CSE508 Network Security

Stony Brook University

2021-02-04

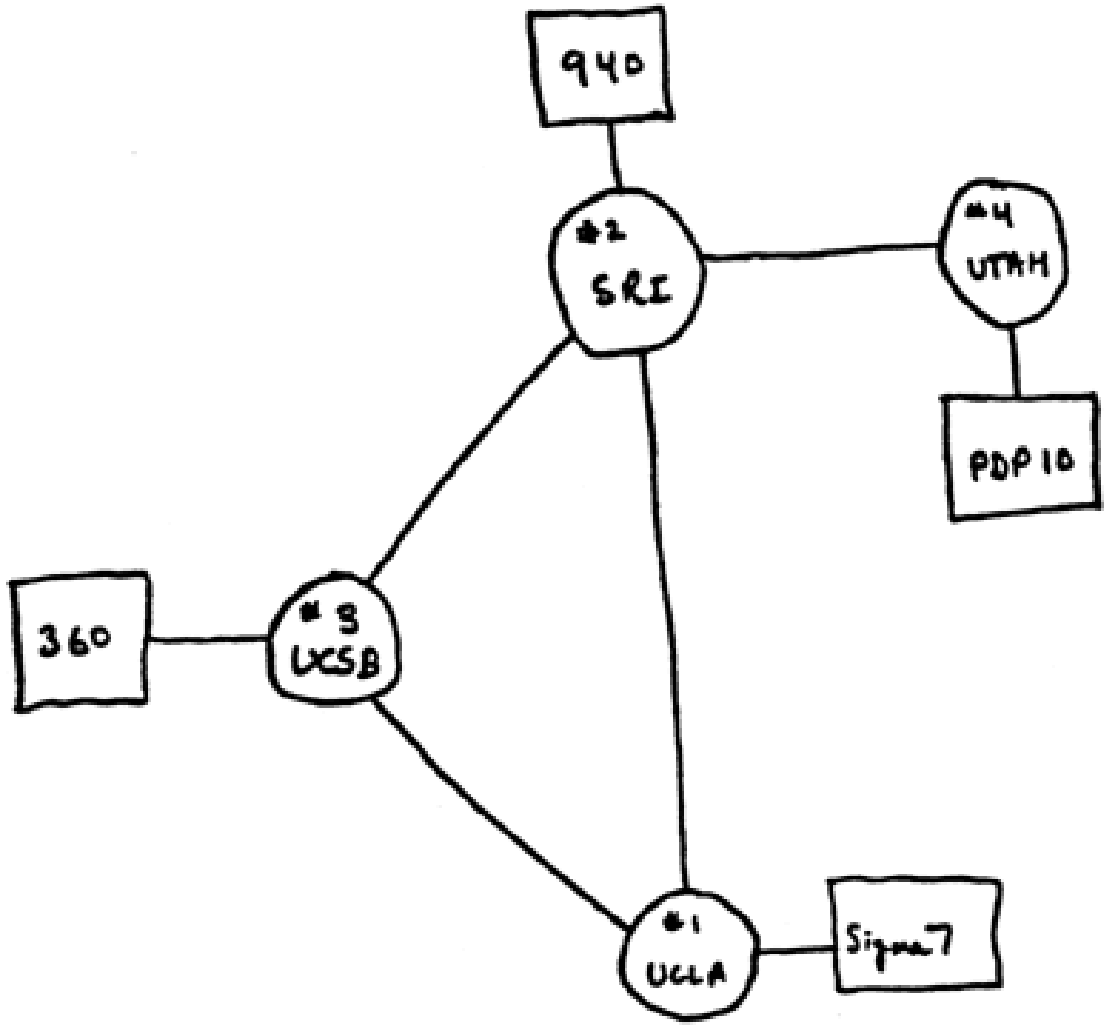
Introduction and Basic Concepts

Michalis Polychronakis

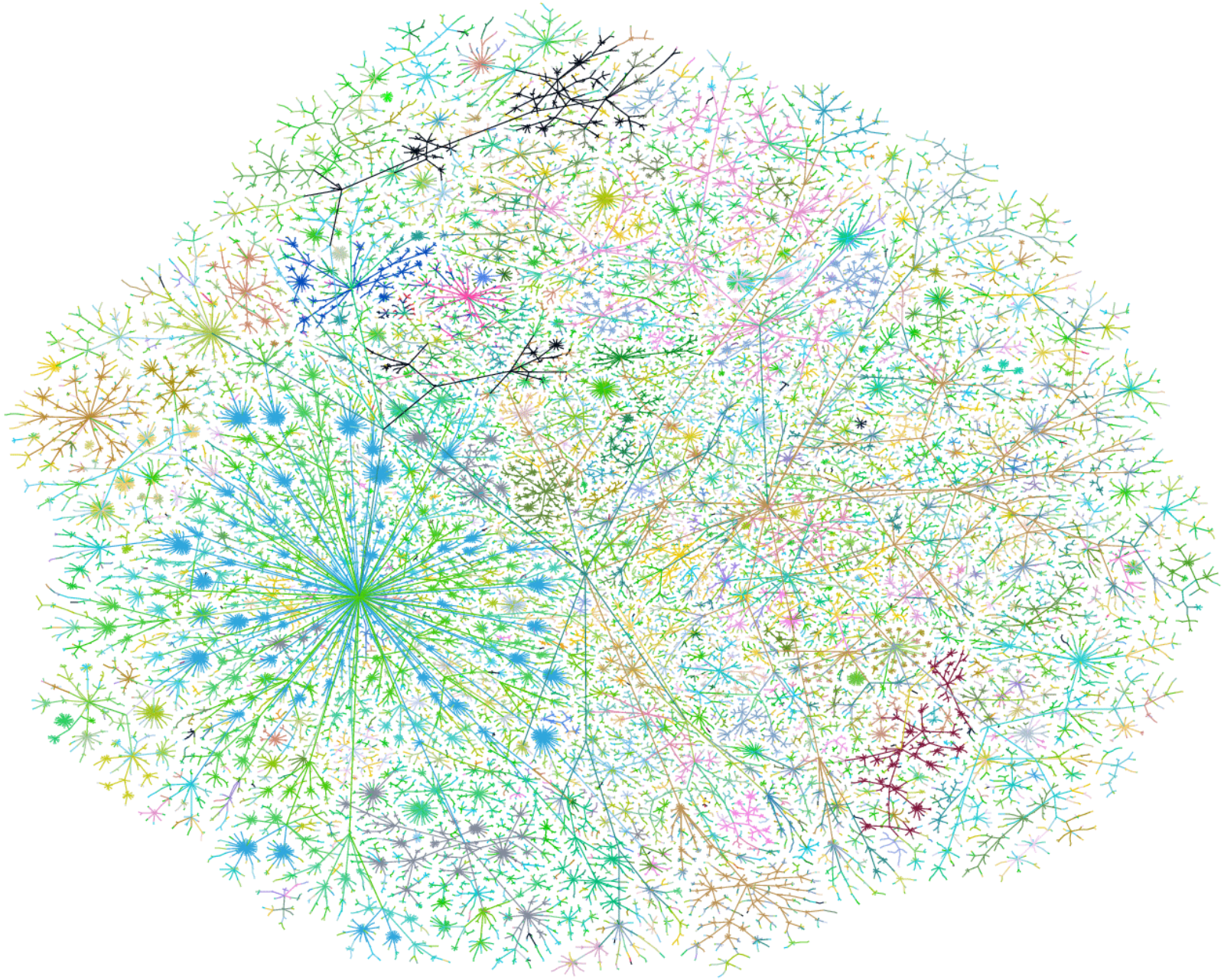
Stony Brook University

Why care about network security?

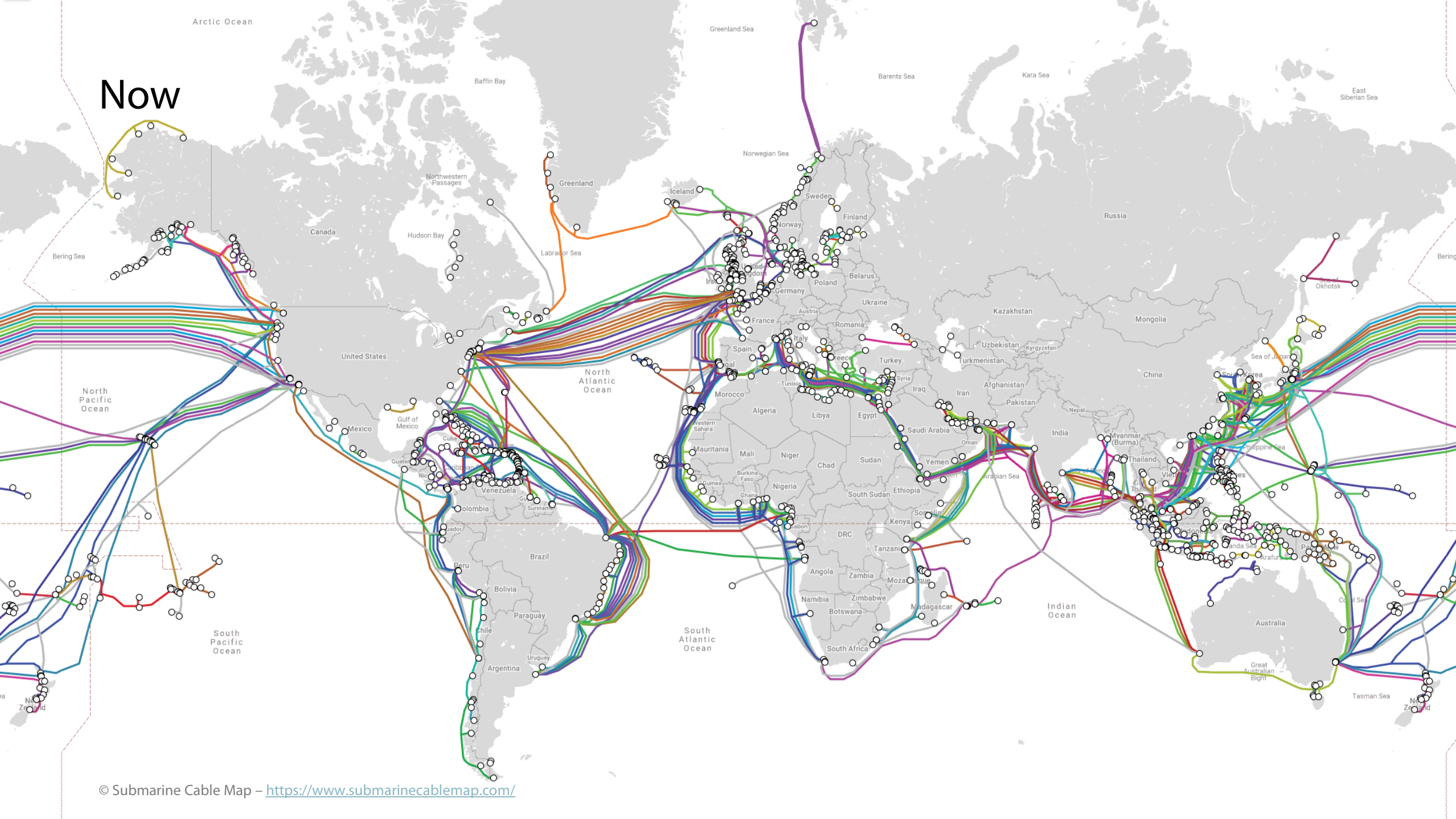
1969



1998



Now



Cisco Annual Internet Report (2018–2023) White Paper

Updated: March 9, 2020

Global Internet adoption and devices and connection

Internet users

Nearly two-thirds of the global population will have Internet access by 2023. There will be 5.3 billion total Internet users (66 percent of global population) by 2023, up from 3.9 billion (51 percent of global population) in 2018.

Devices and connections

The number of devices connected to IP networks will be more than three times the global population by 2023. There will be 3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018.

M2M connections will be half of the global connected devices and connections by 2023. The share of Machine-To-Machine (M2M) connections will grow from 33 percent in 2018 to 50 percent by 2023. There will be 14.7 billion M2M connections by 2023.

The consumer segment will have nearly three-fourths share of total devices and connections by 2023. Globally, consumer segment's share of total devices and connections will be 74 percent, with the business segment claiming the remaining 26 percent.

Internet of Things (IoT) by application

Within the M2M connections category (which is also referred to as IoT), **connected home applications will have the largest share and connected car will be the fastest growing application type**. Connected home applications will have nearly half or 48 percent of M2M share by 2023 and Connected car applications will grow the fastest at 30 percent CAGR over the forecast period (2018–2023).

