Computer Security

01. Introduction

Paul Krzyzanowski

Rutgers University

Fall 2019

What is security?

security

noun se·cu·ri·ty \si-ˈkyu˙r-ə-tē\

the quality or state of being secure: such as

a **:** freedom from danger **:** safety

b **:** freedom from fear or anxiety

c **:** freedom from the prospect of being laid off
<job *security*>

What is computer security?

Keeping systems, programs, and data "safe"

The **CIA**[*] **Triad**:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

[*] *No relationship to the Central Intelligence Agency*

Confidentiality

- Keep data & resources hidden
  - Data will only be shared with authorized individuals
  - Sometimes – conceal the existence of data or communication
- Traditional focus of computer security

Data confidentiality:

> "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]."
>
> – *RFC 4949, Internet Security Glossary*

Confidentiality vs. privacy

Privacy

– Limit what information can be shared with others
– Ability to send messages anonymously
– Control other's use of information about you
– Freedom from intrusion

Secrecy: the ability to conceal messages or exchange messages without anyone else seeing them

> The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.
>
> *See: HIPAA, personal information, Privacy Act of 1974*
> *RFC 4949, Internet Security Glossary*

Privacy is a reason for confidentiality

Integrity

- The trustworthiness of the data or resources
- Preventing unauthorized changes to the data or resources
- **Data integrity**
  - Data integrity: property that data has not been modified or destroyed in an unauthorized or accidental manner
- **Origin integrity**
  - Authentication
- **System integrity**
  - The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

Often more important than confidentiality!

Availability

- Being able to use the data or resources
- Property of a system being accessible and capable of working to required performance specifications

Turning off a computer provides confidentiality & integrity but hurts availability

Denial of Service *(DoS) attacks target availability*

Thinking about security

Security is not

adding encryption

… or using a 512-bit key instead of a 64-bit key

… or changing passwords

… or setting up a firewall

It is a systems issue

= Hardware + firmware + OS + app software + networking + people

= Processes & procedures, policies, detection, forensics

“Security is a chain: it’s only as secure as the weakest link”

– Bruce Schneier

Security is hard

- Software is complex
  - Windows 10: ~50 million lines of code
  - Google services comprise ~2 billion lines of code
  - Linux distribution: ~200 million lines of code
    Over 2 million lines of code added to the kernel in 2018

Try to find the bugs!

- Systems are complex
  - Lots of layers: microcode + firmware + OS + libraries + apps + devices
  - Lots of elements: clients, servers, networks, embedded devices
  - Interaction with cloud services
  - Third party components
  - Complex interaction models
  - All parts are not always under control of one administrator
- Human factor
  - People make mistakes

Some big breaches

Some big breaches

- **2018: City of Atlanta, Georgia**
  - Ransomware attack
- **2018: City of New Haven, Connecticut**
  - Ransomware attack
- **2019: Jackson County, Georgia**
  - Ransomware attack – Georgia paid $400,000 in ransom
- **2019: City of Albany, New York**
  - Ransomware attack
- **2019: More ransomware attacks on municipalities**
  - Augusta, Maine
  - Greenville, North Carolina
  - Imperial County, California
  - Baltimore, Maryland
  - Riviera Beach, Florida (paid $600,000 in Bitcoin)
- **2017: *The Dark Overlord* hacking group leaks *Orange Is the New Black episodes***
  - Leaked the latest season … even after receiving $50,000 in ransom

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Big breaches: 2016 - Petya

- **Encrypting malware that targets Microsoft Windows systems**
  - – Infects boot record & encrypts the system's file system
  - – Prevents Windows from booting and encrypts file contents
  - – Ransomware – demands that a make a payment in Bitcoin to regain access

- **June 2017 – NotPetya – new variant of Petya launched**
  - – Major global cyberattack:
    - Targeted Russia and Ukraine mostly
    - Also hit France, Germany, Italy, Poland, UK, US
  - – Spread via software update mechanism of M.E. Doc, a Ukrainian tax preparation program
  - – CIA attributed NotPetya to Russian military hackers – the GRU spy agency
  - – Damages estimated to be over $10 billion

Some big breaches

- **2017: Equifax**
  - Names, addresses, social security #s, birth dates, etc. of 143 million customers
  - Application vulnerability
- **2016: Adult Friend Finder**
  - 20 years of data from six databases covering 412 million accounts. Passwords were weakly protected, so most could be cracked.
- **2016: Uber**
  - Personal information of 57 million Uber users and 600,000 drivers
  - Uber's GitHub account accessed, which gave hackers access to Uber's AWS account
  - Uber paid the hackers $100,000 to destroy the data (with no proof that was done!)
- **2015: Anthem Insurance**
  - Contact info, birth dates, and social security numbers of 78.7 million current and former customers
- **2014-2018: Marriott**
  - Information on 500 million customers stolen. Contact info, passport numbers, travel information, credit cards of 100M customers. Attackers remained in the system from 2014 to 2018.
- **2013: Adobe**
  - Hackers stole nearly 3M encrypted credit card records & login information for ~150M users

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Some big breaches

- **2013: Target Stores**
  - Credit card & contact information of up to 110 million people
- **2011: Sony's PlayStation Network**
  - 77 million PlayStation Network accounts hacked – site down for 1 month: $171 million loss
  - 12 million accounts had unencrypted credit card numbers
- **2011: RSA Security**
  - Possibility that information on RSA's SecurID authentication tokens was stolen
  - Two separate hacker groups allegedly working with a foreign government launched a series of phishing attacks
- **2008: Heartland Payment Systems**
  - 134 million credit cards processed by 175,000 merchants
  - Well known SQL injection attack – Discovered 10 months after attack
- **2006: TJX Companies**
  - 94 million credit cards stolen; cards, banks, insurers lost close to $200 million

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Some big breaches

- **2012-2014: U.S. Office of Personnel Management**
  - Personal information of 22 million current & former federal employees, including security clearance information, family info, every place people lived & traveled, & fingerprint data
  - Well known SQL injection attack – Discovered 10 months after attack
- **2013, 2014: Yahoo!**
  - Names, addresses, dates of birth, phone #s, passwords, security questions of 3 billion accounts
  - Information on 500M users reported stolen in 2013
- **2014: eBay**
  - Names, addresses, birthdays, encrypted passwords of 145 million users
  - Hackers used credentials of three employees and had complete inside access
- **2014: JP Morgan Chase**
  - Contact & internal info of 76 million households & 7 million small businesses
  - Israeli hackers gained root privileges on >90 of the bank's servers
  - JP Morgan spends $250 million on security every year!
- **2014: Home Depot**
  - 56 million credit cards
  - Malware that posed as anti-virus software

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Just a few recent security breaches

ZDNet

600,000 GPS trackers left exposed online with a default password of ‘123456’

Default password is a danger for customers, but also for the vendor itself.

By Catalin Cimpanu • September 5, 2019

At least 600,000 GPS trackers manufactured by a Chinese company are using the same default password of "123456," security researchers from Czech cyber-security firm Avast disclosed today.

They say that hackers can abuse this password to hijack users' accounts, from where they can spy on conversations near the GPS tracker, spoof the tracker's real location, or get the tracker's attached SIM card phone number for tracking via GSM channels.

OVER 30 GPS TRACKER MODELS IMPACTED

Avast researchers said they found these issues in T8 Mini, a GPS tracker manufactured by Shenzhen i365-Tech, a Chinese IoT device maker.

However, as their research advanced, Avast said the issues also impacted over 30 other models of GPS trackers, all manufactured by the same vendor, and some even sold as white-label products, bearing the logos of other companies.

https://www.zdnet.com/article/600000-gps-trackers-left-exposed-online-with-a-default-password-of-123456/

Twitter disables SMS-to-tweet feature after its CEO got hacked last week

Twitter disables one of the site's earliest features in response to CEO getting hacked last week.

