SENG 460 / ECE 574
Practice of Information Security and Privacy

Week 6:

Legal, Intellectual Property, Liability, Evidence, Breaches/Headlines, Investigations,

Open Source Intelligence, Darknet, Foreign Threats to the Democratic Process

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Legal, Intellectual Property, Liability, Evidence

University of Victoria

Software Licensing

- written, signed, negotiated contracts
- shrink-wrap agreements
  - clause stating you acknowledge agreement simply by breaking the seal on the shrink-wrap
- click-through agreements
  - states you agree when clicking the button you agree
- cloud services license
  - click-through agreements

Laws & Prosecution

- technology is evolving so quickly, laws and law enforcement are challenged to keep up
- jurisdiction is a problem
- evidence is a problem
- prosecution is very difficult – consider you must prove beyond a reasonable doubt
- having the skills and maintaining talent supply is a problem

University of Victoria

Four categories of Intellectual Property (IP)

- **patent**: legal ownership of an invention (eg. bottle design)
- **copyright**: expression of the idea of the resource instead of the resource itself (e.g. book on Coke)
- **trade secret**: something proprietary to the company and essential for its survival and profitability (e.g. Coke recipe)
- **trademark**: word, name, symbol, sound, shape, colour, or combination of these which represent the company (brand identity) to a group/people/the world (eg. Coca Cola™)

University of Victoria

Liability

- **liability**: being responsible to an entity because of your actions or negligence
- **negligence**: organization was careless and as a result some person or organization was negligent and may be found liable
- **due care**: degree of care a reasonable person would exercise (eg. request patch vulnerabilities) .. putting measures in place to protect
- **due diligence**: reasonable steps taken by someone to satisfy a requirement (eg.follow-up and determine vulns were patched) ensuring measures remain in place

Evidence

- **best evidence**: original or primary evidence rather than copy or duplicate
- **secondary evidence**: copy of evidence or oral description – not as reliable as best evidence
- **direct evidence**: proves or disproves a specific act through witness's five senses (e.g. saw harassment); testimony from firsthand witness
- **conclusive evidence**: evidence that cannot be contradicted by any other evidence; incontrovertible; overrides all other evidence

Evidence

- **circumstantial evidence**: inference of information from other, immediate, relevant facts; evidence to support circumstances/other evidence
- **corroborative evidence**: supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence; not on its own
- **opinion evidence**
  - expert: may offer opinion based on personal expertise and facts
  - non-expert: may testify only as to facts

Evidence

- **hearsay evidence** (3rd party): oral or written evidence that is presented in court that is secondhand and has no firsthand proof of accuracy or reliability (usually not admissible in court)

- **real evidence**: physical evidence, tangible – e.g. hard drives

Remember chain of custody!

Preserve evidence, don't tamper with

University of Victoria

Headlines/Breaches

Headlines

- understand how attacks happen
  - what they did, how they did it, why they did it
  - should we blame the companies?
  - who is the victim?
- understand how to prevent them
  - there is a lot to learn from incidents
  - what they did, how they did it
- when there is new vulnerability
  - new website pops up with information
  - eg. www.heartbleed.com
  - it's new (WHOIS), no reputation, why do you trust it?
  - often has a tool to check if your website is vulnerable
  - how do you know they won't say it's good and send the results to the bad guys?
- when there is a new incident
  - people want to know if they are affected
  - eg. www.haveibeenpwned.com

'Never punish somebody for making a mistake': Canadian cybersecurity head on online dangers

CBC Radio · Posted: Feb 24, 2019 9:09 AM ET | Last Updated: February 22

With rising concerns about abuse of our personal data, cyber espionage, and interference in election campaigns, cybersecurity experts have a lot on their plates.

Just ask Scott Jones. He's the head of the new Canadian Centre for Cyber Security, part of the Communications Security Establishment.

The Centre is responsible for cybersecurity on a national level, and as Jones put it, the Centre's "real target is the critical infrastructure sector, and that does include governments, but it includes the infrastructure we rely on in our day-to-day lives."

As part of that focus on our day-to-day lives, they run a program called Get Cybersafe, with practical tips for Canadians.

Jones delivered a keynote address at the 20th anniversary Privacy and Security Conference in Victoria, B.C. earlier this month. The annual event brings together experts in all facets of digital privacy and security, from privacy commissioners to information security experts.

Spark host Nora Young caught up with Scott Jones at the conference to talk about his perspective on the cybersecurity landscape in 2019.

Headlines

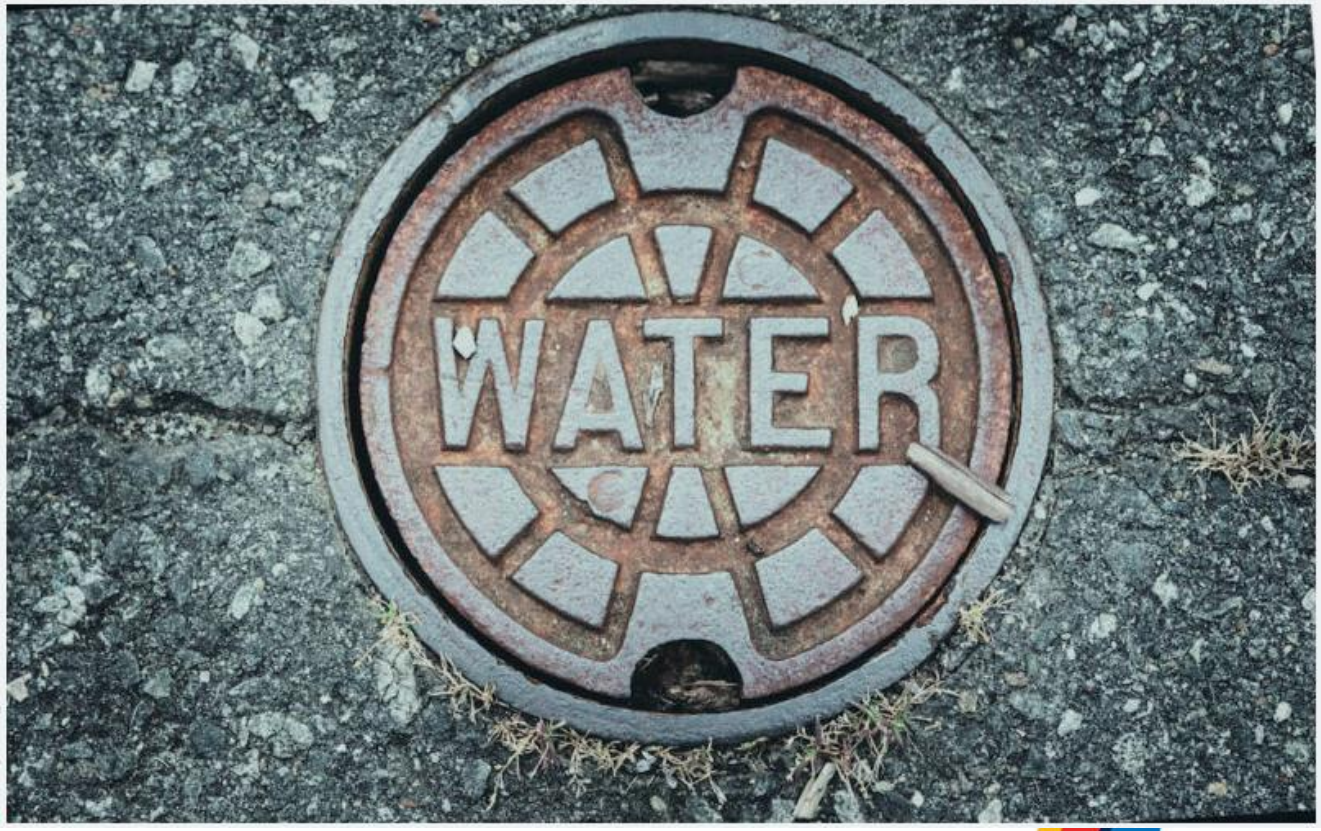
The Florida water treatment facility whose computer system experienced a potentially hazardous computer breach last week used an unsupported **version of Windows with no firewall and shared the same TeamViewer password among its employees,** government officials have reported. The computer intrusion happened last Friday in Oldsmar in Florida.

According to an advisory from the state of Massachusetts, employees with the Oldsmar facility used a computer running Windows 7 to remotely access plant controls known as a SCADA -- short for "supervisory control and data acquisition" -- system. What's more, the computer had no firewall installed and used a password that was shared among employees for remotely logging into city systems with the TeamViewer application. [...] The revelations illustrate the lack of security rigor found inside many critical infrastructure environments. In January, Microsoft ended support for Windows 7, a move that ended security updates for the operating system. Windows 7 also provides fewer security protections than Windows 10. The lack of a firewall and a password that was the same for each employee are also signs that the department's security regimen wasn't as tight as it could have been.

Breached water plant employees used the same TeamViewer password and no firewall

Shortcomings illustrate the lack of security rigor in critical infrastructure environments.

DAN GOODIN - 2/10/2021, 2:59 PM



Clearview AI (patching? not enough info)

Clearview AI has billions of our photos. Its entire client list was just stolen

By Jordan Valinsky, CNN Business

Updated 1824 GMT (0224 HKT) February 26, 2020

New York (CNN Business) – Clearview AI, a startup that compiles billions of photos for facial recognition technology, said it lost its entire client list to hackers.

The company said it has patched the unspecified flaw that allowed the breach to happen.

In an interview with CNN Business earlier this month, Clearview AI founder and CEO Hoan Ton-That downplayed concerns about his technology. He said he wants to build a "great American company" with "the best of intentions." He said he wouldn't sell his product to Iran, Russia or China and claimed the technology is saving kids and solving crimes.

> "Shrugging and saying data breaches happen is cold comfort for Americans who could have their information spilled out to hackers without their consent or knowledge," Wyden said in a statement. "Companies that scoop up and market vast troves of information, including facial recognition products, should be held accountable if they don't keep that information safe."

conducted by customers, which include some police forces.

The company claims to have scraped more than 3 billion photos from the internet, including photos from popular social media platforms like Facebook, Instagram, Twitter and YouTube.

The firm garnered controversy in January after a New York Times investigation revealed that Clearview AI's technology allowed law enforcement agencies to use its technology to match photos of unknown faces to people's online images. The company also retains those photos in its database even after internet users delete them from the platforms or make their accounts private.

Twitter, YouTube and Facebook have all demanded it stop using photos on their platforms.

And **US senator Ron Wyden tweeted** Clearview's activities were "extremely troubling".

"Americans have a right to know whether their personal photos are secretly being sucked into a private facial-recognition database," he wrote.

But Clearview AI chief executive Hoan Ton-That told the CBS This Morning programme it was his First Amendment right to collect public photos.

Clearview AI (patching? not enough info)

5 police officers in B.C. used facial recognition software deemed illegal, privacy commissioner says

U.S. technology company Clearview AI violated Canadian privacy law: report

Privacy commissioners found U.S. company collected photos of Canadians without

Delete photos of Canadians in database, commissioners say

The commissioners called for Clearview AI to stop offering its technology in Canada, stop collecting images of Canadians and to delete the photos of Canadians it had already collected in its database.

If the company refuses to follow the recommendations, the four privacy commissioners will "pursue other actions available under their respective acts to bring Clearview into compliance with Canadian laws," the statement said.

However, the four acknowledged that under current laws, and even under proposed changes to federal privacy laws, their ability to penalize the company or force it to comply with Canadian orders is limited.

Yandex (RU attacked by 5 eyes)

Russia's largest search engine hacked by Western intelligence agencies

By Anthony Spadafora June 27, 2019

New report reveals Yandex was the victim of Five Eyes espionage

Image credit: Yandex (Image credit: '

"This particular attack was detected at a very early stage by the Yandex security team. It was fully neutralized before any damage was done....Yandex security team's response ensured that no user data was compromised by the attack."

Yandex believes that that the agency was after technical information on user authentication processes. Obtaining this information can allow attackers to imitate users and access private messages.

Further, Yandex hired Kaspersky, a Russian cybersecurity firm, to investigate further into the hack. Kaspersky concluded that the hackers were most likely linked to the Western intelligence agencies.

The search engine Yandex, often referred to as Russia's Google, was the target of a cyberattack that occurred late last year which was orchestrated by hackers working for Western intelligence agencies.

The hackers deployed a rare type of malware, called Reign, in an attempt to spy on user accounts according to a new report from Reuters who spoke with four people familiar with the incident. This particular strain of malware is known to be used by the Five Eyes nations as a result of Edward Snowden leaking classified NSA documents.

- While cyberattacks against Western organizations and governments receive a great deal of media attention, similar attacks against Russia are rarely acknowledged or discussed openly in public.

ident were able to determine
nations orchestrated the
in unsure as to whether the
v Zealand or Canada was

ndex took place between
2018 and the hackers were
neir access to the company's
al weeks before they were

LifeLabs (apology, outside firm, delay in notice)

CYBER SECURITY NEWS · 6 MIN READ

Lifelabs Data Breach, the Largest Ever in Canada, May Cost the Company Over $1 Billion in Class-Action Lawsuit

SCOTT IKEDA · JANUARY 8, 2020

LifeLabs cyberattack one of 'several wake-up calls' for e-health security and privacy

CEO says information related to about 15 million customers may have been breached

Mark Gollom · CBC News · Posted: Dec 19, 2019 4:00 AM ET | Last Updated: December 19, 2019

The data breach of Canadian laboratory testing company LifeLabs highlights the security and privacy challenges that come with the push for a medical system in which e-health plays a significant role. (Cole Burston/The Canadian Press)

comments

The data breach of the Canadian laboratory testing company LifeLabs is one of "several wake-up calls" for security and privacy challenges that come with the push for a medical system in which eHealth plays a significant role.

LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario

Canada's largest lab testing company says private data has not been exposed publicly

CBC News · Posted: Dec 17, 2019 11:40 AM PT | Last Updated: December 17, 2019

A LifeLabs clinic is pictured in Vancouver, British Columbia on Tuesday, Dec. 17, 2019. (Ben Nelms/CBC)

LifeLabs (not first rodeo)

Medical lab loses thousands of B.C. patient records

Hard drive went missing in January, containing ECG results and patient information

The Canadian Press · Posted: Jun 24, 2013 6:40 PM PT | Last Updated: June 24, 2013

LifeLabs in Kamloops, B.C., says it lost a hard drive with data 1:52

The personal information of about 16,000 patients of a medical lab service in Kamloops has gone missing, says the company's president.

LifeLabs president Sue Paish said Monday a computer was sent to their main office in Burnaby for servicing in January, but when it was returned, the hard drive was missing.

The hard drive held the results of ECGs, or electrocardiograms, gathered at three local facilities between 2007 and 2013.

- "There was no financial information whatsoever included in the data, no ability to access any financial records or other financial-related data," said Paish, who admitted the drive did include personal information like the patient's name, address, height, age, gender, the ECG results and health care number.
- She said an internal investigation failed to determine who took the drive and where it is now, adding the information is password protected and requires special equipment to read.
- The company has implemented measures to minimize the risk of such incidents in the future, including ensuring that all ECG reports and drives are fully encrypted, said Paish.
- She also apologized for the incident and said this is the first security breach in the Lifelabs' 50-year history.
- Health Minister Terry Lake said he learned of the breach just last week.
- "It's unacceptable to take this amount of time to notify the government and the Office of the Privacy Commissioner about a breach like this," he said. "And again they have assured us that will not happen in the future."

Saskatchewan eHealth

"There were some files that did leave our organization and went to some suspicious IP addresses in Europe," said Jim Hornell, CEO of eHealth.

The files are locked by the attacker, making it difficult for eHealth to determine what's on them.

"At this point, we have no indication whatsoever that there was any personal health information of people on those files," Hornell said. "But we can't say with 100 per cent certainty."

READ MORE: **eHealth Saskatchewan offline while dealing with ransomware attack**

The files were stolen from a server that does not store any personal health information of patients said Hornell. However, this still needs to be verified through a more thorough investigation.

eHealth is looking to crack the password to see the locked files. They also hired a third-party expert to search the internet to see if the files are being sold.

"We have yet to receive a ransom which is a good sign really that this has been thwarted, but I'd be remised not to alert people circumstances have changed," Hornell said.

eHealth hit by ransomware attack but personal health data is secure, says CEO

- The computer system that stores the confidential medical data of Saskatchewan residents was hit by a ransomware attack on the weekend but the CEO of eHealth Saskatchewan says patient data is secure.
- "It certainly looks like someone has found their way to tinker with our system and began encrypting some of our information," said Jim Hornell in a phone interview.
- "They put a lock on it and they say if you want to unlock this again to get back to your information you'll pay us some money," Hornell said, noting that the organization has contacted the RCMP about this attack.
- He said eHealth staff is examining 110 servers that may have been attacked. They're working to assess and repair the damage and restore the information.
- He doesn't know how long this will take but he said once that work is done, the organization will attempt to figure out how the system was breached in the first place.

Government of Saskatchewan

Murray said the Saskatchewan government has not received a ransom demand so far.

"We haven't had to deal with that yet and I hope we don't have to," he said. "We have all of our data backed up and ... we could always go back to our backups and restore systems from an earlier date if we have to."

The attack against the Saskatchewan government appears to be a distributed-denial-of-service -- or DDoS -- attack, said Eric Jardine, a senior fellow at the Centre for International Governance Innovation based in Waterloo, Ont.

Whoever is behind the WannaCry attacks is out to make money, suggested Jardine, who also teaches political science at Virginia Polytechnic Institute and State University.

"To change that tactic all of a sudden and to target a government with a distributed-denial-of-service attack seems like a weird shift, so I suspect they aren't related," he said.

"I suspect it's just two separate things that both happened to involve computers."

City of Saskatoon

Saskatoon Falls Victim to $1 Million Cyber Attack

2019-08-26 2:52:36 PM

CATEGORIES: Access & Privacy

On August 15th, Saskatoon's city manager Jeff Jorgenson announced that the city had been the victim of a cyber-attack.

Jorgenson said a fraudster impersonated a local construction company's Chief Financial Officer (CFO) and asked for a change in banking information. The change of information was completed with the next payment going from the city to the cyber thief instead of the construction company for the amount of $1.04 million.

Saskatoon's Police Service have said that it is unknown how much can be recovered and are warning the public of scammers targeting human resources and finance departments via email.

This case is the latest of a growing trend of municipal governments falling victim to a form of a cyber-attack. Burlington, Ottawa, and the Town of Midland are a few municipalities that have publicly come forward.

Through our Municipal Information Access & Privacy Forum, AMCTO regularly covers topics relating to cyber threats and ransomware attacks where panelists share their insights and first-hand accounts of dealing with an attack. Previous panelists include representatives from the Ontario Provincial Police, insurance company AIG Canada, and staff from municipalities that have been a victim of a cyber-attack.

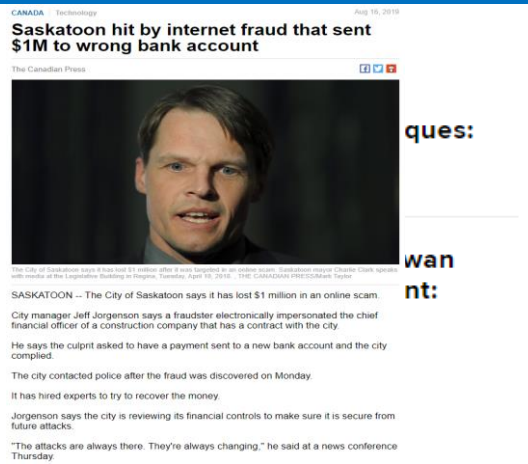
Municipalities must ensure they are aware of the various ways cyber-attackers can target municipalities and have the appropriate infrastructure in place to deter or mitigate such attacks.

To register for AMCTO's upcoming Municipal Information Access & Privacy Forum in November to ensure you and your municipality are equipped to deal with a potential cyber-attack, click here.

For more information, please see below:

Global News: Fraudster hits City of Saskatoon for $1M

CTV News: How other Canadian municipalities lost money to fraudsters and hackers



CANADA · Technology · Aug 16, 2019

Saskatoon hit by internet fraud that sent $1M to wrong bank account

The Canadian Press

The City of Saskatoon says it has lost $1 million after it was targeted in an online scam. Saskatoon mayor Charlie Clark speaks with media at the Legislative Building in Regina, Tuesday, April 16, 2019. THE CANADIAN PRESS/Mark Taylor

SASKATOON -- The City of Saskatoon says it has lost $1 million in an online scam.

City manager Jeff Jorgenson says a fraudster electronically impersonated the chief financial officer of a construction company that has a contract with the city.

He says the culprit asked to have a payment sent to a new bank account and the city complied.

The city contacted police after the fraud was discovered on Monday.

It has hired experts to try to recover the money.

Jorgenson says the city is reviewing its financial controls to make sure it is secure from future attacks.

"The attacks are always there. They're always changing," he said at a news conference Thursday.

ques:

wan

nt:

At a media conference held on the afternoon of Aug. 15, city manager Jeff Jorgenson said a fraudster electronically impersonated the chief financial officer (CFO) of a prominent local construction company and asked for a change in banking information.

READ MORE: Gift card internet scams have cost Edmontonians $683K so far in 2019

"The city complied and as a result, the next (contract) payment intended to go to that company, approximately $1.04 million, was transferred to the fraudster's bank account," Jorgenson said.

"We have no reason to believe that the (construction) company, that this is propagated past the city, we believe that the name used is targeted at the city ... what this was about was effectively identity theft of a real person from an outside agency, the fraudster, so their impersonation of a CFO led to this," Jorgenson said.

The fraudulent activity started a handful of weeks ago, according to Jorgenson.

The city said it notified its internal auditor, Saskatoon Police Service (SPS) and other authorities including banking institutions, after discovering the fraudulent activity on Aug. 12.

University of Saskatchewan

University of Saskatchewan hit with cyberattack

School was able to detect and isolate threat

Morgan Modjeski · CBC News · Posted: Feb 14, 2020 6:00 AM CT | Last Updated: February 14

The University of Saskatchewan was targeted by a cyber attack last week, but the school says its IT was able to detect the threat and isolate the potential for the attack. (Courtney Markewich/CBC)

comments

The University of Saskatchewan was the target of an online denial of service (DoS) attack, becoming the second institution in the province to be hit by cybercrime in as many months.

DoS attacks involve an online perpetrator using a system of computers to overload the system with requests, causing it to crash.

"USask IT security continually monitors our IT services to detect threats and reduce the risk to members of the university community," the University of Saskatchewan said in a statement.

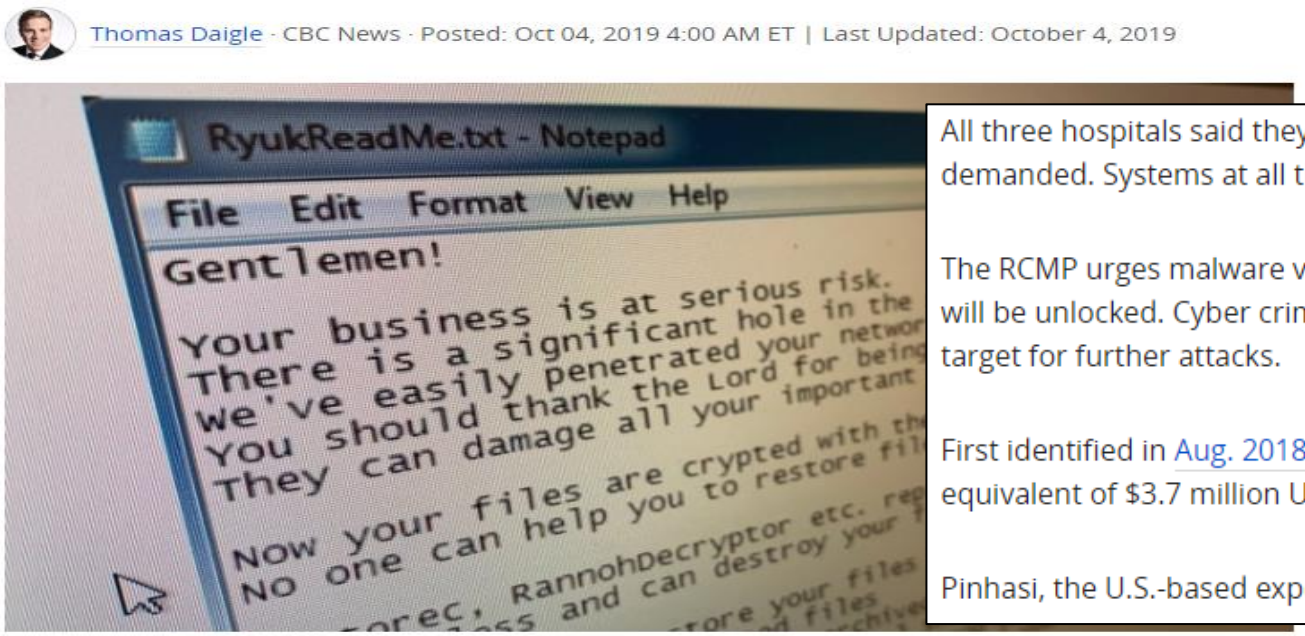
"In this instance we were able to detect the threat and isolate the potential for an attack.“

The U of S noted it continues to introduce new security features "to keep pace with the rapidly changing security environment."