Mobility growth

An increasing part of our business, social, and personal life involves Internet-connected computer systems

- Mobile computing, cyber-physical systems, Internet of things, wearable devices, …
- Web, email, IM, videoconferencing, cloud services, social networks, entertainment, …

Protecting the security and privacy of our digital interactions is critical

- Most of them involve networked systems and applications

Hacking of Government Computers Exposed 21.5 Million People

By Julie Hirschfeld Davis

July 9, 2015

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including Social Security numbers and some fingerprints.

Every person given a government background check for the last 15 years was probably affected, the Office of Personnel Management said in announcing the results of a forensic investigation of the episode, whose existence was known but not its sweeping toll.

The agency said hackers stole “sensitive information,” including

US news

Credit firm Equifax says 143m Americans' social security numbers exposed in hack

- **Atlanta-based company says 'criminals' accessed personal data**
- **Before notifying public, Equifax executives sold $1.8m in shares**

▲ Equifax says 143 million Americans' data was breached. Photograph: Mike Stewart/AP

Olivia Solon *in San Francisco*
@oliviasolon

Thu 7 Sep 2017 21.05 EDT

Credit monitoring company Equifax says a breach exposed the social security numbers and other data of about 143 million Americans.

After discovering the breach, but before notifying the public, three Equifax senior executives sold shares in the company worth almost $1.8m. Since the public announcement, the company's share price has tumbled.

The Atlanta-based company said Thursday that "criminals" exploited a US website application to access files between mid-May and July of this year.

It said consumers' names, social security numbers, birth dates, addresses and, in some cases, driver's license numbers were exposed. Credit card numbers for about 209,000 US consumers were also accessed.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do," said the company's chairman and

World's Biggest Data Breaches & Hacks

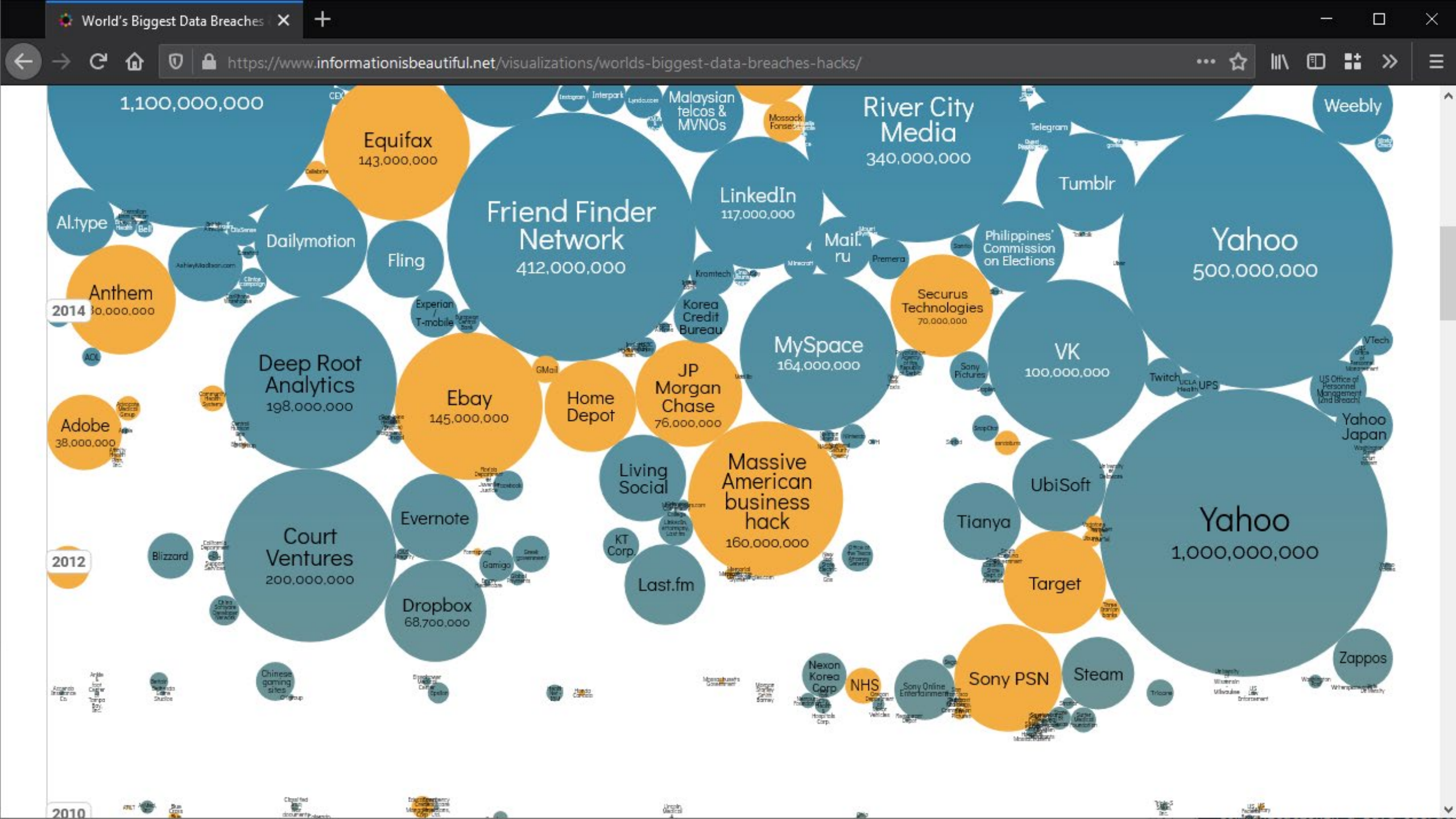
interesting story

Selected events over 30,000 records

UPDATED: Jan 2021

size: records lost **filter**

search...


World's Biggest Data Breaches
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
1,100,000,000
Equifax
143,000,000
Malaysian telcos & MVNOs
River City Media
340,000,000
Weebly
Telegram
Tumblr
Friend Finder Network
412,000,000
LinkedIn
117,000,000
Mail.ru
Philippines' Commission on Elections
Yahoo
500,000,000
Al.type
Dailymotion
Fling
Anthem
2014
Securus Technologies
70,000,000
Experian / T-mobile
Korea Credit Bureau
MySpace
164,000,000
VK
100,000,000
Deep Root Analytics
198,000,000
Ebay
145,000,000
Home Depot
JP Morgan Chase
76,000,000
Sony Pictures
Twitch
UPS
VTech
US Office of Personnel Management (2nd Breach)
Yahoo Japan
Adobe
38,000,000
Living Social
Massive American business hack
160,000,000
UbiSoft
Tianya
Yahoo
1,000,000,000
Evernote
Court Ventures
200,000,000
Blizzard
2012
KT Corp.
Last.fm
Target
Dropbox
68,700,000
Chinese gaming sites
Nexon Korea Corp
NHS
Sony Online Entertainment
Sony PSN
Steam
Zappos
2010

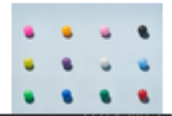
An Unprecedented Look at Stuxnet, the World's First Digital Weapon

IN JANUARY 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery---apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them.

