



CURRENT THREATS & THREATS @ UH

Jodi Ito

Information Security Officer • University of Hawai'i
jodi@hawaii.edu • (808) 956-2400

Information Security Team: infosec@hawaii.edu



National Security

Feds: OPM Breach

Chinese breach data of 4 million federal workers

By **Ellen Nakashima** June 4   [Follow @nakashimae](#)

Hackers working for the Chinese state breached the computer system of the Office of Personnel Management in December, U.S. officials said Thursday, and the agency will notify about 4 million current and former federal employees that their personal data may have been compromised.

<http://preview.tinyurl.com/WP-OPM-breach>



It Gets Worse



Politics



SENATE

Records from government data breach surface on 'darknet,' says expert

By **Malia Zimmerman**

Published June 10, 2015

FoxNews.com

<http://preview.tinyurl.com/FoxNews-OPM-breach>



More than 4M...

As many as 14 million current and former civilian US government employees had their personal information exposed to hackers, according to two people who were briefed on the investigation, representing a far higher figure than the 4 million the Obama administration initially disclosed - and coming amid an apparent second cyber breach that officials said was linked to [China](#).

The newer estimates put the number of compromised records at between 9 million and 14 million going back to the 1980s, said one congressional official and one former US official, who spoke to the Associated Press on condition of anonymity because information disclosed in the confidential briefings includes classified details of the investigation.

There are about 4.2 million federal employees, so the majority of the records exposed relate to former employees. Contractor information also has been stolen, officials said.

<http://preview.tinyurl.com/Guardian-OPM-breach>



IRS "Breach"

IRS system mined for over 100,000 taxpayer records by fraudsters [Updated]

Apparently stolen data from other breaches was used to answer authentication questions.

by Sean Gallagher and Nathan Mattise - May 26, 2015 11:53am HST

Share

Tweet

138

In an official statement issued today, the **IRS announced** that it has shut down an online service to obtain tax records after determining that "unusual activity had taken place on the application, which indicates that unauthorized third parties had access to some accounts on the transcript application." An initial review of that activity revealed "access was gained to more than 100,000 accounts through the Get Transcript application," according to the IRS statement.

After the IRS disclosed more information, it became clear the user data was not obtained because of a direct hack of government systems. Rather, weak authentication used by the IRS to protect access to taxpayer data is likely at fault. The attackers were able to acquire taxpayer records using stolen personal identifying information, possibly pulled from online financial fraud marketplaces.

<http://preview.tinyurl.com/ARSTechnica-IRS>



Anthem Breach

- February 2015
- Potentially 80 million affected

ANTHEM, INC. DATA BREACH

UP TO **80 MILLION** CURRENT & FORMER MEMBERS AT RISK

NO EVIDENCE CREDIT CARDS OR MEDICAL INFORMATION TARGETED

BREAKING OVERNIGHT

CBS THIS MORNING **HEALTH DATA HACKED**
ANTHEM INSURANCE RECORDS STOLEN IN MASSIVE BREACH

ANTHEM, INC. DATA BREACH

INFORMATION ACCESSED:

- SOCIAL SECURITY NUMBERS
- BIRTHDAYS
- ADDRESSES

BREAKING OVERNIGHT

CBS THIS MORNING **HEALTH DATA HACKED**
ANTHEM INSURANCE RECORDS STOLEN IN MASSIVE BREACH



March 2015: 11 million affected

17 **Premera Blue Cross Breach Exposes Financial, Medical Records**

MAR 15



Premera Blue Cross, a major provider of health care services, disclosed today that an intrusion into its network may have resulted in the breach of financial and medical records of 11 million customers. Although Premera isn't saying so just yet, there are indicators that this intrusion is once again the work of state-sponsored espionage groups based in China.

In a statement posted on a Web site set up to share information about the breach — premeraupdate.com — the company said that it learned about the attack on January 29, 2015. Premera said its investigation revealed that the initial attack occurred on May 5, 2014.





May 20, 2015

CareFirst BlueCross BlueShield breached, more than one million individuals notified

Share this article:



CareFirst BlueCross BlueShield is notifying more than one million individuals that their personal information could have been accessed by attackers who gained limited, **unauthorized access** to a single CareFirst database in June 2014.

"Approximately 1.1 million current and former CareFirst members and individuals who do business with CareFirst online who registered to use CareFirst's websites prior to June 20, 2014 are affected by this event," according to an **advisory** posted to the website.



Names, usernames, birth dates, email addresses and subscriber identification numbers could have been acquired.

Monetizing medical data is becoming the next revenue stream for hackers

By [Fred O'Connor](#) | [Follow](#)

IDG News Service | Mar 20, 2015 12:00 PM PT

<http://bit.ly/1ES5gJS>

The personal information found in health care records fetches hefty sums on underground markets, making any company that stores such data a very attractive target for attackers.

“Hackers will go after anyone with health care information,” said John Pescatore, director of emerging security trends at the SANS Institute, adding that in recent years hackers have increasingly set their sights on EHRs (electronic health records).

With medical data, “there’s a bunch of ways you can turn that into cash,” he said. For example, Social Security numbers and mailing addresses can be used to apply for credit cards or get around corporate antifraud measures.

[MORE ON NETWORK WORLD: Free security tools you should try](#)

This could explain why attackers have recently targeted U.S. health insurance providers. On Tuesday, [Premera Blue Cross](#) disclosed that the personal details of 11 million customers had been exposed in a hack that was discovered in January. Last month, [Anthem](#), another health insurance provider, said that 78.8 million customer and employee records were accessed in

RELATED



Hackers compromise 1.8 million medical records from healthcare provider Premera



Health records are the new credit cards

Hackers target health care as industry goes digital

[on IDG Answers](#) →

How to stop a Shady Rat attack on your business?

INSIDER



Six TED Talks that can change your career

Of the hundreds of TED talks available online, many are geared toward helping people view life in a new

[READ NOW](#)

Three unnecessary obstacles holding your company back

On his way to the office, Joe logs in to various work apps to get a head-start on the day. When he arrives at his desk, grande latte in

[Play Video](#)

Say no to no.

[Read More](#)



New Malware

Computerworld Security: March 24, 2015

New malware program PoSeidon targets point-of-sale systems

Retailers beware: A new Trojan program targets point-of-sale (PoS) terminals, stealing payment card data that can then be abused by cybercriminals.

<http://cwonline.computerworld.com/t/9150977/546333388/725444/17/?c1e998ea=Y29tcHV0ZXJ3b3JsZF9zZWV1cmI0eQ%3d%3d&03f17c32=YTM3NzcxYjc1MTAwNmRlZmJmM2NhMGZkNjYxYmU5YTM%3d&x=5cde5ff3>



6/16/2015
06:00 PM



Ericka
Chickowski
News

Connect Directly



New Malware Found Hiding Inside Image Files

Dell SecureWorks CTU researchers say Stegoloader is third example in a year of malware using digital steganography as a detection countermeasure.

Researchers with Dell SecureWorks' Counter Threat Unit (CTU) this week [detailed the kind of Spy-vs.-Spy countermeasures malware authors come up with](#) to evade detection in a new report on a little-known malware family it calls Stegoloader. Targeting organizations in healthcare, education, and manufacturing, Stegoloader uses digital steganography to hide malicious code inside a PNG image file downloaded from a legitimate website.

