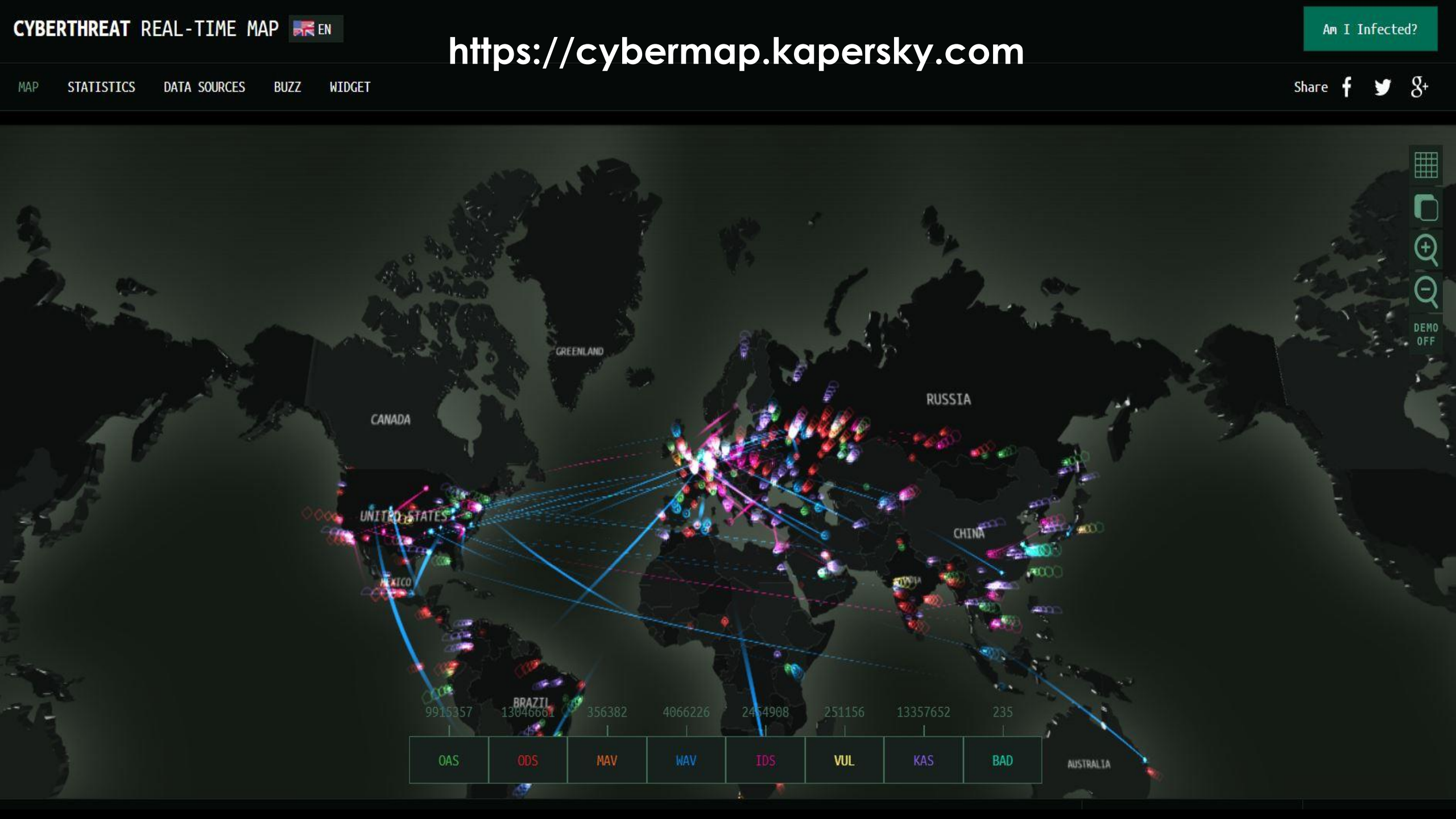
Recently, the “trolley problem,” a decades-old thought experiment in moral philosophy, has been enjoying a second career of sorts, appearing in nightmare visions of a future in which cars make life-and-death decisions for us.

To understand the trolley problem, first consider this scenario: You are standing on a bridge. Underneath you, a railroad track divides into a main route and an alternative. On the main route, 50 people are tied to the rails. A trolley rushes under the bridge on the main route, hurtling towards the captives. Fortunately, there’s a lever on the bridge that, when pulled, will divert the trolley onto the alternative route. Unfortunately, the alternative route is not clear of captives, either — but only one person is tied to it, rather than 50. Do you pull the lever?