Five months later a seemingly unrelated event occurred. A computer

Most Popular

SECURITY
Apple Fixes One of the iPhone's Most Pressing Security Risks
LILY HAY NEWMAN



SCIENCE
Worrisome New Coronavirus Mutations Are Emerging. Why

Cybercrime

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

▲ Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

Alex Hern
@alexhern

Thu 7 Jan 2016 08.20 EST

A power blackout in Ukraine over Christmas and a destructive cyberattack on a major Ukrainian media company were caused by the same malware from the same major hacking group, known as Sandworm, according to security researchers at Symantec.

The blackout, which affected large parts of western Ukraine, is believed to be the first example of a power outage deliberately caused by a hacking attack. The country's state intelligence agency, the SBU, attributed the attacks to state-sponsored hackers from Russia. If true, that would link the hacking of the power grid to the general escalation of cyberwarfare between the two nations in the aftermath of the invasion of Crimea.

That attribution was strengthened by the revelation that the hacking of power company Prykarpattyaoblenergo was carried out using malware substantially similar to an earlier attack, which affected the computers of a

ANDY GREENBERG EXCERPT SECURITY 08.22.2018 05:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller–Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying the Danish flag is planted by the building's northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building's basement, employees can browse a corporate gift shop, stocked with Maersk-branded bags and ties, and even a rare Lego model of the

Most Popular

SECURITY
Apple Fixes One of the iPhone's Most Pressing Security Risks
LILY HAY NEWMAN

SCIENCE
Worrisome New Coronavirus Mutations Are Emerging. Why Now?
MEGAN MOLTENI

Computing

US police force pay bitcoin ransom in Cryptolocker malware scam

Unprepared officials blindsided by sophisticated virus call experience 'an education'

▲ Malware took Massachusetts police computer hostage forcing officials to pay a bitcoin ransom. Photograph: Garry Wade Photograph: Garry Wade /Garry Wade

Samuel Gibbs

Thu 21 Nov 2013 06.34 EST

Massachusetts police have admitted to paying a bitcoin ransom after being infected by the Cryptolocker ransomware.

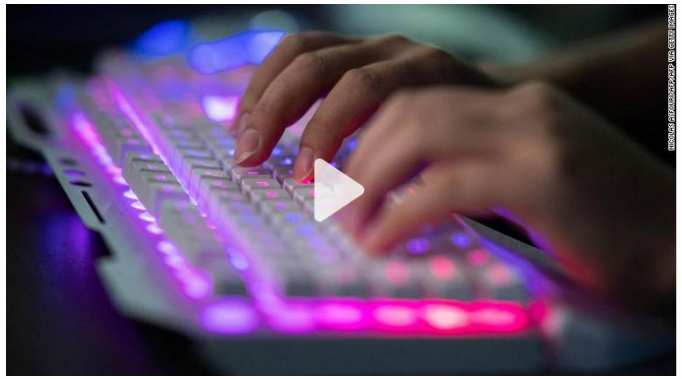
The Cryptolocker malware infects a computer, normally via a legitimate-looking email that urges the reader to open an attachment often posing as a voicemail, fax, invoice or details of a suspicious transaction that is being queried.

Once the Windows computer is infected, the malware encrypts the user's hard drive and then begins displaying a countdown timer, while demanding payment for the release of the data of 2 bitcoins - an almost untraceable, peer-to-peer digital online currency - which at current exchange rates equates to about £832 or $1338.

"(The virus) is so complicated and successful that you have to buy these bitcoins, which we had never heard of," Swansea Police Lt. Gregory Ryan talking to the Herald News. "It was an education for (those who) had to deal

Several hospitals targeted in new wave of ransomware attacks

By Vivian Salama, Alex Marquardt, Lauren Mascarenhas and Zachary Cohen, CNN
Updated 3:45 PM ET, Thu October 29, 2020



(CNN) — Several hospitals across the United States have been targeted in ransomware attacks in what appears to be an escalation and expansion of similar attacks previously launched on other hospitals and medical facilities.

The US Cybersecurity and Infrastructure Security Agency released a warning advisory Wednesday night regarding ransomware activity targeting health care facilities. On Twitter, CISA said "there is an imminent and increased cybercrime threat to U.S. hospitals and healthcare providers."

"CISA, FBI, and (the Department of Health and Human Services) have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers," the advisory stated. "CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

A Trump administration official told CNN that some hospitals have already been affected

Dashboard: Zero-Days in Desktop Web Browsers

The most exploited web browser is Chrome - The least exploited web browser is IE

Dashboard timeframe: 2019-01-01 to date (updated Nov 2020)

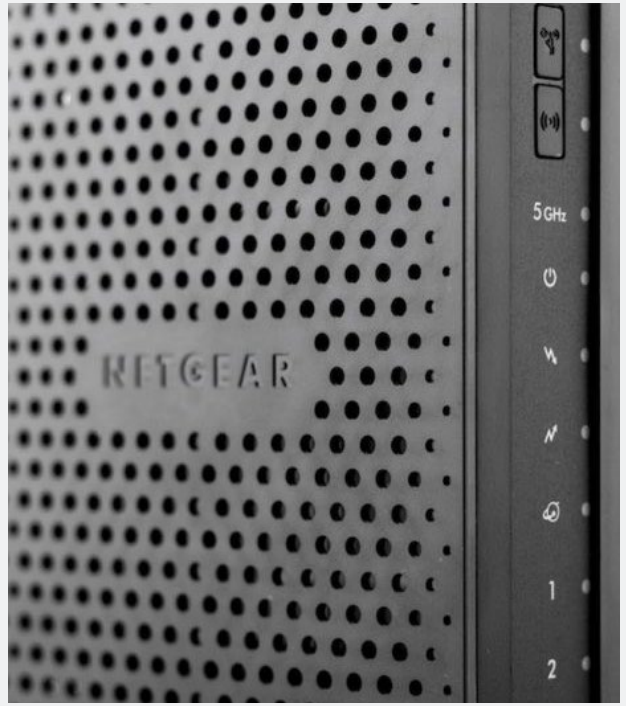
Date	Browser	CVE Reference	CVSS	Type	Vendor Advisory
11 Nov 2020	Chrome	CVE-2020-16017	8.8	Security Bypass	Link
11 Nov 2020	Chrome	CVE-2020-16013	8.8	Heap corruption	Link
02 Nov 2020	Chrome	CVE-2020-16009	8.8	Heap corruption	Link
20 Oct 2020	Chrome	CVE-2020-15999	8.8	Heap corruption	Link
11 Aug 2020	IE	CVE-2020-1380	7.5	Use-after-free	Link
14 Jul 2020	Chrome	CVE-2020-6519	8.2	Security Bypass	Link
03 Apr 2020	Firefox	CVE-2020-6820	8.8	Use-after-free	Link
03 Apr 2020	Firefox	CVE-2020-6819	8.8	Use-after-free	Link
03 Apr 2020	Safari	CVE-2020-3852	N/A	N/A	Link
03 Apr 2020	Safari	CVE-2020-3864	N/A	N/A	Link
03 Apr 2020	Safari	CVE-2020-3865	N/A	N/A	Link
03 Apr 2020	Safari	CVE-2020-3885	N/A	N/A	Link
03 Apr 2020	Safari	CVE-2020-3887	N/A	N/A	Link