<http://preview.tinyurl.com/DarkReading-PNG-malware>



New Vulnerabilities

New OpenSSL vulnerability could facilitate DoS attacks

Vulnerability (CVE-2015-0291) rated as high severity by OpenSSL.

By: **Symantec Security Response** SYMANTEC EMPLOYEE

Created 19 Mar 2015

0 Comments | Share

1 Votes



Schneier on Security

- Blog**
- Newsletter
- Books
- Essays
- News
- Events
- Crypto
- About Me

[← Research on Patch Deployment](#)

The Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange

Logjam is a new attack against the Diffie-Hellman key-exchange protocol used in TLS. Basically:

The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection. The attack is reminiscent of the **FREAK attack**, but is due to a flaw in the TLS protocol rather than an implementation vulnerability, and attacks a Diffie-Hellman key exchange rather than an RSA key exchange. The attack affects any server that supports DHE_EXPORT ciphers, and affects all modern web browsers. 8.4% of the Top 1 Million domains were initially vulnerable.

OpenSSL today released patches for a sle
 the severity rating, the announcement will l
 installations before attackers begin to expl
 attackers in a denial-of-service (DoS) attac



ATTACKS

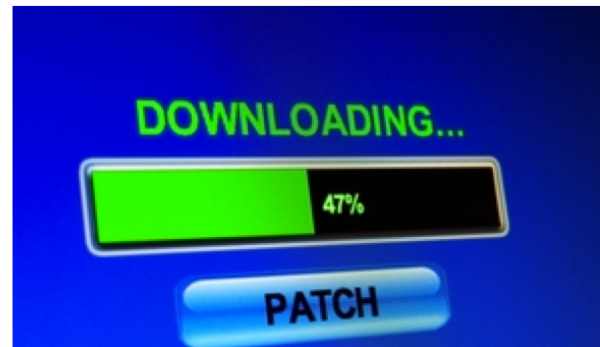
Malware & Vulnerabilities

Malware & vulnerabilities news, trends, analysis and practical advice



NEWS

New malware program PoSeidon targets point-of-sale systems



NEWS

New attacks suggest timeline for patching Flash Player is shrinking



NEWS

All four major browsers hacked at Pwn2Own

Security researchers at this week's Pwn2Own hacking contest demonstrated remote code execution exploits against the top four browsers and hacked the widely used Adobe Reader and

Flash Player plug-ins.

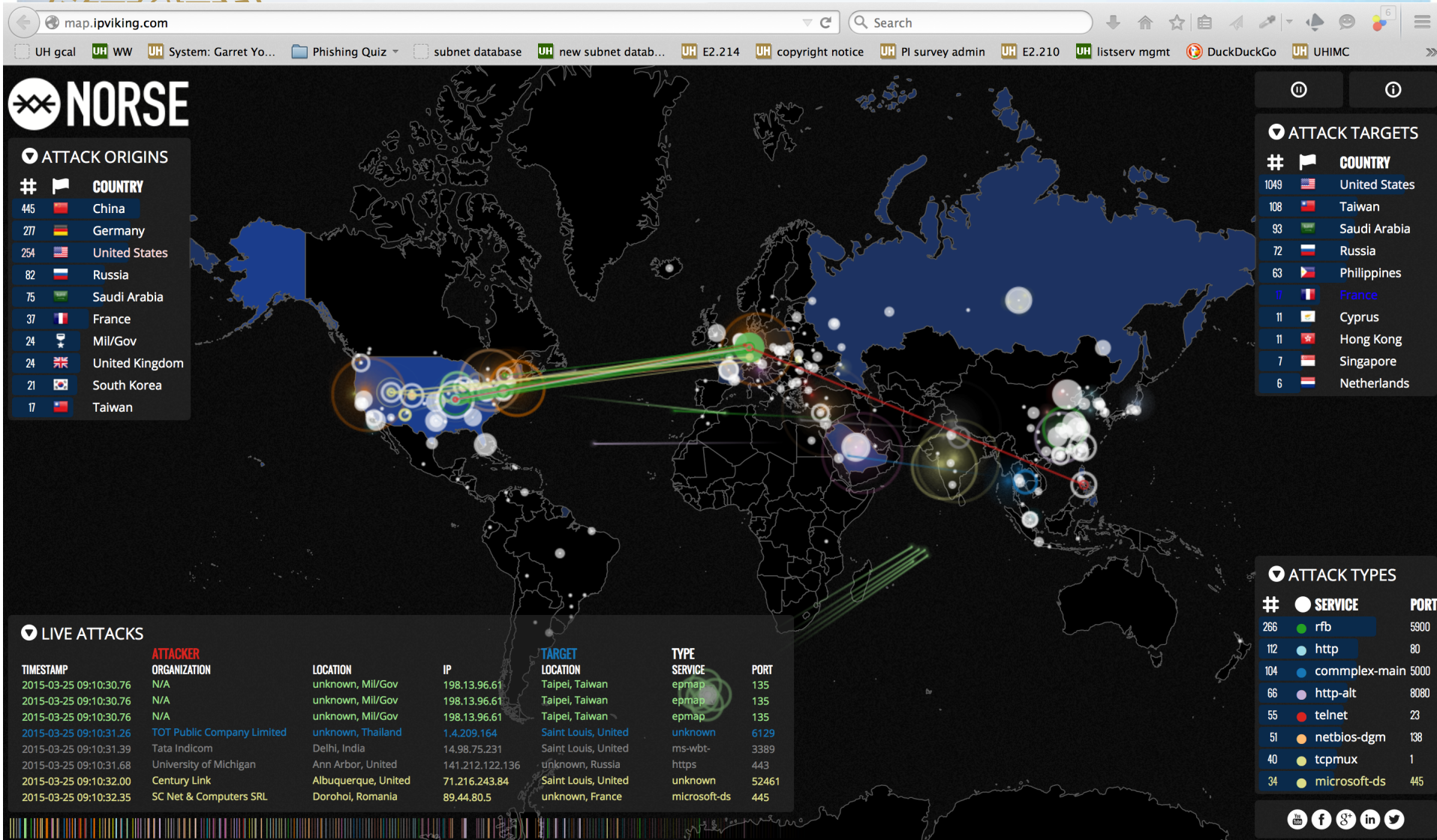
NEWS

At least 700K routers given to customers by ISPs can be hacked

More than 700,000 ADSL routers provided by ISPs to customers have serious flaws that allow remote hackers to take control of them.



LIVE ATTACKS



<http://map.ipviking.com>

Universities Face a Rising Barrage of Cyberattacks

By RICHARD PÉREZ-PEÑA

Published: July 16, 2013 |  325 Comments

America's research universities, among the most open and robust centers of information exchange in the world, are increasingly coming under cyberattack, most of it thought to be from [China](#), with millions of hacking attempts weekly. Campuses are being forced to tighten security, constrict their culture of openness and try to determine what has been stolen.

 [Enlarge This Image](#)



Jeff Miller

A storage server at the University of Wisconsin.