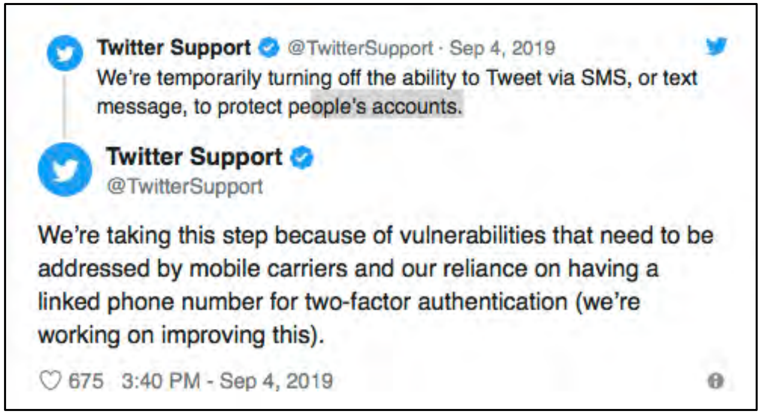
By Catalin Cimpanu • September 4, 2019

Twitter is disabling the ability to send tweets via SMS messages after an incident last week when the company's CEO Twitter account got hacked via this feature.

The social network said the move is only temporary, but did not provide a timeline for the feature's reactivation.

Twitter blamed the whole issue on mobile networks and "vulnerabilities that need to be addressed by mobile carriers."

According to a statement Twitter published last week, hackers took control of Jack Dorsey's phone number and used the SMS-to-tweet feature to publish offensive tweets on the CEO's official account last Friday, August 30.



Twitter Support @TwitterSupport · Sep 4, 2019

We're temporarily turning off the ability to Tweet via SMS, or text message, to protect people's accounts.

Twitter Support
@TwitterSupport

We're taking this step because of vulnerabilities that need to be addressed by mobile carriers and our reliance on having a linked phone number for two-factor authentication (we're working on improving this).

♡ 675 3:40 PM - Sep 4, 2019

TechCrunch

A huge database of Facebook users' phone numbers found online

Zack Whittaker • September 4, 2019

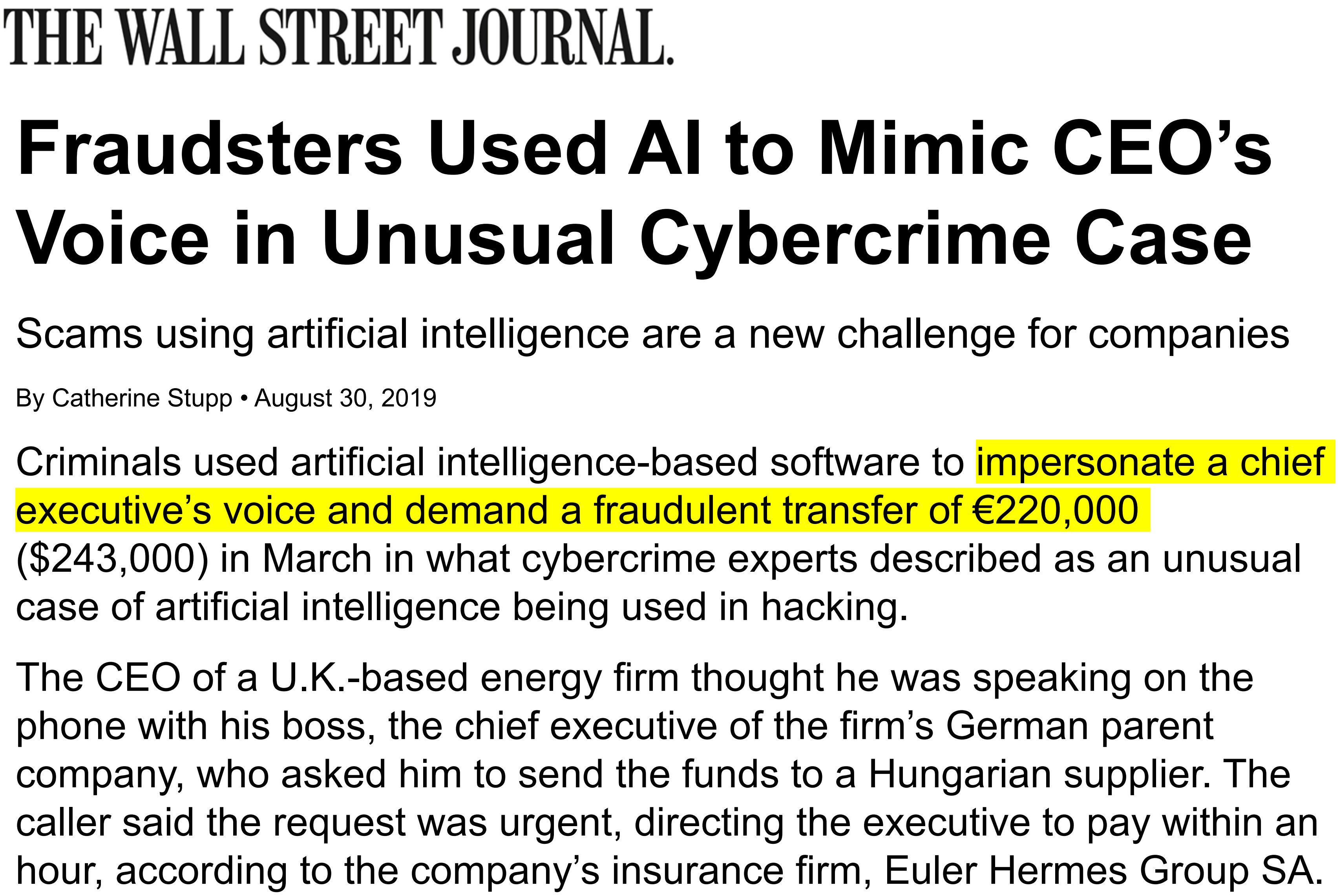
Hundreds of millions of phone numbers linked to Facebook accounts have been found online.

The exposed server contained more than 419 million records over several databases on users across geographies, including 133 million records on U.S.-based Facebook users, 18 million records of users in the U.K., and another with more than 50 million records on users in Vietnam.

But because the server wasn't protected with a password, anyone could find and access the database.

Each record contained a user's unique Facebook ID and the phone number listed on the account. A user's Facebook ID is typically a long, unique and public number associated with their account, which can be easily used to discern an account's username.

https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/



THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp • August 30, 2019

Criminals used artificial intelligence-based software to impersonate a chief executive’s voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm’s German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company’s insurance firm, Euler Hermes Group SA.