CABLE HAUNT —

Exploit that gives remote access affects ~200 million cable modems

Cable Haunt lets attackers take complete control when targets visit booby-trapped sites.

DAN GOODIN - 1/13/2020, 5:00 PM



Netgear

131

Hundreds of millions of cable modems are vulnerable to critical takeover attacks by hackers halfway around the world, researchers said.

The attacks work by luring vulnerable users to websites that serve malicious JavaScript code that's surreptitiously hosted on the site or hidden inside of malicious ads, researchers from Denmark-based security firm Lyrebirds said in a report and accompanying website. The JavaScript then opens a websocket connection to the vulnerable cable modem and exploits a buffer overflow vulnerability in the spectrum analyzer, a small server that detects interference and other connectivity problems in a host of modems from various makers. From there, remote attackers can gain complete control over the modems, allowing them to change DNS settings, make the modem part of a botnet, and carry out a variety of other nefarious actions.

Cable Haunt, as the researchers have named their proof-of-concept exploit, is known to work on various firmware versions of the following cable modems:

How A Coffee Machine Infected Factory Computers with Ransomware

JULY 28TH, 2017 WAQAS HACKING NEWS, CYBER ATTACKS, MALWARE, SECURITY 0 COMMENTS

by Waqas
on July 28th, 2017

Tags
Cyber Crime, *europe*, *hacking*, *internet*, *Malware*, *Ransomware*, *security*

It's no surprise that the Internet of Things (IoT) devices are highly vulnerable to cyber attacks but who would know a time would come when these devices will become a security threat to institutions? This case involves a coffee machine and a ransomware attack.

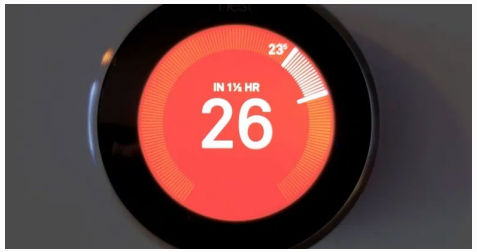
A few months ago researchers exposed life-threatening vulnerabilities in IIoT (Industrial Internet of Things) devices specifically Industrial robots. In their findings, robots could be hacked, but in this case, we are about to discuss a smart coffee machine or an Internet-connected coffee machine.

The incident took place in June 2017 and was shared by a chemical engineer on Reddit who goes by the handle of "C10H15N1." He works as a PLC (Programmable Logic Controllers) expert in a company that has

LATEST POSTS

Hacker talks to baby through Nest security cam, jacks up thermostat

01 FEB 2019 31



by Lisa Vaas

If the internet's army of creeps isn't busy blasting bogus warnings about fake nuclear warhead missiles through people's Nest security cameras, they're trying to parboil kids by jacking up the Nest thermostat.

A smart-home aficionado in the US state of Illinois told NBC News that he and his wife haven't slept well in days, after a stranger accessed his Nest home security cameras and thermostats.

Arjun Sud – whom NBC described as an "avid" user of smart-home technology – told the station that shortly after he and his wife put their 7-month-old baby boy to bed on 20 January 2019, they heard a strange noise coming out of the room. When Sud went to investigate, he said, he heard a deep, male voice coming from a Nest security camera that was installed in the nursery – one of 16 he owns, in addition to a security system and two Nest thermostats.

How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight

By Sapna Maheshwari

July 5, 2018

The growing concern over online data and user privacy has been focused on tech giants like Facebook and devices like smartphones. But people's data is also increasingly being vacuumed right out of their living rooms via their televisions, sometimes without their knowledge.

In recent years, data companies have harnessed new technology to immediately identify what people are watching on internet-connected TVs, then using that information to send targeted advertisements to other devices in their homes. Marketers, forever hungry to get their products in front of the people most likely to

China Is Using Facial Recognition Technology to Send Jaywalkers Fines Through Text Messages

It's the latest update to a widely deployed facial recognition surveillance system in China.

By Daniel Oberhaus

March 28, 2018, 8:00am Share Tweet Snap

In China, law enforcement agencies have been using advanced biometric technology to track citizens for years. These technologies are part of a coordinated national effort to create the "omnipresent, completely

MORE LIKE THIS

Tech

GPS

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

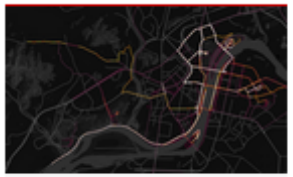
Alex Hern

@alexhern

Sun 28 Jan 2018
16.51 EST

Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company.

The details were released by Strava in a data visualisation map that shows all the activity tracked by users of its app, which allows people to record their exercise and share it with others.



Strava suggests military users 'opt out' of heatmap as row deepens

Read more

The map, released in November 2017, shows every single activity ever uploaded to Strava - more than 3 trillion individual GPS data points, according to the company. The app can be used on various devices including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns.