With driverless cars, however, there can be no wiggle room. Like any computer, a driverless car will not do anything unless instructed. A programmer can’t simply give it instructions for most scenarios and avoid thinking about edge cases. At the same time, a driverless car must make decisions within a fraction of a second. There is no opportunity to present the circumstances to an external, human “road jury” for review. Thus, the instructions must stand on their own merits.

It’s tempting to hope that someone else will come along and solve the trolley problem. After all, finding a solution requires confronting some uncomfortable truths about one’s moral sensibilities. Imagine, for instance, that driverless cars are governed by a simple rule: minimize casualties.


CYBER
ATTACKS


CYBERTHREAT REAL-TIME MAP
EN
https://cybermap.kapersky.com
Am I Infected?
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
Share
DEMO OFF
GREENLAND
CANADA
RUSSIA
UNITED STATES
CHINA
MEXICO
BRAZIL
AUSTRALIA
9915357
13046661
356382
4066226
2454908
251156
13357652
235
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD

ATTACK ORIGINS

#	COUNTRY
14	United States
4	China
2	Switzerland
1	Ukraine
1	Poland
1	Netherlands

ATTACK TYPES

#	PORT	SERVICE TYPE
12	25	smtp
3	8080	http-alt
2	123	ntp
1	334	unknown
1	9846	unknown
1	23	telnet
1	1900	ssdp
1	195	dn6-nlm-aud

ATTACK TARGETS

#	COUNTRY
18	United States
4	United Arab Emirat...
1	Belgium

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
17:17:55.597	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
17:17:55.306	Microsoft Corporation	157.56.111.251	Redmond, US	De Kalb Junctio...	smtp	25
17:17:54.976	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junctio...	smtp	25
17:17:54.616	Microsoft Corporation	65.55.169.250	Washington, US	De Kalb Junctio...	smtp	25
17:17:54.156	Microsoft Corporation	65.55.169.246	Washington, US	De Kalb Junctio...	smtp	25
17:17:53.886	Microsoft Corporation	65.55.169.248	Washington, US	De Kalb Junctio...	smtp	25
17:17:53.757	Singlehop Inc.	198.20.87.98	Chicago, US	Seattle, US	dn6-nlm-aud	195
17:17:53.584	Pppoe Clients Pool	217.112.221.90	Kharkiv, UA	San Francisco, ...	unknown	9846
17:17:53.420	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Dubai, AE	http-alt	8080
17:17:52.932	Hurricane Electric Inc.	184.105.139.89	New York, US	De Kalb Junctio...	ssdp	1900

HOME

EXPLORE

WHY NORSE?

Powered by ThreatCloud Intelligence

THREATCLOUD

LIVE CYBER ATTACK THREAT MAP

Check Point SOFTWARE TECHNOLOGIES, INC.

https://threatmap.checkpoint.com

LEARN ABOUT CHECK POINT THREAT PREVENTION SOLUTIONS ›

ATTACKS TODAY
(since 12AM PST)
11,306,098
ATTACKS YESTERDAY
15,870,484

TOP TARGETS BY COUNTRY

TIME	ATTACK	SOURCE	TARGET
17:22:45	Phishing.dfydmd	TX,USA	Australia
17:22:45	Phishing.dfydmd	TX,USA	Australia
17:22:44	REP.iknyid	China	Australia
17:22:44	REP.iknyid	China	Australia

Source

Target


FireEye
Customer Stories
Blogs
Search FireEye.com
Products
Solutions
Services
Current Threats
Partners
Support
Company
[X] NEW ATTACK: FROM [UNITED KINGDOM] TO [KOREA, REPUBLIC OF]
[X] NEW ATTACK: FROM [FINLAND] TO [DENMARK]
[X] NEW ATTACK: FROM [PORTUGAL] TO [PHILIPPINES]
[X] NEW ATTACK: FROM [UNITED STATES] TO [PHILIPPINES]
LOCAL TIME
17:27:52
ATTACKS TODA
531,15
https://www.fireeye.com/cyber-map/threat-map
FIREEYE CYBER
THREAT MAP
FINLAND
UNITED KINGDOM
FRANCE
UNITED STATES
PORTUGAL
TAIWAN
THAILAND
PHILIPPINES
MALAYSIA
ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)
Powered by FireEye Lab
TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)
FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING
INSURANCE
VIEW FULL SCREEN

Digital Attack Map

Top daily DDoS attacks worldwide

October 5 2017

Showing All Countries
Show Attacks

Large | Unusual | Combined

Large attacks on Belgium and United States

Color Attacks By

Type | Source Port | Duration | Dest. Port

- TCP Connection
- Volumetric
- Fragmentation
- Application

Size (Bandwidth, in Gbps)