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

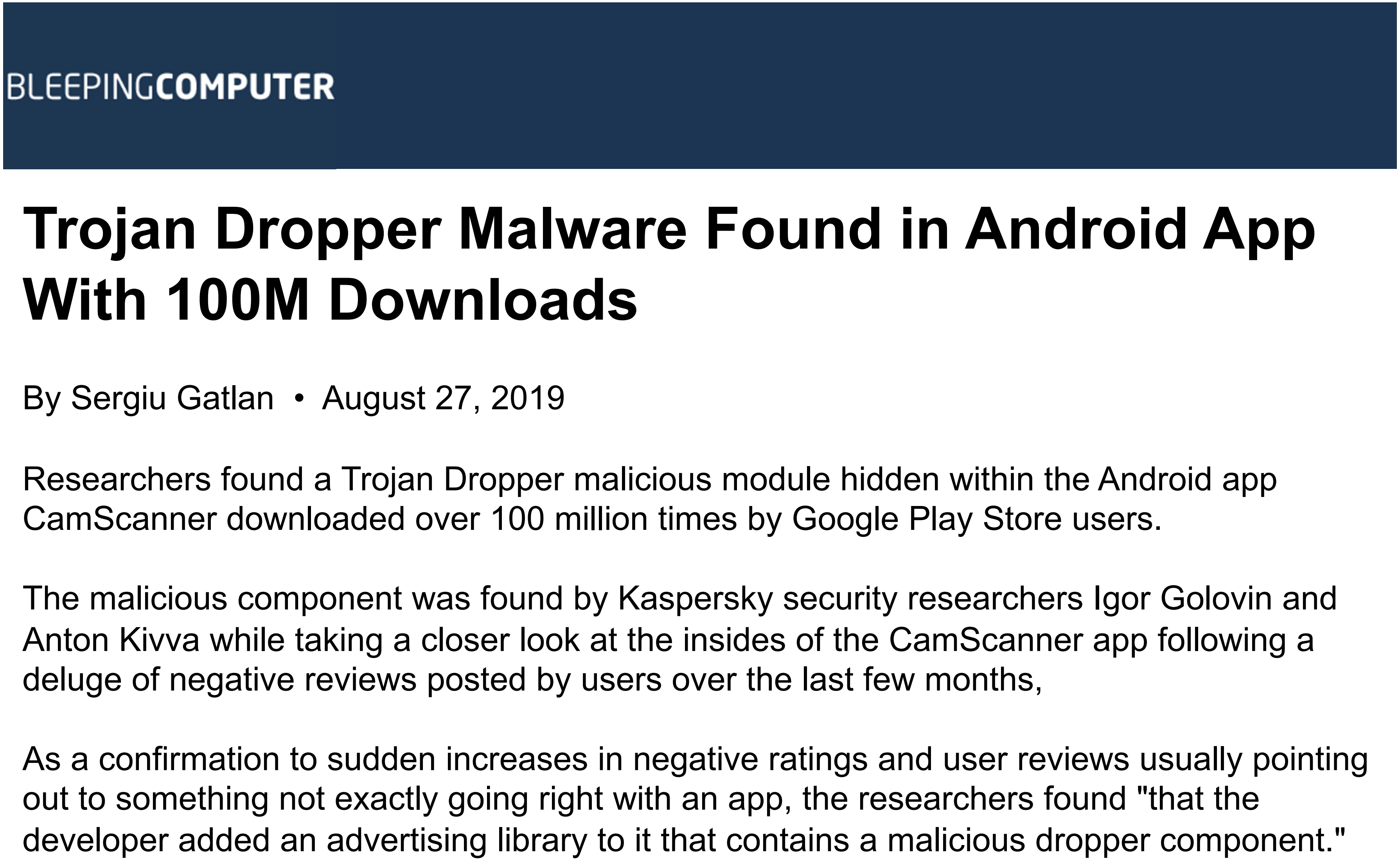
Cybersecurity Firm Imperva Discloses Breach

August 19 2019

Imperva, a leading provider of Internet firewall services that help Web sites block malicious cyberattacks, alerted customers on Tuesday that a recent data breach exposed email addresses, scrambled passwords, API keys and SSL certificates for a subset of its firewall users.

Redwood Shores, Calif.-based Imperva sells technology and services designed to detect and block various types of malicious Web traffic, from denial-of-service attacks to digital probes aimed at undermining the security of Web-based software applications.

https://krebsonsecurity.com/2019/08/cybersecurity-firm-imperva-discloses-breach/



BLEEPINGCOMPUTER

Trojan Dropper Malware Found in Android App With 100M Downloads

By Sergiu Gatlan • August 27, 2019

Researchers found a Trojan Dropper malicious module hidden within the Android app CamScanner downloaded over 100 million times by Google Play Store users.

The malicious component was found by Kaspersky security researchers Igor Golovin and Anton Kivva while taking a closer look at the insides of the CamScanner app following a deluge of negative reviews posted by users over the last few months,

As a confirmation to sudden increases in negative ratings and user reviews usually pointing out to something not exactly going right with an app, the researchers found "that the developer added an advertising library to it that contains a malicious dropper component."

https://www.bleepingcomputer.com/news/security/trojan-dropper-malware-found-in-android-app-with-100m-downloads/

August 2019

Democratic Senate campaign group exposed 6.2 million Americans' emails

Zack Wittaker • August 6, 2019

A political campaign group working to elect Democratic senators left on an exposed server a spreadsheet containing the email addresses of 6.2 million Americans.

Data breach researchers at security firm UpGuard found the data in late July, and traced the storage bucket back to a former staffer at the Democratic Senatorial Campaign Committee, an organization that seeks grassroots donations and contributions to help elect Democratic candidates to the U.S. Senate.

https://techcrunch.com/2019/08/06/democratic-senate-millions-emails/

(April) August 2019

Microsoft catches Russian state hackers using IoT devices to breach networks

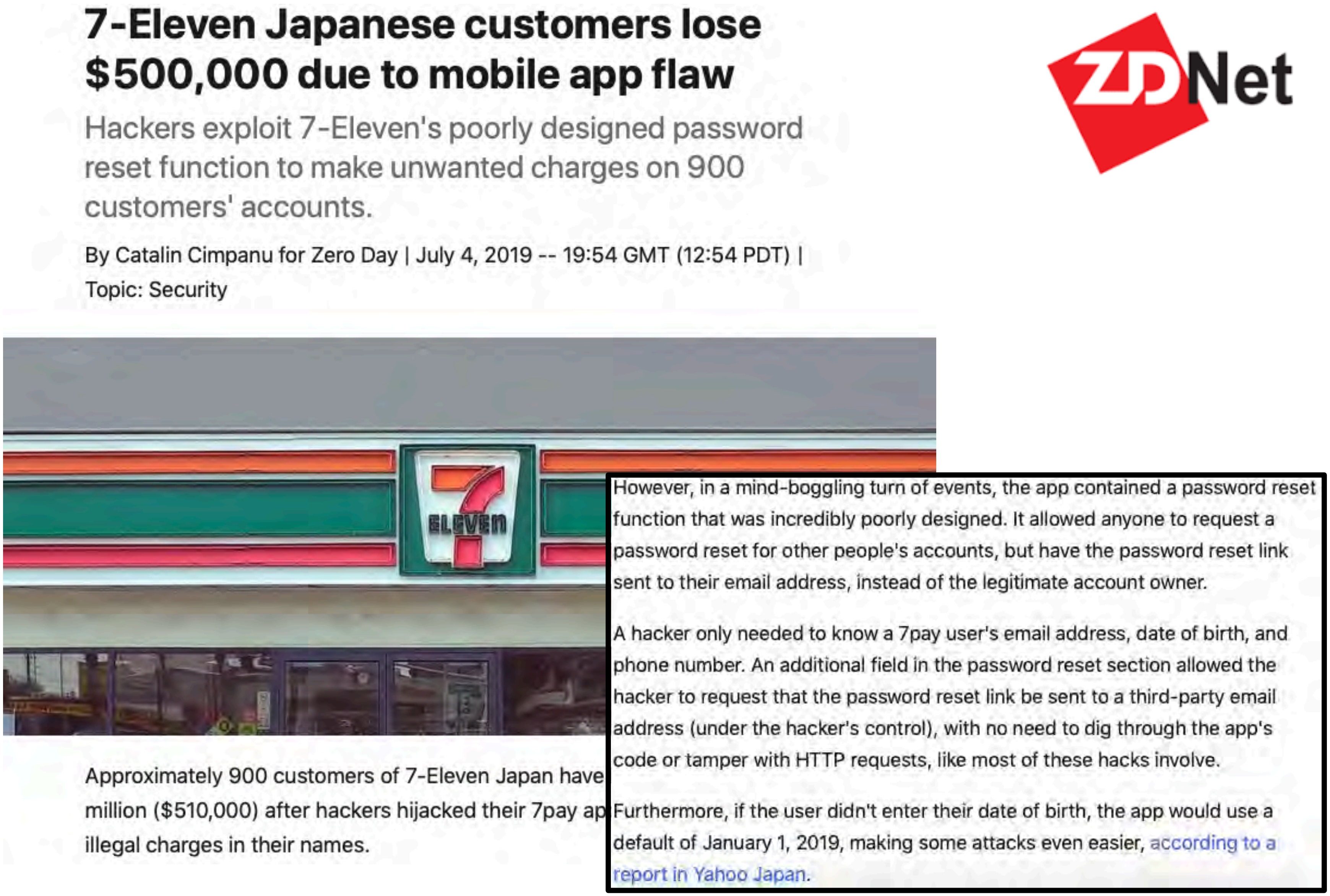
Fancy Bear servers are communicating with compromised devices inside corporate networks.