 [Enlarge This Image](#)


University officials concede that some of the hacking attempts have succeeded. But they have declined to reveal specifics, other than those involving the theft of personal data like [Social Security](#) numbers. They acknowledge that they often do not learn of break-ins until much later, if ever, and that even after discovering the breaches they may not be able to tell what was taken.


 FACEBOOK

 TWITTER

 GOOGLE+

 SAVE

 EMAIL

 SHARE

 PRINT

 REPRINTS





TECHNOLOGY

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING

Hackers target colleges to steal personal data, university research

Cadie Thompson | @CadieThompson

Thursday, 21 Aug 2014 | 8:56 AM ET



Thomas Samson | AFP | Getty Images



College of Engineering network disabled in response to sophisticated cyberattack

Plans in place to allow teaching, research in the college to continue as University moves to recover

May 15, 2015

UNIVERSITY PARK, Pa. – The Penn State College of Engineering has been the target of two sophisticated cyberattacks conducted by so-called “advanced persistent threat” actors, University officials announced today. The FireEye cybersecurity forensic unit [Mandiant](#), which was hired by Penn State after the breach was discovered, has confirmed that at least one of the two attacks was carried out by a threat actor based in China, using advanced malware to attack systems in the college.

SHARE THIS STORY



RELATED CONTENT

[Internal search opens fo](#)



OMG!!

Cyber Security is MAINSTREAM!

**CSI:
CYBER**

Wednesdays 10/9c

#CSICyber



Episode Preview

Watch Preview: "Fire Code"





IoT: INTERNET OF THINGS





IoT: Internet of Things

Self-Driving Car Test: Steve Mahan g+1 438



<http://www.google.com/about/careers/lifeatgoogle/self-driving-car-test-steve-mahan.html>



<http://www.cbsnews.com/news/car-hacked-on-60-minutes/>

CAR HACKED ON 60 MINUTES

No real security on the Internet -- even the military is under daily assault - says the man the Defense Department hired to make the web more secure

2015

FEB 06

COMMENTS

6

FACEBOOK

1.5K

TWITTER

784

STUMBLE



MORE



Even the mightiest military in the world can be vulnerable on the Internet, just like everybody else who uses it. But the government agency that invented the Internet has a brilliant videogame inventor on its side working to make the web safer for all users, starting with the military. Lesley Stahl reports on the U.S. military's Defense Advanced Research Projects Agency (DARPA) and the man who heads its Information Innovation Office, Dan Kaufman, for a 60 Minutes story to be broadcast Sunday, Feb. 8 at 7 p.m. ET/PT.



He's referring to the "Internet of Things," as it's called, where billions of devices - from home appliances to medical equipment to entire urban traffic light grids - are connected online. The Internet of Things is the current consumer electronics buzzword. But it's those devices, says Kaufman, that are the Internet's latest and greatest Achilles Heel; they are gateways for hackers to attack. "Today, all the devices that are on the Internet - the 'Internet of Things' - are fundamentally insecure. There is no real security going on," says Kaufman.

One of the vulnerabilities Kaufman and DARPA are working to eliminate that affects many is in the automobile. Cars today are loaded with computers networked to each other, and those can be hacked remotely. In a dramatic demonstration, he and his colleagues use a laptop computer to hack into a car being driven by Stahl. Much to her surprise, they were able to take control of many of the car's functions, including the braking and acceleration.



Your TV may be watching you

By Bruce Schneier

Updated 9:16 AM ET, Thu February 12, 2015



AdChoices



(CNN)—Earlier this week, [we learned that Samsung televisions are eavesdropping on their owners](#). If you have one of their Internet-connected smart TVs, you can turn on a voice command feature that saves you the trouble of finding the remote, pushing buttons and scrolling through menus. But making that feature work requires the television to listen to everything you say. And what you say isn't just processed by the television; it [may be forwarded over the Internet](#) for remote processing. [It's literally Orwellian.](#)

This discovery surprised people, but it shouldn't have. The things around us are increasingly computerized, and increasingly connected to the Internet. And most of them are listening.

<http://go.hawaii.edu/al>

Mo



ISIS
airbe





Andy Greenberg
Forbes Staff

FOLLOW

Covering the worlds of data security, privacy and hacker culture.

[full bio](#) →



140
COMMENTS

43 CALLED-OUT

[+ Follow Comments](#)

FORBES 7/24/2013 @ 9:00AM | 522,769 views

Hackers Reveal Nasty New Car Attacks-- With Me Behind The Wheel (Video)

This story appears in the August 12, 2013 issue of Forbes.

[+ Comment Now](#) [+ Follow Comments](#)



Charlie Miller (left) and Chris Valasek behind their Prius' dismantled dashboard. Credit: Travis Collins

Stomping on the brakes of a 3,500-pound Ford Escape that refuses to stop—or even slow down—produces a unique feeling of anxiety. In this case it also produces a deep groaning sound, like an angry water buffalo bellowing somewhere under the SUV’s chassis. The more I pound the pedal, the louder the groan gets—along with the delighted cackling of the two hackers sitting behind me in the backseat.

<http://go.hawaii.edu/La>



HOW SMART HOMES GET HACKED

Smart TV. Tablet. Printer. Storage. You have the perfect living room set up, but is it setting you up for a cybercriminal attack?



Smart Devices

With no encryption, your smart TV can be used to intercept onscreen payments, access files and discover other vulnerabilities.

Network Attached Storages

Storage devices have weak default passwords. Once attackers get in, they can inject malware and infect other devices.

Internet Router

Hidden functions let your ISP access everything from your laptop to your webcam. What would happen if a cybercriminal took over?

Every Connection Counts

Remember, every connected device can be used as a stepping-stone for an attack.

HOME SAFE HOME

Follow these tips to keep your connected devices secure:

1

Get the latest software updates for every device.

2

Change weak default username and passwords.

3

Encrypt files on a private network to restrict access.





Mobile Devices





"Today, your cell phone has more computer power than all of NASA back in 1969, when it placed two astronauts on the moon."

Dr. Michio Kaku





Cell Phone Risks

<http://msisac.cisecurity.org/newsletters/2013-02.cfm>

- Common Risks
 - Loss of Device and Information Theft
 - Social Engineering
 - TMI (Too Much Information)
 - Public Wi-Fi
 - Bluetooth & Near Field Communications (NFC)
- Increasing Risks
 - Malware





Cell Phone Safety

- Update Operating System
- Use Security Software (if available)
- Use a Password
- Be Careful Before:
 - Downloading/Installing Apps
 - Click on any links
- Use Encryption
- Know Terms of Use/Service
- Securely Erase Information Before Disposal



Ice Age available on Google Play. © 2012 FOX.
All Rights Reserved. Rated PG



Cell Phone Resources

- 14 Ways to Find a Stolen or Lost iPhone:
<http://ipod.about.com/od/iphonetroubleshooting/tp/14-Ways-To-Find-A-Lost-Or-Stolen-Iphone.htm>
- How to Dispose Your Mobile Device Securely:
<http://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>
- Cyber Threats to Mobile Phones:
http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf
- Android Tool:
<http://www.sophos.com/androidsecurity>
- Secure Your Smartphone:
<http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx>





Human Impact



- Phishing & Spear Phishing
- Lack of Awareness & Understanding
- Mistakes
- Insider Threat
- Security is only as strong as the weakest link





Attacks by Nation States





CYBERSECURITY

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING | CY

FBI details North Korean attack on Sony

<http://www.cnn.com/id/102319817>

Kara Scannell

Thursday, 8 Jan 2015 | 12:55 AM ET

FINANCIAL TIMES



Kevork Djansezian | Reuters

A ticket and a poster of the film "The Interview" at the Christmas Day screening of "The Interview" in the Van Nuys section of Los Angeles, California December 25, 2014.