However, over the weekend military analysts noticed that the map is also

Digital Ambulance Chasers? Law Firms Send Ads To Patients' Phones Inside ERs

May 25, 2018 · 2:38 PM ET
Heard on All Things Considered

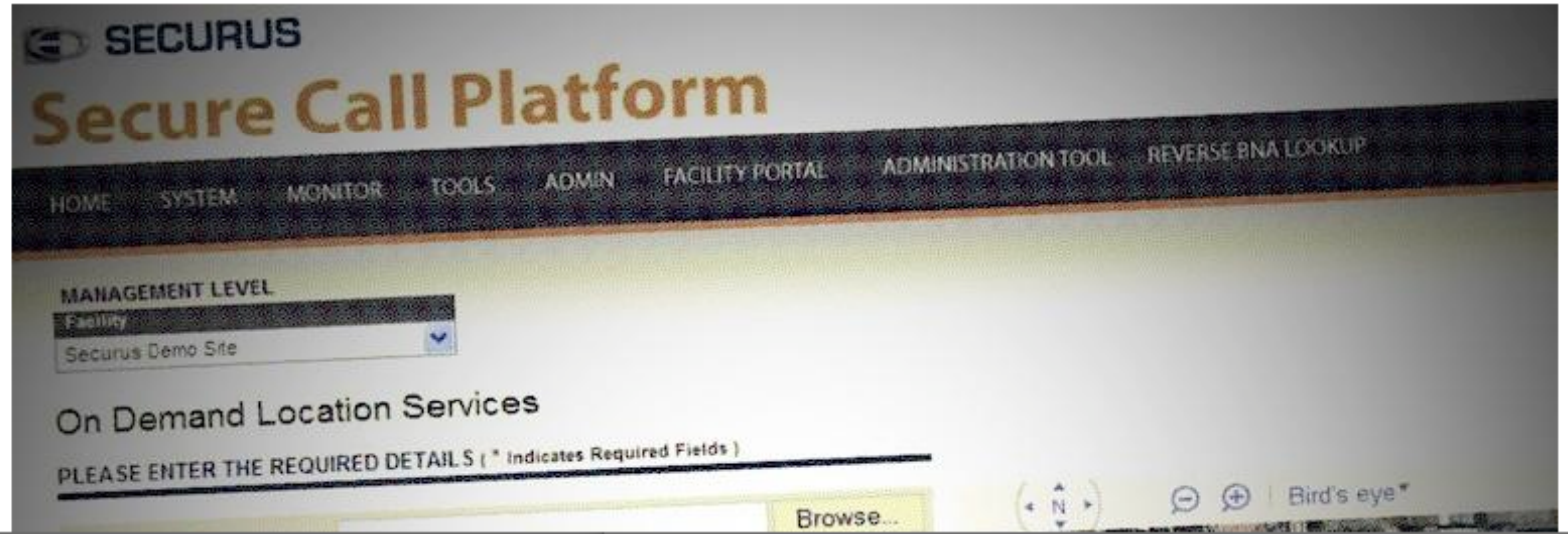
Patients sitting in emergency rooms, at chiropractors' offices and at pain clinics in the Philadelphia area may start noticing on their phones the kind of messages typically seen along highway billboards and public transit: personal injury law firms looking for business by casting mobile online ads at patients.

The potentially creepy part? They're only getting fed the ad because somebody knows

US cell carriers are selling access to your real-time phone location data

The company embroiled in a privacy row has "direct connections" to all major US wireless carriers, including AT&T, Verizon, T-Mobile, and Sprint -- and Canadian cell networks, too.

By Zack Whittaker for Zero Day | May 14, 2018 -- 19:00 GMT (12:00 PDT) | Topic: Security



MORE FROM ZACK WHITTAKER


Security
Online security 101: Tips for protecting your privacy from hackers and spies


Security
US government's "do not buy" list shuts out Russia, China

Security

{* NETWORKS *}

Verizon fined just $1.4m for stalker supercookies

Weakest slap on the wrist – and FCC lets mobile giant keep its opt-out for subscribers

Kieren McCarthy in San Francisco Mon 7 Mar 2016 // 20:55 UTC SHARE

Verizon will pay $1.35m for its use of "supercookies," but its customers will still have to opt out of the permanent trackers, under an agreement [PDF] reached with the US Federal Communications Commission (FCC) on Monday.

The mobile giant will be required to tells its customers the supercookie exists and provide a simple option to have their tracker removed. Verizon will also have to actively seek permission from its millions of users before they can share the data with third parties.

But with the opt-out still in place, it will allow the company to gather and use huge amounts of information on its individual users and their browsing habits.

Back in 2012, Verizon started injecting its "unique identifier token header" (UIDH) into each HTTP request sent via its mobile data network. Each token is unique to each Verizon subscriber.

When users with the supercookie browse any website via Verizon, all the

// MOST READ


'It's dead, Jim': Torvalds marks Intel Itanium processors as orphaned in Linux kernel


Synology to enforce use of validated disks in enterprise NAS boxes. And guess what? Only its own disks exceed 4TB


Missing GOV.UK web link potentially cost taxpayers £50m as civil servants are forced to shuffle paper forms


Countless emails wrongly blocked as spam after Cisco's SpamCop failed to

Comcast continues to inject its own code into websites you visit

by TRISTAN GREENE — Dec 11, 2017 in INSIGHTS

Comcast believes it's acceptable to inject hundreds of lines of code into any web page you visit if it thinks you're in need of a hardware upgrade. And even if you don't need an upgrade, you're wrong.

A user recently took to the company's forums to complain of its practice of running its own code on webpages customers visit in order to prompt them with special Comcast messages.

Posting under the name "bham3dman" on the company's official forum, the user stated:

> *Comcast began injecting 400+ lines of JavaScript code in to pages I requested on the internet so that when the browser renders the web page, the JavaScript generates a pop up trying to up-sell me a new modem. When you call the number in the popup, they're quick to tell you that you need a new modem, which in my case is not true. I later verified with level-2 support that my modem is perfectly fine and I don't need to*

{* SECURITY *}

CBS's Showtime caught mining crypto-coins in viewers' web browsers

Who placed the JavaScript code on two primetime dot-coms? So far, it's a mystery

Kieren McCarthy in San Francisco Mon 25 Sep 2017 // 20:33 UTC SHARE

The websites of US telly giant CBS's Showtime contained JavaScript that secretly commandeered viewers' web browsers over the weekend to mine cryptocurrency.

The flagship Showtime.com and its instant-access ShowtimeAnytime.com sibling silently pulled in code that caused browsers to blow spare processor time calculating new Monero coins – a privacy-focused alternative to the ever-popular Bitcoin. The hidden software typically consumed as much as 60 per cent of CPU capacity on computers visiting the sites.