Dan Goodin – 8/5/2019 3:15 PM

Hackers working for the Russian government have been using printers, video decoders, and other so-called Internet-of-things devices as a beachhead to penetrate targeted computer networks, Microsoft officials warned on Monday.

“These devices became points of ingress from which the actor established a presence on the network and continued looking for further access,” officials with the Microsoft Threat Intelligence Center wrote in a post. “Once the actor had successfully established access to the network, a simple network scan to look for other insecure devices allowed them to discover and move across the network in search of higher-privileged accounts that would grant access to higher-value data.”

https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/



7-Eleven Japanese customers lose $500,000 due to mobile app flaw

Hackers exploit 7-Eleven's poorly designed password reset function to make unwanted charges on 900 customers' accounts.

By Catalin Cimpanu for Zero Day | July 4, 2019 -- 19:54 GMT (12:54 PDT) | Topic: Security

Approximately 900 customers of 7-Eleven Japan have
million ($510,000) after hackers hijacked their 7pay ap
illegal charges in their names.

However, in a mind-boggling turn of events, the app contained a password reset function that was incredibly poorly designed. It allowed anyone to request a password reset for other people's accounts, but have the password reset link sent to their email address, instead of the legitimate account owner.

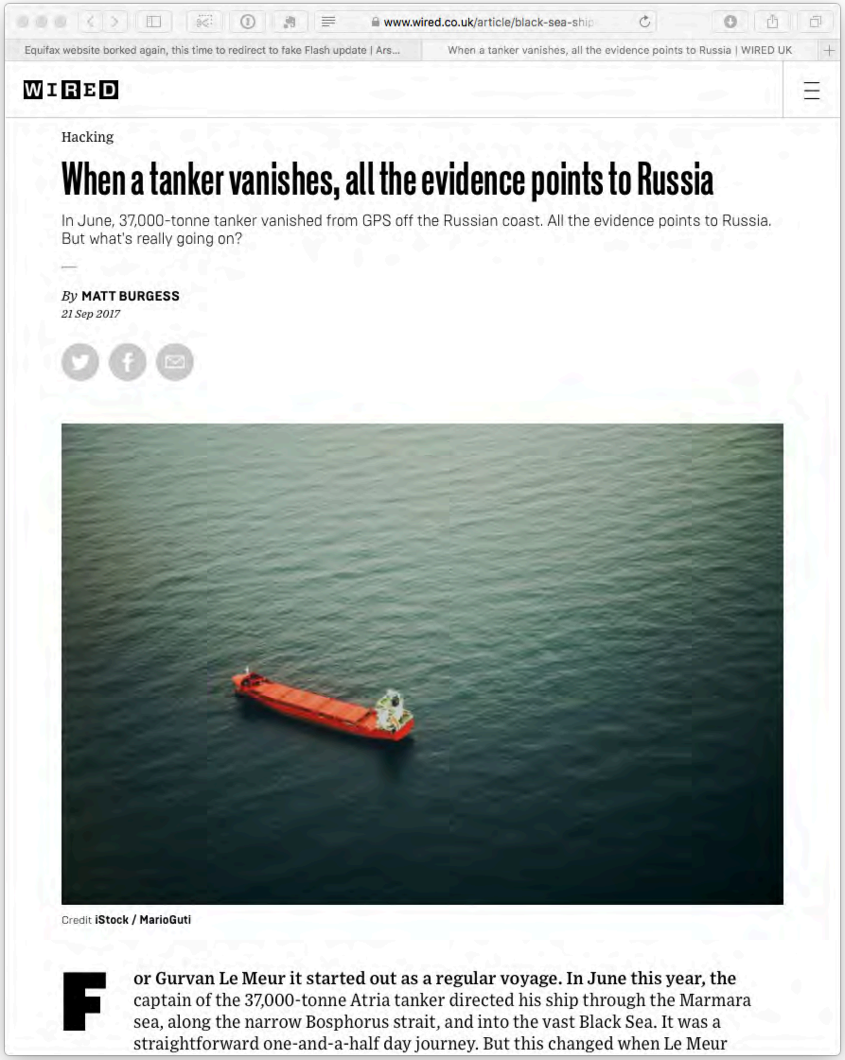
A hacker only needed to know a 7pay user's email address, date of birth, and phone number. An additional field in the password reset section allowed the hacker to request that the password reset link be sent to a third-party email address (under the hacker's control), with no need to dig through the app's code or tamper with HTTP requests, like most of these hacks involve.

Furthermore, if the user didn't enter their date of birth, the app would use a default of January 1, 2019, making some attacks even easier, according to a report in Yahoo Japan.

https://www.zdnet.com/article/7-eleven-japanese-customers-lose-500000-due-to-mobile-app-flaw/

Some more things to worry about

2017 – GPS hacking



www.wired.co.uk/article/black-sea-ship

Equifax website borked again, this time to redirect to fake Flash update | Ars...

When a tanker vanishes, all the evidence points to Russia | WIRED UK

WIRED

Hacking

When a tanker vanishes, all the evidence points to Russia

In June, 37,000-tonne tanker vanished from GPS off the Russian coast. All the evidence points to Russia. But what's really going on?

—

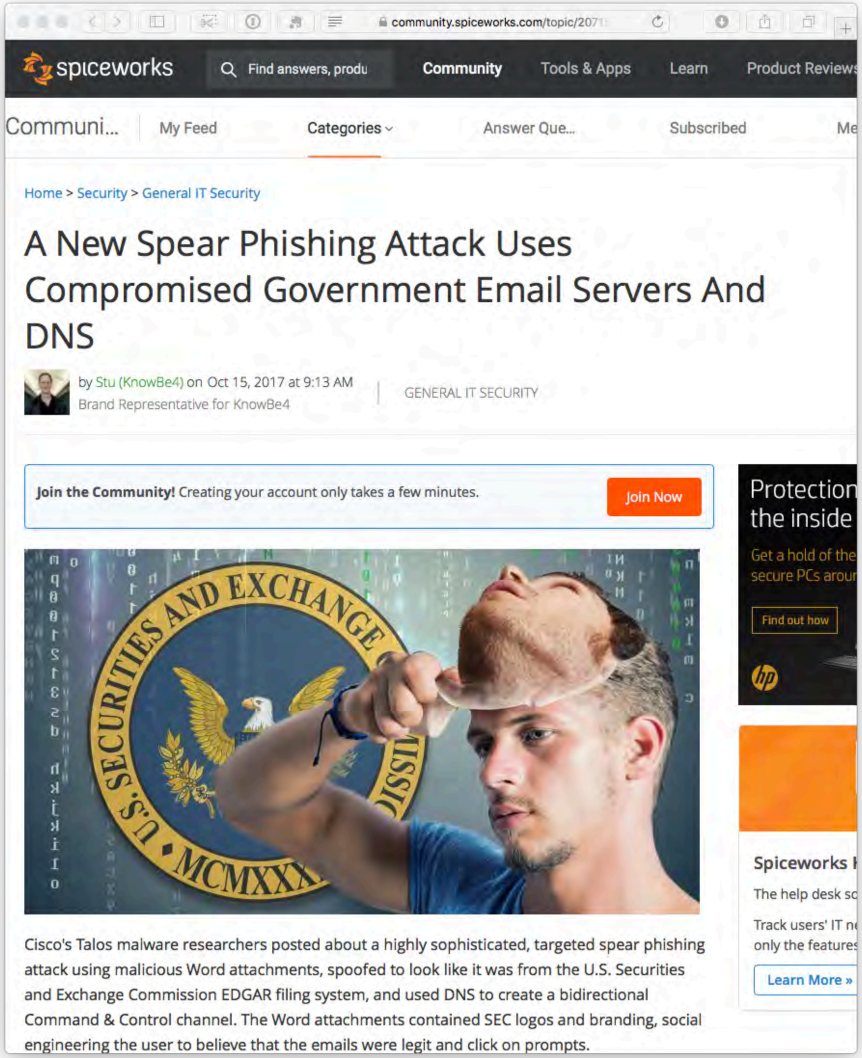
By **MATT BURGESS**

21 Sep 2017

Credit **iStock / MarioGuti**

For Gurvan Le Meur it started out as a regular voyage. In June this year, the captain of the 37,000-tonne Atria tanker directed his ship through the Marmara sea, along the narrow Bosphorus strait, and into the vast Black Sea. It was a straightforward one-and-a-half day journey. But this changed when Le Meur