The director of the Federal Bureau of Investigation has offered fresh details of the cyber attack on Sony Pictures as he defended the US claim that North Korea was responsible.



SCIENCE & TECHNOLOGY

China's 'Code War' attacks on US internet titans

Online security researchers say Beijing has launched major cyber strikes against American IT giants eyeing its market.

[Kevin Holden](#) | 14 Feb 2015 23:48 GMT | [Science & Technology](#), [Asia](#), [China](#), [United States](#), [Xi Jinping](#)

 1605  931  0 

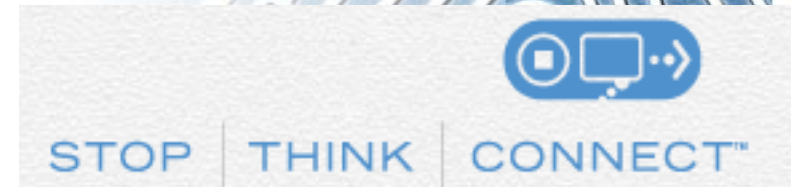


101011101010011010



Cyber Security is National Concern

- Department of Homeland Security (DHS)
 - <http://www.dhs.gov/topic/cybersecurity>
 - <http://stophinkconnect.org/>
- Multi-State Information Sharing & Analysis Center (MS-ISAC)
<http://msisac.cisecurity.org/>
- United States Computer Emergency Readiness Team (US-CERT)
<http://www.us-cert.gov/cas/tips/>



Homeland Security

Home

Topics

How Do I?

Get Involved

News

About DHS



Why?

- Technology is deeply embedded into Critical Infrastructures
- Technology touches every facet of our lives
- Vulnerable
 - Losing access to services
 - Losing personal data
 - Financial losses



[about Target](#) | [careers](#) | [corporate responsibility](#) | [investors](#) | [press](#)

[home](#) / [about](#) / [shopping experience](#) / [payment card issue FAQ](#)

data breach FAQ

Answers to commonly asked questions for guests impacted by the recent data breach.

A message to our guests

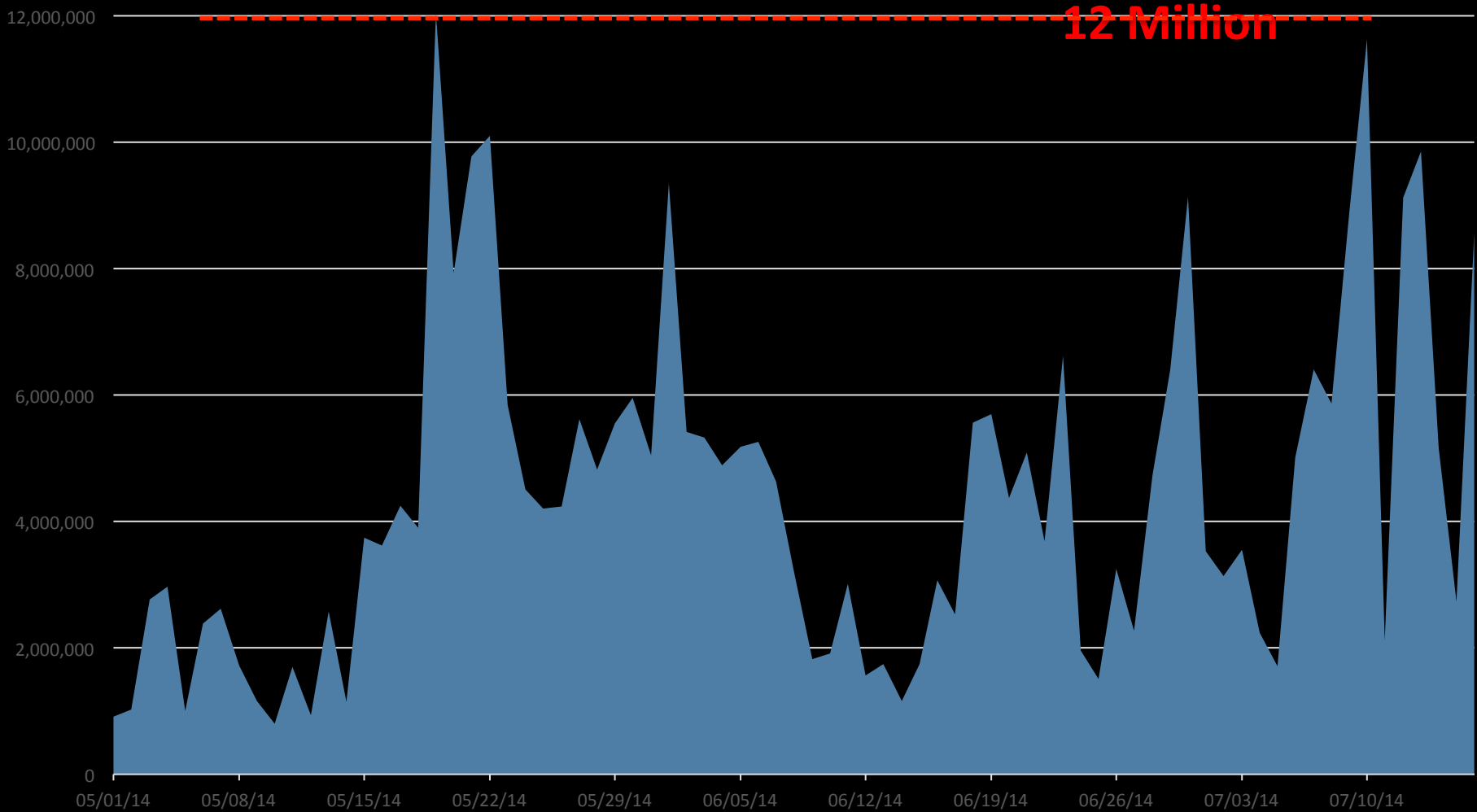
We truly value our relationship with you, our guests, and know this incident had a significant impact on you. We are sorry. We remain focused on addressing your questions and concerns.

- You have zero liability for any charges that you didn't make.
- No action is required by you unless you see charges you didn't make.
- Be wary of call or email scams that may appear to offer protection but are really trying to get personal information from you.



Magnitude of Attacks

Number of Attacks Per Day





Attacks by Cyber Criminals



WORLD

Bank Hackers Steal Millions via Malware

By DAVID E. SANGER and NICOLE PERLROTH FEB. 14, 2015



The bank's internal computers, used by employees who process daily transfers and conduct bookkeeping, had been penetrated by malware that allowed cybercriminals to record their every move. The malicious software lurked for months, sending back video feeds and images that told a criminal group — including Russians, Chinese and Europeans — how the bank conducted its daily routines, according to the investigators.