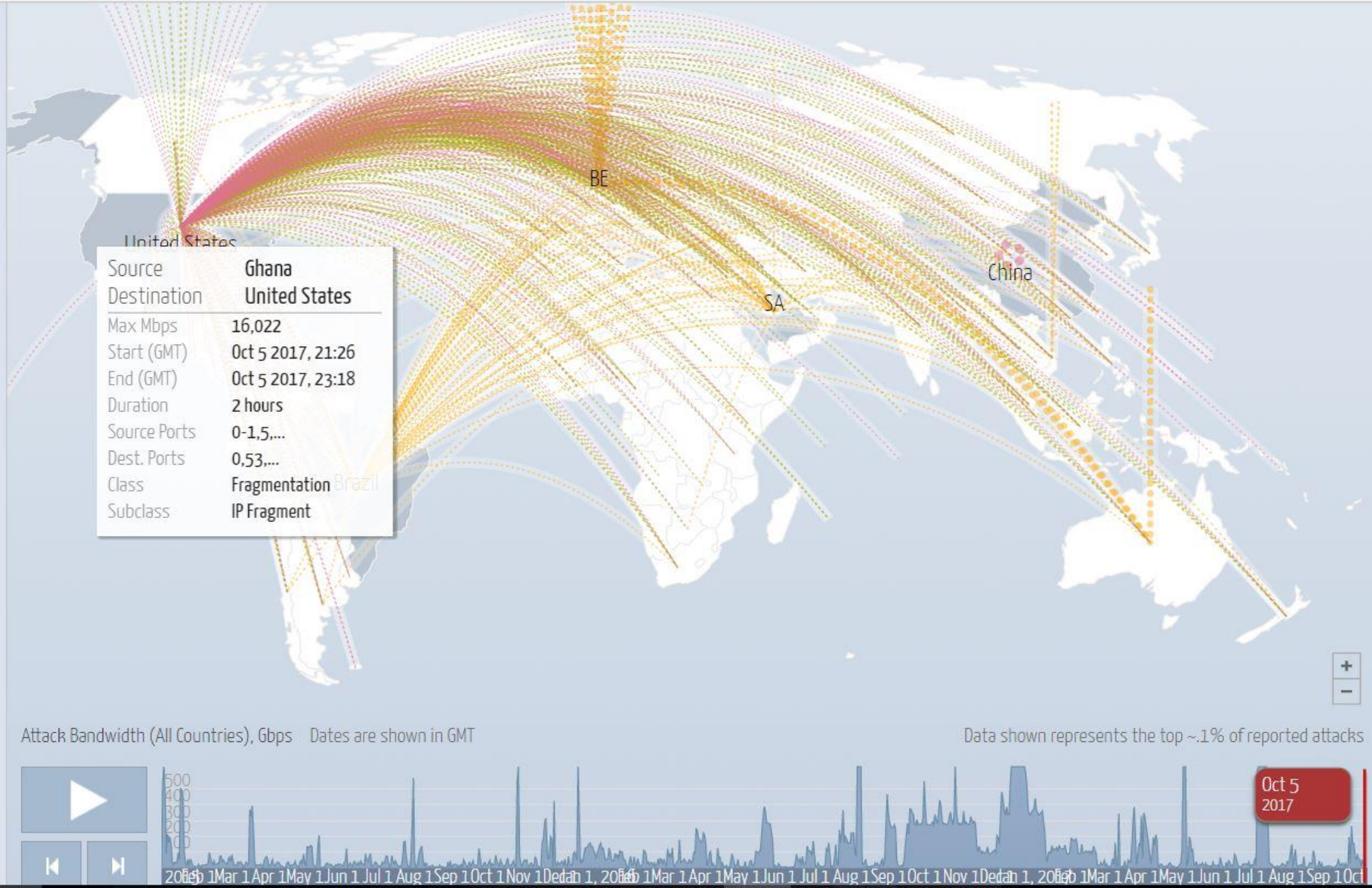
25 5 1

Shape (source + destination)

- between two countries
- internal
- either source or dest. unknown

<Get Embed Code>

Map | Table



The Equifax data breach compromised personal information for some 143 million Americans, but there are still two other major credit bureaus — Experian and TransUnion — whose digital vaults are filled with the same sensitive info. New York's top prosecutor is now asking these companies to explain how they won't be the next source of a massive consumer data leak.

New York Attorney General Eric Schneiderman announced this morning that his office has initiated a probe into the security practices of Experian and TransUnion.