The scripts were written by Code Hive, a legit outfit that provides JavaScript to website owners: webmasters add the code to their pages so that they can earn slivers of cash from each visitor as an alternative to serving adverts to generate revenue. Over time, money mined by the Code-Hive-hosted scripts adds up and is transferred from Coin Hive to the site's administrators. One Monero coin, 1 XMR, is worth about $92

// MOST READ


'It's dead, Jim': Torvalds marks Intel Itanium processors as orphaned in Linux kernel


Synology to enforce use of validated disks in enterprise NAS boxes. And guess what? Only its own disks exceed 4TB


Missing GOV.UK web link potentially cost taxpayers £50m as civil servants are forced to shuffle paper forms


Countless emails wrongly

Starbucks cafe's wi-fi made computers mine crypto-currency

By Leo Kelion
Technology desk editor

13 December 2017

Starbucks has acknowledged that visitors to one of its branches were unwittingly recruited into a crypto-currency mining operation.

The wi-fi service provided by one of the coffee chain's Buenos Aires outlets surreptitiously hijacked connected computers to use their processing power to create digital cash.

Starbucks said that it had taken "swift action" to address the problem.

But one expert said it highlighted the risks of using public wi-fi.

It is not clear how long the malware involved was active or how many customers were affected.

Top Stories

Russia jails Putin critic Navalny despite protests

Alexei Navalny had returned to Russia after treatment in Germany for Novichok poisoning.

1 hour ago

'Hero' fundraiser Capt Sir Tom Moore dies aged 100

19 minutes ago

Oxford vaccine could substantially cut spread

47 minutes ago

Features

BIZ & IT —

French agency caught minting SSL certificates impersonating Google

sharyn morrow

Unauthorized credentials for Google sites were accepted by many browsers.

DAN GOODIN - 12/9/2013, 2:05 PM

61

Rekindling concerns about the system millions of websites use to encrypt and authenticate sensitive data, Google caught a French governmental agency spoofing digital certificates for several Google domains.

The secure sockets layer (SSL) credentials were digitally signed by a valid certificate authority, an imprimatur that caused most mainstream browsers to place an HTTPS in front of the addresses and display other logos certifying that the connection was the one authorized by Google. In fact, the certificates were unauthorized duplicates that were issued in violation of rules established by browser manufacturers and certificate authority services.

The certificates were issued by an intermediate certificate authority linked to the Agence nationale de la sécurité des systèmes d'information, the French cyberdefense agency better known as ANSSI. After Google brought the certificates to the attention of agency officials, the officials said the intermediate certificate was used in a commercial device on a private network to inspect encrypted traffic with the knowledge of end users. Google security engineer Adam

KEVIN POULSEN SECURITY 09.13.2013 04:17 PM

FBI Admits It Controlled Tor Servers Behind Mass Malware Attack

IT WASN'T EVER seriously in doubt, but the FBI yesterday acknowledged that it secretly took control of Freedom Hosting last July, days before the servers of the largest provider of ultra-anonymous hosting were found to be serving custom malware designed to identify visitors.

Freedom Hosting's operator, Eric Eoin Marques, had rented the servers from an unnamed commercial hosting provider in France, and paid for them from a bank account in Las Vegas. It's not clear how the FBI took over the servers in late July, but the bureau was temporarily thwarted when Marques somehow regained access and changed the passwords, briefly locking out the FBI until it gained back control.

```
589. function f(var15,view,var16)
590. {
591.         var magneto = "";
592.         var magneto =
("\ufc60\u8ae8"+"\u0000\u6000"+"\ue589\ud231"
593.         var var29 = magneto;
594.         var var17 = "\u9060";
595.         var var18 = "\u9061";
596.         var var19 = "\uC481\u0000\u0008" ;
597.         var var20 = "\u2589\u3000"+String.fro
598.         var var21="\u258B\u3000"+String.fromC
599.         var var22 = "\uE589";
600.         var var23 ="\uC3C9";
601.         var var24  = "\uE889";
602.         var24 += "\u608D\u90C0";
```

THE PAYLOAD FOR THE TOR BROWSER BUNDLE MALWARE IS HIDDEN IN A VARIABLE CALLED "MAGNETO."

BOMBSHELL! —

"Unauthorized code" in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

DAN GOODIN - 12/17/2015, 6:50 PM

133

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections," Juniper Chief Information officer Bob Worrall wrote. "Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

Summary

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software

SHARE

Recent Posts

26 Jan 2021
Phishing Campaign Leverages WOFF Obfuscation and Telegram Channels for Communication >

21 Jan 2021
Training Transformers for Cyber Security Tasks: A Case Study on Malicious URL Prediction >

20 Jan 2021
Emulation of Kernel Mode Rootkits With Speakeasy >

RSS FEED: STAY CONNECTED

Help users in Iran reconnect to Signal

jlund on 04 Feb 2021

Just over a week ago, we announced that Iranian censors had started blocking all Signal traffic in the country. As an interim solution to help people in Iran get connected again, we've added support in Signal for a simple TLS proxy that is easy to set up, can be used to bypass the network block, and will securely route traffic to the Signal service.

This new connection method is supported in the latest Signal Android beta release, and will be rolling out to production users in a few days. Our hope is that this will help many people in Iran start sending and receiving messages again while we continue to explore additional censorship circumvention techniques that will work there.

Network vs. System vs. Computer vs. Information Security

Not always a clear distinction

- Infrastructure
- Protocols
- Applications
- Hosts/devices

Complex interactions

- Core internet protocols/services
- Distributed systems
- Web/cloud/IoT applications

There is more

- People
- Physical security

Threats span all these areas

Network Security Arsenal

Cryptography: wide range of techniques for enabling secure, confidential, and anonymous communication

Access Control: authentication and authorization, firewalls, …

Monitoring: packet/network flow monitoring, intrusion detection, …

Rigorous protocol and system design and implementation: account for both benign failures and malicious actions

- Data corruption, timeouts, dead hosts, routing problems, …
- Eavesdropping, modification, injection, deletion, replay, …
- Software bugs: may turn into **vulnerabilities**

Threats

Exposure of data

Tampering with data

Denial of service

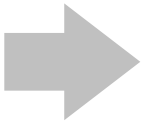
Impersonation

Forbidden access

Exposure of personal information

Identification of individuals

Threats	Goals
Exposure of data	Confidentiality
Tampering with data	Integrity
Denial of service	Availability
Impersonation	Authentication
Forbidden access	Authorization
Exposure of personal information	Privacy
Identification of individuals	Anonymity



Confidentiality

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [RFC2828]

Sensitive data must be protected

- In transit: network packets, network connections, messages, documents, …
- At rest: main memory (buffers, message queues), flash/disk storage, backups, …