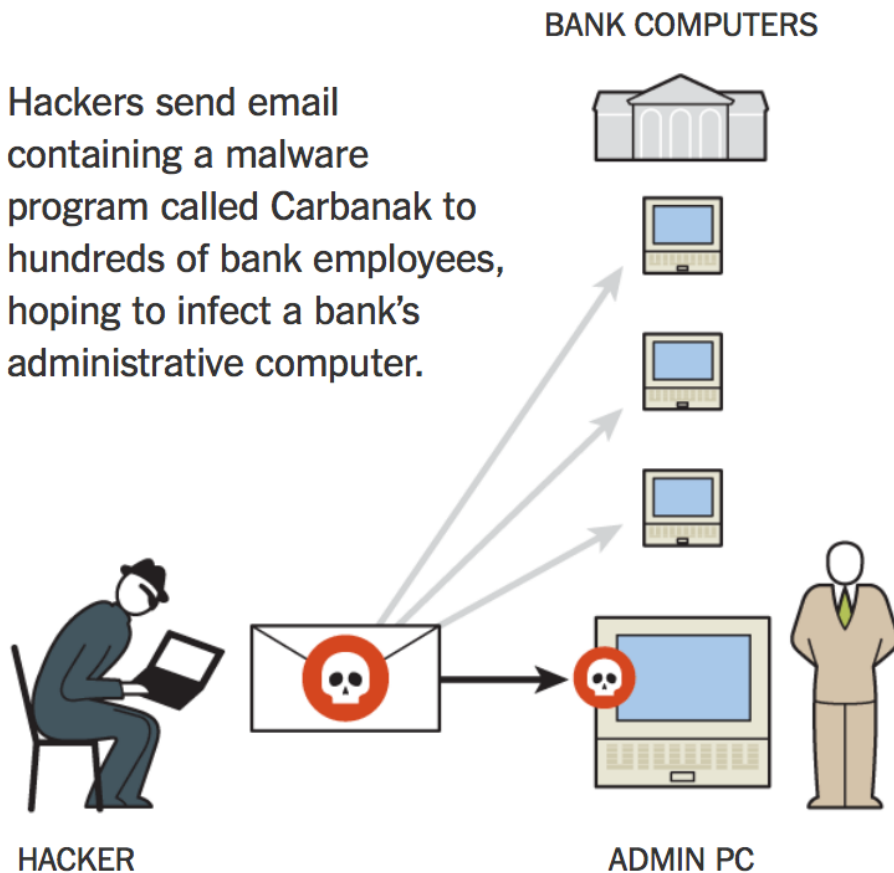
"The goal was to mimic their activities," said Sergey Golovanov of Kaspersky, about how the thieves targeted bank employees. Raphael Satter/Associated Press



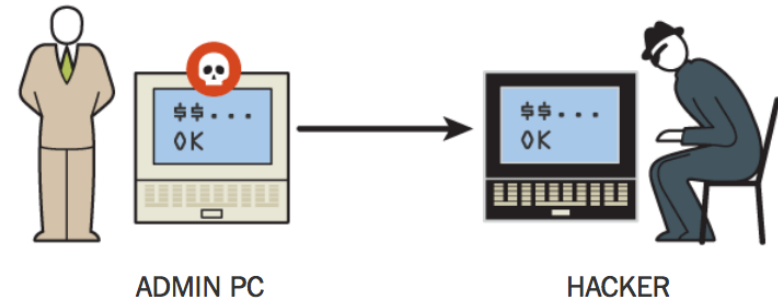
How Hackers Infiltrated Banks

Since late 2013, an unknown group of hackers has reportedly stolen \$300 million — possibly as much as triple that amount — from banks across the world, with the majority of the victims in Russia. The attacks continue, all using roughly the same modus operandi:

Hackers send email containing a malware program called Carbanak to hundreds of bank employees, hoping to infect a bank's administrative computer.



Programs installed by the malware record keystrokes and take screen shots of the bank's computers, so that hackers can learn bank procedures. They also enable hackers to control the banks' computers remotely.



By mimicking the bank procedures they have learned, hackers direct the banks' computers to steal money in a variety of ways:

Transferring money into hackers' fraudulent bank accounts

Using e-payment systems to send money to fraudulent accounts overseas

Directing A.T.M.s to dispense money at set times and locations

Cyber-Safe

Insurance giant Anthem hit by massive data breach



By Charles Riley @CRileyC

Hackers have stolen information on tens of millions of Anthem Inc. customers, in a massive data breach that ranks among the largest in corporate history.

The information stolen from the insurance giant includes names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.

Sponsored Links

Visa® Black Card™
The Stainless Steel Card Gets You
Luxury Without Limits. Apply Today!

▶ Anthem said there is no evidence that credit card or medical information was compromised. While damage is still being assessed, the compromised database contained up to 80 million customer records.

Sell Your Car Online

... on the bir
... zone exit as
... alks collapse

... aire boom:
... the money

... viewers thin
... Williams
... res a shot at
... ption



So



Cybercrime Remains Growth Industry With \$445 Billion Lost

Don't Miss Out —

Follow us on:



by
Chris Strohm

June 9 (Bloomberg) -- Cybercrime remains a growth industry.

3:57 AM GMT+10
June 9, 2014

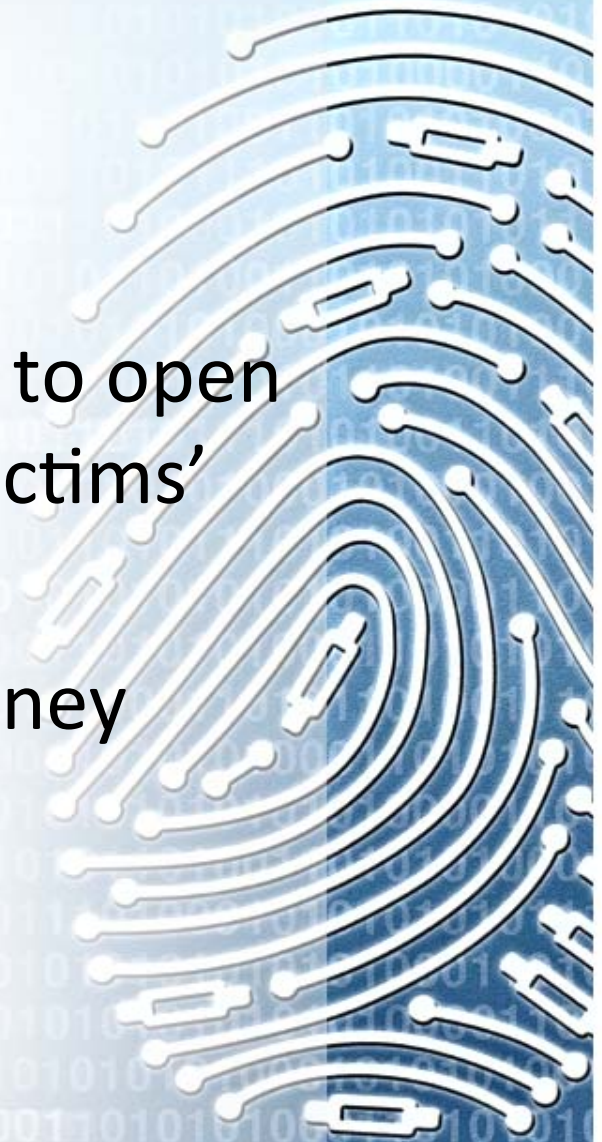


That's the main message from former U.S. intelligence officials, who in a report today outlined scenarios for how \$445 billion a year in trade theft due to computer hackers will worsen. They warned that financial companies, retailers and energy companies are at risk from thieves who are becoming more sophisticated at pilfering data from their servers.