Additionally, New York Governor Andrew Cuomo is pushing for new regulations to ensure that all three major credit agencies aren't putting consumers in harm's way.

The breach happened because Equifax security staff failed to promptly install a security fix to a flaw found in a web application tool used by many major corporations, the industry group that oversees the open-source software said earlier this week

It turned out that Chief of Security Susan Mauldin, the top executive handling cybersecurity at Equifax, didn't have much formal training in technology. She had studied music composition at the University of Georgia.

EQUIFAX BREACH

In light of the Equifax breach, among countless others, and since October is Cyber Security Awareness Month, you can complete this in about 20 minutes. Total out-of-pocket cost, $20 - $10 each for Experian / TransUnion, for some reason Equifax is free right now ;). Just keep in mind if you have a background investigation coming up (or pending), you'd probably need to "unfreeze" your credit report(s) to allow them to do a pull. You can re-freeze them once everything is done.

Source for material below: http://uspirg.org/sites/pirg/files/reports/USPIRGFREEZE_0.pdf

Before you freeze anything, you can request your free credit reports online: www.annualcreditreport.com – this is the official website authorized by the federal government for requesting these reports. Make sure to type this accurately. As of the printing of this report, misspelled websites are currently inactive but have existed in the past to misdirect people to unofficial services.

Whether your personal information has been stolen or not, your best protection against new account identity theft is the security freeze (also known as the credit freeze). Credit monitoring only lets you know after someone has opened a new account in your name (you still have to deal with the aftermath). A security freeze, on the other hand, prevents most new accounts from being opened in the first place. The best course of action for most consumers is to have their credit reports at each of the three major national credit bureaus frozen until they want to apply for credit, at which time they can easily unfreeze or "thaw" their reports. If you chose the security freeze, it is still advisable to request and monitor your free annual credit reports, available under federal law with each of the three major credit bureaus. It is also recommended that you consider opting out of pre-approved credit and insurance offers.

Equifax: https://www.freeze.equifax.com

Experian: https://www.experian.com/freeze/center.html

TransUnion: http://www.transunion.com/securityfreeze

Innovis (smaller, new bureau): https://www.innovis.com/personal/securityFreeze

Opting out of pre-approved (pre-screened) credit & insurance offers is your legal right and is recommended for all consumers. Credit and insurance companies buy "prescreened" lists from the credit bureaus to make pre-approved offers to prospective customers. While such offers provide consumers with information about possible credit options, identity thieves may steal these pre-approved offers and apply for them with your personal information. www.optoutprescreen.com is the official website sponsored by the four national credit bureaus where by law you can opt out of receiving these offers for five years (online) or permanently (by mail).

There's a great summary of pros / cons of a security freeze here: https://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/

Don't confuse a security / credit "freeze" with a "lock" that Equifax, in particular, is pushing. Here's a quick quote to illustrate the confusion going on around the "locks" right now: "Equifax and the other credit bureaus fought for years against our right to freeze our credit reports in the first place and then demanded fees to do so. We are still trying to figure out why they are pushing a newer thing they call a "lock." (http://www.uspirg.org/news/usp/equifax%E2%80%99s-offer-free-%E2%80%9Clock%E2%80%9D-raises-questions-best-protection-still-credit-freezes-all-three)

Hilton to pay $700,000 in data breach settlement with New York, Vermont

Hilton hotels has reached a $700,000 joint settlement with New York and Vermont for a pair of data breaches that were discovered in 2015, including one that exposed more than 350,000 credit card numbers.

A press release from New York Attorney General Eric Schneiderman states that Hilton Domestic Operating Company did not practice reasonable data security at the time of the breaches, and failed to provide consumers with timely notification, following the incidents.

New York will receive $400,000 from the settlement, with the remainder going to Vermont, whose AG's office investigated the breaches alongside Schneiderman's office.

As part of the settlement, Hilton has agreed to comply with New York State General Business Law 899-aa, which requires companies to provide notice to affected New York residents and the Attorney General's office when a personal without valid authorization acquires private information. The company has also agreed to design and maintain a program for securing consumer cardholder data, as well as obtain a written assessment of its compliance with Payment Card Industry (PCI) standards.

“Businesses have a duty to notify consumers in the event of a breach and protect their personal information as securely as possible,” said Schneiderman in his release. “Lax security practices like those we uncovered at Hilton put New Yorkers' credit card information and other personal data at serious risk."