Ontario Hospitals

Here's what we know about the ransomware that hit 3 Ontario hospitals

Malicious software can remain dormant for months



Thomas Daigle · CBC News · Posted: Oct 04, 2019 4:00 AM ET | Last Updated: October 4, 2019

The Ryuk malware is known to store a ransom note in infected computers. (Thomas Daigle/CBC)

comments

Hackers have crippled the computer systems of three Ontario hospitals in recent weeks, prompting concern about the type of malicious software used and whether more facilities may be at risk.

The malware, known as "Ryuk," attacks computer networks but remains invisible to average users for weeks or months. During that time, it collects information about the organization and its perceived ability to pay a ransom.

All three hospitals said they paid no money to retrieve their files and no specific amount was demanded. Systems at all three facilities are in the process of being restored, the hospitals said.

The RCMP urges malware victims not to pay any ransom because there's no guarantee the files will be unlocked. Cyber criminals may even demand more money or identify the victim as a target for further attacks.

First identified in Aug. 2018, cybersecurity experts estimate Ryuk netted hackers the Bitcoin equivalent of $3.7 million US within five months.

Pinhasi, the U.S.-based expert, said the hackers "are sitting on a goldmine."

WannaCry

How the North Korean hackers behind WannaCry got away with a stunning crypto-heist

The so-called Lazarus group has used elaborate phishing schemes and cutting-edge money-laundering tools to steal money for Kim Jong-un's regime.

by **Mike Orcutt** Jan 24, 2020

Cyberattacks waged against cryptocurrency exchanges are now common, but the theft of just over $7 million from the Singapore-based exchange DragonEx last March stands out for at least three reasons.

First there is the extremely elaborate phishing scheme the attackers used to get in, which involved not only fake websites but also fake crypto-trading bots. Then there's slick way they laundered the crypto-cash they stole. Last but not least: they appear to have been working for Kim Jong-un.

WannaCry

U.S. Government Confirms 'Malicious' New Malware Threat: Beware—This Is The WannaCry Hackers Again

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

GETTY IMAGES

If it isn't cybersecurity alerts of malware from one despotic regime, it's warnings relating to another. Just as the world settles down post the Iranian cyber-hype in the aftermath of Suleimani, now multiple U.S. government agencies have warned of a newly intensifying threat from North Korea. Some of the malware is new and some of it is updated. And this particular state-sponsored threat group has pretty terrifying form—remember WannaCry?

The U.S. has shared malware samples on VirusTotal, including the six new variants (Bistromath, Slickshoes, Crowdedflounder, Hotcroissant, Artfulpie and Buffetline) and the seventh, Hoplight, which is an update on a previous strain. If allowed to take root, the various strains of malware enable remote access to machines and networks, the download of further malicious software, as well as the exfiltration of credentials and files.

It is assumed that the same attackers thought responsible for the WannaCry ransomware attack in 2017 are likely behind these latest campaigns—referred to as Lazarus by the private sector and "Hidden Cobra" by the U.S. government.

CISA, the primary U.S. cybersecurity agency responsible for advising industry on new threats and defense recommends the usual mitigation: patching as soon as practically possible; applying strong passwords to file sharing and broader IoT set-ups, including printers and other networked devices; use of updated antivirus software; email defense and user training on unknown senders and attachments; some levels of user monitoring to prevent dangerous activity; and restrictions on external drives and internet software downloads.

And that's the crux here. It actually doesn't matter that this is a state-sponsored campaign, the fact is that these and similar malware strains can be used by both criminal organizations and nation-state threat groups. The mitigating actions are the same. If you follow the advice, you are significantly more likely to escape unscathed. A hardened system is akin to locked doors and windows—you are encouraging the attackers to go try next door.

NotPetya (masqueraded as ransomware, disruption, Russia)

Shipping container firm Maersk, FedEx's Dutch delivery subsidiary TNT Express, and UK firm Reckitt Benckiser were among global firms that suffered severe disruptions and several hundred million dollars in lost revenue. However, the firms however were collateral damage in the ongoing conflict between Ukraine and Russia.

NotPetya employed the NSA exploits for Windows known as EternalBlue and EternalRomance as well as credential-dumping tools to spread internally across networks once one machine was infected. The exploits were leaked in April by The Shadow Brokers.

The malware initially infected organizations via a compromised update from Ukraine accounting software provider MEDoc. Its MEDoc software is one of two accounting packages required for companies doing business in the Ukraine and is widely used by Ukraine agencies.

Maersk, which used MEDoc at its Ukraine offices, recently revealed it was forced to reinstall 45,000 PCs, 4,000 servers and 2,000 applications hit by NotPetya. The company reported losses of $300m due to the incident.

NCSC notes that Ukraine's financial, energy and government institutions bore the brunt of NotPetya. However, the "indiscriminate design" of the malware caused it to spread to other European and Russian businesses.

Though it is unusual to officially blame another nation for a cyberattack, the US and Five-Eye partners blamed the WannaCry ransomware attack on North Korea. The idea, in part at least, is to name and shame nation-state attackers for their actions.

Russia and North Korea have consistently denied responsibility for the NotPetya, WannaCry, and other cyberattacks.

Maersk

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

NotP
code
NotP
irrev
that t
make
conte

$870,000,

Pharmaceutical company Mer

$400,000,

Delivery company FedEx (thro
subsidiary TNT Express)

$384,000,

French construction company

The
was
blas
enti
equ
nuc
ach
vict

$300,000,

Danish shipping company Ma

$188,000,

Snack company Mondelēz (pa
of Nabisco and Cadbury)

$129,000,

prod
costs

British manufacturer Reckitt B
(owner of Lysol and Durex cor

On a national scale, NotPetya was eating Ukraine's computers alive. It would hit at least four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency. "The government was dead," summarizes Ukrainian minister of infrastructure Volodymyr Omelyan. According to ISSP, at least 300 companies were hit, and one senior Ukrainian government official estimated that 10 percent of all computers in the country were wiped. The attack even shut down the computers used by scientists at the Chernobyl cleanup site, 60 miles north of Kiev. "It was a massive bombing of all our systems," Omelyan says.

When Derevianko emerged from the restaurant in the early evening, he stopped to refuel his car and found that the gas station's credit card payment system had been taken out by NotPetya too. With no cash in his pockets, he eyed his gas gauge, wondering if he had enough fuel to reach his village. Across the country, Ukrainians were asking themselves similar questions: whether they had enough money for groceries and gas to last through the blitz, whether they would receive their paychecks and pensions, whether their prescriptions would be filled. By that night, as the outside world was still debating whether NotPetya was criminal ransomware or a weapon of state-sponsored cyberwar, ISSP's staff had already started referring to it as a new kind of phenomenon: a "massive, coordinated cyber invasion."

Atlanta, Baltimore, New Orleans, Florida

CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million

A cyber expert says the report shows the city was forced to make drastic changes

December cyber attack costs New Orleans $7 million, so far

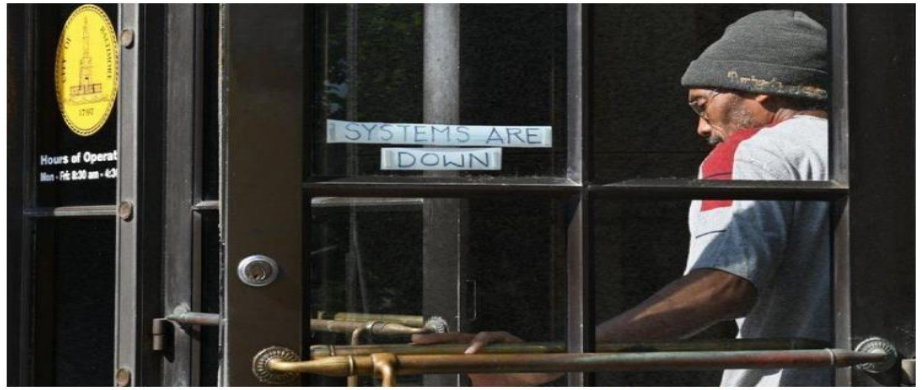
by Filip Truta on January 20, 2020

Employees were told to disconnect all computer systems, including servers, and halt all work. The attackers had made no ransom demands, suggesting the attack was meant to disrupt the city and dent its economy. However, this is not confirmed.

A ransomware attack targeting the city of New Orleans has inflicted $7 million in losses so far, with more to be incurred in coming months, Mayor Latoya Cantrell said in a recent update.

Baltimore acknowledges for first time that data was destroyed in ransomware attack

By IAN DUNCAN
BALTIMORE SUN | SEP 11, 2019 | 4:08 PM



Baltimore's auditor said Wednesday that IT department performance data was lost when hackers locked city files in May — the first disclosure of data being destroyed in the attack.

LATEST POLITICS

POLITICS
Weeks after blasting Baltimore a rodent-infested, Trump to pay a to Charm City
46m

POLITICS
Ruppersberger, Cummings, Sarb call on ICE to end alleged 'bait an switch' practices
1h

POLITICS
Baltimore officials impose rare $40,000 penalty for contractor th failed to meet goal for working w

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems. Wilfredo Lee/Associated Press

Ottawa, Adobe

City of Ottawa treasurer fell victim to US$100K phishing scam: auditor general

BY:
Craig Lord

PUBLISHED:
Apr 8, 2019 3:07pm EDT

3 COMMENTS

SHARE:

TOPIC:
Local > City Hall

ORGANIZATIONS:
Ottawa City Hall

PEOPLE:
Marian Simulik , Ken Hughes , Steve Kanellakos

The City of Ottawa's treasurer fell victim to an increasingly prevalent form of cyber attack last year, costing Ottawa more than $100,000 to a U.S. fraudster, the city's audit committee heard Monday.

The city's auditor general Ken Hughes reported findings from this past year's audits at Monday's meeting as well as an investigation into a reported transfer of funds to a fraudster south of the border.

Hughes confirmed that his investigation found that city treasurer Marian Simulik was scammed into sending roughly US$98,000 from Ottawa's treasury to a fraudulent account in July 2018.

ADOBE DATA BREACH EXPOSED ALMOST 7.5 MILLION CREATIVE CLOUD ACCOUNTS TO THE PUBLIC

October 26, 2019 by Dunja Djudjic · 18 Comments

Adobe was recently hit with a massive data breach, exposing nearly 7.5 million Creative Clouds accounts to the public. Reportedly, a database containing sensitive user info was easily accessible to anyone through a web browser.

According to Mashable, security researcher Bob Diachenko and Comparitech were the first to discover the database. It contained the data for almost 7.5 million Creative Cloud accounts, including the following: email addresses, the Adobe products they are subscribed to, account creation date, subscription and payment status, local time zone, member ID, time of the last login, and whether they were an Adobe employee.

Comparitech claims that Diachenko discovered the open database on 19 October and reach out to Adobe immediately. Adobe acted promptly to address the issue and they secured the database on the same day. After securing the database, Adobe issued a statement regarding the data breach:

BC Municipalities

THE COLUMBIA VALLEY PIONEER

The City of Cranbrook says personal data wasn't compromised following a malware attack in March 2018.

B.C. city's computer system suffered malware attack last year

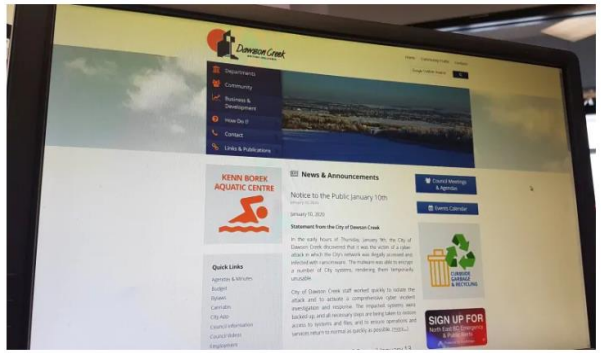
No personal data was compromised when City of Cranbrook was hit by ransomware last spring.

TREVOR CRAWLEY / Jan. 15, 2019 3:15 p.m. / NEWS

Hackers attack City of Dawson Creek's computer systems

Mayor says attack was isolated quickly, no data appears to be lost

Andrew Kurjata · CBC News · Posted: Jan 11, 2020 5:26 PM PT | Last Updated: January 11



The City of Dawson Creek's computer systems were attacked by hackers on Thursday. (Andrew Kurjata/CBC)

City of Dawson Creek a victim of a cyber-attack

Jan 10, 2020

The City of Dawson Creek has discovered that it's the victim of a cyber-attack.

In the early hours of Thursday, January 9, the City's network was illegally accessed and infected with ransomware. The attack encrypted and locked a number of City systems, disabling access to files and data.

Dawson Creek's Mayor, Dale Bumstead, says they haven't been contacted by whoever infected the City, asking for a ransom to unlock the system. He adds that, fortunately, the City has cyber-insurance to help deal with this situation.

"So whenever we're in this situation, we turn it over to the insurers and the experts who have the expertise to be able to deal with, hopefully, the perpetrators, and/or the communications around that in terms of what we need to do in terms of our next steps in recovering access to our system. So that's what they're dealing with right now."

Ransomware attack corrupts many of Squamish's municipal computer server files

District says no personal information was obtained, most files recovered

Steven Chua / Squamish Chief
AUGUST 15, 2019 10:01 AM
UPDATED: AUGUST 15, 2019 10:26 AM

Whistler reports security breach on municipal website

BY LAUREN BOOTHBY
Posted Jan 4, 2019 10:15 pm PST Last Updated Jan 4, 2019 at 10:51 pm PST

(Source: iStock)

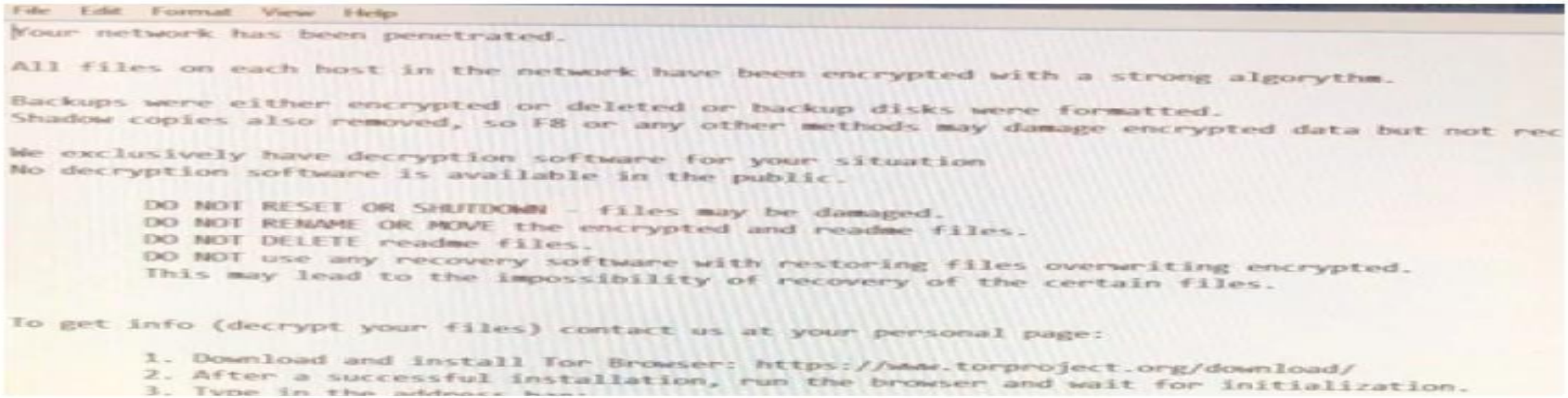
WHISTLER (NEWS 1130) — Whistler says it's website has been hacked.

Nunavut

Nunavut government rebuilding network after ransomware attack

Most government departments and Nunavut communities are affected

Sara Frizzell · CBC News · Posted: Nov 04, 2019 7:01 PM CT | Last Updated: November 4, 2019



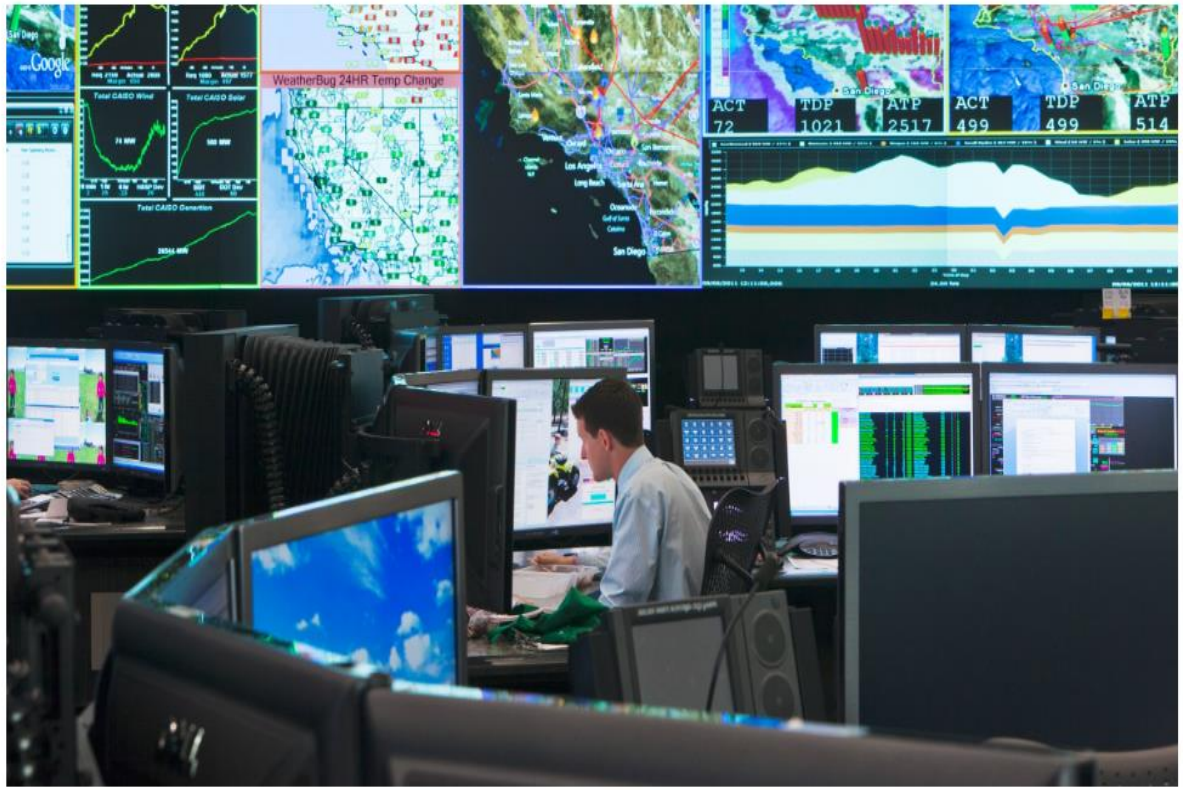
This ransom note appeared on government of Nunavut computers when users attempted to open any files. (Name withheld by request)

The government of Nunavut is rebuilding its communications network after a ransomware attack encrypted its files.

Power Grids

Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities

Exposed Facebook phone numbers, an XKCD breach, and more of the week's top security news.



PHOTOGRAPH: ULLSTEIN BILD/GETTY IMAGES

US and Russia clash over power grid 'hack attacks'

18 June 2019 Share

The complexity of Russia's electricity grid makes it a hard target, says expert

Russia has said it is "possible" that its electrical grid is under cyber-attack by the US.

Kremlin spokesman Dmitry Peskov said reports that US cyber-soldiers had put computer viruses on its electrical grid was a "hypothetical possibility".

His comments came in response to a New York Times (NYT) story which claimed **US military hackers were targeting Russian power plants.**

The report drew scepticism from experts and a denunciation by President Trump.

Ontario Municipalities

Politics

Mayor of latest Canadian town to be hit for online 'ransom' calls for national strategy

'We are all vulnerable,' says Stratford Police Chief Greg Skinner

Katie Simpson · CBC News · Posted: Jun 11, 2019 4:00 PM ET | Last Updated: June 11

Canadian municipalities are "sitting ducks" for "cyber terrorists," says the mayor of Stratford, Ont. — the latest Canadian community to find itself targeted by an online ransom attack.

Dan Mathieson said that if his fellow mayors across the country don't start working together on the problem, more communities may be hit by online extortionists holding municipal data for ransom.

"We're not the first and we definitely won't be the last that will experience something like this," Mathieson told CBC News from his city hall office.

"As long as we are holding information that is deemed to be valuable to attackers ... the new terrorists of the century ... I think we need to find a way to [co-operate]."

On April 14, cyber criminals hijacked part of the city's computer servers, locking out some municipal employees. Stratford Police Chief Greg Skinner confirmed the incident was a 'ransomware' attack.

Cyber attack costs Woodstock more than $660K: Report

Kathleen Saylors

More from Kathleen Saylors

Published on: December 9, 2019 | Last Updated: December 9, 2019 5:57 PM EST

Municipalities, school boards, hospitals and even police forces in Southwestern Ontario have been left reeling by cyber attacks in recent weeks that have crippled their computer systems. (Photo illustration/Getty)

University of Victoria

https://www.woodstocksentinelreview.com/news/local-news/cyber-attack-costs-woodstock-more-than-660k-report

Desjardins (insider!)

National News posted Jun 20, 2019 @ 07:00pm by Megan Trudeau

Desjardins suffers data breach affecting 2.9 million members after inside job

One of Canada's leading financial groups has suffered a massive data breach that affects millions of members.

Desjardins issued a statement today saying that they were contacted by police in Laval, Que. with information confirming that the personal information of more than 2.9 million members had been shared with individuals outside of the organization.

Photo credit: 123RF

The company said that includes 2.7 million individual members and 173,000 business members.

Massive Desjardins breach will happen again due to lax regulations, zero punitive measures: cyber expert

Desjardins data is gone, so what can customers do?

Desjardins to offer all members free, lifelong protection after data breach

Former Desjardins president falls victim to identity theft after data breach

University of Victoria

Capital One (6 million Canadians, cost estimated $150M)

Not a Capital One customer? Your personal information could still have been hacked

Credit card applicant shocked at data breach

A Scarborough man said he was "terribly upset" after his credit card information was hacked, even though he was never a customer.

Pat Foran, Consumer Reporter, CTV News
@PatForanCTVNews

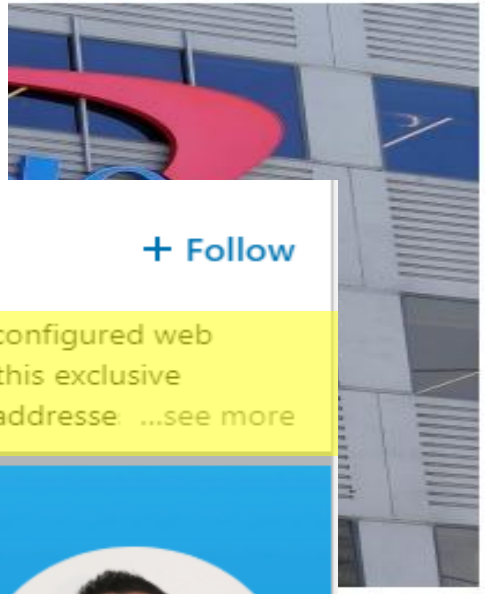
Published Tuesday, September 10, 2019 5:52PM EDT
Last Updated Wednesday, September 11, 2019 1:06PM EDT

A Scarborough man whose application for a Capital One credit card was denied said he was "terribly upset" after he got a letter from the company saying his pe had been breached in a cyber-attack.