Cryptography is a tool to achieve confidentiality

- Not the only one: access control, steganography, …

Content protection is often not enough

- Data vs. metadata (e.g., phone call content vs. phone call records)

Data Integrity

"The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner." [RFC2828]

Cryptography is a tool to achieve data integrity

- Intentional or accidental data changes should be detectable

System integrity

"Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system." [CNSSI No. 4009]

- Fragile: weak authentication, vulnerable software, supply chain attacks, …

Availability

"The property of being accessible and useable upon demand by an authorized entity." [CNSSI No. 4009]

Denial of Service (DoS) attacks are the most common way of affecting the availability of networked systems

- Saturation of resources (bandwidth, CPU, memory, …)
- Disruption of configuration or state (routing, DNS, …)
- Jamming, interference, physical damage, …

Malware can do more harm

- Ransomware: encrypt user files and then demand a ransom (Gpcode, Cryptolocker, WannaCry, Bad Rabbit, Petya, Ryuk, …)
- Just wipe out data/brick the system (Wiper, NotPetya, …)

Authentication

"The process of verifying an identity claimed by or for a system entity." [RFC2828]

Different approaches

- Something you know (password, pin, …)
- Something you have (phone, token, …)
- Something you are (fingerprint, face, …)

Multi-factor authentication is a must

Cryptography is a tool to achieve authentication

Password theft/leakage is a huge problem

Authorization

"Access privileges granted to a user, program, or process or the act of granting those privileges." [CNSSI No. 4009]

Authorization verifies that a user has the proper privileges to access a resource (presumes successful authentication)

Related term: *access control*

Access restriction based on various properties: identity, role, labels, date/time, IP address, domain, access frequency, …

One of the core goals of network security:

Keep unauthorized parties from gaining access to resources

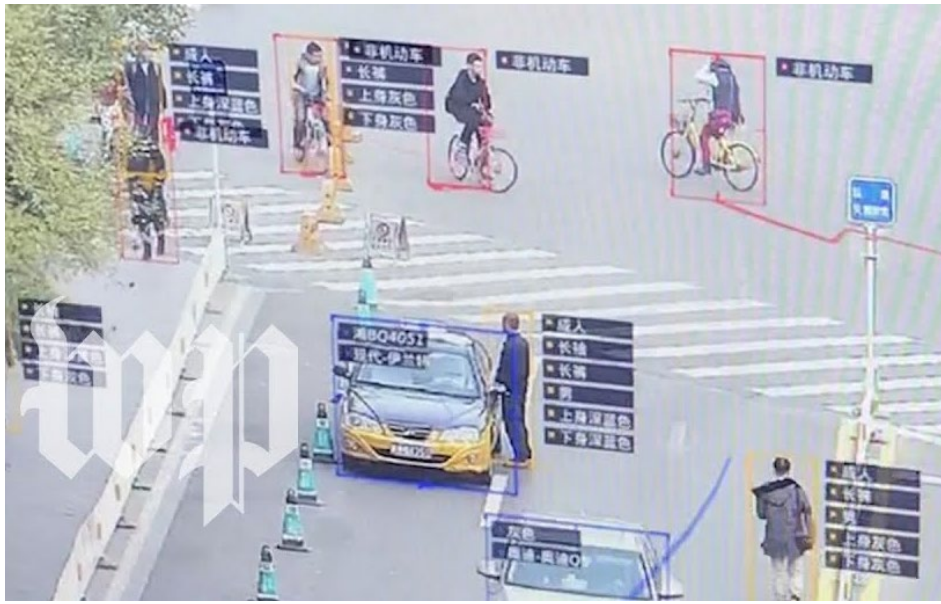
Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Beyond private data (messages/files):

- Activities (browsing history, voice commands, …)
- Location (3/4/5G, GPS, WiFi, cameras, …)
- Preferences ("likes," Amazon, Netflix, …)
- Health (Fitbit, iWatch, …)
- …

Metadata is equally important!



Anonymity

"The state of being not identifiable within a set of subjects, the anonymity set." [Pfitzmann and Köhntopp]

The larger the anonymity set, the stronger the anonymity

Very different from privacy:

An anonymous action may be public, but the actor's identity remains unknown (e.g., vote in free elections)

Anonymous communication

Sender anonymity	(unknown sender, known receiver)
Receiver anonymity	(known sender, unknown receiver)
Unlinkability of sender and receiver	(unknown sender, unknown receiver)

Course Focus (you got the idea…)

Internet technologies, protocols, applications, attacks, and defenses, from a practical perspective

Indicative topics

- Network protocols, eavesdropping, scanning, DoS attacks, firewalls, VPNs, proxies, intrusion detection, forensics, honeypots, encrypted communication, authentication, services and applications, botnets, targeted attacks, privacy, anonymity, …

Cultivate the "security mindset"

- Understand the modus operandi of attackers
- Find vulnerabilities, subvert protections, bypass all the things
- Think sideways
- How to secure a system – know what to defend against

Play Fair

Cannot teach defense without offense, but:

Breaking into systems is illegal!

Unauthorized data access is illegal!

Computer Fraud and Abuse Act (CFAA)

http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Practice on your own systems or controlled environment

Scanning/penetration testing/etc. of third-party systems may be allowed only after getting permission by their owner

Course Information

Mixed format

Lectures, hands-on sessions, research paper discussions, online discussion

Requirements

Four programming assignments

Midterm and final exams (format TBA)

Grading

Assignments: 70%

Final: 30%

Late Policy

You are allowed 5 “late days” throughout the semester

- To be used at your discretion for any homework or project deliverables
- No prior communication is necessary
- Each day (24h) is indivisible, and can be used only as a whole
- Even if a submission is just a few minutes late, this still counts as a whole day

Once all late days are used up, late submissions will receive zero credit

Schedule (Tentative)

Threat Landscape

Lower Layers

Core Protocols

Denial of Service

Firewalls and Gateways

Encrypted Communication

Authentication

SSL/TLS

Crypto Failures

Reconnaissance and Scanning

Intrusion Detection

Malware and Botnets

Honeypots, Deception, Covert Channels

Email

Spam

Web/Cloud

Tracking/Privacy

Anonymity/Online Freedom

Course web page

http://www.cs.stonybrook.edu/~mikepo/CSE508/

All slides will be posted on the Schedule page

Please sign up on Piazza

Q&A, discussions, homework descriptions, and additional resources

- Piazza supports private messages: please use that functionality (instead of email to the instructor or TAs) for private questions related to the lectures or homework
- You may want to install the Piazza app on your mobile device