The first of the two breaches was discovered in February 2015, after Hilton learned a system based in the UK had been infected with malware that may have exposed payment card data in November and December of 2014. From Apr. 21, 2015 through July 27, 2015, a second breach involving point-of-sale (POS) malware prompted a forensic investigation, which determined that 363,952 credit card numbers had been aggregated for removal by attackers. Hilton did not reveal its findings until Nov. 24, the release states.

Why is it a good idea to have a penetration test done on your organization?

1) Statistics have shown that 73% of hacks have come from external sources. 39% Implicated business partners and 30% involved multiple parties and 18% were caused by insiders.

2) This mean's unfortunately we have to look at disgruntled employees, people who have access to our facilities and may not follow procedures and protocols.

3) Some hacks are a result of organizations not providing training for their employee's as to be aware of people and access people have into their buildings or office space.

Piggybacking/Tailgaiting

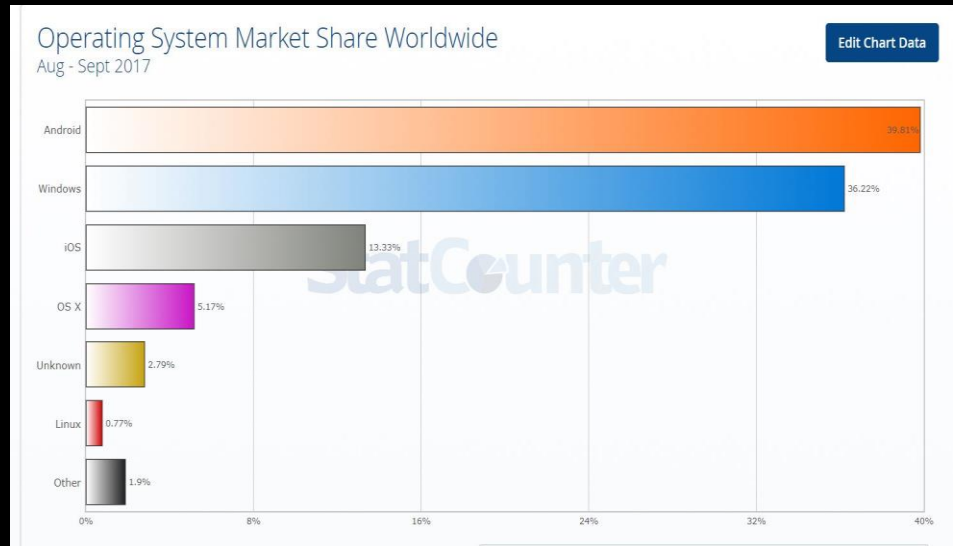
Popular Operating Systems

1) Windows 7 is the most popular operating system for desktop and laptop computers.

2) Linux are most widely used in the Internet of things and smart devices.

3) Android is the most popular smartphone operating system.

4) iOS is the most popular tablet operating system.



The most common passwords in 2016 are truly terrible the most popular one of all? “123456.”

Cybersecurity is on many people’s minds these days, and yet using “password” as a password is apparently still a thing.

On Friday, password management company Keeper Security released a list of the most common passwords of 2016 — and it’s, well, shameful.

The most popular password, making up nearly 17 percent of the 10 million passwords the company analyzed, was “123456.” “Password” was also among the top 10 passwords, coming in as the eighth most common.

*Passwords should be at least 15 characters long. Experts are suggesting that people start thinking of using password phrases that have some meaning for the individual, but will not be easy for people to know about you.

01/18/2017-HuffPost

THE TOP 25 MOST COMMON PASSWORDS OF 2016:

1.123456
2.123456789
3.qwerty
4.12345678
5.111111
6.1234567890
7.1234567
8.password
9.123123
10.987654321
11.qwertyuiop
12.mynoob
13.123321
14.666666
15. 18atcskd2w
16. 7777777
17. 1q2w3e4r
18. 654321
19. 555555
20. 3rjs1la7qe
21. google
22. 1q2w3e4r5t
23. 123qwe
24 zxcvbnm
25. 1q2w3e

Michael Lynton on Sony Hack: CEO Wasn't Sure Studio Would Survive Crisis

By Todd Spangler | @xpangler

CREDIT: UNIMEDIA IMAGES/REX SHUTTERSTOCK

Michael Lynton revealed professional and personal lessons learned from the devastating 2014 hack by North Korea on Sony Pictures Entertainment — admitting that he thought there was a "better than even chance" that the studio was not going to make it through

Michael Lynton the CEO of Sony was hacked and a big reason was the strength of his password. Lynton's password was "sonyml3". This made it easy for hacker's to gain access to all of Sony's records and allowed the breach of security.