2017 – Spear phishing from govt servers



Home > Security > General IT Security

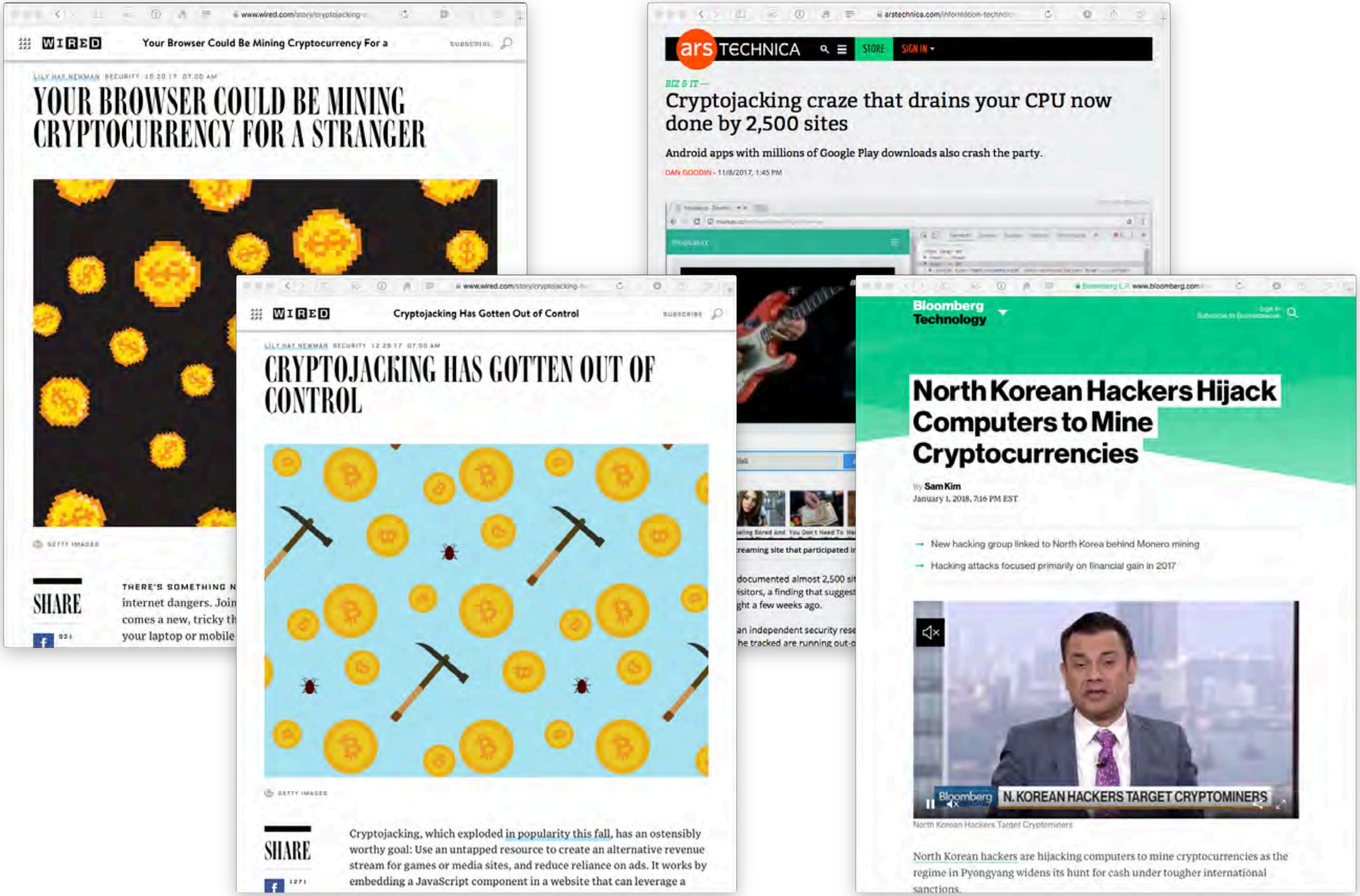
A New Spear Phishing Attack Uses Compromised Government Email Servers And DNS

by Stu (KnowBe4) on Oct 15, 2017 at 9:13 AM
Brand Representative for KnowBe4

Join the Community! Creating your account only takes a few minutes.

Cisco's Talos malware researchers posted about a highly sophisticated, targeted spear phishing attack using malicious Word attachments, spoofed to look like it was from the U.S. Securities and Exchange Commission EDGAR filing system, and used DNS to create a bidirectional Command & Control channel. The Word attachments contained SEC logos and branding, social engineering the user to believe that the emails were legit and click on prompts.

Fall 2018-now – Cryptojacking



www.wired.com/story/cryptojacking-

WIRED Your Browser Could Be Mining Cryptocurrency For a

LILY HAY NEWMAN SECURITY 10.20.17 07:00 AM

YOUR BROWSER COULD BE MINING CRYPTOCURRENCY FOR A STRANGER

GETTY IMAGES

SHARE

921

THERE'S SOMETHING N
internet dangers. Join
comes a new, tricky th
your laptop or mobile

arstechnica.com/information-technolo

ars TECHNICA STORE SIGN IN

BIZ & IT —

Cryptojacking craze that drains your CPU now done by 2,500 sites

Android apps with millions of Google Play downloads also crash the party.

DAN GOODIN - 11/8/2017, 1:45 PM

treaming site that participated in

documented almost 2,500 sit
isitors, a finding that suggest
ght a few weeks ago.

an independent security rese
he tracked are running out-o

www.wired.com/story/cryptojacking-h

WIRED Cryptojacking Has Gotten Out of Control

LILY HAY NEWMAN SECURITY 12.20.17 07:00 AM

CRYPTOJACKING HAS GOTTEN OUT OF CONTROL

GETTY IMAGES

SHARE

1271

Cryptojacking, which exploded in popularity this fall, has an ostensibly worthy goal: Use an untapped resource to create an alternative revenue stream for games or media sites, and reduce reliance on ads. It works by embedding a JavaScript component in a website that can leverage a