Identity Theft & Financial Fraud

- Use stolen personal information to open credit accounts or loans in the victims' name
- Steal financial information & money





CryptoWall is a million-dollar business.

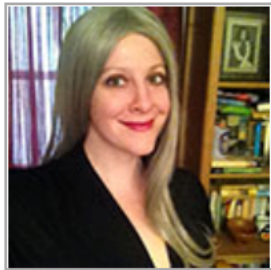
The **file-encrypting ransomware** has netted the criminal gang responsible for its development and dispersal, more than \$1.1 million in the six months it's been in the wild, researchers at Dell SecureWorks' Counter Threat Unit said in a **report** this week.



CRYPTOWALL'S HAUL: \$1M IN SIX MONTHS

<http://threatpost.com/cryptowalls-haul-1m-in-six-months/107978>

6/9/2015
06:01 AM



Sara Peters
News

Connect Directly



1 COMMENT
[COMMENT NOW](#)

Cybercrime Can Give Attackers 1,425% Return on Investment

Going rates on the black market show ransomware and carding attack campaign managers have plenty to gain.

While security professionals often find it difficult to prove return on investment, a standard ransomware campaign could earn an attacker a 1,425 percent ROI, according to a [report released today by Trustwave](#).

<http://preview.tinyurl.com/DarkReading-ROI>



TRENDS

 THE VICTIM	It could be you. All sizes of business and all industries are at risk of some kind of security event. Even if you think your organization is at low risk of external attacks, there remains the possibility of insider misuse and errors that harm systems and expose data.
 THE CULPRIT	Most attacks are perpetrated by external actors, as opposed to employees and partners. Financially motivated criminal gangs are still the dominant type of perpetrator in external attacks — although espionage appears increasingly often in our data set. Despite all the emphasis on “hacktivism” in the press, ideology-driven attacks remain a very small percentage of the total.
 THE TARGET	Attackers are mainly going for payment and bank data, which they can quickly convert into cash. User credentials are also a popular target, but mainly as a gateway to other kinds of data or other systems. Reflecting the rise in espionage attacks is a growth in theft of secrets and internal data.
 THE ATTACK	Hacking and malware are the most popular attack methods. Servers and user devices (such as PCs) are the main targets. Physical tampering attacks are becoming less common, but social attacks have grown in recent years.
 THE CHASE	Attackers have got faster at breaching systems. Defenders are getting faster too — but they’re falling further behind. Many successful breaches are detected by third parties, such as law enforcement agencies, specialist fraud detection organizations, or even customers.



Primary Attack Motivations

- Cyber Crime
- Cyber Espionage
- Cyber Warfare
- Hacktivism
- Script Kiddies





Primary Attack Modalities

- Malware
 - Viruses & Worms, Trojans, Keystroke Loggers, Botnets, etc.
- Phishing
- Distributed Denial of Service (DDoS)
- Web Defacement
- Brute Force Attacks & Account Hijacking
- SQL injection
- Vulnerability exploits including zero-day exploits





UH State of Security

- Many “security incidents”
- Many compromised systems; possible “pivot attacks”
- Unable to secure entire network
- Unable to restrict devices





PHISHING STATS





Phishing Trends

- Previously, UH heavily targeted at the start of each semester
- Fall 2014: 83 unique phishing campaigns in August and September
- Aug-Sept 2014: 178 compromised accounts
- Total 2014: 180 unique phishing campaigns
- Total 2014: 325 compromised accounts
- Jan-May 2015: 304 unique phishing campaigns
- Jan-May 2015: 1051 compromised accounts



Phisher's Method of Operation



On average,
7 days pass
between account
compromise and use



Phisher sends 20
emails per hacked
account in less
than 4 minutes



Each phishing
email sent will
often have a
different URL



Each email is bcc'd
to ~50 recipients in
alphabetical order
(~1K total per run)



Phisher then
deletes the
emails from the
"Sent" folder

www.hawaii.edu/infosec/ncsam



Cybercriminals craft legitimate-looking email to trick you into divulging your personal information. To keep yourself from becoming a victim, remember to **“SEAR the Phish”**.

Stop

Don't panic and don't be too quick to click on email links even if the message looks urgent and threatening.

Examine

Look at the email closely. Does the message look suspicious, does the link look unusual, does the request make sense?

Ask

Question the sender (if you know him/her personally). Check with the ITS Help Desk (help@hawaii.edu) to determine if the email is legitimate or not.

Report

Notify ITS if you receive any UH-related phishing emails by forwarding it to phishing@hawaii.edu

Signs of a Phishing Email

- *Makes the recipient believe that their email account has been compromised or will be suspended.*
- *Threatens the recipient and conveys a sense of urgency with the need to respond.*
- *The URL of the phishing link is suspicious and the domain name does not look legitimate.*