About 106 million Capital One customers and applicants had their personal info last month in a data breach including about six-million Canadians. What surpris is that some were affected by the hack even though they were not Capital One

Oliver Williams said he had heard about the data breach at Capital One, but wa as his application for a credit card had been denied.

llions of each



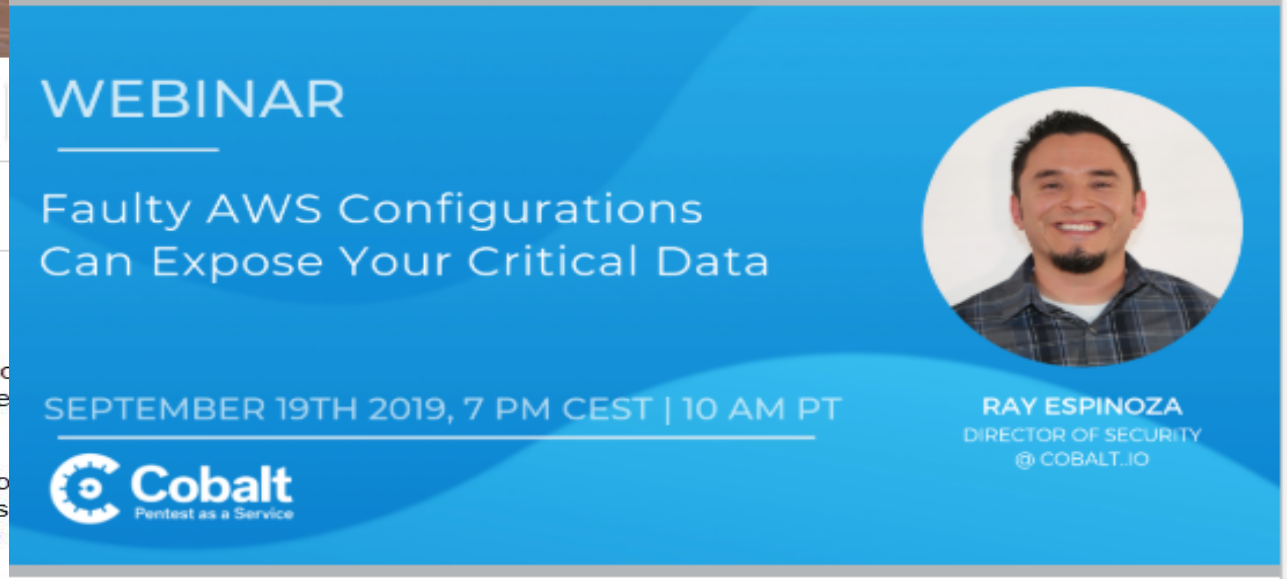
rosecutors
(AP

ed by a

sday.

Cobalt.io
3,426 followers
2d • Edited
+ Follow

Did you know that the Capital One Breach was caused by a misconfigured web application firewall (WAF) hosted in the AWS cloud? Join us for this exclusive webinar with Cobalt's Director of Security, Ray Espinoza, as he addresse ...see more



46 • 3 Comments

Health Breaches

Campbell County Health reported a systemwide crippling of their computers that affected its flagship hospital and nearly 20 clinics located in the city of Gillette. For eight hours, the hospital's emergency department was forced to transfer patients e
away. The health ca
shuttered and som
normal order.

The cause was rans
that doubled acros
McAfee Labs. Toda
America's health ca

But you may be sur
after hackers relea

New research finds
death rate among h
afterward. This inc
perpetrators thems
medications or doctors. Rather the issue may lie with how health care systems adjust their cybersecurity after an attack, according to a study published in October's issue of Health Services Research.

"In spending time in a lot of different health care organizations, what we saw in terms of reactions to breaches was rather predictable — that is, installing better security controls," said Eric Johnson, an IT security researcher and dean of Vanderbilt University's Owen Graduate School of Management who co-led
ıg

They found the time it took for a patient to receive an electrocardiogram increased by as much as 2.7 minutes after a data breach, and this lag remained as high as 2 minutes even after three to four years.

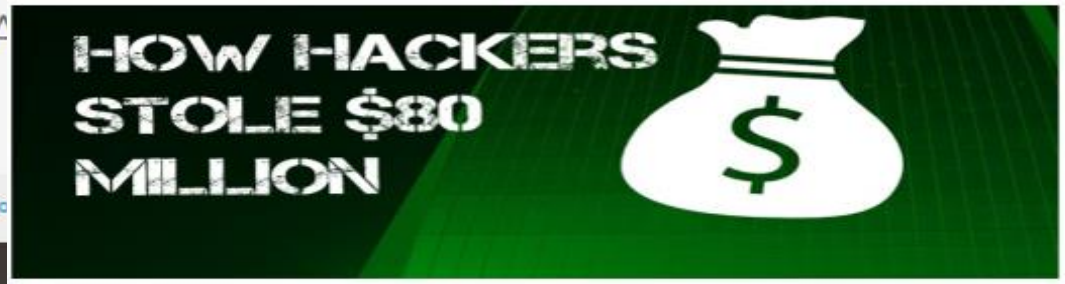
"Our hypothesis is that the time connection is driving the 30-day mortality rates," Johnson said. "There's a clear association for hospitals that saw these breaches. They definitely saw increases in 30-day mortality rate."

> **Cybersecurity remediation at hospitals appears to be slowing down doctors, nurses and other health professionals as they offer emergency cardiac care.**

breaches has risen 20 percent in 2019 compared to all of last year. Those breaches involved the medical records of 38 million health care customers, the largest number since 2015 when massive hacks struck Anthem, Blue Cross, Excellus and UCLA Health System.

University of Victoria

Bangladesh Bank



The recent cyber attack on Bangladesh's central bank that let hackers stole over $80 Million from the Institutes' Federal Reserve bank account was reportedly caused due to the **Malware** installed on the Bank's computer systems.

Few days ago, reports emerged of a group of unknown hackers that broke into Bangladesh's central bank, obtained credentials needed for payment transfers from Federal Reserve Bank of New York and then transferred large sums to fraudulent accounts based in the Philippines and Sri Lanka.

The criminal group was able to steal a total value of about $81 Million from the Federal Reserve's Bangladesh account through a series of fraudulent transactions, but a typo in some transaction prevented a further **$850 Million Heist**.

How a Typo Stopped Hackers from Stealing $1 Billion from Bank

Friday, March 11, 2016 Swati Khandelwal

Here's what actually was happened:

Nearly three dozen requests hit the Federal Reserve Bank of New York on 5 February using the Bangladesh Bank's SWIFT code, out of which four resulted in successful transfers, for a total value of about $81 million.

However, when the hackers attempted to make their fifth transfer of $20 Million to a Sri Lankan non-governmental organization called the **Shalika Foundation**, they made a typo by attempting a transfer to the Shalika "**Fandation.**"

Staff at Deutsche Bank, which was involved in routing funds, spotted this spell error and got asked the Bangladeshis for clarification on the typo. The Bangladesh bank then canceled the remaining transfers.

BANGLADESH BANK
Central Bank of Bangladesh

- most expensive typo in history
- typo between "Foundation" and "Fandation" allowed staff to find the fraud
- bank cancelled remaining transfers of ~$800 million

Canada NRC

Canadian research body relied on paper communications after Chinese hack, documents show

COLIN FREEZE
The Globe and Mail
Published Friday, Sep. 02, 2016 3:57PM EDT
Last updated Friday, Sep. 02, 2016 5:33PM EDT

35 Comments | G+1 6 | Print / License | AA

Upon discovering that it had been hacked by China, the Canadian government's scientific-research body did digital damage control on an enormous scale. Firing up its vintage fax machines, it jettisoned scores of computer servers, bought its staff hundreds of new laptops and drew up a list of about 20,000 corporate partners in Canada whose secrets risked being collateral damage.

Records newly released to The Globe and Mail reveal these and other details about the extensive fallout from this nightmare at the National Research Council. The hack of the NRC was highlighted in July 2014, when the then-Conservative government blamed China, making it the only cyber-espionage campaign that Canada has ever pinned on a specific state adversary.

While hacks of government departments occur relatively routinely, the NRC could be considered a more valuable target than most. For decades, it has been routing tax dollars to fund cutting-edge research in agriculture, engineering and computer science. Placing bets on Canadian companies helps the NRC work to ensure future prosperity, and its staff gets a glimpse of emerging technologies and proprietary business plans.

That's why the Canadian government was alarmed when federal officials announced two years ago that they had "detected and confirmed a cyber intrusion" within the NRC by "a highly sophisticated Chinese state-sponsored actor."

- NRC hack nearly brought agency 'back to the buggy'
- NRC had to 'fire up vintage fax machines'
- "jettisoned scores of servers"
- "only cyber-espionage campaign Canada has ever pinned on a specific state adversary"
- network deemed unfit, thrown away
- replacement >$32M and 4 years to build

Chinese hackers installed malware on National Research Council computers

Canada
CNRC·NRC

Nova Scotia

Nova Scotia freedom of information website hacked

Teen charged after personal information exposed in Nova Scotia government website breach

Halifax police make arrest after 7,000 documents accessed from FOIPOP website

Michael Gorman · CBC News · Posted: Apr 11, 2018 12:33 PM AT | Last Updated: April 11

Internal Services Minister Patricia Arab and deputy minister Jeff Conrad spoke to reporters Wednesday. (CBC)

PEI

P.E.I. government website running again after ransomware attack

P.E.I. government website hit by ransomware attack

Ryan Ross (ryan.ross@theguardian.pe.ca)
Published: 16 hours ago
Updated: 7 hours ago

Casino (IoT…)

Security researchers reveal mystery North American casino was hacked through its connected FISH TANK

- A new report from security firm Darktrace reveals even a fish tank can be hacked
- A North American casino installed a high-tech tank that can control temperature
- But, despite efforts to protect it, it turned out to be a weakness in their network
- Before being stopped, hackers transfered 10GB of data to a device in Finland

How a fish tank helped hack a casino

Criminals Hacked A Fish Tank To Steal Data From A Casino

Smart fish tank exposes casino to hackers

Hacking Nemo: Adversary compromises smart fish tank at casino

Go phish: A smart fish tank let hackers into a casino

The smart fish tank contains sensors to regulate temperature and feeding. The casino used an individual VPN for the tank data, *"to ensure these communications remained separate from the commercial network,"* cybersecurity company Darktrace explained.

Darktrace discovered the tank had been compromised and detected *"highly unusual"* data activity being sent from a device in Finland. The fish tank attack was revealed in its security report published this week.

Ten GB of data had been sent outside the network, and no other company device had been in communication with the Finland location. *"Communications took place on a protocol normally associated with audio and data,"* they explained.

Various

119 service

Network Tallahassee Internet pr hacked, pays ransom to get bac

TaMaryn Waters, Tallahassee Democrat Published 1:34 p.m. ET Feb. 26, 2019

Hackers are busy trying to steal details about your personal and financial life. Here's how to them. DAVID P. WILLIS

CONNECT TWEET LINKEDIN COMMENT EMAIL MORE

Hackers attacked a Tallahassee-based broadband provider and demanded $6 ransom to get its operations back online.

Network Tallahassee's website is down and calls to its landline go directly to a recorded message, explaining how the hacking, which was discovered Saturd compromised its entire network.

"We have been in contact with the hackers and paid the ransom and have bee advised it will be tomorrow, Tuesday (today), before we get the compiled encry tools," the message recorded shortly after 5 p.m. Monday said. "If the hackers it will probably be Wednesday before we are partially back up and running."

500px Hacked: Personal Data for All 14.8 Million Users

FEB 13, 2019 MICHAEL ZHANG

Share 2K Tweet

The popular photo-sharing service 500px has announced that it was the victi and that personal data was exposed for all the roughly 14.8 million accounts t

In an email sent out to users and an announcement posted to its website, 50 only on February 8th, 2019, that its team learned of an unauthorized intrusion occurred on or around July 5th, 2018.

The personal data that may have been stolen by the intruder includes first an usernames, email addresses, password hashes (i.e. not plaintext passwords), country), birth date, and gender.

Israeli cyber-hotline offers help for the hacked

Dan Williams 3 MIN READ

BEERSHEBA, Israel (Reuters) - Israel has launched a cyber hotline, staffed mostly by veterans of military computing units, to enable businesses and private individuals to report suspected hacking and receive real-time solutions.

Lavy Shtokhamer, director of Israel's Computer Emergency Response Centre (CERT) stands in front of screens displaying a world map and other data as employees work at a cyber hotline facility in Beersheba, southern Israel February 14, 2019. REUTERS/Amir Cohen

The 119 call-in number to the Computer Emergency Response Centre (CERT) is being billed by Israel and cyber experts as a world first.

"Our job is to mitigate the damage as quickly as possible, to learn about the threats and to spread the knowledge where relevant," CERT director Lavy Shtokhamer told Reuters at the facility in the southern hi-tech hub city of Beersheba.

"A cyber-attack may not be limited only to property or financial damage. It can also threaten lives."

Various (awareness, patching, offline back

phishing
awareness, patching, offline backups
cloud saved the day

Most Canadians 'likely to encounter' cybercrime, expert says after attack on youth services organization

Marymound, which cares for vulnerable Manitoba kids, says 3rd-party server kept data safe in ransomware attack

Kristin Annable · CBC News · Posted: Feb 27, 2019 5:00 AM CT | Last Updated: February 27

Marymound — which provides services for Manitoba kids through its school, foster homes and community programs — was the target of a ransomware attack earlier this month. (CBC)

Parker said because Marymound's information was backed up to an off-site server, it was secure and could be restored without paying the ransom.

Ontario police warn of recent cyberattacks targeting local governments

Attacks launched through direct hacking into vulnerable systems or through phishing emails, OPP said

The Canadian Press · Posted: Sep 14, 2018 4:39 PM ET | Last Updated: September 14, 2018

The OPP didn't disclose how many municipalities had been temporarily crippled by the ransomware attacks, but at least two recently had their systems compromised and the mayor of one of them said he's heard of multiple cases. (Kacper Pempel/Reuters)

A rash of cyberattacks on Ontario municipal governments in which hackers demand a ransom to unlock compromised systems has prompted the provincial police force to warn about what it describes as a recent trend.

On Sept. 1, officials discovered that many of the town's servers had been compromised and locked down. McKay did not disclose exactly how much ransom was paid through an insurance company to the hackers, and said the cyberattack remains under investigation.

Australia, UK

use of the word ‘sophisticated’
targeted notification warnings
awareness, passwords/MFA, mail security, endpoint security, didn’t say China but came close

‘Sophisticated state actor’ hacks Australia’s political parties months before election

The hacks were discovered during the investigation of a previous attack

By Jon Porter | @JonPorty | Feb 18, 2019, 8:58am EST

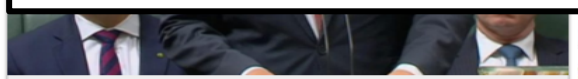
SHARE

Australia cyber hack raises privacy concerns

Brian Pearlman, Nation & World Editor | February 25, 2019

Australia’s Parliament House computer network suffered a “malicious intrusion” on Feb. 8, according to Prime Minister Scott Morrison; on Feb. 18, he revealed before the House of Representatives that a number of specific political parties were hacked as part of that intrusion, among them his own Liberal party, the opposition Labor party and the National party. The attack, he said, was perpetrated by a “sophisticated state actor,” though he added that there was no electoral interference.

The publication adds that just four states — China, Russia, Israel, and the United States — have the capability to perform such an attack.



Australian Broadcasting Corporation Via AP

He did not provide details on what information was stolen in the breach.

Speculation began almost immediately that China may have been responsible, with senior intelligence sources telling the Sydney Morning Herald that the malware used in the attack suggests the work of China or Russia. China is believed to be responsible for previous hacks against Australia’s government networks in 2011 and 2015.

At a Feb. 18 media briefing, Chinese foreign ministry spokesman Geng Shuang warned that, “Irresponsible reporting, accusation, pressure and sanctions will only aggravate the tension and confrontation in cyberspace and poison the environment of cooperation.” He made similar comments later in the week, stressing that “a sound and stable China-Australia relationship serves the common interests of both countries and peoples.”

Iran-backed hackers hit both U.K., Australian parliaments, says report

The cybersecurity firm Resecurity has connected a 2017 attack on the U.K. Parliament with the February hack of the Australian Parliament.

The Iranian flag Ronald Zak / AP file

Feb. 28, 2019, 11:54 AM PST

By Ken Dilanian

WASHINGTON – The Iranian-backed hackers who stole personal data on Australian lawmakers earlier this year are the same group that attacked the British Parliament in 2017, according to new research by a cybersecurity firm that sheds light on Iran’s campaign of cyberespionage against its adversaries.

Using brute force attacks that guessed passwords, the hackers obtained thousands of records from both parliaments containing names, email addresses, birthdates and other information on lawmakers and their staff.

Various (awareness, patching, offline backups)

ransomware, got files back
awareness, patching, offline backups
threats to military systems

Hack of Melbourne medical records shows risk to health data

By Elise Thomas
Updated Tue at 5:34pm

PHOTO: Lockers effectively lock the legitimate users out of their own system entirely. (ABC News: Nic MacBean)

Are you worried about your medical records falling into the wrong hands?

RELATED STORY: My Health Record opt-outs top 2.5 million

RELATED STORY: Hackers want your medical records far more than your credit card info

RELATED STORY: My Health confusion — how is a privacy breach defined anyway?

For patients at the cardiology private practice Melbourne Heart Group, that scenario may have just become a reality after a ransomware attack saw their medical files hacked and scrambled.

It's unclear whether the private practice has paid a ransom to the attackers, but weeks later many of the files have not been recovered.

What's in those files? Only some of the most lucrative information for those who might want to pursue identity theft.

The ransomware attack shows just how vulnerable our health institutions can be, in a month where opt-outs of the My Health Record scheme ticked over to 2.5 million Australians.

Iranian Hackers Drew Worryingly Close to Israel's Missile Alarm

By Gwen Ackerman
February 24, 2019, 2:00 PM PST *Updated on February 24, 2019, 11:40 PM PST*

- Global effort needed against Iran cyber attacks: cyber chief
- Israel's cyber defense focused largely on Ira and its proxies

Netanyahu stands near a naval Iron Dome defence system on Feb. 12. *Photographer: Jack Guez/AFP via Getty Images*

SHARE THIS ARTICLE
Share
Tweet
Post
Email

In this article

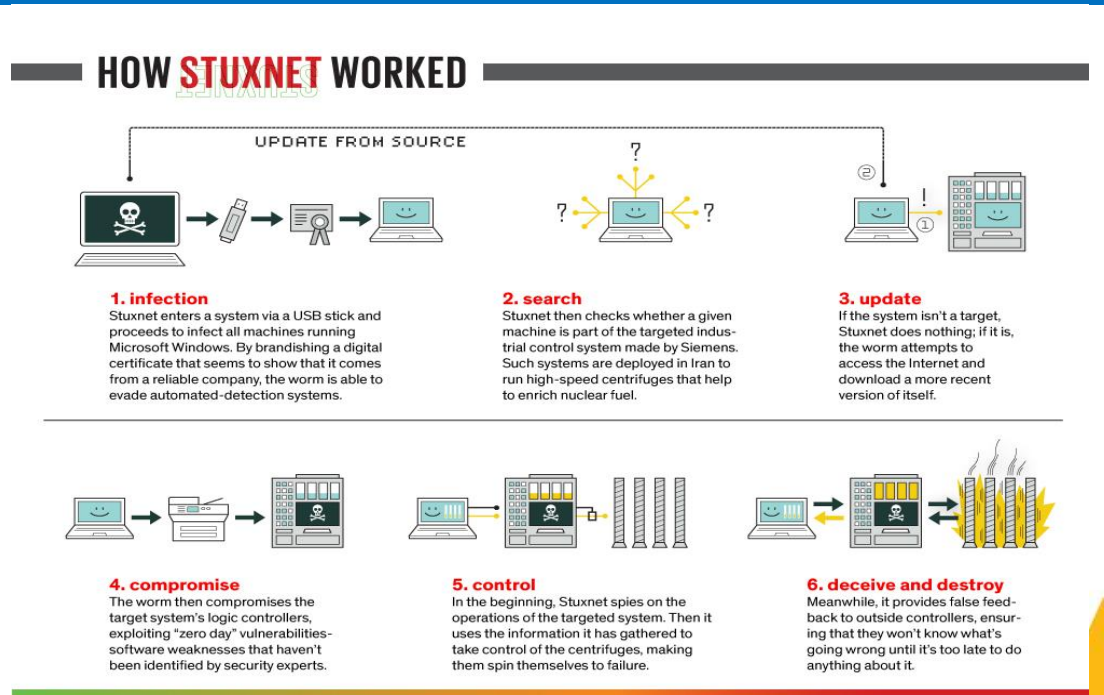
Iranian hackers came worryingly close to Israel's missile warning system, sending the military scrambling to protect alerts from being compromised, its top cyber defense chief said.

After detecting the hackers in 2017 and monitoring them to discern their intent, the military blocked them when it became clear what their target was, said Brigadier General Noam Shaar, outgoing head of the cyber defense division in the army's Cyber Defense Directorate.

Stuxnet (Awareness)

awareness, no USB
Israel, US

- first cyber weapon given physical destruction
- reportedly developed by US and Israel
- targeted programmable logic controllers (PLCs)
- introduced by USB
- worm executed payload
- LNK files and propagation
- rootkit to hide files and processes
- reports that it was unintentionally released in the wild when engineer connected work laptop to home network



University of Victoria

Cyberattack that crippled Ukrainian power grid was highly coordinated

1st power outage caused by cyberattack suggests similar attacks possible around the globe

Thomson Reuters | Posted: Jan 11, 2016 11:52 AM ET | Last Updated: Jan 11, 2016 12:17 PM ET

Hackers did indeed cause Ukrainian power outage, US report concludes

DHS officials say well-coordinated hack cut power to 225,000 people.

by **Dan Goodin** - Feb 26, 2016 11:14am PST

Share Tweet Email 32

Hackers Infiltrated Ukrainian Power Grid Months Before Cyber-Attack

By Robert Lemos | Posted 2016-03-23 Print

Tweet LinkedIn 78 Like 8 G+ Shar 1 Share 86 Email

Attackers controlled some systems within three Ukrainian power companies' networks for more than six months, a fact only revealed after they cut power to more than 225,000 people in December 2015.

The cyber-attackers that targeted Ukraine's energy distribution infrastructure in December were "highly structured and resourced," taking down than 27 substations in an attack against Ukrainian power companies, according to a report released by the Electricity Information Sharing and Analysis Center (E-ISAC) on March 21.

DHS: CYBERATTACK ON THE UKRAINE POWER GRID COULD HAPPEN HERE

Ukraine Power Grid (patching, awa

patching, awareness
elections
Russia

Ukraine reports cyb
country's election c

18:45, 26 February 2019 POLITICS

Ukraine has already devel
servers.

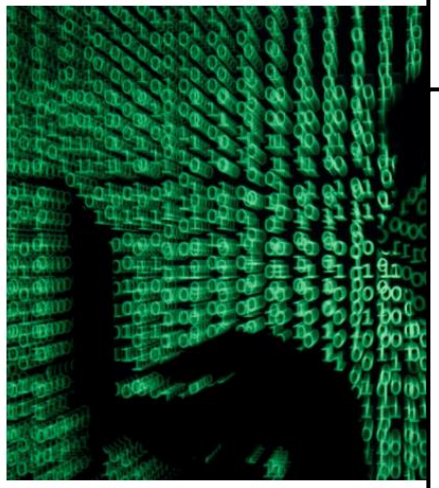
President Petro Poroshenko on
24-25 on the servers of the Cen

The attacks were launched fro
representatives of the IT indus

U.S. Cyber Command operatic
access of Russian troll factory
midterms – The Washington P

21:45, 26 February 2019 WORLD 601 0

The operation marked the first muscle-f
Command, with intelligence from the N



REUTERS

The U.S. military blocked Internet access to an i
sow discord among Americans during the 2018 r
said, a warning that the group's operations agai
free.

Exclusive: Ukraine says
cyber attacks targeting

Pavel Polityuk

KIEV (Reuters) - Hackers likely controlled by R
Ukraine's presidential election in March with cy
personal computers of election staff, the head o

Serhiy Demedyuk told Reuters the attackers we
shopping invitations, offers for software update
material intended to steal passwords and perso

Ten weeks before the elections, hackers were al
officials, Demedyuk said, paying in cryptocurre
accessible only through certain software and ty

"There are constant attacks - they go from simp
or another employee uses," he said, adding they
the country's energy, transport and banking sys

"Payment occurs in cryptocurrency in most cas
were used to finance the previous attacks. This
organizations that are under the control of Russ
this," Demedyuk said.

18:45, 26 February 2019 POLITICS 548 0

Ukraine has already developed a cyber defense mechanism for CEC servers.

REUTERS

President Petro Poroshenko on Tuesday said cyber attacks had been recorded Feb 24-25 on the servers of the Central Election Commission.

The attacks were launched from Russia, Poroshenko told a Kyiv meeting with representatives of the IT industry, according to an UNIAN correspondent.