Bloomberg L.P. www.bloomberg.com

Bloomberg Technology

North Korean Hackers Hijack Computers to Mine Cryptocurrencies

By Sam Kim
January 1, 2018, 7:16 PM EST

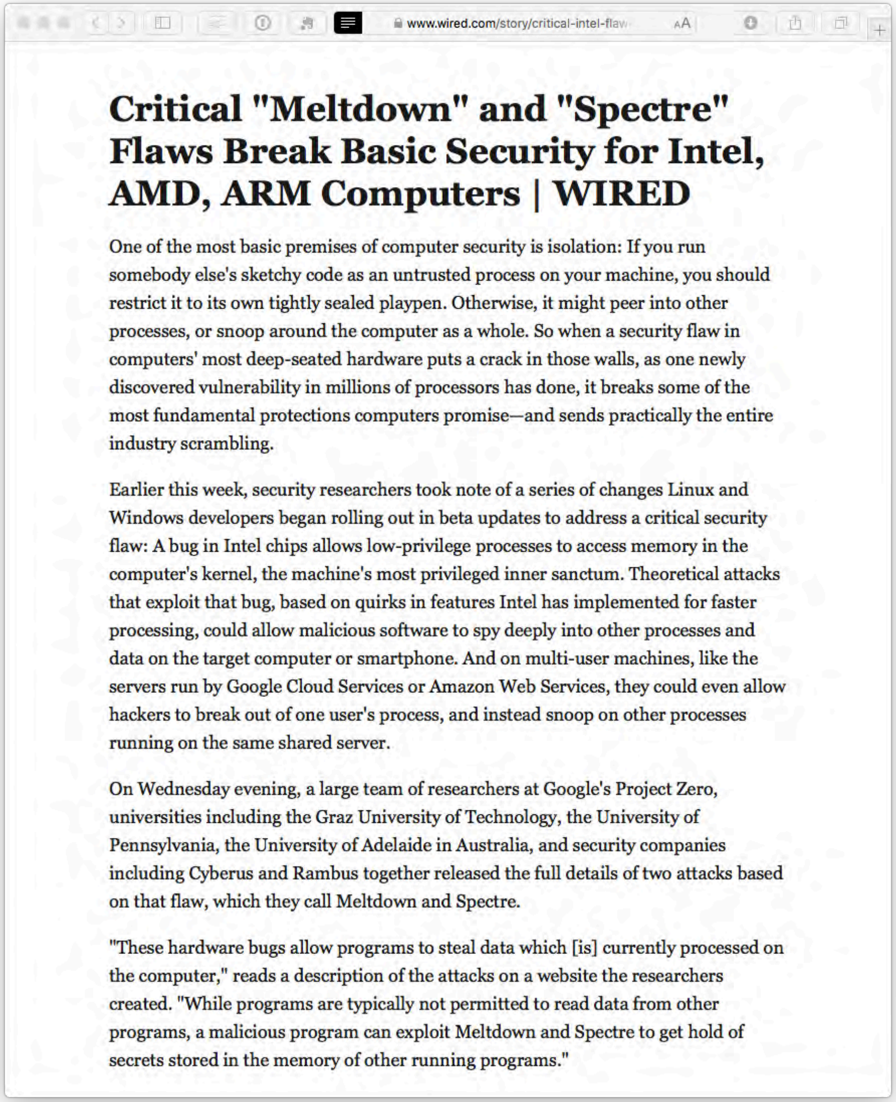
- New hacking group linked to North Korea behind Monero mining
- Hacking attacks focused primarily on financial gain in 2017

North Korean Hackers Target Cryptominers

North Korean hackers are hijacking computers to mine cryptocurrencies as the regime in Pyongyang widens its hunt for cash under tougher international sanctions.

Jan 2018 – Meltdown & Spectre

- Intel chips do not do full memory protection when doing speculative execution
- Vulnerability existed for 20 years!
- Meltdown
  - Allows processes to access kernel memory
- Spectre
  - Allows processes to steal data from the memory of other processes
- Also affects ARM & AMD CPUs



Critical "Meltdown" and "Spectre" Flaws Break Basic Security for Intel, AMD, ARM Computers | WIRED

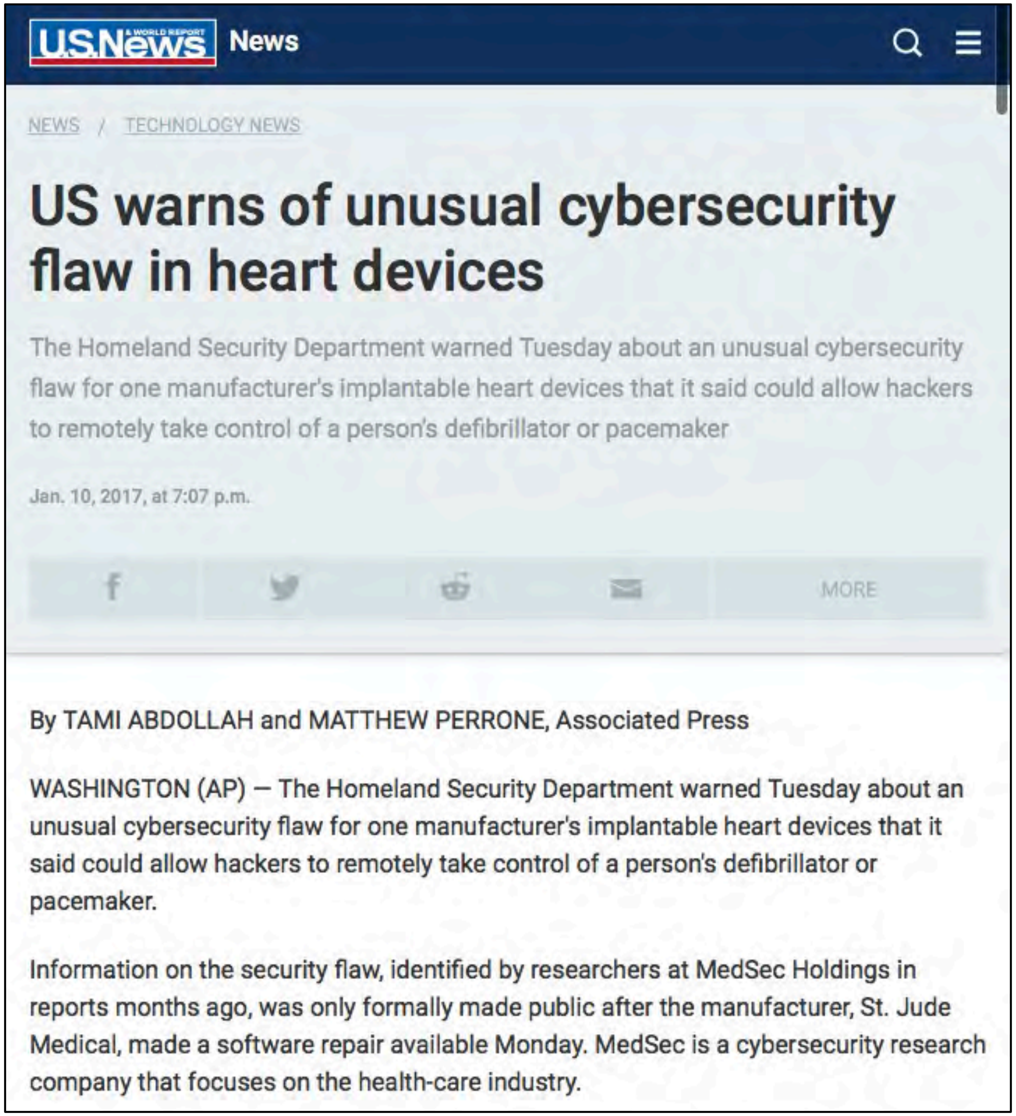
One of the most basic premises of computer security is isolation: If you run somebody else's sketchy code as an untrusted process on your machine, you should restrict it to its own tightly sealed playpen. Otherwise, it might peer into other processes, or snoop around the computer as a whole. So when a security flaw in computers' most deep-seated hardware puts a crack in those walls, as one newly discovered vulnerability in millions of processors has done, it breaks some of the most fundamental protections computers promise—and sends practically the entire industry scrambling.

Earlier this week, security researchers took note of a series of changes Linux and Windows developers began rolling out in beta updates to address a critical security flaw: A bug in Intel chips allows low-privilege processes to access memory in the computer's kernel, the machine's most privileged inner sanctum. Theoretical attacks that exploit that bug, based on quirks in features Intel has implemented for faster processing, could allow malicious software to spy deeply into other processes and data on the target computer or smartphone. And on multi-user machines, like the servers run by Google Cloud Services or Amazon Web Services, they could even allow hackers to break out of one user's process, and instead snoop on other processes running on the same shared server.