PASSWORDS

Its estimated that 34% of Americans don't protect their mobile devices with any security measures at all including just a four number locking code.

There are 3 common ways to lock you phone, whether it's a IOS device or Android.

The first is a sequence of numbers that you enter to unlock your phone. You can go into the settings of your phone and go beyond the 4 digit number lock and customize your numbers and make it even more difficult for someone to gain access to your phone. Some phones will allow you a text based passcode .

Secondly there is a visual lock options (most common with android phones. It allows you to connect dots in a specific sequence and this becomes your passcode. In 2015 researchers found that there was predictable patterns in how people utilize this lock option. Researchers found that people were using the dots in the middle and not the remote four corners.

Lastly there is a biometric lock which includes things like fingerprint or facial recognition. This is not a completely secure way of locking a phone as it has been found to be flawed on several levels. Fingerprints capture a certain number of characteristics in your fingerprint and as a result if those main characteristics are all on one fingerprint, it will unlock the phone. Also with facial recognition the have found that high resolution photo's can unlock the phone as well, so the lesson learned is nothing is full proof.
***Combinations of biometric, password or visual locks will work best to keep you device secure.**

Source-Art of Invisability

Watching Identical Twins Fool the iPhone X’s Face ID

Face ID is possibly the iPhones X's make-it-or-break-it feature. Apple is asking previous iPhone owners to put a lot of faith into their home button replacement, and so far, the results seem pretty good. That is until CNN tested the security feature with identical twins.

It's actually pretty hilarious. CNN Tech correspondent Rachel Crane asks one of the identical twins to set up Face ID, then hands the phone over to the other twin who is charged with attempting to unlock it with her face.

Crane clearly expects Face ID to at least put up a little fight here, as per her reaction when the iPhone X immediately unlocks to the second twin's face.

To be fair, this is something Apple has already addressed. In their Sept. event, they said that the iPhone X could be unlocked by an "evil twin," and their support documentation says something along the same lines.

Xbox password flaw exposed by five-year-old boy

A five-year-old boy who worked out a security vulnerability on Microsoft's Xbox Live service has been officially thanked by the company.
Kristoffer Von Hassel, from San Diego, figured out how to log in to his dad's account without the right password.
Microsoft has fixed the flaw, and added Kristoffer to its list of recognised security researchers.

The boy worked out that entering the wrong password into the log-in screen would bring up a second password verification screen.
Kristoffer discovered that if he simply pressed the space bar to fill up the password field, the system would let him in to his dad's account.

Rainbow Table

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password (or credit card numbers, etc) up to a certain length consisting of a limited set of characters.

Dictionary Attack

A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

Brute Force

brute-force attack consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

What should I do if my email has been hacked?

Change Password-reset- Make a stronger password.

Check the sent box to see what was sent in your name. You may notice messages that were sent to your contact list or multiple parties.

Check to see if anyone added anyone to your contact lists or accounts.

Terminology

- Be as familiar with the terminology as possible, this will increase your understanding and Knowledge when identifying potential network vulnerabilities.

Hax0r-Hacker
Uberhacker-good hacker
L33t Sp33k-Replacing Characters to avoid filters
Full Disclosure-Revealing vulnerabilities
Hactivism-Hacking for a cause
Suicide Hacker-Hopes to be caught
Ethical Hacker-Hacks for defensive purposes
Penetration Test-Determine true security risks
Vulnerability Assessment-Basic Idea of security

White Hat-Hacks with permission
Grey Hat-Believes in full disclosure
Black Hat-Hacks without permission

White box-a test everyone knows about
Grey box-a test with a very specific goal/unspecific means
Black box-a test no one knows is happening

Rootkit-Hides process that creates backdoors
Botnet-Robot network
Darknet-Network that does not appear in Search engines.
Buffer Overflow-Hijack the execution steps of a program.
OSSTMM-Open Source Security Testing Methodology Manual.
ISO27001-Implementable Requirements
ISO27002-Guidelines for Security

Also Be Familiar with various ports and whether they are TCP (Secure & Slower) or UDP (Unsecure & Faster)

Emerging Threats

Trust Attacks-This involves social engineering and can be used against executives. This attack involves watching when and how you talk to people. It may involve using voice recognition software.

When people learn your pattern of behavior, they can exploit it as a vulnerability to gain access to network or physical location. It can also involve employees who are getting ready to leave the company who gain or assist in gaining this intelligence. Insider threats can start as non-malicious and turn into malicious attacks.

Phishing

Any attempt to compromise a system and/or steal information by tricking a user into responding to a malicious message. The most common phishing attacks involve emails armed with malware hidden in attachments or links to infected websites, although phishing can be conducted via other methods such as voicemail, text messages, and social media too.