Poroshenko noted that earlier this morning, he had visited the General Staff of the Armed Forces of Ukraine where he met with commanders of various levels.

How Ukraine became a test bed for cyberweaponry

As Russian hackers face down Western spies, the country has become a live-fire space for hackers.

By LAURENS CERULUS | 2/14/19, 11:30 AM CET | Updated 2/20/19, 4:13 AM CET

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

University of Victoria

Atlanta (awareness, patching, backup

ransomware (SamSam brute-forces pws)
awareness, patching, offline backups
Iranian charged

The damage from Atlanta's huge cyberattack is even worse than the city first thought

Taylor Hatmaker @tayhatmaker / 9 months ago

Comment

The ransomware is believed to be from the group known as SamSam, which has been operating and executing similar attacks since at least 2015.

In the days following the March 22 incident, Atlanta residents were unable to do simple city system-dependent tasks like paying parking tickets or utility bills. City employees didn't get the all-clear to turn on their computers until five days later and many city systems still have not recovered.

On Wednesday during a budget meeting, Daphne Rackley, Atlanta's Interim Chief Information Officer and head of Atlanta Information Management, disclosed new details about the extent of the damage. As Reuters reports, at least one third of the 424 software programs that the city runs remain offline or partially inoperable. Almost 30 percent of those programs are deemed "mission critical" by the city meaning that they control crucial city services like the court system and law enforcement. In the meeting, Rackley explained that the city initially believed only

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

s the city worked to available.

244

he word on urn their

But as the city government's desktops, hard drives and printers flickered back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi.

Atlanta's municipal government has been brought to its knees since Thursday morning by a ransomware attack — one of the most sustained and consequential cyberattacks ever mounted against a major American city.

Feds: Iranians led cyberattack against Atlanta, other U.S. entities

DoorDash

The food delivery company said in a blog post Thursday that 4.9 million customers, delivery workers and merchants had their information stolen by hackers.

The breach happened on May 4, the company said, but added that customers who joined after April 5, 2018 are not affected by the breach.

It's not clear why it took almost five months for DoorDash to detect the breach.

DoorDash spokesperson Mattie Magdovitz blamed the breach on "a third-party service provider," but the third-party was not named. "We immediately launched an investigation and outside security experts were engaged to assess what occurred," she said.

Users who joined the platform before April 5, 2018 had their name, email and delivery addresses, order history, phone numbers and hashed and salted passwords stolen.

The company also said consumers had the last four digits of their payment cards taken, though full numbers and card verification values (CVV) were not taken. Both delivery workers and merchants had the last four digits of their bank account numbers stolen. Around 100,000 delivery workers also had their driver's license information stolen in the breach.

The news comes almost exactly a year after DoorDash customers complained that their accounts had been hacked. The company at the time denied a data breach and claimed attackers were running credential stuffing attacks, in which hackers take lists of stolen usernames and passwords and try them on other sites that use the same passwords. But many of the customers we spoke to said their passwords were unique to DoorDash, ruling out such an attack.

Company	Rec	Year	Notes
Yahoo	3B	2013	breaks previous record for largest breach; Verizon acquired; data bought; password reuse
Marriott	500M	2018	Marriott discovered [China]
Yahoo	500M	2014	reset password, or find a new provider….
Adult Friend Finder	412M	2016	included deleted accounts, vulnerability – remote code execution; passwords cracked
American Biz	160M	2012	Nasdaq, 7-11, various others
Adobe	152M	2013	questionable encryption, quick to reset passwords, data posted online, 10G
Under Armour	150M	2018	MyFitnessPal; good password management, strong encryption, rapid notification
eBay	145M	2014	stole encrypted passwords and personal information, no financial info, **password reuse**
Equifax	143M	2017	half the US population, various bungles, delayed notification, sold shares,
Quora	100M	2018	I didn't know people actually had accounts here. ☺
TJ Maxx	94M	2007	wardriving + WiFi + WEP + carding = Rolex
AOL	92M	2004	AOL worker sold 92 million names used to promote gambling site, used coworkers access
Anthem	80M	2015	paid $16M in settlement with government and $115M to class action suit [China]
Sony	70M	2011	repeat breaches; The Interview; 40G leaked; employee data, internal emails, IP, movies
JP Morgan	76M	2014	actually 83M – 76M personal, 7M small business; JP discovered [Israel]
Target	70M	2014	supply chain compromised; HVAC vendor; BlackPOS malware
Tumblr	66M	2013	user information stolen, passwords were salted and hashed
Uber	57M	2017	paid criminals $100k to delete data and coverup; paid $148M penalty
Home Depot	56M	2014	unique custom built malware; cost $179 million; $27 million fine
Facebook	50M	2018	3 vulnerabilities introduced in video uploader
Evernote	50M	2013	waterholing – developers go to website frequented by developers
Living Social	50M	2013	likely web app vulnerability or possibly SQL injection
Ashley Madison	32M	2015	no account verification, guilty until innocent, infidelity, bogus accounts, bounty [Impact]
US Office of PM	21.5	2015	government staff, including passports, security clearance, and fingerprints [China]

Yahoo

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

After years of struggling, Yahoo sold itself to Verizon for $4.48 billion. But the deal was nearly derailed by the disclosure of breaches that Yahoo had suffered. David Ramos/Bloomberg

By Nicole Perlroth

Oct. 3, 2017

12

It was the biggest known breach of a company's computer network. And now, it is even bigger.

In March, the **Department of Justice charged four men, including two Russian intelligence officers, with the 2014 breach**. Investigators said the Russian government used stolen Yahoo data to spy on a range of targets in the United States, including White House and military officials, bank executives and even a gambling regulator in Nevada, according to an indictment.

The stolen data was also used to spy on Russian government officials and business executives, federal prosecutors said.

What made that theft particularly egregious, Justice Department officials said, **was that the two intelligence officers who were indicted had worked for an arm of Russia's Federal Security Service,** or F.S.B., that is charged with helping foreign intelligence agencies track cybercriminals.

Yahoo confirms 'state-sponsored' hackers stole personal data from 500m accounts

Details including names, passwords, email addresses, phone numbers and security questions were taken from the company's network in late 2014

Yahoo is investigating the breach with law enforcement but currently believes that credit card or bank details were not included in the stolen data. Photograph: Ethan Miller/Getty Images

Hackers stole the personal data associated with at least 500m Yahoo accounts, the Sunnyvale, California-based company confirmed on Thursday.

Yahoo

Yahoo Breach Payout: How To Claim Up To $25,000 Before The Deadline

Kate O'Flaherty Senior Contributor
Cybersecurity
I'm a cybersecurity journalist.

If you had a Yahoo account back when the firm was breached in 2016, you may be eligible for up to ... [+] NURPHOTO VIA GETTY IMAGES

The Yahoo breach is known as one of the worst of all time, partly because of its size. When the firm was hacked twice in 2016, all of Yahoo's 3 billion users were affected. Worse still, hackers had stolen highly sensitive information including names, security questions and answers, and passwords.

It's only fair, then, that those impacted are given compensation of some kind. Last year, Yahoo said it would pay up to $25,000 to each person affected by the breach, with $100 or free credit monitoring available to most users. It is part of a $117.5 million breach settlement for 194 million people.

The higher $25,000 is available if you can prove the financial damage you suffered due to the Yahoo hack. You are eligible for the $100 payout if you can prove you already have credit monitoring in place. Last week, you might have received an email telling you more about the Yahoo payout. The deadline of July 20 this year is getting closer, so what better time to apply for your compensation? Here's what you need to do.

Marriott's breach respons
experts are filling in the ga

Zack Whittaker @zackwhittaker / 2 days ago

Last Friday, Marriott sent out millions of emails warning
reservations had been stolen from its Starwood databa

One problem: the email sender's domain didn't look lik

Marriott sent its notification email from "email-marriott.c
behalf of the hotel chain giant. But there was little else
doesn't load or have an identifying HTTPS certificate. I
real, except a buried note on Marriott's data breach not

But what makes matters worse is that the email is easil

Often what happens after a data breach, scammers wil
over their private information with their own stream of f
think. People who think they're at risk after a breach ar

Marriot
More T

David V
Manufac
I am an e

Signage on a door to a
Starwood's reservatior
many as 500 million g
BLOOMBERG FINANCE LP

Marriott Interna
a billion guests, l
that's incredibly
defend where we
our heads when

The company no
subsequently fall

Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

Marriott and Starwood's challenges with cybersecurity go back years, cybersecurity researchers say. AFP/GETTY IMAGES

On Friday, hospitality giant Marriott revealed a massive hack led to the theft of personal data of a whopping 500 million customers of its Starwood hotels.

t Data Breach Is Traced
se
Cr

detected during/after merger

blamed on China

hat the Marriott's computer systems had been breached, there was
: the hacking was part of a broad spy campaign to amass Americans' personal
ges

ger, Nicole Perlroth, Glenn Thrush and Alan Rappeport

316

閱讀繁體中文版

ON — The cyberattack on the Marriott hotel chain that
sonal details of roughly 500 million guests was part of a
ligence-gathering effort that also hacked health insurers
ity clearance files of millions more Americans, according
briefed on the investigation.

AdultFriendFinder

vulnerabilities
poor password management, weak hash

AdultFriendFinder data breach – you need to know

GRAHAM CLULEY | Follow @gcluley

NOV 14, 2016 | IT SECURITY AND DATA PROTECTION

What has happened?

The AdultFriendFinder website appears to have been hacked, exposing the personal info of millions of user accounts.

What is AdultFriendFinder?

I don't want to be indelicate, so I'll just tell you it's strapline: "Hookup, Find Sex or Meet Someone Hot Now".

Are passwords at risk too?

Yes. It appears that many of the passwords appear to have been stored in the database in plaintext. Also, most of the others were hashed weakly using SHA1 and have already been cracked.

A quick look at the passwords that have been exposed, sorted by popularity, tells a familiarly depressing tale.

Rank	Password	Frequency
1	123456	900,420
2	12345	635,995
3	123456789	585,150
4	12345678	145,867
5	1234567890	133,414
6	1234567	112,956
7	password	101,046
8	qwerty	86,050
9	qwertyuiop	43,755
10	987654321	40,627

Those are terrible passwords! Why do people choose such lousy passwords?

AdultFriendFinder network hack exposes 412 million accounts

Almost every account password was cracked, thanks to the company's poor security practices. Even "deleted" accounts were found in the breach.

By Zack Whittaker for Zero Day | November 13, 2016 -- 14:00 GMT (06:00 PST) | Topic: Security

ing and entertainment company Friend Finder
on accounts.

om AdultFriendFinder.com, which the company
swinger community."

" accounts that wasn't purged from the databases.

ams.com, and 7
as well as a few
ed by the company.

of data from the
ch notification

time as one security
a local file inclusion
f successfully
tely run malicious

st recent hack. When asked, Revolver denied he was behind the data breach, and instead blamed users of an underground Russian hacking site.

SECURITY IN 2016

These were the biggest hacks, leaks and data breaches of 2016

And the list of attacks keeps getting longer...

Read More

Adobe

poor practices… vulnerabilities
passwords, same encryption key
not nation-state

Adobe hack: At least 38 breached

30 October 2013

Adobe has confirmed that a recent cyber-attack compromised many more customer accounts than first reported.

The software-maker said that it now believed usernames and encrypted passwords had been stolen from about 38 million of its active users.

It added that the attackers had also accessed details from an unspecified number of accounts that had been unused for two or more years.

The firm had originally said 2.9 million accounts had been affected.

Adobe has also announced that the hackers stole parts of the source code to Photoshop, its popular picture-editing program.

It had previously revealed that the source code for its editing software and ColdFusion web application creation product. The attackers are believed to be the same criminals that hacked other entities, including LexisNexis, the National White Collar Crime Center and, most recently, PR Newswire.

illegally accessed.

Adobe sai
been stole

Adobe pays US$1.2M plus settlemen to end 2013 breach class action

Popped Photoshop factory happy to see court case end.

By Darren Pauli 17 Aug 2015 at 06:58 10 SHARE ▼

Adobe has paid an undisclosed amount to settle customer claims and faces US$1.2 million in legal fees after its 2013 data breach which compromised the details of 38 million users.

The creative content king was served a November 2013 class action lawsuit filed in California in which it is claimed "shoddy" security practises lead to the breach.

The breach occurred when hackers raided a backup server on which they found, and subsequently published, a 3.8GB file containing 152 million usernames and poorly-encrypted passwords, plus customers' credit card numbers.

Adobe initially reported the breach affecting three million users and later increased that figure to 38 million.

The company knew its security practices at the time were poor since it used the same encryption key for all passwords.

bacts closer to 38 million

cted in a breach disclosed earlier this month has skyrocketed to
times the roughly three million affected users the company

pokesperson, told SCMagazine.com in a emailed statement that
ing the roughly 38 million impacted customers.

here has been unauthorized activity on any Adobe ID account

inactive Adobe IDs, Edell said, as well as invalid encrypted
dded that Adobe is in the process of notifying those customers
her those users are active or not, have been reset.

Holden, CISO at Hold Security, aided Adobe in responding to the

able file hosted on AnonNews.org this weekend contained 150
assword pairs. He said the 3.8 GB file, which has since been
iscovered by he and Holden earlier this month.

UnderArmour

reported fast, good segmented
good password encryption… for some
others were simply SHA-1 hash
SHA stands for Secure Hashing Algorithm
it is no longer secure

Under Armour says data b affected about 150 million MyFitnessPal accounts

- The breach affected an estimated 150 million users of its food ar application, MyFitnessPal.
- The investigation indicates that affected information may include email addresses, and hashed passwords.

Chloe Aiello | @chlobo_ilo
Published 4:38 PM ET Thu, 29 March 2018 | Updated 8:20 PM ET Thu, 29 March 2018

CNBC

Shares of Under Armour dropped 3.8 percent, before p after the active-wear company informed users of its on and nutrition website their data had been compromise

Under Armour announced on Thursday that the breach estimated 150 million users of its food and nutrition ap MyFitnessPal.

LILY HAY NEWMAN SECURITY 03.30.18 06:10 PM

THE UNDER ARMOU EVEN WORSE THAN BE

Given how many high-profile data bre significant damage over the years, it' that hold sensitive data to build their limit the potential fallout. On that fro hack incident contains some (relative intrusion only exposed usernames, e passwords, indicating that Under Arr least segmented enough to protect th birthdays, location information, or cr from being scooped up. And the comp breach occurred in late February and March 25, meaning it did a public disc That's laudably fast; remember, Uber up to its data-theft woes.

Under Armour also said that it had us password hashing function "bcrypt" passwords it stored into chaotic, unir of characters. When implemented pro cryptographic process makes it incre time-consuming for attackers to atte passwords and revert them to their u bcrypt hashing, a strong password ca break, if not longer. As a result, even passwords leak they are still protecte

'You get some amateur hour stuff.'

—MATTHEW GREEN, JOHNS HOPKINS UNIVERSITY

Here's where things get hairy, though. While Under Armour says it protected "the majority" of the passwords with bcrypt, the remainder weren't nearly so lucky. Instead, in a Q&A site about the breach, Under Armour admitted that some proportion of the exposed passwords were only hashed using a notoriously weak function called SHA-1, which has had known flaws for a decade and was further discredited by research findings last year. "The MyFitnessPal account information that was not protected using bcrypt was protected with SHA-1, a 160-bit hashing function," Under Armour wrote in the Q&A.

"Bcrypt is designed to be extremely slow and SHA-1 is designed to be extremely fast," says Kenneth White, director of the Open Crypto Audit Project. SHA-1 requires less computing resources devoted to implementing and managing a hashing scheme, making it an appealing option —especially if you don't understand the tradeoff you're making. "The vast majority of developers [just] think they're both types of hashes."

The speed hit is well worth it from a security standpoint, though.

eBay

swift disclosure
3 employees credentials led to issues
awareness, passwords

Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees

Jim Finkle and Deepa Seetharaman May 27, 2014, 6:02 AM

BOSTON/SAN FRANCISCO (Reuters) - EBay Inc initially believed that its customers' data was safe as forensic investigators reviewed a network security breach discovered in early May and made public this week, a senior executive told Reuters on Friday.

How ebay sees the future of commerce Glassdoor/eBay

EBay has come under fire over its handling of the cyberattack, in which hackers accessed personal data of all 145 million users, ranking it among the biggest such attacks launched on a corporation to date.

"For a very long period of time we did not believe that there was any eBay customer data compromised," global marketplaces chief Devin Wenig said, in the first comments by a top eBay executive since the e-commerce company disclosed the breach on Wednesday.

EBay moved "swiftly to disclose" the breach after it realized customer data was involved, he said.
Wenig would not say when the company first realized that the cyberattackers accessed customer data, nor how long it took to prepare Wednesday's announcement.
He said hackers got in using the credentials of three corporate employees, eventually making their way to the user database.
Hackers accessed email addresses and encrypted passwords belonging to all eBay users. "Millions" of users have since reset their passwords and the company had begun notifying users, though it would take some time to complete that task, Wenig said.

Equifax data breach a 'digital disaster' for Canadians

Columnist David Shipley weighs in on the Equifax data breach announced last week

By David Shipley, CBC News · Posted: Sep 17, 2017 8:00 AM AT | Last Updated: Sep 17, 2017 8:00 AM AT

The Canadian Automobile Association informed thousands of its members last week that their personal information may have been compromised as a result of the cyberhack on Equifax. (Brendan McDermid/Reuters)

patching, patching, patching

- industry
- began mid-May
- patch available March
- handling
  - notification (6 weeks)
  - new site vulnerabilities & credentials
  - executives
  - CISO

x2

The Equifax Breach and 5 Years of Missed Warning Signs

Equifax faces mounting pressure after data breach as CAA reveals 10,000 clients hit

"Equifax has not been forthcoming with information to us," a CAA spokesperson said

Nearly 40 states probe Equifax's handling of massive data breach

University

Canadian privacy commissioner launches probe of Equifax breach

Equifax Data Breach: Stock Price Falls as Criticism Mounts

Equifax data breach likely touched millions of Canadians

Equifax CEO out amid fallout from data breach

Class action lawsuits

Its stock has lost a third of its value — a $5.5-billion setback.

Equifax tried to appease incensed lawmakers, consumers and investors by announcing the unceremonious retirement of its chief security officer and chief information officer, who were responsible for managing and protecting the company's technology. But that wasn't enough, with lawmakers drawing up bills that would impose sweeping reforms on Equifax and its two main rivals, Experian and TransUnion.

Breach preventable

Equifax CEO suddenly 'retires' following an epic data breach affecting up to 143 million people

Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack

Equifax

Equifax used default 'admin' password to secure hacked portal

Lawsuit claims firm failed to take even 'the most basic precautions'

Always. Change. The. Default. Credentials

EQUIFAX STAFFERS used the default 'admin' username and password to secure a portal containing sensitive customer information.

That's according to a **class-action lawsuit launched against the company in the US**, claiming securities fraud by the company over the 2017 data breach that spilled information on **around 148 million accounts of people in the US, Canada and the UK**.

"This case arises out of a massive data breach incident. The plaintiff alleges that the defendants committed fraud in connection with the data breach that caused a loss in value of [Equifax shares]," claims the lawsuit.

It alleges the company made "multiple false and misleading statements and omissions about the sensitive personal information in Equifax's custody, the vulnerability of its internal systems to cyber attack, and its compliance with data protection laws and cybersecurity best practices".

The lawsuit goes on to claim that the company failed to take even "the most basic precautions to protect its computer systems from hackers".

These include failing to ensure staff used adequate authentication measures to secure systems. "Equifax's authentication measures were insufficient to protect the sensitive personal data in its custody from unauthorised access", the report continues.

"These mechanisms included weak passwords and security questions. For example, Equifax relied upon four-digit PINs derived from [US] Social Security numbers and birthdays to guard personal information, despite the fact that these passwords had already been compromised in previous breaches.

"Furthermore, Equifax employed the user name 'admin' and the password 'admin' to protect a portal used to manage credit disputes. This portal contained a vast trove of personal information."

University of Victoria

Equifax 2020 (patching, China)

America's Hopele … of the Largest Personal-

The government has indicted f… acking into the credit-reporting agency Equifax. The …

FEBRUARY 12, 2020

Robert D. Williams

Executive director of the Paul Tsai China Ce…
at Yale Law School

It doesn't matter if China hacked Equifax

Hop on the cybersecurity hayride from hell.

Violet Blue, @violetblue
02.14.20

323
Shares

E STORIES

…iavirus Quarantine …ica Could Be a Giant …ess

…PRICE

…vate Equity Ruined …d Grocery Chain

…PPELBAUM AND …W. PARK

…e That Conservative …s Really Do Self-

…RIEDERSDORF

Equifax

- “The company made more money in 2018 than it did in 2017, and it made more in 2017 than it did in 2016.”
- Prosecutors say they exploited a software vulnerability to gain access to Equifax’s computers, obtaining log-in credentials that they used to navigate databases and review records. They also took steps to cover their tracks, the indictment says, wiping log files on a daily basis and routing traffic through about three dozen servers in nearly 20 countries.
- Besides stealing personal information, the hackers also made off with some of the company’s sensitive trade secrets, including database designs, law enforcement officials said.
- Equifax, headquartered in Atlanta, maintains a massive repository of consumer information that it sells to businesses looking to verify identities or assess creditworthiness. All told, the indictment says, the company holds information on hundreds of millions of people in America and abroad.

Experts and U.S. officials say the Equifax theft is consistent with the Chinese government's interest in accumulating as much information about Americans as possible.

The case resembles a 2014 indictment that accused five members of the PLA of hacking into American corporations to steal trade secrets. U.S. authorities also suspect China in the 2015 breach of the federal Office of Personnel Management and of intrusions into the Marriott hotel chain and health insurer Anthem.

This is why it is so upsetting that the US government has been so feckless when it comes to protecting our data. For years tech companies have been lobbying against privacy and cybersecurity legislation on a federal level. And that — combined with a Republican Party captured by a near-religious anti-regulatory mania — basically left a key under the mat for the Chinese military to walk right in and loot an American company.

What's more, corporate carelessness in data-breach situations basically goes unpunished, so there's no deterrent for stupid behavior. Equifax's stock took a hit after it announced the hacking (two months after it happened, I might add), but it has since fully recovered and then some. The breach was a blip.

Equifax

- what information was stolen
- what was done with it?
- “Equifax tried to blame the breach on a single vulnerability in Apache Struts; Apache wasted no time releasing a statement showing Equifax was to blame for not patching it. The company had been notified about it six months before the alleged incident occurred.”
- “within an hour of the breach's public admission, information emerged that three Equifax executives sold stock just before the breach and after the company had internal knowledge of the incident (a month prior to the public acknowledgement).”

Equifax

From any angle, we consumers – none of whom consented to being in Equifax's databases – got the worst of it. Equifax was pwned in a completely stupid and avoidable way and are now the biggest plop in the swirling toilet bowl of our modern privacy apocalypse.

Eventually, one big class-action lawsuit revealed that wasn't all: we found out Equifax used 'admin' as a username and password internally.

But okay. They want us to blame China.

The breach earned Equifax a lot of public humiliation – besides all the bad press, at least 240 lawsuits were filed. Still, it seemed like the company liked that sort of thing. Security company FireEye quietly removed its boasting about protecting Equifax from its website, but was still hired to handle Equifax's incident response.

Equifax's response to everything was a masterclass in how to do everything wrong.

The company had been warned by a security researcher to fix its vulnerabilities months before the first attack was alleged to have happened. That researcher shared their findings with press, showing that a public web portal allowed anyone "with no authentication whatsoever ... to access the personal data of every American, including social security numbers, full names, birthdates, and city and state of residence." What's more:

> ***While probing Equifax servers and sites, the researcher said that they were also able to take control—or get shell access as hackers refer to it—on several Equifax servers, and found several others vulnerable to simple bugs such as SQL injection, a common, basic way of attacking sites. Many servers were running outdated software ... Equifax had thousands of servers exposed on the internet...***

The researcher reported all of this to the company. "If it took me three hours to find that website, I definitely think I'm not the only one who found it," they told Motherboard. "It wasn't just one breach. It was maybe dozens."

Six months after that first researcher notified the company about the vulnerability, Equifax patched it – but only after the massive breach had already taken place, according to Equifax's own timeline.

Equifax

Overall, the breach cost Equifax more than $1.7 billion since it was first disclosed in 2017.

Equifax expects to pay out another $100 million for data breach

States it believes this will be the last of the payouts

February 14, 2020, 6:24 pm *By Ben Lane*

Share On

The **Department of Justice** may think it knows who hacked **Equifax** and exposed the sensitive personal information of 148 million U.S. consumers, but that doesn't mean the breach is behind Equifax quite yet.