On Wednesday evening, a large team of researchers at Google's Project Zero, universities including the Graz University of Technology, the University of Pennsylvania, the University of Adelaide in Australia, and security companies including Cyberus and Rambus together released the full details of two attacks based on that flaw, which they call Meltdown and Spectre.

"These hardware bugs allow programs to steal data which [is] currently processed on the computer," reads a description of the attacks on a website the researchers created. "While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs."

Potential for physical harm



US warns of unusual cybersecurity flaw in heart devices

The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker

Jan. 10, 2017, at 7:07 p.m.

By TAMI ABDOLLAH and MATTHEW PERRONE, Associated Press

WASHINGTON (AP) — The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker.

Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry.

Hacking against the hackers

Cops Hijack Botnet, Remotely Wipe Malware From 850,000 Computers

Police in France took down a large cryptocurrency-mining malware operation with the help of a cybersecurity firm.

By Lorenzo Franceschi-Bicchierai • Aug 28 2019, 4:10pm

French police, with help from an antivirus firm, took control of a server that was used by cybercriminals to spread a worm programmed to mine cryptocurrency from more than 850,000 computers. Once in control of the server, the police remotely removed the malware from those computers.

https://www.vice.com/en_us/article/wjwd7x/cops-hijack-retadup-botnetwipe-malware-from-850000-computers

Security Goals & Definitions

Security Goals

- Prevention: prevent attackers from violating security policy
  - Implement mechanisms that users cannot override
  - *Example: ask for a password*
- Detection: detect & report attacks
  - Important when prevention fails
  - Indicates & identifies weaknesses with prevention
  - Also: detect attacks even if prevention is successful
- Recovery: stop the attack, repair damage
  - … Or continue to function correctly even if attack succeeds
  - Forensics: identify what happened so you can fix it
  - *Example: restoration from backups*

Policies & Mechanisms

Policy: what is or is not allowed

- Can be expressed in natural language ("this is our security policy")
- Mathematics
- Policy language - to provide precision together with ease of understanding

Mechanisms: implement and enforce policies

- E.g., password entry & authentication

- *What mechanisms do we need to secure a system?*
- *What level of assurance is associated with them?*

Security Engineering

- Security Architecture
  - How do we put a secure system together?
  - How do we identify potential weaknesses?
- Security Engineering
  - Implement mechanisms & policy into a system
- Engineering = making compromises
  - Understand tradeoffs
  - Security vs. cost, performance, acceptability, usability, security
  - Cost-benefit analysis
    - Is it cheaper to prevent an attack or recover?
    - Who pays & who gets punished?
      - Microsoft is not responsible for dealing with your loss

Protection: Know Your Enemy!

Different attackers

… Who have different goals

… And different skill levels

What we want to – or need to – guard against?

What are you securing your system against?

And from whom?

- Yourself accidentally deleting important system files?
- Your colleagues not being able to look at your files on a file server?
- A company trying to find out about you and get personal data?
- A phone carrier tracking your movement?
- A grenade destroying your system?
- Video surveillance on streets?
- The NSA?

Risk analysis

- Should we protect something?
- How carefully?
- How much should we spend?

Laws & customs

- Are any security measures illegal?
  - Example: types of encryption
- Are any measures unlikely to be used?
  - Example: retina scans, urine tests
  - Conformance: balance security vs. effort

Definitions

- Vulnerability
  - A weakness in the implementation or operation of a system
- Attack vector
  - A means of exploiting a vulnerability
- Threat
  - an adversary that is capable of attacking

Vulnerabilities

- Failures in the system
- Bugs
- Big focus in security classes

What if a system had no vulnerabilities?

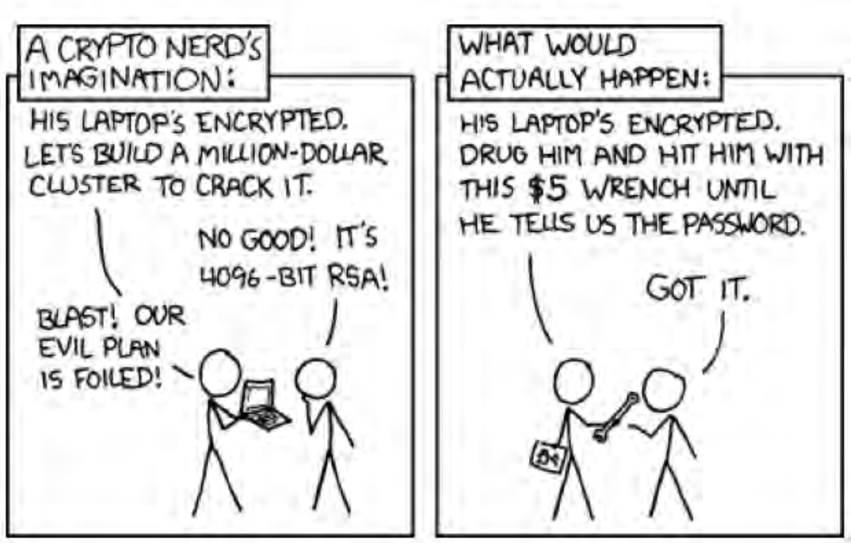
Would you not worry about threats?

Attack surfaces & vectors

- **Attack vector**
  - Failure in a line of defense
  - Technique that a security attack uses to compromise the security
  - Examples: email attachments, instant messages, phishing, malware
  - Attack vectors exploit vulnerabilities (in users or programs)
    - Input buffer limit checks, input validation bugs, protocol bugs, unprotectd files
- **Attack surface**
  - The total number of all possible places in a system that an attacker might use to try to get into an environment
  - These places may or may not have vulnerabilities
- **Goal**: be aware of the attack surface of an environment
  - Otherwise you don't know what to defend
  - If possible, reduce the attack surface: less to protect

Threats

- Lot of variations
- Different attackers have different abilities
- Are enemies sufficiently motivated to attack you?
- Attackers can often resort to the three Bs:
  - Burglary, Bribery, or Blackmail


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

AT&T employees took bribes to plant malware on the company's network

DOJ charges Pakistani man with bribing AT&T employees more than $1 million to install malware on the company's network, unlock more than 2 million devices.

By Catalin Cimpanu for Zero Day | August 6, 2019 -- 14:02 GMT (07:02 PDT) | Topic: Security

AT&T employees took bribes to unlock millions of smartphones, and to install malware and unauthorized hardware on the company's network, the Department of Justice said yesterday.

These details come from a DOJ case opened against Muhammad Fahd, a 34-year-old man from Pakistan, and his co-conspirator, Ghulam Jiwani, believed to be deceased.

Threat categories

- Disclosure: Unauthorized access to data
  - *Snooping (wiretapping)*
- Deception: Acceptance of false data
  - *Injection of data, modification of data, denial of receipt*
- Disruption: Interruption or prevention of correct operation
  - *Denial of service, data deletion, or modification*
- Usurpation: Unauthorized control of some part of a system
  - *May lead to modification, spoofing, delay, denial of service*

Types of threats

- Snooping: unauthorized interception of information
  - Form of disclosure
  - Counter with confidentiality services
- Modification or alteration: unauthorized change of information
  - Form of deception, disruption or usurpation
  - Counter with integrity services
- Masquerading or spoofing: impersonation of one entity by another
  - Form of deception and usurpation
  - Counter with integrity services
- Repudiation of origin: false denial that an entity sent or created something
  - Form of deception and usurpation
  - Counter with integrity services

Types of threats

- Denial of receipt: false denial that an entity received data or a message
  - Form of deception
  - Counter with integrity & availability mechanisms
- Delay: temporary inhibition of a service
  - Form of disruption (possibly via usurpation)
  - Counter with availability mechanisms
- Denial of service: long-term inhibition of a service
  - Form of disruption (possibly via usurpation)
  - Counter with availability mechanisms

The Internet Introduces Risks

“The internet was designed to be open, transparent, and interoperable. Security and identity management were secondary objectives in system design. This lower emphasis on security in the internet’s initial design not only gives attackers a built-in advantage. It can also make intrusions difficult to attribute, especially in real time. This structural property of the current architecture of cyberspace means that we cannot rely on the threat of retaliation alone to deter potential attackers. Some adversaries might gamble that they could attack us and escape detection.”