Scammers can take over legitimate email accounts or spoof their email addresses to make it look like messages are coming from someone employees trust. Once a victim is tricked and becomes compromised, the attacker now has their access credentials. They can reach all the same servers, log into the same web applications, and download the same files as if they were that person.

People need to be on the lookout for suspicious emails, some phishing attacks can be extremely targeted and look just like any other email from a trusted source who is being impersonated. The most convincing examples of these “spear phishing attacks” don’t provide any red flags until it’s too late.

Phishing attack jeopardizes patient info at Medical College of Wisconsin

By
Joseph Goedert

Published
November 22 2017, 3:33pm EST

More in
Phishing
Hacking
Data breaches
HIPAA regulations

The Medical College of Wisconsin is in the later stages of resolving issues related to a July hack attack that compromised the protected health information of about 9,500 patients, according to officials at the school.

In July, a small number of faculty and staff members were victimized by spear phishing attacks; in these attacks, a hacker sends emails to individuals under a legitimate employee name and fools one or more recipients into revealing security information about the network.

It has not been publicly announced when the college became aware of the breach; when it did, it immediately disabled affected email accounts, changed passwords, launched an

10 Phishing Examples in 2017 that Targeted Small Business

Aug 29, 2017 by Gabrielle Pickard-Whitehead In Technology Trends

The ‘Shipping Information’ Phishing Scam-phishing scam specifically targeting small businesses. Phishing emails were sent out to more than 3,000 businesses, including the subject line ‘Shipping Information’. The email noted a forthcoming delivery by United Parcel Service (UPS) and included a seemingly innocent package tracking link.

WannaCry exploited a weakness in Microsoft’s operating systems to deliberately infect computers. When the worm was infiltrated, it encrypted the infected operating systems, rendering them unusable. The hackers subsequently demanded a ransom for unlocking the encryption.

Petya ransomware attack hit businesses, preventing victims from accessing their data until they paid $300 in bitcoin. The ransom ware exploited vulnerabilities in Microsoft systems.

Hacking group Shadow Brokers first surfaced in August 2016, but in April this year the group made its most impactful release yet. The attack comprised of a trove of alleged NSA tools, including a Windows exploit known as ExternalBlue.

10 Phishing Examples in 2017 that Targeted Small Business

IRS W2 Tax Season Spear-Phishing Scam- At the beginning of this year's tax season in the United States, a spear-phishing attack circulated. The W-2 Phishing scam involved cyber criminals sending out fake emails. The hackers deliberately made the emails look like they were being sent from corporate executives.

Nigeria-based Business Email Compromise (BEC) attack hit over 50 countries, targeting more than 500 businesses, predominantly industrial companies. The phishing scam prompted recipients to download a malicious file. When the file was downloaded, malware would gain authorized access to business data and networks.

Phishers sent out fraudulent emails invitations on Google docs inviting recipients to edit documents. When the recipients opened the invitations, they were taken to a third-party app, which enabled hackers to access individuals' Gmail accounts.

Amazon Prime Day phishing attack, hackers are sending out seemingly legitimate deals to customers of Amazon. When Amazon's customers attempted to purchase the 'deals', the transaction would not be completed, promoting the retailer's customers to input data that could be compromised and stolen.

A group of cyber-criminals in Eastern Europe sent out emails laden with malware to staff of Chipotle. By clicking on the fake emails, the oblivious staff inadvertently enabled the hackers to compromise the POS systems

Qatar's phishing attacks involved the hackers sending out malicious emails and SMS texts to businesses, designed to compromise valuable information and data.

Just say no to LinkedIn requests from strangers; some may be phishing scams

SAN FRANCISCO – Most of us have done it: eager to build professional leads that might open a door to the next job or sales deal, we've accept that LinkedIn request from an unknown contact.
Wrong move.
A go-to staple for professionals, LinkedIn can pose dangers to unsuspecting users because people have come to have confidence in it and by extension, implicit faith that all accounts on the platform are legitimate. Enter the hackers. Cybersecurity firms say criminals have figured out how to subvert the network by posing as authentic, boring, cubicle-office dwellers.
“It’s got trust built into it, and hackers leverage that trust to their own nefarious purposes,” said Allison Wikoff, a senior researcher with the counter threat unit at SecureWorks, an Atlanta-based security company. Last month hackers stole and posted over three terabytes of files from the music video site Vevo — a breach that began with a single phishing attack through LinkedIn. A group called OurMine claimed responsibility.