In fact, the credit reporting agency disclosed this week that it expects to pay out an additional $100 million for its role in the breach.

Last year, the company set aside then agreed to pay out nearly $700 million to settle numerous federal and state investigations.

But the company revealed this week in its fourth-quarter earnings report that it set aside another $99.6 million in the fourth quarter for "certain legal proceedings and government investigations related to the 2017 cybersecurity incident."

According to the company, it believes this accrual will cover the remainder of its expected payouts for the breach. More specifically, the company said it "represents completed settlements and our best estimate of remaining
2017 cybersecurity incident."

All in all, the company set aside just over $800 m
which does not include the company's legal or p

Then, the $700 million data breach settlement. This turned into $125 per person. Except Equifax only planned to pay 248,000 of the actual victims – and over four and a half million applied, bringing the payout down to $6.80 per victim.

TransUnion

Business

TransUnion says data on 37,000 Canadians may have been compromised

TransUnion says someone fraudulently accessed data using a customer's login credentials

The Canadian Press · Posted: Oct 09, 2019 5:57 PM ET | Last Updated: October 9

TransUnion said in a statement Wednesday that someone fraudulently accessed its data through the use of one of its business customer's login credentials this past summer, compromising personal information of about 37,000 Canadians. (Ryan Remiorz/The Canadian Press)

126 comments

TECHNOLOGY

Oct 10, 2019

TransUnion br[illegible]ows rising third-party cyber[illegible]t in Canada

Ian Bickis, The[illegible]

A person uses a laptop computer with illuminated English and Russian Cyrillic character keys in this arranged photograph in Moscow, Russia, on Thursday, March 14, 2019. Russian internet trolls appear to be shifting strategy in their efforts to disrupt the 2020 U.S. elections, promoting politically divisive messages through phony social media accounts instead of creating propaganda themselves, cybersecurity experts say. , Bloomberg

TORONTO - A cybersecurity breach at TransUnion has underscored the rising threat of third-party attacks and the difficulty of preventing them.

The credit monitoring agency confirmed this week that the personal data of 37,000 Canadians was compromised when someone illegally used a legitimate business customer's login to access TransUnion data.

Daniel Tobok, CEO of Cytelligence Inc., said he's seen a rise in these kinds of attacks in which criminals gain access to their target through the account of a trusted third party such as a customer or vendor.

"The reasons criminals are really liking that is because it's very difficult to detect. There is normal usage, as a partner leveraging services."

Quora

insufficient details

27,800 views | Dec 4, 2018, 03:24am

Quora Hacked: What Happened, What Data Was Stolen And What Do 100 Million Users Need To Do Next?

Davey Winder Contributor

Cybersecurity

I report and analyse breaking cybersecurity an

Yet another breach notification in my email, this time informing me that Quora has been hacked... DAVEY WINDER

Like 100 million other Quora users, I awoke this morning to find an ominous email waiting for me that began: "We are writing to let you know that we recently discovered that some user data was compromised as a result of unauthorized access to our systems by a malicious third party." Hot on the heels of the Marriott International hotel group breach that impacted half a billion users, the question and answer site has confirmed that its systems have been hacked leaving account and user information potentially compromised.

The Hack of 100 Million Quora Users Could Be Even Bigger Than It Sounds

Rhett Jones

12/04/18 10:10am • Filed to: OH RIGHT I REMEMBER QUORA

15.3K 11 5

We've seen a lot of data breaches lately, but this is one worth giving your undivided attention. On Monday, the question and answer site Quora announced that a third-party was able to gain access to virtually every data point the company keeps on 100 million users. Even if you don't recall having a Quora account, you might want to make sure.

In a blog post, Quora CEO Adam D'Angelo explained that the company first noticed the data breach on Friday and has since enlisted independent security researchers to help investigate what happened and mitigate the damage. D'Angelo said that affected users should be receiving an email that explains the situation, but if you have a Quora account, it's probably a good idea to go ahead and change your password—especially if you reuse passwords. In all, the attackers were able to compromise a lot of data. Quora says that information includes:

- Account information, e.g. name, email address, encrypted (hashed) password, data imported from linked networks when authorized by users
- Public content and actions, e.g. questions, answers, comments, upvotes
- Non-public content and actions, e.g. answer requests, downvotes, direct messages (note that a low percentage of Quora users have sent or received such messages)

T.J. Maxx hack exposes consumer data

Intruders accessed systems used to process, store customer transaction data, putting unspecified numb

BY JORIS EVERS

TJX, operator of discount chains including T.J. Maxx and Mars computers were hacked, putting shoppers at risk of identity f

Intruders accessed systems used to process and store Framingham, Mass.-based TJX said in a statement. The customer information that was taken, but the full exten number of affected customers is yet unknown, it said.

"TJX is conducting a full investigation of the intrusion," company is committed to providing its customers with becomes available."

The intrusion involves systems that handle credit card, return transactions for T.J. Maxx, Marshalls, HomeGoo the U.S. and Puerto Rico, and the Winners and HomeS said. The exposed data covers 2003 and the period fr December 2006, it said.

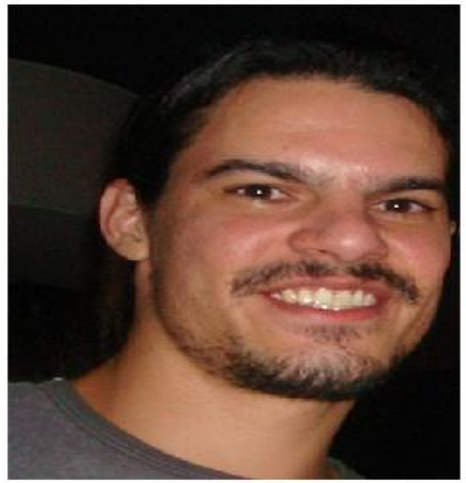
It is also possible that transaction data for T.K. Maxx st and Bob?s Stores in the U.S. was exposed in the breac

"It is pretty obvious that it was a very well orchestrated Avivah Litan, an analyst with Gartner. Litan suspects th people who have broken into systems at other retailer together information on millions of Americans. It is qui

informant war-driving, WiFi, WEP, sniffer, get PINs, encode cards, withdraw money awareness, encryption…….

KIM ZETTER SECURITY 03.25.10 02:02 PM

TJX HACKER GETS 20 YEARS IN PRISON



BOSTON – Convicted TJX hacker Albert Gonzalez was sentenced to 20 years in prison on Thursday for leading a gang of cyberthieves who stole more than 90 million credit and debit card numbers from TJX and other retailers.

The sentence for the largest computer-crime case ever prosecuted is the lengthiest ever imposed in the United States for hacking or identity-theft. Gonzalez was also fined $25,000. Restitution, which will likely be in the tens of millions, was not decided Thursday.

Clean-cut, wearing a beige jail uniform and wireframe glasses, the 28-year-old Gonzalez sat motionless at his chair during Thursday's proceedings, his hands folded in front of him.

d TK Maxx security breach

as brought about largely because of lax wireless LAN security, it

curity

h-Performing AppSec Strategy
lid strategy to address new threats, architectures, and the eatly expanding the application...
Register Now

arent company of TK Maxx did so rged on Monday.

etwork using Wired Equivalent ireless LANs. Hackers broke in ard numbers — in the second half

WEP encryption protocol used to ers and computers at a store in tted by employees logging on to usernames and passwords.

ts on TJX's system. Over the 18- cluding credit-card numbers, into s, which was unencrypted by TJX,

RECOMMENDED FOR YOU

IBM Cloud for VMware Solutions: Bringing VMware Environments to the Public Cloud
White Papers provided by IBM
DOWNLOAD NOW

MORE FROM TOM ESPINER

Mobility
Photos: Tesco pilots 'virtual store' for Gatwick airport travellers

Security
NHS trust fined £175,000 over data leak

Start-Ups
Vodafone to open Tech City incubator

TJX's failur

The news of the TJ Maxx data cost hundreds of millions or e March that the TJ Maxx breac now reporting that it happene

uld cost $1B

, and many estimate that it will s already widely reported back in rk, but the Wall Street Journal is

By George Ou for Real World IT | May 7, 2007 -- 18:23 GMT (11:23 PDT) | Topic: Servers

Details of Anthem's massive cyberattack remain in the dark a year later

few details early on, more over time
reference to 'sophisticated'
China

By Bob Herman | March 30, 2016

It's been more than a year since health insurer Anthem disclosed what was by far the largest data breach in healthcare history, yet almost nothing further is known about the causes, costs and ramifications of the breach.

The cyberattack—in which hackers stole the names, birth dates, Social Security numbers, home addresses and other personal information of 78.8 million current and former members and employees—gave Anthem's reputation a black eye early on. The company and the industry at large scrambled to do damage control. Consumers questioned whether Anthem and other healthcare organizations could manage the volumes of data they had.

But the breach essentially has been treated as a footnote since then. Anthem's pending acquisition of Cigna Corp., other high-profile healthcare digital attacks, and time have overshadowed Anthem's large-scale breach. Unresolved legal issues likely have stifled further disclosure of what is known.

RELATED CONTENT

Hackers breach Anthem; 80M exposed

Anthem's data hack prompts probe by national insurance group

Huge data hack not expected to hurt Anthem's bottom line

Anthem

Millions of Anthem Customers Targeted in Cyberattack

Outside the Anthem facility in Indianapolis. Anthem said it detected a data breach on Jan. 29, and that it was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images

By Reed Abelson and Matthew Goldstein

Feb. 5, 2015

Anthem, one of the nation's largest health insurers, said late Wednesday that the personal information of tens of millions of its customers and employees, including its chief executive, was the subject of a "very sophisticated external cyberattack."

The company, which is continuing its investigation into the exact scope of the attack, said hackers were able to breach a database that contained as many as 80 million records of current and former customers, as well as employees. The information accessed included names, Social Security numbers, birthdays, addresses, email and employment information, including income data.

Anthem said no credit card information had been stolen, and it emphasized that it did not believe medical information like insurance claims or test results were compromised. It said hospital and doctor information was also not believed to have been taken.

Still, the attack, which was first reported by The Wall Street Journal, could be the largest breach of a health care company to date, and one of the largest ever of customer information.

Anthem said that the breach was detected on Jan. 29, and that the company was now working with the Federal Bureau of Investigation. The company said it had also hired Mandiant, a well-known cybersecurity firm, to look into vulnerabilities of its computer system.

Sony

passwords, patching, SMB vulnerability
so much information they had problems sharing it all
Korea?

A Look Through The Sony Pictures Data Hack: This Is As Bad As It Gets

From details of named employees' medical histories to an unreleased pilot script written by the creator of *Breaking Bad*, the unprecedented leak of Sony Pictures data will reverberate for a long time to come.

Tom Gara
BuzzFeed News Business Editor

Charlie Wa
BuzzFeed St

Posted on December 2, 2014, at 9:51 p.m. ET

After sifting through almost 40GB of leaked inte
Pictures appears to have suffered the most emba
internal corporate data ever made public.

The data dump, which was reviewed extensively
criminal background checks, salary negotiations
medical rationale for leaves of absence. There ar
6,800 global employees, along with Social Security numbers for 3,500 U.S. staff. And there is extensive documentation of the company's operations, ranging from the script for an unreleased pilot written by *Breaking Bad* creator Vince Gilligan to the results of sales meetings with local TV executives.

The documents made public this weekend, covering the company's human resources, sales, and marketing teams, among others, are just a fraction of approximately 100TB of data the hackers claim to have taken from Sony. They say it will all be made freely available online, once they figure out how to distribute such an enormous amount of information.

The hackers, who call themselves the Guardians of Peace, took credit for the attack this weekend, emailing members of the media with links to download dozens of compressed files, each

ast troves of data stolen from the
ny Pictures. Earlier, the hackers leaked
video files of five unreleased Sony films.
e impact of that release, analysts told
ws, [probably won't be that bad](). But the
to Sony of this new round of leaks — to
n, its employee morale, and its
standing — seems impossible to

Years after that hack, Sony Pictures still seems to have a long way to go. One of the files leaked this weekend was a Word document titled "Passwords" that contained an executive's computer, LotusNotes, and American Express usernames and passwords, as well as Amex credit card numbers, expiration dates, and four-digit security codes.

estimate.

Sony CEO apologizes after data breach

CBC News Posted: May 06, 2011 10:31 AM ET | Last Updated: May 06, 2011 1:38 PM ET

0 shares

Facebook
Twitter
Reddit
Google
Share
Email

Related Stories

- Sony links Anonymous to Playstation hack
- Data breach fines sought by privacy watchdog
- Ont. woman sues Sony over data breach
- Sony data breach update reveals 'bad practices'
- PlayStation data breach deemed in

Sony Corp. president Howard Stringer has personally apologized for a massive breach of customers' personal information in a cyberattack and promised identity theft insurance for affected customers.

Sony Corp. president Howard Stringer, shown here in March, said in a blog post Thursday that there is 'no confirmed evidence any credit card or personal information has been misused.' (Rafiq Maqbool/Associated Press)

"As a company we — and I — apologize for the inconvenience and concern caused by this attack," Stringer said in a post on Sony's PlayStation blog Thursday afternoon. "We are absolutely dedicated to restoring full and safe service as soon as possible and rewarding you for your patience. We will settle for nothing less."

He added that Sony had launched a program to provide U.S. customers affected by the breach with an identity theft insurance policy worth $1 million per user, and similar announcements for customers in other countries would be coming soon. However, he added that there is "no confirmed evidence any credit card or personal information has been misused."

Sony CEO apologizes for PSN breach: Free identity theft protection detailed

INDUSTRY NEWS › TECHNOLOGY

CEO heads may roll for security breaches in wake of Sony boss' exit, experts say

What CEOs Can Learn From the Sony Cyberattack

All companies—not just big, public firms—are vulnerable to security breaches. Fortunately, there are measures CEOs can take to mitigate risk.

Insurance to Fully Cover Sony's Cyber Attack, Says CEO

By Mary Milliken | January 12, 2015

THE UNINSURED CONSEQUENCES OF THE SONY DATA BREACH

From the moment the malware was launched—months after the hackers first broke in—it took just one hour to throw Sony Pictures back into the era of the Betamax. The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks.

JP Morgan

MFA on most servers, missing on one born in Russia, moved to Israel, paid $403M to US Gov

JPMorgan Chase Hacking Affects 76 Million Households

BY JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN AND NICOLE PERLROTH OCTOBER 2, 2014 12:50 PM

528

The Manhattan headquarters of JPMorgan Chase, which securities over the summer. Andrew Burton/Getty Images

Email Share Tweet Save More

Updated, 9:03 p.m. | A cyberattack t compromised the accounts of 76 million small businesses, a tally t the bank and puts the intrusion a

The details of the breach — discl Thursday — emerge at a time wh digital operations of corporate A Target, Home Depot and a numb major data breaches. Last year, the information of 40 million cardholders and 70 million others were compromised at Target,

The ha

Feds Charge a Russ of 80 Million JP Mor

The Department of Justice announced the indictment of a Russian citizen. He is the man to be charged for targeting several U financial institutions between 2012 and 2

On Friday, the feds announced the indictment of Andrei Tyurin, 35. Tyuri extradited from Georgia and arrived in New York City on Friday, according authorities.

"Tyurin's alleged hacking activities were so prolific, they lay claim to the larg U.S. customer data from a single financial institution in history, accounting staggering 80 million-plus victims," Manhattan U.S. Attorney Geoffrey S. Be in a statement.

For years, the identity of the person who actually hacked JP Morgan Chase others financial institutions at the direction of Shalon remained a mystery now allegedly been solved.

At the time of the breach, it was reported that the hackers took advantage infamous Heartbleed bug to hack into the financial institution. In the indic prosecutors say Tyurin was exploited Heartbleed to get into the network of

Tyurin has been charged with hacking, securities market manipulation, illeg gambling and payment processing fraud.

JPMorgan Chase mega-hack was a simple two-factor auth fail

Bank bods didn't follow security 101, mayhem happened

By John Leyden 23 Dec 2014 at 16:54 20 SHARE

Hackers broke into JPMorgan's network through a giant security hole left open by a failure to switch on two-factor authentication on an overlooked server.

The *New York Times* reports that technicians at JPM had failed to upgrade one of its network servers, meaning that access was possible without knowing a combination of a password *and* the value of a one-time code.

The newspaper learnt of this failure to apply industry-standard security practice from unnamed sources familiar with the details of ongoing investigations into the breach.

THE WALL STREET JOURNAL.

passwords, supply chain username and password -> PoS malware, segmentation

Target Earnings Slide 46% After Data Breach

Target's fourth-quarter profit was nearly halved, cut down by a weak holiday season and a massive data breach that spooked customers. But the stock is up today on the news. Spencer Jakab joins MoneyBeat. Photo: Getty Images.

By PAUL ZIOBRO

Updated Feb. 26, 2014 6:36 p.m. ET

US Target Gregg Steinhafel fired for data breach

This story was published: 1 YEAR AGO | MAY 05, 2014 11:36PM

Target ... Gregg Steinhafel has been pushed out of the top job at Target for a data breach over the Christmas shopping period. *Source: AP*

TARGET'S massive data breach has now cost the company's US CEO his job.

Target has announced that Chairman, President and CEO Gregg Steinhafel is out nearly five months after the retailer disclosed the breach, which has hurt its reputation among customers and has derailed its business.

The nation's third-largest retailer said Mr Steinhafel, a 35-year veteran of the company and CEO since 2008, has agreed to step down, effective immediately. He also resigned from the board of directors.

A company spokesman declined to give specifics on when the decision was reached.

The departure suggests the company is trying to start with a clean slate as it wrestles with the fallout from hackers' theft of credit and debit card information on tens of millions of customers. The company's sales, profit and stock price have all suffered since the breach was disclosed.

NEWS

Target CIO resigns following breach

The retailer announces the resignation after data breaches affecting up to 110 million people

By Grant Gross FOLLOW

IDG News Service | Mar 5, 2014 1:38 PM PT

RELATED TOPICS

Cybercrime & Hacking

IT Careers

IT Personnel

Target CIO Beth Jacob has resigned following a data breach at the retailer that may have affected as many as 110 million U.S. residents.

Jacob's resignation was reported by the Associated Press Wednesday. She has been CIO at Target since 2008, and is former director of guest contact centers and vice president of guest operations at Target. She earned a bachelor's degree in retail merchandising from the University of Minnesota in 1984 and a masters of business administration in 1989.

In mid-December, Target reported a data breach that compromised 40 million credit and debit card accounts from late November to mid-December. ID thieves compromised the retailer's point-of-sale system, according to reports.

In January, the company reported a theft of additional personal information from up to 70 million customers.

Tumblr

good passwords, salted
made value of dump only $150 on Darknet

More than 65m Tumblr emails for sale on the darknet

Company only now discloses scale of hack three years ago – shortly before purchase by Yahoo – as database of passwords is leaked

▲ Yahoo acquired Tumblr in May 2013. The security breach took place earlier that year. Photograph: Karen Bleier/AFP/Getty

Personal information from more than 65m Tumblr accounts has been discovered for sale on the darknet.

Tumblr disclosed the leak, which it says took place in early 2013, this month, but had not previously acknowledged the scale of the database that was compromised.

The database includes email addresses and passwords, but the latter are heavily protected: Tumblr salted and hashed the passwords, a procedure which renders it practically impossible to restore the passwords to a useable state. It has since turned up for sale on darknet marketplace The Real Deal, with a sale price of just $150, according to Motherboard's Lorenzo Franceschi-Bicchierai.

Hackers Stole 65 Million Passwords From Tumblr, New Analysis Reveals

Two weeks after Tumblr disclosed a 2013 data breach, we finally know how big it was.

SHARE TWEET

Image: josh james/Flickr

On May 12, Tumblr revealed that it had just found out about a 2013 data breach affecting "a set" of users' email addresses and passwords, but the company refused to reveal how many users were affected.

As it turns out, that number is 65 million, according to an independent analysis of the data.

Hunt told Motherboard that the data contained 65,469,298 unique emails and passwords. (Tumblr did not immediately respond to a request to confirm the figure).
The passwords, however, were not in plaintext, but were "hashed," a process that turns the actual password into a different string of digits. The company also added a series of random bytes at the end of the passwords before hashing them, or "salted" them, as Tumblr said when it disclosed the breach. The company, however, didn't say exactly what algorithm it used to hash the passwords.
Since Tumblr's announcement, the hacked data appears to have been circulating within the internet underground. A hacker known as Peace, who also claims to have the data and was selling it on the darknet marketplace The Real Deal, said Tumblr used SHA1 to hash the passwords. Given that it also used salt, they are very hard for hackers to crack.

Uber

blackmailed
paid $100k not to tell

Uber Paid Hackers to Delete Stolen Data on 57 Million People

By Eric Newcomer
November 21, 2017, 1:58 PM PST *Updated on November 21, 2017, 7:21 PM PST*

Hackers stole the personal data of 57 million customers and drivers from Uber Technologies Inc., a massive breach that the company concealed for more than a year. This week, the ride-hailing firm ousted its chief security officer and one of his deputies for their roles in keeping the hack under wraps, which included a $100,000 payment to the attackers.

Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said.

"None of this should have happened, and I will not make excuses for it."

Hackers stole the personal data of 57 million customers and drivers from Uber Technologies Inc., a massive breach that the company concealed for more than a year. This week, the ride-hailing firm ousted its chief security officer and one of his deputies for their roles in keeping the hack under wraps, which included a $100,000 payment to the attackers.

Home Depot Hackers Exposed 53 Million Email Addresses

Hackers Used Password Stolen From Vendor to Gain Access to Retailer's Systems

supply chain, stolen vendor credentials, malware

Home Depot offers $19M to settle customers' hacking lawsuit

Home Depot admits 56 million cards hit by security breach

Home Depot

Cost of a Retail Data Breach Home Depot

Mar 14, 2017 | Cybersecurity News

When considering how much to invest in cybersecurity def
retail data breach. Poor security practices and a lack of app
company dearly.

A data breach of the scale of that suffered by Home Depot
dollars to resolve. The home depot data breach was massi
involving a point of sale system that has been reported to
criminals to steal more than 50 million credit card number
million email addresses.

The attack was made possible due to the use of stolen cred
Those credentials were used to gain a foothold in the netw
elevated, the Home Depot network was explored, and whe
malware was installed to capture credit card details. The m
months between April and September 2014.

Last year, Home Depot agreed to pay out $19.5 million to c
breach. The payout included the costs of providing credit n
Depot has also paid out at least $134.5 million to credit car
further $25 million settlement has been agreed to cover da
breach.

The latest settlement amount will allow banks and credit ca
compromised credit card without having to show evidence
they will receive up to 60% of uncompensated losses.

Home Depot to Pay Banks $25 Million in Data Breach Settlement

A Home Depot store is seen on May 17, 2016 in Miami. Photograph by Joe Raedle—Getty Images

Facebook

Chris Wylie the whistleblower from Victoria

Facebook has 'tentatively' concluded that spammers, not foreign agents, are to blame f the biggest hack in its history

ALEXEI ORESKOVIC
OCT 18, 2018, 1:27 PM

FACEBOOK TWITTER REDDIT LINKEDIN EMAIL

Chip Somodevilla/Getty Images
Facebook cofounder, chairman and CEO Mark Zuckerberg

- Facebook has "tentatively" concluded that spammers pretending to be a digital marketing firm are responsible for the biggest hack in the company's history,

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

- **'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower**
- **Mark Zuckerberg breaks silence on Cambridge Analytica**

▲ Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles' – video

The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box.

Facebook

Russian court fines Facebook $63,000 over data law breach

The Tagansky District Court in Moscow fined Facebook for its refusal to put its server holding data about Russian citizens on Russian territory

Reuters
@moneycontrolcom

Listen to the Audio Version of the Article
00:39 Powered by Trinity Audio

A Russian court fined social media company Facebook 4 million roubles ($62,922) on February 13 for its failure to comply with a Russian data law, the RIA news agency reported.

The Tagansky District Court in Moscow fined Facebook for its refusal to put its server holding data about Russian citizens on Russian territory, after earlier handing Twitter an identical fine for the same offence.