ATTACK METRICS

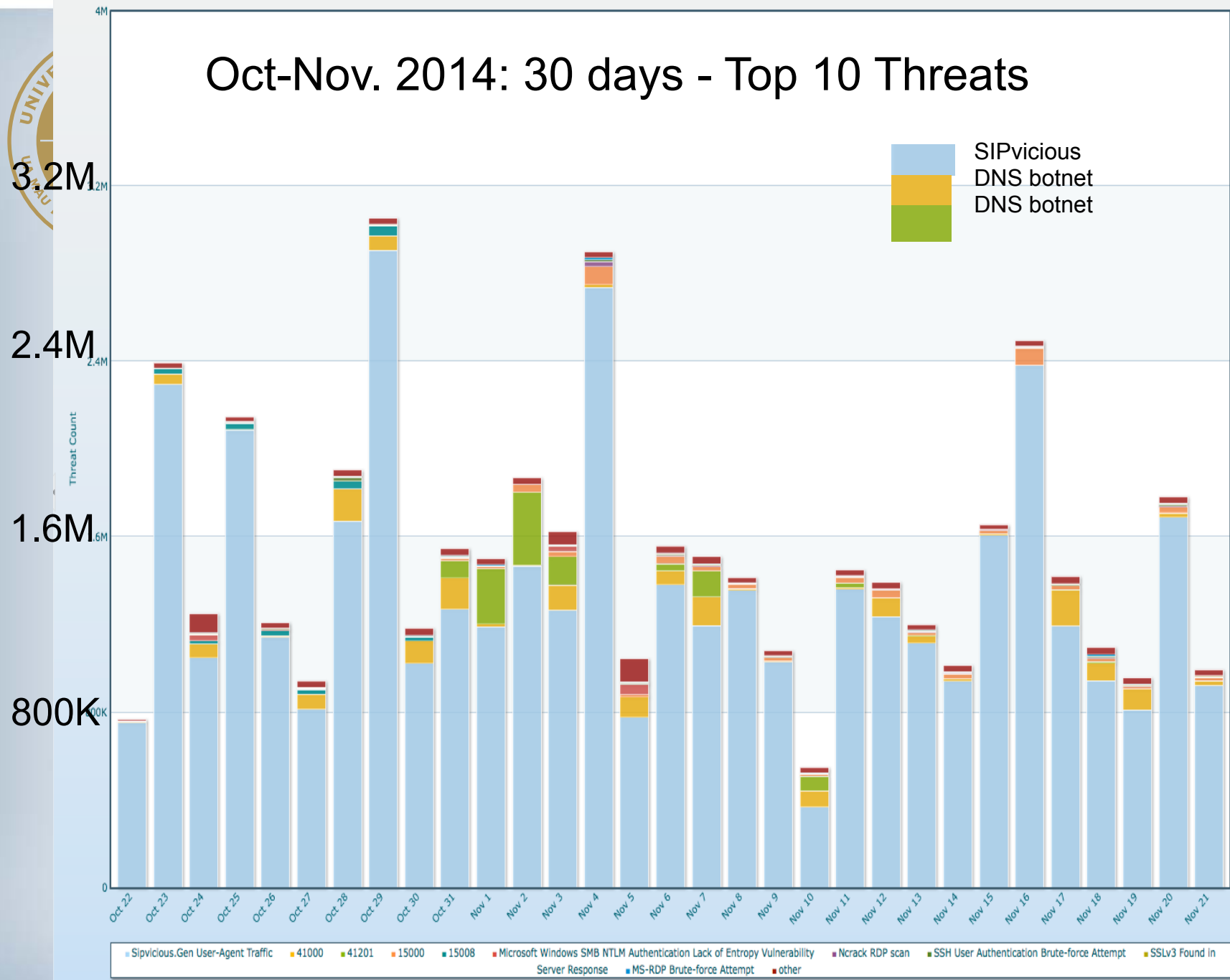




Attacks Per Day



Oct-Nov. 2014: 30 days - Top 10 Threats





NOTABLE SECURITY INCIDENTS





Chronological List

- Apr 2014 – Web server compromised and backdoor installed on server; identified as APT
- May 2014 – Heartbleed exploit could have resulted in compromises; 38 hosts identified as vulnerable (NMAP scan)
- Jun 2014 – 13 web servers compromised via SQL injection
- Jun 2014 – Web server compromised with numerous backdoors



July-Aug

- Jul 2014 – Video server compromised twice in less than a month
- Jul 2014 – Perl script contained 0-day vuln could have resulted in compromises
- Aug 2014 – Server infection with backdoor





September-October

- Sep 2014 – Backup server contained passwords for servers/database
- Sep 2014 – Web server compromised with numerous backdoors
- Oct 2014 – 3 compromised web servers; exploited via Drupal 7 vulnerability



Ongoing Attacks & Threats

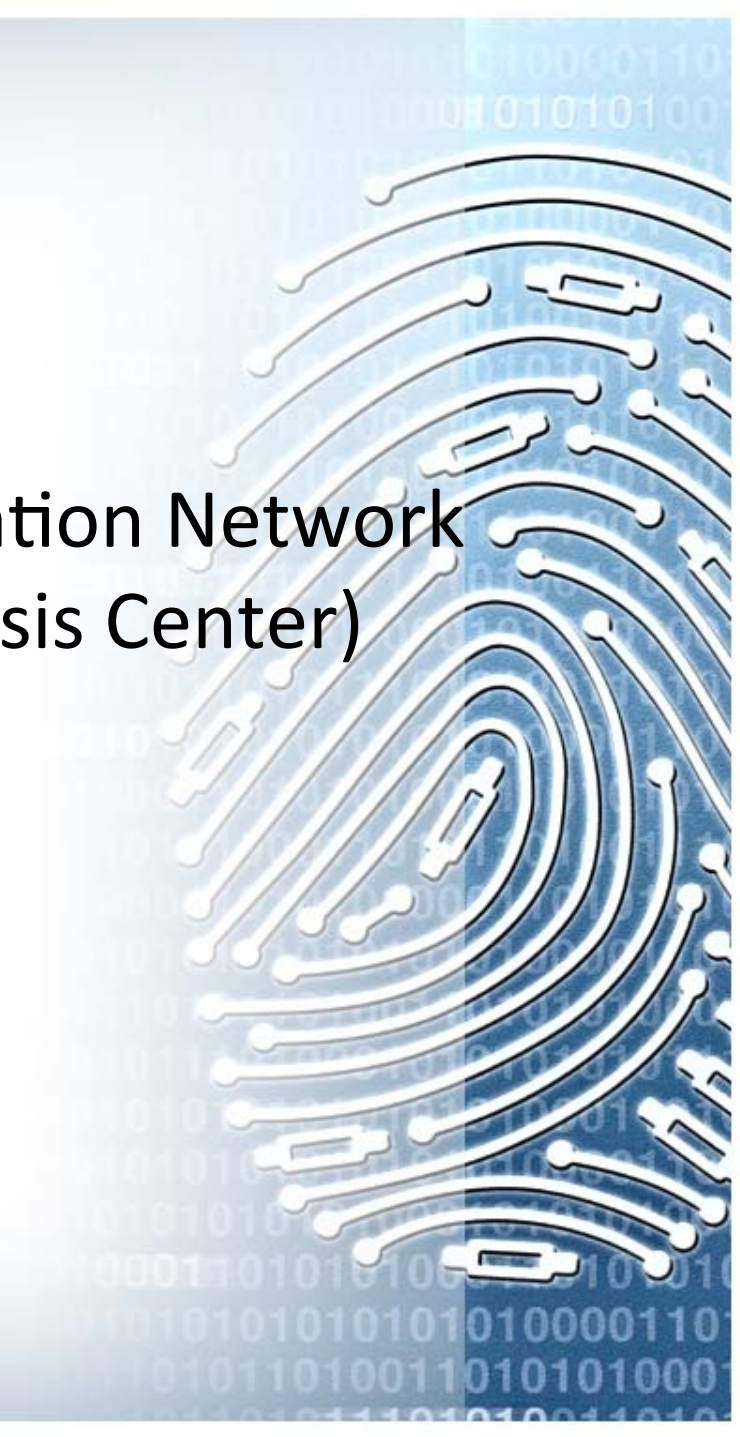
- Ransomware: 7 known infections; Koler ransomware via SMS on Android phones
- Printer spam; compromised printers
- NullCrew targeting universities
- Brute-Force logins
- SSH attacks
- Phishing & compromised accounts





Alerts

- REN-ISAC (Research & Education Network Information Sharing & Analysis Center)
- MS-ISAC (Multi-State ISAC)
- US-CERT
- Other vetted sources





Sharing Restrictions

TLP | TRAFFIC LIGHT PROTOCOL

When should it be used?

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.

Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.

Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Color



Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.



Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.



Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.



TLP: WHITE information may be distributed without restriction, subject to copyright controls.