Once part of a user's network, a LinkedIn contact can see another's email address (if the user has made that available). He or she has also established a personal connection that makes it more likely the target will open an email that contains malware.

"The most important thing LinkedIn members can do to protect themselves is to only accept requests from people they know or recommended contacts from a trusted connection," said Paul Rockwell, head of LinkedIn's trust and safety unit.

Sometimes attackers are simply trying to harvest email addresses to send spam to.

This Netflix-flavoured phishing attack targets your business emails

A phishing campaign which sees cybercriminals send messages claiming to be from Netflix is targeting business email accounts in an attack which, if successful, could provide hackers with the login credentials required to access corporate services.

While this might seem like a fruitless endeavour at first -- watching TV shows and films isn't exactly a corporate activity -- there's a significant number of people who use their business email addresses to sign up for the consumer services which they use in their free time.

The campaign aims to trick people into giving up log-in information and credit card details. The idea is that if the attackers can trick a victim into giving up their log in details, they're able to snoop around the corporate networks and potentially steal data from any services not locked with two-factor authentication.

There's also the prospect of the attackers cross-referencing a successfully phished corporate account with personal emails and, if the same password is shared across multiple accounts, breaking into those too.

Social Engineering

There are two ways to steal anything — you either take it yourself or you get someone else to give it to you.

Social engineering is any tactics designed to exploit and manipulate trust, so the victim hands the attacker what they want — access to information, accounts, or computers inside a secured area. Think fake customer service calls designed to reset passwords or a criminal spoofing your CEO's email address and asking someone in finance to send an urgent wire transfer.

Everyone — repeat, everyone — can be conned, defrauded, fooled, or manipulated. Being vulnerable can sometimes come down to a lack of training or experience, but more often it can simply come down to distraction and mental fatigue.

The tactics here include surveillance, access to trash (just like LE drug trash picks), access to people through email or phone, gathering information on potential targets (scams on elderly, scams of people's information.

It can also be gathering financial information (last 4 digits of your credit card are commonly on receipts and can be used to compromise accounts when given as verification of ownership)

FOOTPRINTING

This is learning as much information about our potential target as possible through many different Sources of information.

This information can come from Organizational websites, Directories, Email, IP addresses, Access Points. Job sites, LinkedIn, Social Networks. We will look at DNS information and WhoIS information.

Internal-DNS (Scheme), Private Websites (employee directories, portals), Dumpster diving (digging through the trash), Documenting what you may learn from physical location-traffic pattern, how the security is set up, does front desk person leave desk to check on something you have asked and does that leave system vulnerable. You will also watch employee's as to where they may gather and get information direct from them (Hey, do you work for Avis? I was thinking of applying, but unsure if I am skilled enough, what kind of systems do they expect you to know?) Are they accessing email from these locations?

How is the URL laid out, what are they disclosing in the URL and What aren't they disclosing.

Job sites and descriptions of what and who they may be looking for, we need someone who is skilled in Microsoft Windows-This may be a give away as to the operating system that is being used.

Social Networks assist in locating potential connections to target.

There are Laws that address violation of ethics, gaining unauthorized access to any computer system/ networks and related activity.

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- December 5, 2017 – **The SBA 8(a) Certification Program** – CLICK HERE for additional information – presented by Shane Mahaffy, Lead Business Opportunity Specialist, US.Small Business Administration (SBA)
- December 6, 2017 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – CLICK HERE for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)
- December 12, 2017 – **Intellectual Property for Government Contractors and Subcontractors** – CLICK HERE for additional information – presented by Laura J. Grebe, Attorney, Husch Blackwell LLP

UPCOMING EVENTS

Pre-Marketplace Series: Money, Markets and Margins (M3) – Increasing Your Profitability, Networks and Net Worth

November 30, 2017 – Wauwatosa, WI December 6, 2017 – Green Bay, WI

End of Year Federal Contractor Update – January 17, 2018 – Milwaukee, WI

Preparing a Winning Proposal – January 23, 2018 – Milwaukee, WI

Is a GSA Schedule Right for your Business? – February 20, 2018 – Milwaukee, WI

Developing your Marketing Materials for Government Sales – March 13, 2018 – Milwaukee, WI

UPCOMING EVENTS

MARKETPLACE 2017 – Governor's Conference on Minority Business Development **– December 13 – 14, 2017 – Milwaukee, WI**

QUESTIONS?

SURVEY

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

George Chavez | Chavez Consulting, LLC
wigangdet@gmail.com 608-215-7823

Benjamin Blanc, CFCM, CPPS | Government Contract Specialist
Benjaminb@wispro.org 414-270-3600

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226