($1 = 63.5700 roubles)

Ashley Madison

Online Cheating Site AshleyMadison Hacked

HACKERS FINALLY POST STOLEN ASHLEY MADISON DATA

Ashley Madison Offering $500,000 Reward For Info

Ashley Madison hack victims receive blackmail letters

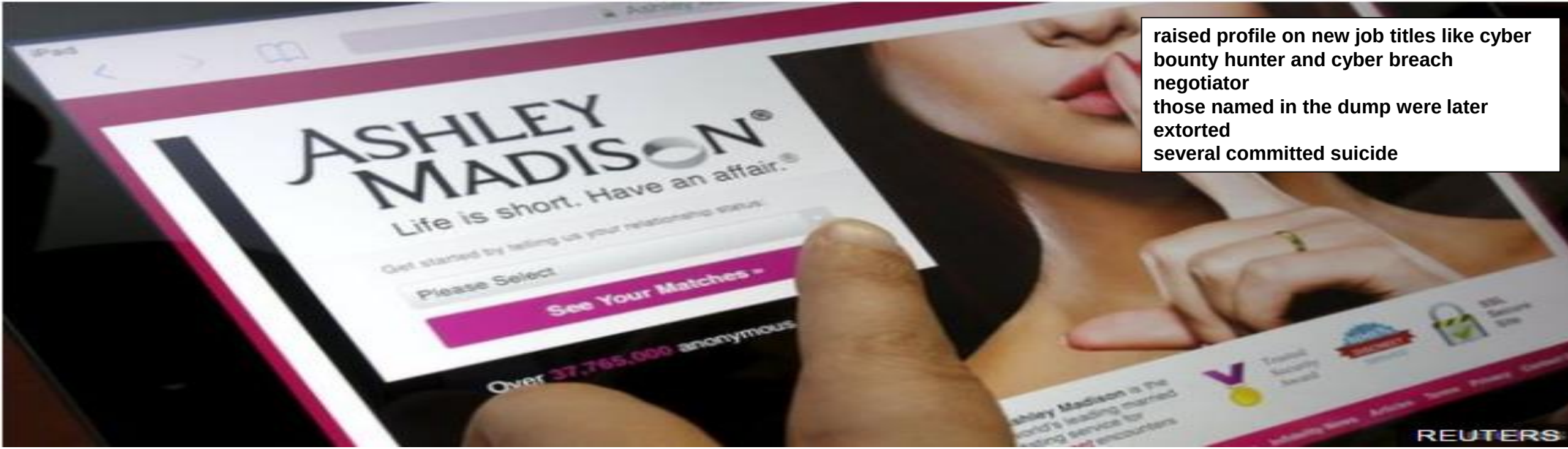
- information posted online
- people felt entitled to download
- subscribers were guilty until proven innocent
- vast majority of accounts were fraudulent
- accounts registered from IP address 127.0.0.1
- gave rise to whole new job titles
- gave rise to new scams

University of Victoria

Ashley Madison

likely vulnerability – SQL inject or externally accessible
Impact Team claimed responsibility

- 300G of user data stolen and company told to close down site or would be exposed
  - included personal details, payment information
- site did not validate email addresses
  - guilty until proven innocent
- site required you to pay to delete profiles
- revealed significant number of fake profiles
  - registered by IP address 127.0.0.1
- 12,000 of 5.5 million female accounts were used



raised profile on new job titles like cyber bounty hunter and cyber breach negotiator
those named in the dump were later extorted
several committed suicide

Online Cheating Site AshleyMadison Hacked

HACKERS FINALLY POST STOLEN ASHLEY MADISON DATA

Ashley Madison Offering $500,000 Reward For Info

University

Ashley Madison hack victims receive blackmail letters

Extortion scam personalized with Ashley Madison data breach

The target receives an email threatening to share their Ashley Madison account, along with other embarrassing data, with family and friends on social media and via email. The aim is to pressure the recipient into paying a Bitcoin ransom (in the example below, 0.1188 BTC or about $1,059) to avoid the shame of having this very personal—and potentially damaging—info made publicly available for anyone to see, including spouses.

From top to bottom, the emails are highly personalized with information from the Ashley Madison data breach. The subject includes the target's name and bank. The body includes everything from the user's bank account number, telephone number, address, and birthday, to Ashley Madison site info such as their signup date and answer to security questions. The email example below even references past purchases for 'male assistance products'.

[redacted] account on A.Madison! Going Public (Bank Of America, N.a.)

MO

Madelyn Odonnell [redacted]

[redacted]

Wednesday, January 15, 2020 at 5:20 AM

Show Details

[redacted].pdf

6 KB

Download All Preview All

[redacted] I know everything about you. I even know that you ordered some .. lets call them 'male assistance products' online on 12/11/2018 using your account at Bank Of America, N.a., routing# 121000358 account# [redacted] for $75 for mailing to [redacted] CA [redacted]! I even know about the other 3 other similar orders. Do your friends and family know you have been buying these aids? Do the partners you find on AMadison know you have been using 'chemical help' to have a good time? Very soon they could find it all out. Social media is a great way of spreading an embarrassing message. Of course I will use email also. Your devices have been compromised. I know everything. **The attached pdf says what you need to do to stop this. Because of filters and keyword this pdf has a password to stop a mail server reading it, the password is 2227. I am giving you very little time.** If you do not act very fast, your full AMadison profile and proof of it will be shared with friends, family, and online over social media - and of course your internet orders..... The end of [redacted] (415) [redacted] One of the addresses I have for you : [redacted] CA [redacted] Date of birth (claimed on AM site) : [redacted] First signed up for A.Madison : July 28, 2011, from [redacted] - an IP address registered in or near [redacted] Username on A.Madison [redacted] Security answer on A.Madison : [redacted]

Ashley Madison Breach Extortion Scam Targets Hundreds

Author:
Lindsey O'Donnell

February 3, 2020
/ 10:56 am

3 minute read

Write a comment

Share this article:

A new extortion attack has targeted hundreds of users affected by the Ashley Madison breach over the past week.

Nearly five years after the high-profile Ashley Madison data breach, hundreds of impacted website users are being targeted by a new extortion attack this past week.

The 2015 data breach of the adultery website led to 32 million accounts being publicly dumped online, including victims' names, passwords, phones numbers, credit card information and more. Up to a year after the hack, researchers with Kaspersky said that affected users were still being hit with an array of attacks, from credit card scams to spam emails.

National Security

Chinese breach data of 4 million federal workers

OPM breach: 4.5 million more individuals open to future fingerprint abuse

password, awareness issues, known as problematic, privilege escalation, malware
insufficient MFA
attributed to China

US OPM breach was preventable

By Dylan Bushell-Embling
Monday, 12 September, 2016

The high-profile data breach involving the theft of information from millions of US federal employees was preventable, a year-long House of Representatives investigation has found.

A damning report from the US House Oversight and Government Reform committee found that the Office of Personnel Management failed to prioritise cybersecurity despite repeated warnings leading up to last year's breach that their data stores were vulnerable to attack.

The investigation also found that the OPM failed to implement a long-standing federal requirement to use multifactor authentication to control access to the n
damage of the breach.

6/9/2016
04:30 PM

Kelly Jackson Higgins
News

Connect Directly

2 COMMENTS
COMMENT NOW

Login

OPM Data Breach: A New Twist On The Discovery Of The Malware

Congressional members lay out details of the chain of events that led to the revelation of the Office of Personnel Management's big data breach.

The DLL file disguised as a McAfee antivirus executable was confirmation that something was amiss. That's what convinced Office of Personnel Management contractor Brendan Saulsbury that this was not legitimate traffic in the agency's network: OPM doesn't use McAfee's AV software.

Saulsbury told a congressional committee earlier this year that he was the first person to spot malicious activity that ultimately revealed the now-infamous and historic data breach at the Office of Personnel Management (OPM), shooting down previous reports that it was found by forensics security vendor CyTech Services during a product demonstration at the agency in April 2015.

US Office of Personnel Mgmt (OPM)

US hacking: Military and intelligence data 'accessed'

13 June 2015

Hackers with suspecte
data on US intelligence

Details of a major hack e
a potential second breac

It is feared that the attac
to blackmail.

The agency involved, the
comment on the reports.

Officials, who spoke on condition of anonymity to the Associated Press (AP) news agency, believe the attackers have targeted the forms submitted by intelligence and military personnel for security clearances.

Shared admin accounts

MFA, privilege escalation, malware, McAfee looking file, domains, Avengers

What is clear is that OPM's technical leadership, overly confident that they had defeated X1 with the "big bang," did not use the intrusion as a "wake up call" and failed to take measures that would have
largely failed to institute a number of im
measures, the most the important of wh
authentication. Under a two-factor authe
enhanced ID card that correlates with th
log into the system. Without it, an attack
username and password—as X2 did, us
free access to the system. OPM finally i
January 2015, after X2 had already wor

At any rate, once X2 had access to OPI
privilege escalation technique to obtain
variant of the PlugX malware, a remote
navigate around OPM's systems and co
OPM servers—including, crucially, the "
was used to log into other servers. Sakula, another linked piece of remote control malware, was installed around the same time.

OPM breach response

As noted, X2's infiltration was finally detected on April 15, 2015, when a security engineer was investigating encrypted SSL traffic on OPM's networks. The researcher determined a beacon-like ping was connecting a component on OPM's infrastructure called mcutil.dll to a website called opmsecurity.org. At very casual first glance this may seem on the up-and-up; but mcutil.dll looks like part of a McAfee security software suite, something OPM didn't use, and opm-security.org, despite its name, wasn't registered by the agency. In fact, mcutil.dll was cloaking the PlugX malware, and opm-security.org was one of several sites acting as command-and-control servers for the attackers. (The attackers had a sense of humor: the domain name, and others like it, were registered to "Steve Rogers" and "Tony Stark," aka Marvel's Captain America and Iron Man.)

However, the
the OPM

2018, failing

eased to the public in June 2016, GAO made four recommendations to OPM, to
ns, run a thorough evaluation of security controls, update action plans and track
ning.

In more specific terms, the agency did not protect some of the systems from unauthorized information exchange, enforce password policies for authenticated access and restrict access to relevant individuals, turn on encryption for a database, or enable sufficient logging to help with monitoring or auditing systems.

Google

vulnerability

Russian bitcoin forum

Google will shut down Google+ four months early afte

The underloved social network will

By Nick Statt and Russell Brandom | Dec 10, 2018, 12:

SHARE

Illustration by Alex Castro / The Verge

4.93 million Gmail usernames and passwords published, Google says 'no evidence' its systems were compromised

by EMIL PROTALINSKI — Sep 10, 2014 in GOOGLE

7,561 SHARES

http://tnw.to/g4sPM

Approximately 4.93 million Gmail usernames and passwords were published to a Russian Bitcoin forum on Tuesday, as first reported by Russian website CNews. That's the bad news. The good news is that this leak doesn't seem as massive upon further inspection.

Google+ has suffered another data leak, and Google has decided to shut down the consumer version of the social network four months earlier than it originally planned. Google+ will now close to consumers in April, rather than August. Additionally, API access to

r Google+ vulnerability was
xposed private user data to
ong as three years. The bug
l in March, but not publicly
ober, resulting in significant
erns. In response, Google
o shut down the consumer
, which had long struggled to
ime around, Google says it
on its own and it was live for
ween November 7th and

Cathay

unknown

turn on MFA

Cathay Pacific stocks plunge after airline reveals mass data breach by hacker

Updated 25 Oct 2018, 1:54am

Cathay Pacific Airways stocks have plunged to their lowest level in nearly a decade after the airline revealed a massive data breach has affected the information of 9.4 million passengers.

Hong Kong's flagship carrier said it had discovered unauthorised access to the personal data but had no evidence the leaked information had been misused.

Data breach documents from Hong Kong Exchanges — which operates the Hong Kong Stock Exchange — noted on Wednesday that Cathay Pacific first discovered suspicious activity on its network in March.

The documents state "unauthorised access to certain personal data was confirmed in early May 2018".

PHOTO: Cathay Pacific first learnt about the data breach in March. (Facebook: Cathay Pacific)

RELATED STORY: British Airways data breach affects almost 400,000 customers

RELATED STORY: 'Oops!': Cathay Pacific spells its name wrong on its own plane

The airline noted in a statement on Wednesday that the breach was discovered during "ongoing security processes".

Cathay Pacific said the stolen data included names, nationalities, birth dates, phone numbers, addresses, passport and identity card numbers and expired credit card numbers, among other information.

It noted 403 expired credit card numbers were accessed, and 27 credit card numbers with no CVV were accessed.

The company said no passwords were compromised.

Privacy commissioner orders investigation

Hong Kong's privacy commissioner, Stephen Kai-yi Wong, expressed "serious concern" over the lapse and urged companies to improve protection of personal data.
He said his office would begin a compliance check of the airline.
He urged people to change their passwords and enable "two-factor authentication" to help protect their data.

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

The Dropbox data breach has highlighted the problem of password reuse. Photograph: Alamy

Popular cloud storage firm Dropbox has been hacked, with over 68m users' email addresses and passwords leaking on to the internet.

The attack took place during 2012. At the time Dropbox reported a collection of user's email addresses had been stolen. It did not report that passwords had been stolen as well.

Dropbox

passwords

leverage MFA

Technology Intelligence

Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself

share Save

A huge cache of personal data from Dropbox that contains the usernames and passwords of nearly 70 million account holders has been discovered online.

The information, believed to have been stolen in a hack that occurred several years ago, includes the passwords and email addresses of 68.7 million users of the cloud storage service.

Dropbox confirmed that the credentials were stolen in a hack that occurred in 2012 when hackers used stolen employee login details to access a document containing the email address and passwords of users. The number of users affected by the hack was not known until now, and the company had previously said only email addresses were taken - not passwords.

"This is not a new security incident, and there is no indication that Dropbox user accounts have been improperly accessed," said Patrick Heim, the head of trust and security at Dropbox.

The company discovered the details for sale online when it was conducting routine security work. Motherboard then revealed the exact number of affected users after Leakbase, a breach notification service, provided it with the full set of data.
Dropbox, which has around 500 million registered users, is the fourth major company this year to have found user credentials stolen in a 2012 hack circulating online. MySpace and LinkedIn both confirmed in May that hundreds of millions their users' of passwords and email addresses stolen in 2012 hacks were for sale online.
Earlier this month Yahoo said it was investigating reports that 200 million of its users accounts were up for sale, allegedly taken in a hack that was previously unreported.

LinkedIn

passwords

leverage MFA

Hackers selling 117 million LinkedIn passwords

by Jose Pagliery @Jose_Pagliery

May 19, 2016: 10:59 AM ET

Recommend 4

My hack stole your credit card

LinkedIn was hacked four years ago, and what initially seemed to be a theft of 6.5 million passwords has actually turned out to be a breach of 117 million passwords.

LinkedIn was hacked four years ago, and what initially seemed to be a theft of 6.5 million passwords has actually turned out to be a breach of 117 million passwords.

On Wednesday, the professional social network company acknowledged that a massive batch of login credentials is being sold on the black market by hackers.

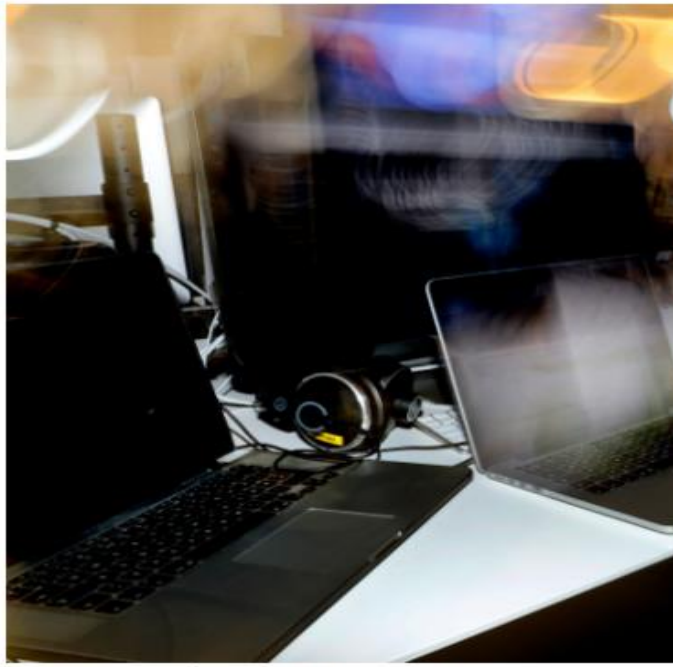
The worst part about it is that, because people tend to reuse their passwords, hackers are more likely to gain access to 117 million people's email and bank accounts.

The advice for everyone who uses LinkedIn (LNKD) at this point is: Change your password and add something called two-factor authentication, which requires a text message every time you sign in from a new computer.

Swedish Transport Agency

includes names of law enforcement, witnesses, judges, etc

Swedish authority handed over 'keys to the Kingdom' in IT security slip-up



File photo: Lise Åserud/NTB scanpix/TT

Criticism is mounting over IT security at Swedish emerged that millions of Swedes' driving licence countries.

Sweden's security police Säpo has investigated the Swedish Transport Agency (Transportstyrelsen) after information about all vehicles in the country – including police and military – was made available to IT workers in Eastern Europe who had not gone through the usual security clearance checks when the agency outsourced its IT maintenance to IBM in 2015.

Besides the entire national driver's licence database, the records potentially included information on intelligence agents, military and police transport and personnel, people with criminal records and those in witness protection programmes, Swedish media have reported.

The Swedish military confirmed that details of its staff, vehicles, and defence and contingency planning could have been included in the breach, although the transport agency insisted it held no military data and there was no indication that any of the data had been "spread in an improper way".

Sweden scrambles to tighten data security as scandal claims two ministers

ecked after leak of sensitive data nation on people in witness protection

the media as he comments on his resignation. Photograph: Ari

ought urgent assurances on data security from national agencies including the health, education and pensions services after a huge leak of private and sensitive information that has cost two ministers their jobs.

Amid reports by the Dagens Nyheter newspaper that confidential medical details were being handled by unscreened IT workers in Romania, the national broadcaster SVT said data outsourcing arrangements at six state agencies were being checked.

Cellebrite

organization is responsible for doing forensics for others

Hacker Steals 900 GB of Cellebrite Data

A hacker provided Motherboard with a large cache of customer information, databases, and more.

The hackers have been hacked. Motherboard has obtained 900 GB of data related to Cellebrite, one of the most popular companies in the mobile phone hacking industry. The cache includes customer information, databases, and a vast amount of technical data regarding Cellebrite's products.

The breach is the latest chapter in a growing trend of hackers taking matters into their own hands, and stealing information from companies that specialize in surveillance or hacking technologies.

Cellebrite is an Israeli company whose main product, a typically laptop-sized device called the Universal Forensic Extraction Device (UFED), can rip data from thousands of different models of mobile phones. That data can include SMS messages, emails, call logs, and much more, as long as the UFED user is in physical possession of the phone.

Cellebrite is popular with US federal and state law enforcement, and, according to the hacked data, possibly also with authoritarian regimes such as Russia, the United Arab Emirates, and Turkey.

The data appears to have been taken, at least in part, from servers related to Cellebrite's website. The cache includes alleged usernames and passwords for logging into Cellebrite databases connected to the company's my.cellebrite domain. This section of the site is used by customers to, among other things, access new software versions.

The dump also contains what appears to be evidence files from seized mobile phones, and logs from Cellebrite devices. According to the hacker, and judging by timestamps on some of the files, some of the data may have been pulled from Cellebrite servers last year.

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

Doctors reverted to pens and paper after hospital taken offline by a ransomware attack

By Lauren O'Neil, CBC News Posted: Feb 16, 2016 10:59 PM ET | Last Updated: Feb 17, 2016 10:03 PM ET

popularized ransomware
awareness
backups

The Hollywood Presbyterian Medical Center hack may be part of a larger trend predicted for this year, in which ransomware is used to target the medical sector – potentially leading hackers to threaten victims with their own lives if they don't pay up. (Hollywood Presbyterian Medical Center/Facebook)

A Los Angeles hospital paid a ransom in bitcoins equivalent to about $17,000 US to hackers who infiltrated and disabled its computer network, the medical centre's chief executive said Wednesday.

It was in the best interest of Hollywood Presbyterian Medical Center to pay the ransom of 40 bitcoins — currently worth $16,664 — after the

University Of Calgary Paid $20,000 In Ransom To Hackers

The Huffington Post Alberta | By Sarah Rieger

Posted: 06/07/2016 5:53 pm EDT | Updated: 06/07/2016 5:59 pm EDT

popularized cyber insurance
awareness
backups
Iran

The University of Calgary paid $20,000 in ransom after a malware attack on the school's computers last week.

The university announced the payment in a release Tuesday, 10 days after a cyberattack that left students and staff unable to access university-issued computers, email or Skype.

"A ransomware attack involves an unknown cyberattacker locking or encrypting computers or computer networks until a ransom is paid, and when it is, keys, or methods of decryption, are provided," wrote Linda Dalgetty, vice-president of finances and services at the university, in a release.

briankrebs
@briankrebs

Follow

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

3:02 AM - 21 Sep 2016

vulnerabilities
passwords
security on IoT in general

Brian Krebs site hit with 665 Gbps DDoS attack; Largest Internet has ever seen

Colossal 1 terabyte per second DDoS attack hits French tech firm

Armies of hacked IoT devices launch unprecedented DDoS attacks

DDoS attacks got a power boost thanks to hundreds of thousands of insecure IoT devices

Canada Treasury Board

awareness

China

Three Canadian government agencies hacked from China-based computers

February 17, 2011, 4:46 PM ET

SHARE: Like 0 Tweet MOR

By Bill Mann

Three of the Canadian gove
Canada's financial nerve ce
hackers, it was learned this

But Thursday, **Canadian Pri**
Canada does have a systen

The Canadian Broadcast Co
ministries had been penetrat
Department and the Treasur
ministries cut off their interne

But Thursday, the CBC repo
Research and Development
National Defence, had also

The Chinese government ins
Canadian officials were quic
government. Chinese Foreig
attaches great importance to
cracks down on hacking acti

Harper wouldn't comment specifically on the unprecedented attacks, but he said at a press conference in Toronto Thursday that he recognized cyber security was "a growing issue of importance, not just in this country, but across the world."

Foreign hackers attack Canadian government

Computer systems at 3 key departments penetrated

Greg Weston · CBC News · Posted: Feb 16, 2011 9:03 PM ET | Last Updated: February 17, 2011

An unprecedented cyberattack on the Canadian government also targeted Defence Research and Development Canada, making it the third key department compromised by hackers, CBC News has learned.

The attack, apparently from China, also gave foreign hackers access to highly classified federal information and also forced the Finance Department and Treasury Board — the federal government's two main economic nerve centres — off the internet.

Defence Research and Development Canada works to assist in the scientific and technological needs of the Canadian Forces. It is a civilian agency of the Department of National Defence.

The cyberattack, first detected in early January, left Canadian counter-espionage agents scrambling to determine how much sensitive government information may have been stolen and by whom.

Highly placed sources tell CBC News the cyberattacks were traced back to computer servers in China.

They caution, however, that there is no way of knowing whether the hackers are Chinese, or some other nationality routing their cybercrimes through China to cover their tracks.

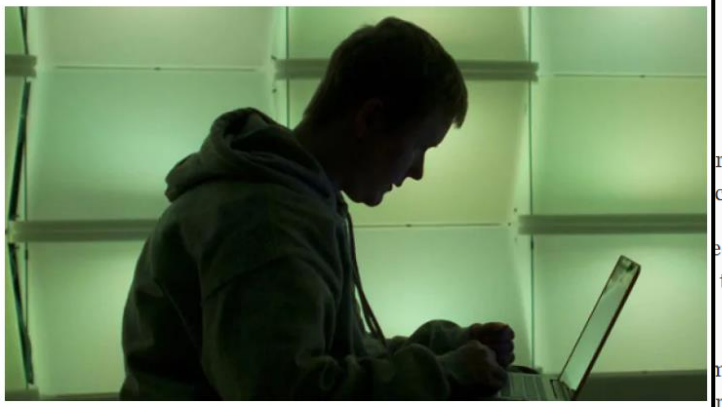
Other hacking cases

February 2011: U.S. computer security firm McAfee reports hackers operating from China stole sensitive information from Western oil companies in the United States, Taiwan, Greece and Kazakhstan, beginning in November 2009.

CSIS warned government of cyber attacks just weeks before crippling hack

Hackers stole secret Canadian government data

Julie Ireton · CBC News · Posted: Jun 02, 2011 4:16 PM ET | Last Updated: June 3, 2011



A cyber attack discovered in January resulted in hackers getting secret information from government departments, CBC News has learned. (CBC)

Hackers who attacked two of Canada's federal departments stole classified information before being discovered last January, CBC News has learned.

The revelation comes from documents obtained under Access to Information laws, and contradicts what the minister in charge said at the time.

Six months ago, hackers launched an unprecedented cyber attack on the federal government. In January, the government's computer system came under attack.

Hackers sent malicious emails to staff that appeared to be coming from senior managers. When staff opened the attachments, hackers found a path into the federal network, providing access to classified information.

rtments were computers.

ed a security the very kind

ments have been rvice report.

on Canadian ress under the

irect references aterial.