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM



Recent Vulnerabilities

Notes by Date Updated

Updated	ID	Title
19 May 2015	VU#177092	KCodes NetUSB kernel driver is vulnerable to buffer overflow
15 May 2015	VU#550620	Multicast DNS (mDNS) implementations may respond to unicast querie...
11 May 2015	VU#264212	Recursive DNS resolver implementations may follow referrals infinitely
08 May 2015	VU#110532	Subrion CMS vulnerable to SQL injection by an authenticated user
07 May 2015	VU#260780	NetNanny uses a shared private key and root CA
07 May 2015	VU#602540	ICU Project ICU4C library contains multiple overflow vulnerabilities
05 May 2015	VU#978652	Bomgar Remote Support Portal deserializes untrusted data
30 Apr 2015	VU#581276	EMC AutoStart is vulnerable to remote code execution via specially craf...
28 Apr 2015	VU#534407	Barracuda Web Filter insecurely performs SSL inspection
17 Apr 2015	VU#672268	Microsoft Windows NTLM automatically authenticates via SMB when fo...

« First

Previous

Displaying results 1 - 10 of 3196

Next

Last »



Time to Remediate

- Average: 5 days between patch announcement and release of exploit;
- And Δ is decreasing
- Drupal7 vuln: only 7 hours



Largest Potential for Compromise

- Web Servers
 - “anyone” can do it.....
 - “everyone” wants one.....
 - Unmanaged and not maintained
 - Poor/insecure coding practices
 - Forgotten applications/plugin/data/databases
 - Content Management Systems not patched/maintained (WordPress, Drupal, Joomla, etc.)
 - Plug-ins not patched/maintained





US-CERT Enterprise Recommended Mitigations

- **Application directory whitelisting** – helps prevent malicious software and unapproved programs from running
- **Patch applications** – e.g., Java, PDF viewers, Flash, web browsers, Microsoft Office
- **Patch operating system vulnerabilities**
- **Restrict administrative privileges** – based on user roles & responsibilities
- **Network segmentation and segregation into security zones** – helps protect sensitive information & critical services



Top 10 Personal Safe Computing Habits

- Recognize that **YOU** are a target; know the threats
- Apply operating system and application updates frequently and regularly
- Install and update protective software such as anti-virus software
- Practice good password management
- Never leave your devices unattended and control access to your machines



5 more...

- Use email & the Internet safely; be careful when clicking on attachments or links in email
- Use a secure network for sensitive transactions
- Back up your data regularly and protect sensitive information
- Monitor your accounts for suspicious activity
- Be careful what you share on social media





Protecting Sensitive Institutional Assets

- Risk-based Approach
 - IDENTIFY critical assets
- Top Concerns:
 - BREACHES
 - COMPLIANCE
- Use/Handling of Sensitive data
- Vulnerable Servers/Services
- End User Awareness & Education





UH Information Security Program

- www.hawaii.edu/infosec
- Data Governance and Oversight
- Information Security Audits & Risk Assessments
- Information Security Policies & Procedures
- Identity Management & Access Controls
- Information Security Training and Awareness





Data Governance @ UH

- Framework to effectively manage data
- Be able to understand how Sensitive Data is used
- Be able to protect Sensitive Data
- Eliminate unnecessary use & repositories of Sensitive Data
- Establish Data Classification Categories
- www.hawaii.edu/uhdtagov



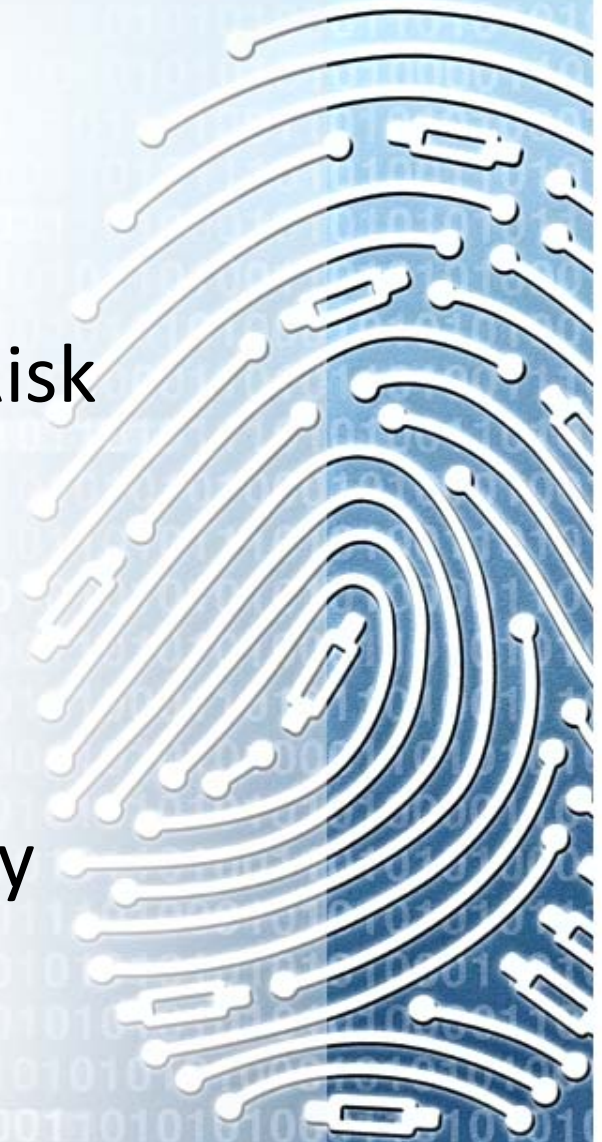
Data Classification Categories

- Public: Access is not restricted and is subject to open records requests
- Restricted: Used for internal UH business only
- Sensitive: Data has privacy considerations or has been classified as confidential and subject to protection from public access
- Regulated: inadvertent disclosure or inappropriate access requires a breach notification in accordance with Hawai'i Revised Statutes §487N or is subject to financial fines.



Audits & Risk Assessments

- Internal Audit – Survey of High Risk Areas:
 - Financial Aid
 - HIPAA (Health Insurance Portability & Accountability Act)
- Server & PII Risk & Accountability





Server & PII Registrations

- Servers & Repositories of sensitive information must be updated annually
- Process begins in September
- Currently, two separate processes
- Servers must be scanned for vulnerabilities and PII
- All repositories (paper & electronic) of sensitive information must be reported



Server Stats

- 2014 Registered Servers: 832
- 2014 Unregistered Servers: 1640
- Data Security Leadership Council Rep (or designee) must vet existence of server
- Total Printers: 1821
- (external reports of hacked printers)
- Will start blocking unregistered servers



2015: Server & PII Reports

- Will be sent out first week of August
- Completion date is end of September
- Please start updating before notification are sent out
- If update not completed, server will be taken off the network



Policies & Procedures

- www.hawaii.edu/infosec/policies.html
- Updating E2.210, E2.214
- New Policies: HIPAA, PCI
- Mandatory Information Security Awareness Training
- www.hawaii.edu/its/acer



IAM & Awareness

- Centralize authentication using ITS-supported CAS
- Prototyping use of DUO (multi-factor)
- Focused training
 - By functional groups/roles
 - Phishing!!
 - <http://www.hawaii.edu/infosec/phishing/>





Current & Near Future

- Notifying units about reported compromised systems
- ITS will be more proactive and begin blocking compromised systems
- Implementing multi-factor authentication





Jodi Ito • UH Information Security Officer
jodi@hawaii.edu • (808) 956-2400