Canadian research body relied on paper communications after Chinese hack, documents show

COLIN FREEZE
The Globe and Mail
Published Friday, Sep. 02, 2016 3:57PM EDT
Last updated Friday, Sep. 02, 2016 5:33PM EDT

Upon discovering that it had been hacked by China, the Canadian government's scientific-research body did digital damage control on an enormous scale. Firing up its vintage fax machines, it jettisoned scores of computer servers, bought its staff hundreds of new laptops and drew up a list of about 20,000 corporate partners in Canada whose secrets risked being collateral damage.

Records newly released to The Globe and Mail reveal these and other details about the extensive fallout from this nightmare at the National Research Council. The hack of the NRC was highlighted in July 2014, when the then-Conservative government blamed China, making it the only cyber-espionage campaign that Canada has ever pinned on a specific state adversary.

While hacks of government departments occur relatively routinely, the NRC could be considered a more valuable target than most. For decades, it has been routing tax dollars to fund cutting-edge research in agriculture, engineering and computer science. Placing bets on Canadian companies helps the NRC work to ensure future prosperity, and its staff gets a glimpse of emerging technologies and proprietary business plans.

Chinese hackers installed malware on National Research Council computers

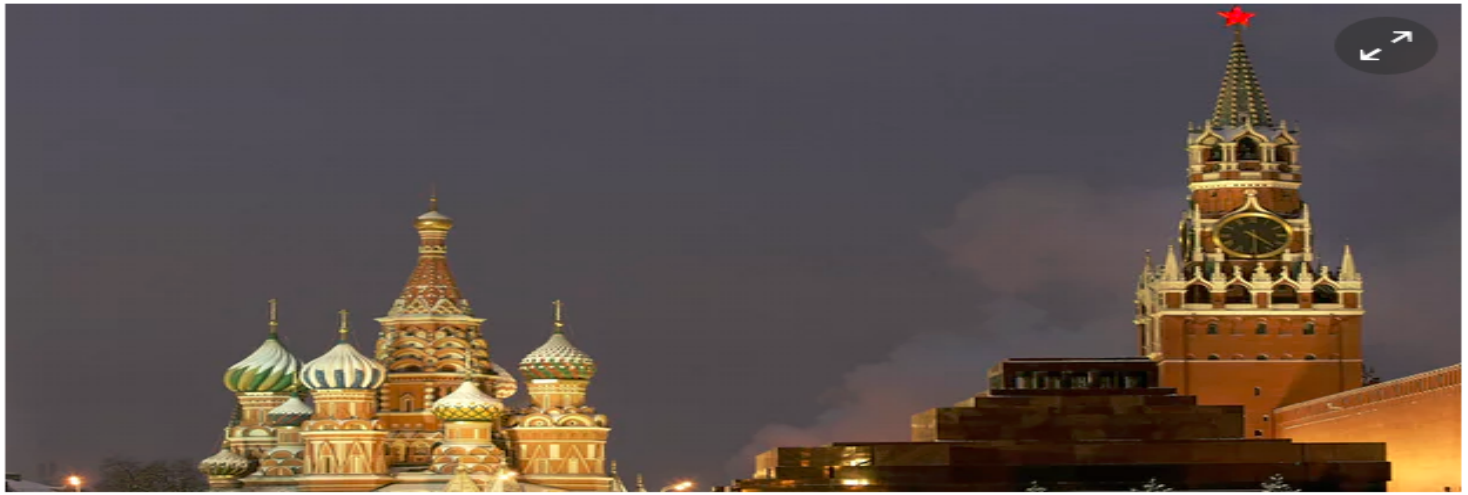
Canada
CNRC-NRC

known poor security
likely awareness…
attribution to China

- NRC hack nearly brought agency 'back to the buggy'
- NRC had to 'fire up vintage fax machines'
- "jettisoned scores of servers"
- "only cyber-espionage campaign Canada has ever pinned on a specific state adversary"
- network deemed unfit, thrown away
- replacement >$32M and 4 years to build

US officially accuses Russia of hacking DNC and interfering with election

Administration says 'only Russia's senior-most officials' could have signed off on cyber-attacks and urges states to seek federal security aid for voting systems



The accusation against Russia came shortly after the US also called for the country to be investigated for war crimes in Syria. Photograph: Misha Japaridze/AP

The US government has formally accused Russia of hacking the Democratic party's computer networks and said that Moscow was attempting to "interfere" with the US presidential election.

Obama expels 35 Russian diplomats in retaliation for US election hacking

- Trump wants to 'move on' but says he will meet intelligence officials
- FBI and Homeland Security detail Russian hacking in new report

Vladimir Putin talks to Barack Obama during a meeting at the sidelines of the G20 Summit in Hangzhou, China, on 5 September 2016. Photograph: Alexei Druzhinin/Sputnik/Kremlin/EPA

awareness

attribution to Russia

The Obama administration on Thursday announced its retaliation for Russian efforts to interfere with the US presidential election, ordering sweeping new sanctions that included the expulsion of 35 Russians.

WORLD

U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate

Sanctions follow U.S. assessment Russia used cyberattacks to interfere with presidential election

By CAROL E. LEE and PAUL SONNE
Updated Dec. 29, 2016 8:42 p.m. ET

President Barack Obama on Thursday issued a dramatic response to Russia's alleged use of cyberattacks to interfere with the 2016 presidential election, including imposing sanctions on Russian agencies and companies and expelling dozens of suspected intelligence operatives from the U.S., in one of the biggest diplomatic confrontations between Washington and Moscow since the end of the Cold War.

Summary

BIG DATA | Back to Home

Human Error Not Cybersecurity is Leading GDPR Data Breach Trend

CONOR REYNOLDS
6TH FEBRUARY 2020

+ INCREASE / DECREASE TEXT SIZE −

Summary

13 FEB 2020 OPINION

Why Leaky Clouds Lead to Data Breaches

Dean Sysman CEO and co-founder, Axonius
Follow @AxoniusInc Connect on LinkedIn

This past summer, we witnessed yet another massive data breach due to a misconfigured AWS cloud instance, and hundreds of thousands of Capital One's customers' Social Security and bank account numbers were exposed as a result.

Smaller-scale data breaches like this occur frequently, and unfortunately, we're bound to see more of these breaches in the future even though they're easy to avoid. So why can't we seem to prevent them? It comes down to intent and access.

When Backup Becomes Kryptonite

Let's say you've just set up an Amazon S3 bucket. It's got some customer data in it, but you're not concerned because it's just a backup. You also set permissions so that you're able to access this backup from anywhere in the world, and over time, you continue to add more and more data to it. At a certain point, quite a bit of time has passed, and you've added so much to it, that you've stopped inspecting it. Its original permissions haven't been verified since initial set-up, and you haven't thought about what would happen if any of the data got leaked to the public.

Most of the time, the backup data that gets placed into an Amazon S3 bucket is harmless, but other times, it's not. For example, suppose it contained your entire company's Salesforce data: if that data were to be exposed, not only would your customer records now be out in the open, but perhaps your sales team also made a not-so-nice note about a particularly difficult prospect. Suddenly a bad situation is made even worse.

The "Any Authenticated User" Permission

Another reason we continue to witness data breaches as a result of public cloud instances has to do with permissions - specifically, Amazon's definition of "any authenticated user." Initially, you might think this means any user in your organization, but unfortunately, it actually means any user with an AWS account. Let's face it, that's just about everyone, including those who might have malicious intent when looking for public cloud instances to hack.

The good news is that Amazon has taken steps to mitigate this confusion, and it now features a disclaimer when setting up a public S3 bucket to ensure you truly understand the meaning of "any authenticated user". However, it offers a good lesson to double-check the authentication permissions you're putting in place before moving forward.

Related to This Story

A Tricky Transition: Why Organizations Struggle with Secure, Multi-Cloud Migrations

A New Approach to Data Breach Prevention: Early and Pervasive Breach Detection

#RackspaceSolve Board Needs to Understand Security to Adopt Cloud

Top Ten: Things Learned About the Capital One Breach

The GDPR Disclosure Conundrum

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1
13 FEB 2020 NEWS
Cyber-criminals Lure Victims with Coronavirus Cure Conspiracy Theories

2
12 FEB 2020 NEWS
Crypto AG Unmasked: CIA Spied on Governments For Decades

3
14 FEB 2020 NEWS
Report Reveals Worst State for Healthcare Data Breaches in 2019

4
11 FEB 2020 NEWS
DevOps Alert: 12,000 Jenkins Servers Exposed to DoS Attacks

5
6 FEB 2020 NEWS

Investigations

University of Victoria

Headlines

TRANSPORTATION

Toyota data breach affects up to 3.1 million

Written by Sean Lyngaas

MAR 30, 2019 | CYBERSCOOP

Automotive maker Toyota sai
sales offices in Japan, exposi
customers.

The breach affected Toyota T
enterprises, and possibly thr
according to Toyota Motor Co
"unauthorized access" to the

"We take this situation seriou
information security measure
the statement said.

It was the second cybersecur
months. In February, Toyota's
"the victim of an attempted c

The company's security woes
Vietnamese hacking group, A
spearphishing campaign agai
Southeast Asian country is tr
and data stolen by APT32 cou

OceanLotus APT Uses Steganography to Shroud Payloads

Author:
Lindsey O'Donnell
April 3, 2019 / 10:44 am

2 minute read

Write a comment

Share this article:

The OceanLotus APT is using two new loaders which use steganography to read their encrypted payloads.

The advanced persistent threat (APT) group OceanLotus has switched up its tactics to use steganography to cloak encrypted payloads within .png image files.

Researchers said that they discovered the OceanLotus APT group – a Vietnam-linked cyber-espionage group also known as APT32 – using the tactic to hide their payloads since September 2018. After victims click on malicious files sent via phishing emails, a loader will execute a next-stage encrypted payload that is obfuscated using steganography – a method of hiding code within an image. Once decoded, decrypted, and executed, the payload will deploy the APT's backdoor.

APT	Attacker	Target
38	North Korea	Financial Institutions
37	North Korea	Various
34	Iran	Various
33	Iran	Aerospace, Energy
32	Vietnam (OceanLotus)	Foreign countries investing in Vietnam
30	China	Southeast Asian Nations
29	Russia (Cozy Bear)	Western European
28	Russia (Fancy Bear)	Eastern Europe, NATO (aka Tsar Team)
19	China	Legal, Investment
18	China	Aerospace, Defence
17	China	US Government

Headlines

HEALTHCARE

German drug giant Bayer blames Chinese hacking group Wicked Panda for breach: report

Written by Jeff Stone

APR 4, 2019 | CYBERSCOOP

German drug conglomerate Bayer says it was victimized in a cyberattack that originated with Chinese hackers, German media reported Thursday.

The $39 billion pharmaceutical giant said it found malicious software on its computer networks last year and contained the breach, according to the outlets BR and NDR.

Investigators examining the breach said attackers used the Winnti malware, which is tied to a Chinese-based hacking group known as Wicked Panda. The group in the past has been blamed for attacks on targets including the online gambling industry and companies with intellectual property that would benefit Beijing.

Wicked Panda "makes use of a number of open-source and custom tools to infect and move laterally in victim networks," according to a CrowdStrike description. "The group's tools have been traced to "contractors who count multiple Chinese government agencies as clients, including the Ministry of Public Security. Observed targeting by the Wicked Panda adversary has focused on high-value entities in the engineering, manufacturing and technology sectors, aligning with the PRC's strategic economic plans."

Meet CrowdStrike's Adversary of the Month for July: WICKED SPIDER

July 26, 2018 Adam Meyers Research & Threat Intel

WICKED SPIDER (PANDA) is a suspected China-based adversary that likely operates as an exploitation group for hire. The use of two cryptonyms for this group exemplifies how this adversary has demonstrated two different motivations for conducting malicious cyber operations.

Headlines

Name	Adversary
Anchor Panda Deep Panda Goblin Panda Mustang Panda Samurai Panda Comment Panda Foxy Panda Impersonating Panda Karma Panda Keyhole Panda Poisonous Panda Putter Panda Toxic Panda Union Panda Vixen Panda	China
Clever Kitten Helix Kitten Magic Kitten Cutting Kitten	Iran
Stardust Chollima Silent Chollima	North Korea

Name	Adversary
Mythic Leopard	Pakistani
Cozy Bear Fancy Bear Venomous Bear Voodoo Bear Energetic Bear	Russia
Deadeye Jackal Ghost Jackal Corsair Jackal Extreme Jackal	Hacktivist/Terrorist
Viceroy Tiger	India
Cobalt Spider Dungeon Spider Mummy Spider Wicked Spider Singing Spider Union Spider Andromeda Spider	Non-State Criminal Groups

Headlines

Meet CrowdStrike's Adversary of the Month for October: DUNGEON SPIDER

Common “threats” to consider (cont.)

- Advanced Persistent Threat Groups

Group ID	Group Alias	Suspected attribution
APT37	None	North Korea
APT34	None	Iran
APT33	None	Iran
APT32	OceanLotus Group	Vietnam
APT30	None	China
APT29	None	Russian government
APT28	Tsar Team	Russian government
APT19	Codoso Team	China
APT18	Wekby	China
APT17	Tailgator Team, Deputy Dog	China
APT16	None	China
APT12	Calc Team	China
APT10	Menupass Team	China
APT5	None	Undisclosed
APT3	UPS Team	China
APT1	Unit 61398, Comment Crew	China’s People’s Liberation Army

Source: https://www.fireeye.com/current-threats/apt-groups.html

Review

- insiders are threat actors that operate within the organization and have legitimate reason to be there and legitimate access and knowledge
- they may use this access and knowledge to do illegitimate things
- they may do this knowingly or unknowingly – intentionally or unintentionally
- difficult to detect, can be very harmful

Open Source Intelligence

OSINT

- for articles and studies - check your sources
  - exercise critical thinking
  - who wrote the article or sponsored the study?
  - what do they have to gain?
- is the story legitimate? is it fake news?
  - is the person knowingly spreading false information?

Snopes

- is there a lesson to be learned even though it isn't true?
- examples:
  - **https://www.youtube.com/watch?v=TlO2gcs1YvM** (7:47)
  - https://www.youtube.com/watch?v=Y2rCB-1AlGc (3:16)

University of Victoria

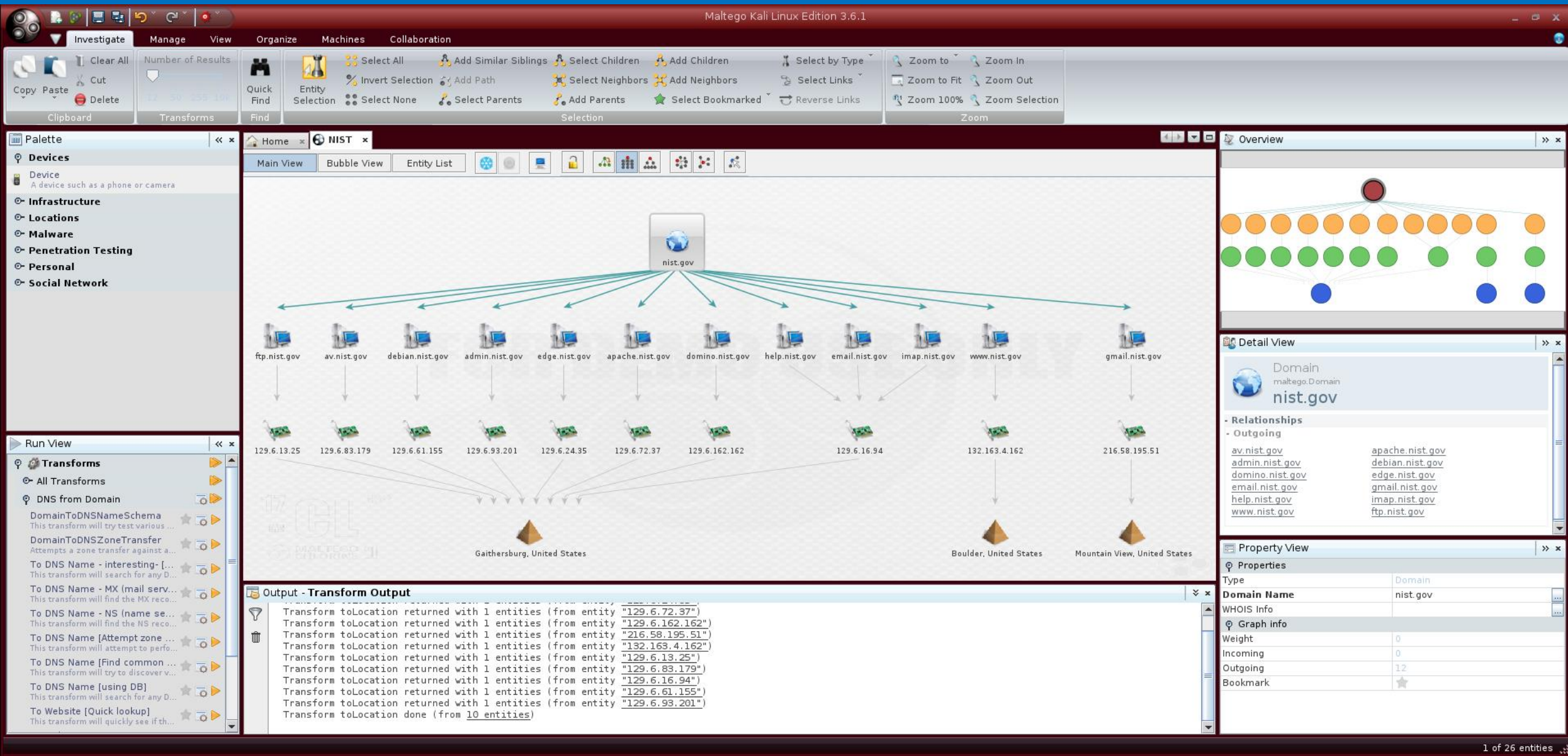
OSINT - Maltego

- OSINT = Open-source Intelligence
- there are many sources of information, intelligence
- some open source, some not
- when you correlate the available information can synthesize or determine additional pieces of information

Maltego video: https://www.youtube.com/watch?v=VExg83LzZ1Q

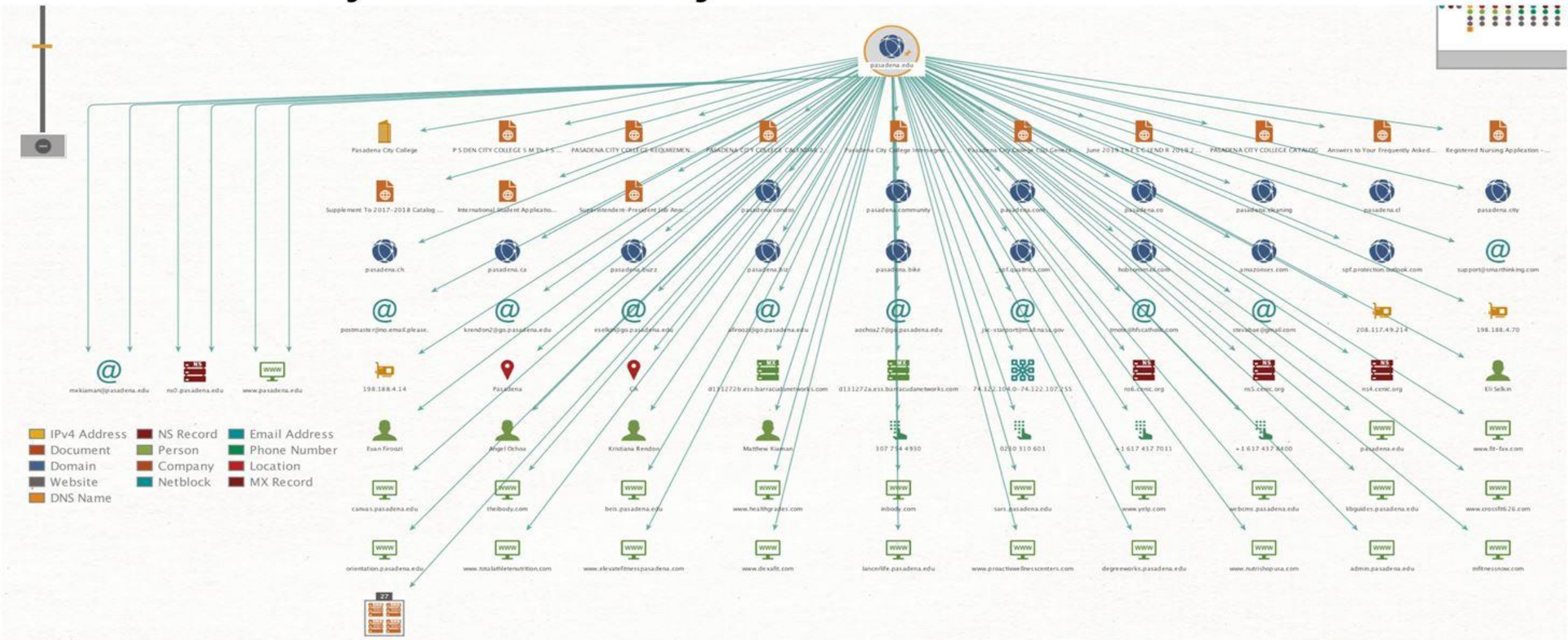
University of Victoria

OSINT - Maltego



OSINT - Maltego

What can you find with just a domain?



OSINT - Example

- many sites with information available
- just need to know where to look
- e.g. courts

University of Victoria


DARKNET

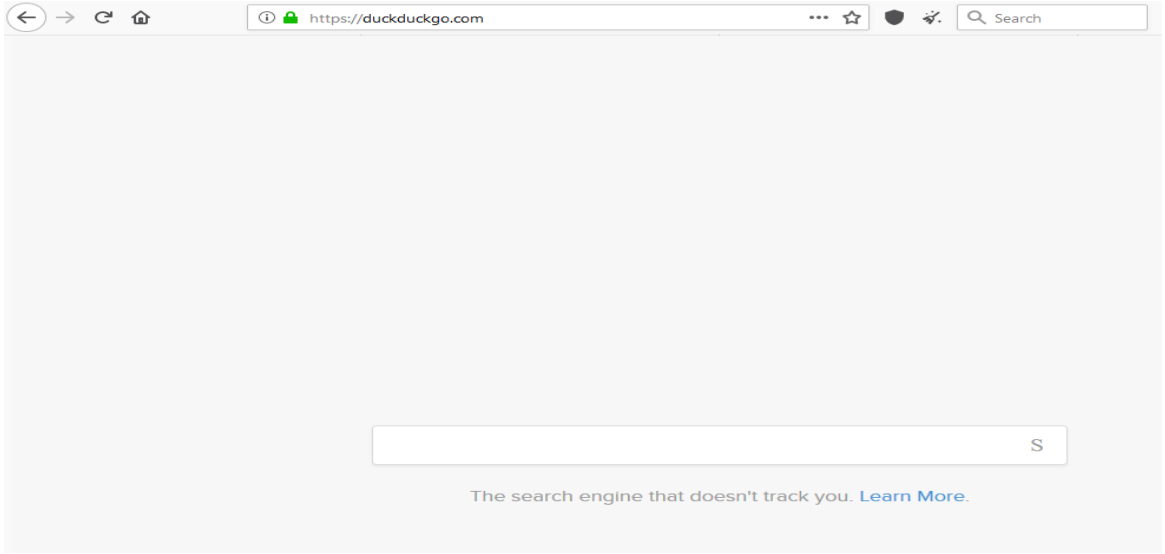
DarkNet

- WARNING: Don’t go there
  - when you go where the bad people are…
- often accessed through ToR browser*
- take precautions
  - use VPN
  - turn off all scripts
- WARNING: Don’t go there

DarkNet

https://www.import.io/post/the-difference-between-surface-web-deep-web-and-dark-web/

DarkNet



search engine like DuckDuckGo

pages of links

University of Victoria

6ngvt5ueyjyo62zx – Darkweb Marketplace – **Empire Market** – Newly launched marketplace which is clone of Alphabay Marketplace, looking alternative store on Alphabay, you may try Empire market, Like another darkweb market, here users also can deals legal or illegal items (Drugs, Digital Products, Games, Virus, Hacking service, Hosting and etc). Empire market accepts fee in **multiple crypto coins like BTC, BCH, LTC, XMR**. They also plan to add new crypto coins on this store.

elite6c3wh756biv7v2fyhnoitizvl2gmoisq7xgmp2b2c5ryicottyd – Darknet Marketplace – **Elite Market** – A non wallet-less, advance-deposit requiring Darknet escrow marketplace is what Elite Market is. Independent/third-party vendors are allowed for a non-refundable fee of USD $150.00. All trades are allowed except weapons, non-legal porn, chemicals which may harm others, murder-services and prostitution. Registration is free & fast. No sale-data is kept after 14 days of sale finalization. Standard darknet security measures available. BTC is the only mode of payment.

grymktgwyxq3sikl – Darknet Marketplace – **Grey Market (Exit Scam)** is a market both for Vendors and Buyers. Buyers can order from over 700 listings on the marketplace in various categories such as **E-books, Software, Weed, Stimulants, Seeds** etc. While Vendors can sell those products for a vendor-bond of USD $99.00 and a fee of 5%-3% on each sale (depends on vendor levels). Payment modes: BTC and XMR. Security: Escrow/ Wallet-less deposits. PGP available as well.

samsaraccrn2jmin – Darknet Markets – **Samsara Market** – This is most trusted dark web marketplace, that have more than 1 Lakh listed items, products or services and these are related to **Drugs, Digital Goods, Services, Electronics, Carding, Hacking, Porns Accounts, Counterfeit, Malware, Virus, Exploit** and much more. Since from couple of months, dream marketplace getting his fee in three popular cryptocurrencies (Bitcoins, Bitcoin Cash, Monero). For Security reason you can set 2FA at your accounts by PGP Key.

berlusconifsfwkp – Darknet Marketplace – Two primary aspects of any DNM include its "**Products**", and "**Security Features**". Products on **Berlusocni market** include anything and everything from Drugs, Carded items, Jewellery, Gold etc. Security features include 2-Factor authentication via PGP, Escrow and Multisig for safer transaction and trades, and PIN for Withdrawal and refund-address changes. Bitcoin, Litecoin and even Monero accepted as payment modes. Can be accessed only after registrations.

SENG 460 / ECE 574
Practice of Information Security and Privacy

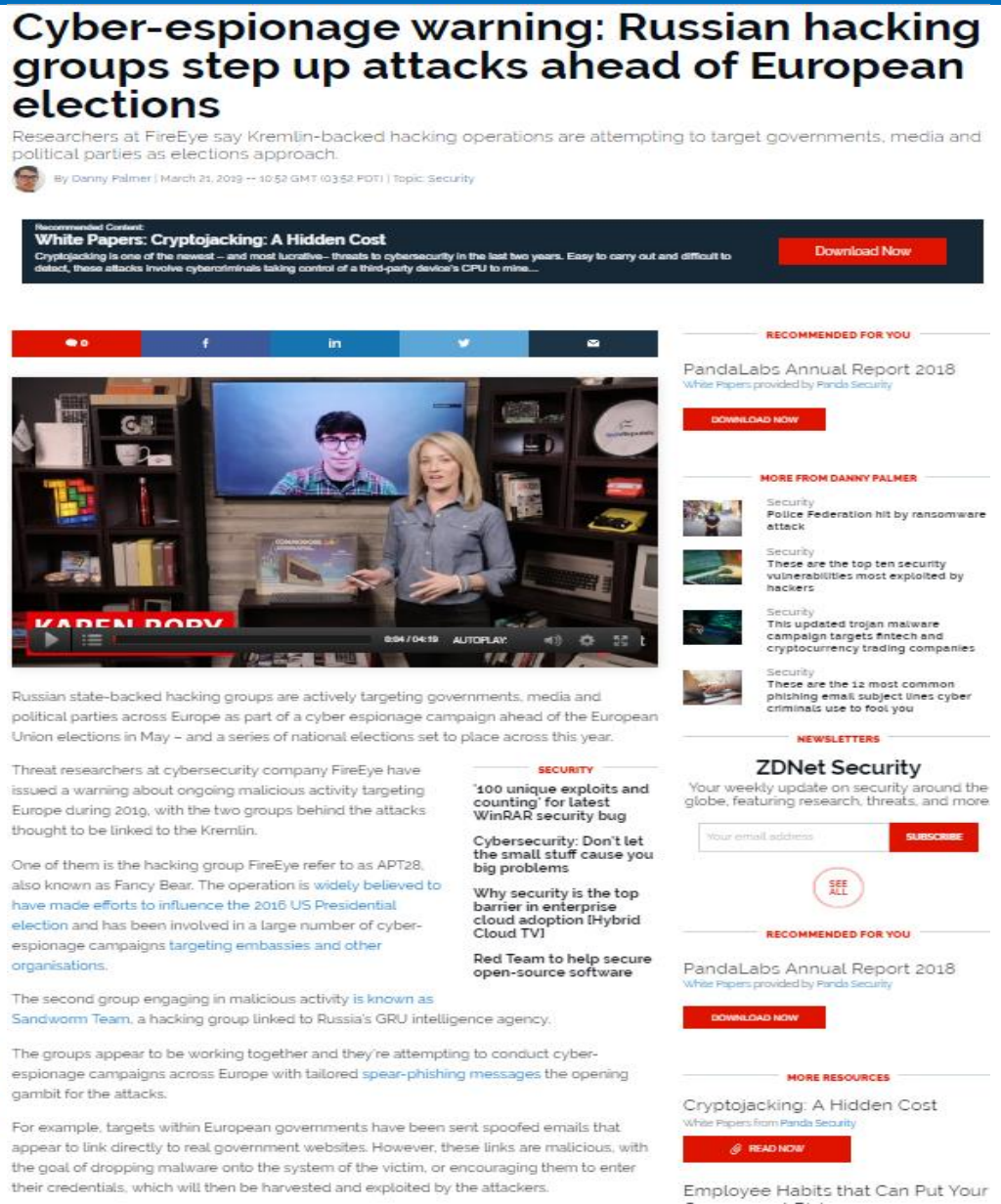
Week 6: Threats to Canada's Democratic Process

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Headlines



Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections

Researchers at FireEye say Kremlin-backed hacking operations are attempting to target governments, media and political parties as elections approach.

By Danny Palmer | March 21, 2019 -- 10:52 GMT (03:52 PDT) | Topic: Security

Recommended Content:
White Papers: Cryptojacking: A Hidden Cost
Cryptojacking is one of the newest -- and most lucrative-- threats to cybersecurity in the last two years. Easy to carry out and difficult to detect, these attacks involve cybercriminals taking control of a third-party device's CPU to mine...
Download Now

0 | f | in | t | ✉

Russian state-backed hacking groups are actively targeting governments, media and political parties across Europe as part of a cyber espionage campaign ahead of the European Union elections in May – and a series of national elections set to place across this year.

Threat researchers at cybersecurity company FireEye have issued a warning about ongoing malicious activity targeting Europe during 2019, with the two groups behind the attacks thought to be linked to the Kremlin.

One of them is the hacking group FireEye refer to as APT28, also known as Fancy Bear. The operation is widely believed to have made efforts to influence the 2016 US Presidential election and has been involved in a large number of cyber-espionage campaigns targeting embassies and other organisations.

The second group engaging in malicious activity is known as Sandworm Team, a hacking group linked to Russia's GRU intelligence agency.

The groups appear to be working together and they're attempting to conduct cyber-espionage campaigns across Europe with tailored spear-phishing messages the opening gambit for the attacks.

For example, targets within European governments have been sent spoofed emails that appear to link directly to real government websites. However, these links are malicious, with the goal of dropping malware onto the system of the victim, or encouraging them to enter their credentials, which will then be harvested and exploited by the attackers.

SECURITY

'100 unique exploits and counting' for latest WinRAR security bug

Cybersecurity: Don't let the small stuff cause you big problems

Why security is the top barrier in enterprise cloud adoption [Hybrid Cloud TV]

Red Team to help secure open-source software

RECOMMENDED FOR YOU

PandaLabs Annual Report 2018
White Papers provided by Panda Security
DOWNLOAD NOW

MORE FROM DANNY PALMER

Security
Police Federation hit by ransomware attack

Security
These are the top ten security vulnerabilities most exploited by hackers

Security
This updated trojan malware campaign targets fintech and cryptocurrency trading companies

Security
These are the 12 most common phishing email subject lines cyber criminals use to fool you

NEWSLETTERS

ZDNet Security
Your weekly update on security around the globe, featuring research, threats, and more
Your email address
SUBSCRIBE
SEE ALL

RECOMMENDED FOR YOU

PandaLabs Annual Report 2018
White Papers provided by Panda Security
DOWNLOAD NOW

MORE RESOURCES

Cryptojacking: A Hidden Cost
White Papers from Panda Security
READ NOW

Employee Habits that Can Put Your

"They tailored phishing in several cases we observed. They even faked local institution websites and content to encourage their victims to share credentials," David Grout, EMEA CTO at FireEye, told ZDNet.

"The attackers are using several phishing technologies, including some large-scale approaches and tailored approaches to increase their chance in getting the information they are looking for".

Researchers believe the attacks have several objectives: to collect information and credentials for future operations, to understand each of the target countries and groups to help make decisions on how to act and to collect enough intelligence to build and conduct disinformation campaigns.

"The groups could be trying to gain access to the targeted networks in order to gather information that will allow Russia to make more informed political decisions, or it could be gearing up to leak data that would be damaging for a particular political party or candidate ahead of the European elections," said Benjamin Read, senior manager of cyber-espionage analysis at FireEye.

5 Eyes

- 5 Eyes countries include: United States, Canada, Australia, New Zealand, United Kingdom

- countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence

- processed intelligence is gathered from multiple sources, the intelligence shared is not restricted to signals intelligence (SIGINT) and often involves defence intelligence as well as human intelligence (HUMINT) and geospatial intelligence (GEOINT)

- OSINT = Open Source Intelligence

University of Victoria

Threats to Canada's Democratic Process

- All material and notes are attributed to:
- Cyber Threats to Canada's Democratic Process
- produced by the Communications Security Establishment

University of Victoria

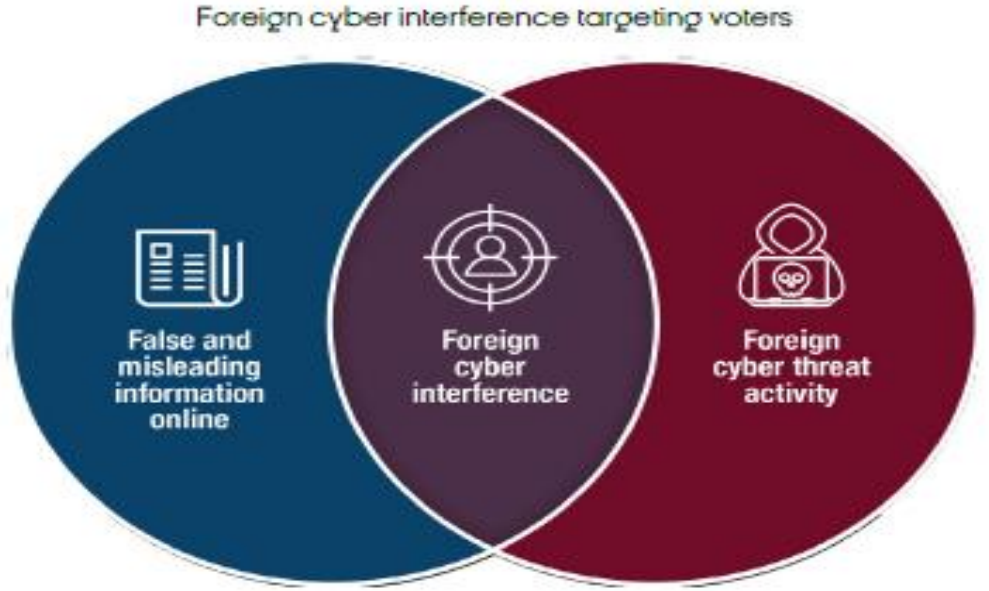
Global Context

US officially accuses Russia of hacking DNC and interfering with election

Administration says 'only Russia's senior-most officials' could have signed off on cyber-attacks and urges states to seek federal security aid for voting systems

The accusation against Russia came shortly after the US also called for the country to be investigated for war crimes in Syria. Photograph: Misha Japaridze/AP

The US government has formally accused Russia of hacking the Democratic party's computer networks and said that Moscow was attempting to "interfere" with the US presidential election.



WORLD

U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate

Sanctions follow U.S. assessment Russia used cyberattacks to interfere with presidential election

By CAROL E. LEE and PAUL SONNE

Updated Dec. 29, 2016 8:42 p.m. ET

President Barack Obama on Thursday issued a dramatic response to Russia's alleged use of cyberattacks to interfere with the 2016 presidential election, including imposing sanctions on Russian agencies and companies and expelling dozens of suspected intelligence operatives from the U.S., in one of the biggest diplomatic confrontations between Washington and Moscow since the end of the Cold War.

Obama expels 35 Russian diplomats in retaliation for US election hacking

- Trump wants to 'move on' but says he will meet intelligence officials
- FBI and Homeland Security detail Russian hacking in new report

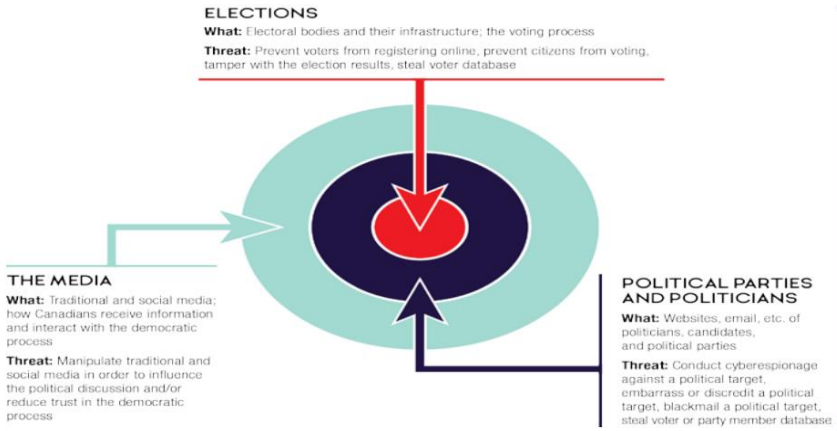
Vladimir Putin talks to Barack Obama during a meeting at the sidelines of the G20 Summit in Hangzhou, China, on 5 September 2016. Photograph: Alexei Druzhinin/Sputnik/Kremlin/EPA

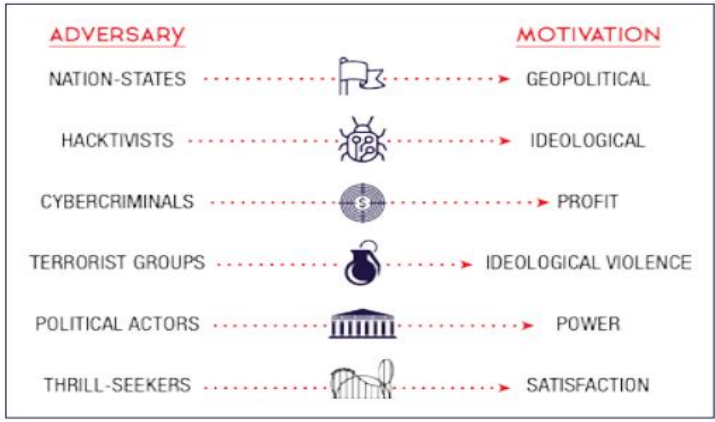
The Obama administration on Thursday announced its retaliation for Russian efforts to interfere with the US presidential election, ordering sweeping new sanctions that included the expulsion of 35 Russians.

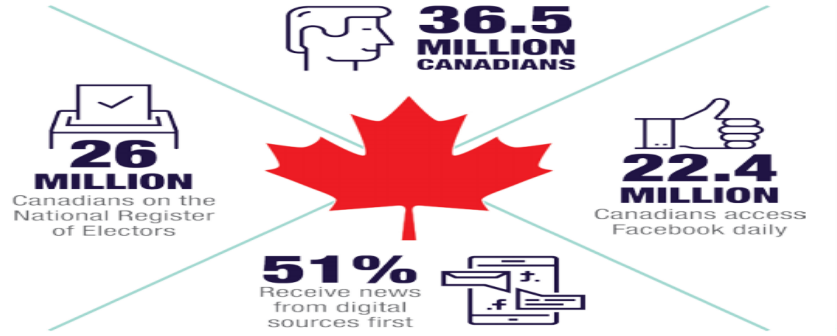
- **loose attribution of cyberattacks is a dangerous thing**
- **impacts of cyber attacks extend beyond cyberspace**
- **signals beginning/continuance of cyber cold war**

Threats to Canada's Democratic Process

- We judge it very likely that Canadian voters will encounter some form of foreign cyber interference related to the 2019 federal election. However, at this time, it is improbable that this foreign cyber interference will be of the scale of Russian activity against the 2016 United States presidential election.







Threats to Canada's Democratic Process

WHY TARGET CANADA'S DEMOCRATIC PROCESS?

CANADA IN THE WORLD

Canada is a G7 country, a NATO member, and an active member of the international community. As a result, the choices that the Government of Canada makes about military deployments, trade and investment agreements, diplomatic engagements, foreign aid, or immigration policy are of interest to other states. Canada's stance can affect the core interests of other countries, foreign groups, and individuals. Foreign adversaries may use cyber tools to target the democratic process to change Canadian election outcomes, policy makers' choices, governmental relationships with foreign and domestic partners, and Canada's reputation around the world.

CANADA IS ONLINE, AS ARE FOREIGN ADVERSARIES

Living in one of the most connected societies in the world, Canadians must be more vigilant against cyber tools than those in less connected nations. The vast majority of Canadians use the services provided by major Internet companies to obtain information, communicate with one another, and build communities.[1] Foreign adversaries wanting to interfere with the democratic process in Canada may take advantage of our highly connected society and use cyber tools to amplify their interference activity in Canada.

FIGURE 2: Why do nation-states use cyber capabilities to influence democratic processes of foreign countries?

IMMEDIATE GOAL

- Affect popularity of candidates
- Call into question legitimacy of election process
- Promote desired election outcome

MID-TERM GOAL

- Polarize political discourse
- Weaken confidence in leaders

LONG-TERM GOAL

- Promote foreign economic, ideological, military interests
- Reduce confidence in democracy
- Create divisions in international alliances

Threats to Canada's Democratic Process

- two types of threats
  - known (those that you can anticipate)
  - unknown (those that you are unable to anticipate)
- two types of attacks:
  - direct (attacks directly against voting assets)
  - indirect (attacks intended to shift perception of the voting process)
- goal is to prepare for the known so when the time comes can focus on the unknown that arise

University of Victoria

Examples & Remedies

- what can you do about indirect attacks? misinformation…

CYBER ESPIONAGE AGAINST POLITICAL PARTIES IN AUSTRALIA

A cyber threat actor compromised the information systems of Australia's parliament and three major political parties in February 2019, a year in which Australia will hold national elections. The Australian Prime Minister noted that Australia's "cyber experts believe that a sophisticated state actor is responsible for this malicious activity." The case highlights that the information of democratic institutions, including political parties, represents an attractive target for state-sponsored cyber threat activity in an election year.[6]

FOREIGN INFLUENCE AND INTERFERENCE OUTSIDE THE ELECTION PERIOD

Since the 2015 federal election, Canadian political leaders and the Canadian public have been targeted by foreign cyber interference activities. For example:

- More than one foreign adversary has manipulated social media using cyber tools to spread false or misleading information relating to Canada on Twitter, likely to polarize Canadians or undermine Canada's foreign policy goals;
- Foreign state-sponsored media have disparaged Canadian cabinet ministers;[7] and
- A foreign adversary has manipulated information on social media to amplify and promote viewpoints highly critical of Government of Canada legislation imposing sanctions and banning travel of foreign officials accused of human rights violations.[8]

University of Victoria

Headlines

Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities

Exposed Facebook phone numbers, an XKCD breach, and more of the week's top security news.

PHOTOGRAPH: ULLSTEIN BILD/GETTY IMAGES

University of Victoria

US and Russia clash over power grid 'hack attacks'

18 June 2019 Share

The complexity of Russia's electricity grid makes it a hard target, says expert

Russia has said it is "possible" that its electrical grid is under cyber-attack by the US.

Kremlin spokesman Dmitry Peskov said reports that US cyber-soldiers had put computer viruses on its electrical grid was a "hypothetical possibility".

His comments came in response to a New York Times (NYT) story which claimed **US military hackers were targeting Russian power plants.**

The report drew scepticism from experts and a denunciation by President Trump.

Threats to Canada's Democratic Process

- cyber threat activity against the democratic process is increasing around the world (more than tripled)
  - Canada is not immune
  - small number of nation-states have undertaken majority of cyber activity against democratic process
- multiple groups will likely deploy cyber capabilities against future elections ranging in sophistication
- elections are largely paper-based and have controls in place

University of Victoria

Threats to Canada's Democratic Process

- threat to Canada's democratic process remains at 'low' level
- 3 targeted areas of democratic process:

  1) elections

  2) political parties and politicians

  3) traditional and social media
- highly probable threat activity will increase
- cyber capabilities are publicly available and cheap and easy to use

University of Victoria

Threats to Canada's Democratic Process

- rapid growth of social media and other factors without sufficient checks and balances means spreading 'fake news' is easier than ever
- **elections are increasingly using technology**
- **deterring cyber threat activity is challenging because it is difficult to detect, attribute, and respond to in a timely manner**

University of Victoria

Threats to Canada's Democratic Process

- different types of threats: strategic threats and incidental threats
- cyber threats can be a show of force to deter other nation-states
- adversaries may seek to change Canadian election outcomes, policy choices, government relationships

University of Victoria

Threats to Canada's Democratic Process

- goals of threat actors:
  - reduce trust in a free and fair democratic process
  - shift policy in a preferred direction or promote core interests
- elections are targeted to:
  - prevent citizens registering, prevent voters from voting, tamper with election results, steal voter database
- three essential phases:
  1) registering voters
  2) voting
  3) disseminating results

University of Victoria

Threats to Canada's Democratic Process

N.W.T. to be 1st province or territory to use online voting in general election

Simply Voting software system allows voters to cast their ballots online

Hilary Bird · CBC News · Posted: Jul 04, 2019 5:00 AM CT | Last Updated: July 4, 2019

N.W.T. voters can use a new website called Electorhood to access an online voting system called Simply Voting to cast their ballots. Using the site, voters in the territory can vote online from Sept. 6 up until the end of voting day on Oct. 1. (Hilary Bird/CBC)

Threats to Canada's Democratic Process

- threats to political parties and politicians include: cyberespionage, blackmail, embarrass/discredit, steal/manipulate voter or party database
- cyber capabilities to disable a website are simple to buy or rent
- adversaries may steal a voter database in order to sell it on the DarkWeb

Threats to Canada's Democratic Process

- covert manipulation of traditional and social media to influence political discussion
- troll farms: groups of people paid to spread propaganda on social media
- social botnets: series of computers commanded by a single person
- DDoS: distributed denial of service attack – could be against a political or media website

Threats to Canada's Democratic Process

- deface a website: attackers could modify the content to embarrass, discredit, or spread false content
- spearphishing: targeted phishing against a political target or other
- ransomware: restricts access and compels victims to pay to have access returned
- **the most effective defenses against ransomware are user awareness and offline or disconnected backups**

University of Victoria

Threats to Canada's Democratic Process

- redirect/man-in-the-middle attack: when the attacker logically inserts themselves between the source and recipient of the traffic

- sophistication levels
  - low: single capability, single target, little or no planning, no lasting effect
  - medium: a few capabilities, more than one target, planning, multiple affected
  - high: several capabilities used expertly, numerous targets, extensive planning, long impacts

Threats to Canada's Democratic Process

- possible attack - gain access, move laterally, monitor, analyze, contact rival…
- "Many effective cyber capabilities are readily available, cheap, and easy to use…. Deterring cyber threat activity is challenging. We are unable to attribute about 20 percent of incidents to a particular adversary. Of those incidents that are attributed, most appear to have gone unpunished."

University of Victoria

Threats to Canada's Democratic Process

- "The rapid growth of social media coupled with the decline in longstanding authoritative sources of information make it easier for adversaries to use cyber capabilities and other methods to inject disinformation and propaganda into the media to influence voters.
- Elections and election agencies are adopting more online processes, making them more vulnerable to cyber threats. "

University of Victoria

Threats to Canada's Democratic Process

- "There is a dynamic of success emboldening adversaries to repeat their activity, and to inspire copycat behaviour."
- during the 2015 federal election, Canada was targeted by low sophistication cyber activity
- next federal election was set for 2019
- nation-states have demonstrated the highest sophistication

University of Victoria

Threats to Canada's Democratic Process

- All material and notes are attributed to:
- Cyber Threats to Canada's Democratic Process
- produced by the Communications Security Establishment

University of Victoria

Assigned Reading

- read Chapters 25, 26, 32 for next time
- consider the lab


University
of Victoria