– William J. Lynn III, Deputy Defense Secretary, 2010

http://archive.defense.gov/speeches/speech.aspx?speechid=1593

The Internet Makes It Easier To Attack

- Security was not a design consideration
- Intelligence is at the edges of the network – distributed among many players
- Access and routing not centrally managed
  - Routing decisions distributed
  - No access control: any system can be added to the Internet
- Bad actors can hide!

Conflicker worm: 2008

- Used bugs in Microsoft Windows and dictionary attacks on passwords to propagate and form a **botnet**
- Infected millions of computers in over 190 countries
  - United Kingdom Ministry of Defence, Bundeswehr (German armed forces), French Navy, Manchester City Council, Manchester Police Network
- Origin: unknown (speculation is Ukraine)

How the Internet Creates Vulnerabilities

- **Action at a distance**
  - People can be beyond our control or visibility.
- **Asymmetric medium**
  - Actors can project or harness greater force. Low barriers to entry. Offense can be more effective than defense. A small number of actors can have a large effect.
  - E.g., Anonymous, fraud spam email, or Facebook requests for money.
  - Sending millions of messages costs almost nothing
  - Small counties can hurt countries like the US or China.
- **Actors can be anonymous**
  - Nobody knows who ran Conficker. Identifying a source can be difficult.
  - Attack with impunity. Trust becomes a challenge. Are you really communicating with your bank? We don't know who fired the missile.
- **There are no borders or checkpoints**
  - China and North Korea are the only counties that control data flow to/from their country.
- **No distinction**
  - Hard to distinguish valid data from attacks
  - Can't tell what code will be harmful until it's executed

Asymmetric force

> Information Technology has “opened up a whole new asymmetry in future warfare”
>
> *– William J. Lynn III, Deputy Defense Secretary, 2010*

- Pentagon’s 15,000 networks and 7+ million computers are being probed thousands of times daily
- Traditional deterrence models of retaliation do not apply in cyberspace
- Example: **Distributed Denial of Service** (**DDoS**)
  - One company has only so many servers
    - Overload the servers and the server gets overloaded
    - Nobody can get through
    - Nothing happens to the data but service is disrupted
  - Attacks come from a network of helpers
    - Many attacks are carried out by **botnets** - computers owned by innocent people with malware
    - The botnet program periodically contacts a **command & control server** for directions

Attack Techniques

- **Social engineering**
  - Manipulating, influencing, or deceiving targets to get them to take some action that isn't in their best interest.
  - E.g., download software, plug in an infected USB device
  - Phishing & spear phishing are forms of social engineering
- **Phishing**
  - Email that looks reputable sent to a broad group of people
  - Often from bank or shipping company asking you to click on a link and fill out a form – or has a malicious attachment
- **Spear Phishing**
  - Small, focused attack via email on a particular person or organization
  - Often contains highly specific information known to the target: account number, name of friend

Areas of Attack

- **Compromised access, code/command injection**
  - Exploit known credentials
  - Take advantage of coding errors to provide input to execute arbitrary code
  - Includes keystroke logging, camera monitoring, content upload, ransomware
- **File types**
  - Unsafe in many cases as they can open an app and cause it to take action on malicious content
  - Example: execute Visual Basic programs from Microsoft Office documents
- **Web sites**
  - Offer free downloads: software, books, movies
  - Reputable sites can get infected
  - Drive-by downloads
- **Social Media**
  - Not an attack but a great source of information for hackers
  - E.g., post when you're going on vacation or going on a conference
  - Adversary can use this info for impersonation or spear phishing

Computer vs. Real-World Risks

- Attacking in the computer world is easier & less risky
  → computer attacks are more common than real-world attacks

- Privacy rules may be the same but getting data is easier
  - E.g., collect data on recent real-estate sales automatically

- Attack from a distance
  - Cowards can attack – little danger of physical capture

- Easy to cast a wide net
  - Scripting lets you knock on millions of doors
  - Automation enables attacks on a large scale
  - Attacks with small chances of success or small returns are profitable
    - Email scams, phishing, transferring fractional cents, looking for weaknesses

Computer vs. Real-World Risks

- Physical world risks are low (for most of us)
  - Most people are not attacked
  - Most people are not victims of espionage
- Same threats in cyberspace as real-world threats:
  - Theft, vandalism, extortion, fraud, coercion, con games
- Same motivation by criminals
  - But the mechanisms, risks, and access are different

Threat matrix

Assess adversaries by skill vs. focus

		Focus	
		Low=Opportunistic	High=Targeted
Skill	High		Advanced Persistent Threats
	Low	Script Kiddies	

Types of threats

- **Opportunistic**
  - Attackers are not out to get you specifically
  - Cast a wide net and see who is vulnerable
  - Varying levels of skill
    - **Script kiddies**: low-skill; download hacking tools others created
    - High skill: discover vulnerabilities & create custom exploits

- **Targeted attacks**
  - They're out to get you specifically
  - Will gather background info on you
  - Low skill
    - Still requires some work – social engineering, distribution of malware, …
  - High skill: **Advanced Persistent Threats** (APT)
    - Skilled & focused attackers
    - Determined to achieve goal – may take a long time and multiple steps
    - Most difficult to guard against
    - Usually attributed to national intelligence agencies

Characteristics of attackers

- Goals
  - Damage, financial gain, get information
  - Knowing goals helps develop countermeasures
- Levels of access
  - Insiders vs. outsiders
- Risk tolerance
  - Are you willing to die? Go to jail?
- Resources
  - With money, you can buy computers & expertise – or bribe someone
  - Time is also a resource
- Expertise
- Economics
  - A rational adversary will balance time, money, risk, and likelihood of success

Who are the adversaries?

- Hackers
  - Good or evil
  - Test boundaries of the system – get to know system better than designers
  - Only a small % are smart; the rest are script kiddies
  - Bug hunters – find vulnerabilities
  - Exploit writers – write code to exploit the vulnerabilities
  - White hat hackers: do not intend to cause damage – goal = profit or fixing bugs
  - Black hat hackers: profit by hacking or selling services to highest bidder
- Criminals
  - Individuals or small groups
  - Don’t necessarily reap huge $ but are often creative
- Malicious insiders
  - Insidious because they are indistinguishable from legitimate, trusted insiders
  - Perimeter defenses don’t work
  - Often have high levels of access
  - E.g., Edward Snowden (sysadmins can have a LOT of access)

Who are the adversaries?

- Industrial spies
  - Product designs, trade secrets, project bids, finances, employee info
  - Can hire/bribe employees to reveal trade secrets or become inside attackers
  - … or resort to dumpster diving
  - Risk averse: reputation of company (or country) damaged if caught
- Press (& politicians)
  - Get the scoop!
  - Social engineering, bribing, dumpster diving, track movements, eavesdrop, break in
  - Also generally risk averse for fear of losing one's reputation & career

Who are the adversaries?

- Organized crime
  - More opportunities to make money!
    Steal & sell cell phone IDs, credit card #s, debit card info, get cash
  - Money laundering easier with EFT and anonymous currency like bitcoin

- Police
  - Risk averse but have law on their side (e.g., search warrants, seizing evidence)
  - Not above breaking law: wiretaps, destruction of evidence, disabling body cameras, illegal search & seizure

- Terrorists (freedom fighters)
  - Motivated by geopolitics, religion, or a set of ethics
  - Examples: Earth First, Hezbollah, ISIS,
    Aryan Nations, Greenpeace, and PETA
  - Usually more concerned with causing harm than getting specific information
  - Usually (not always) low budgets & low skill levels

Who are the adversaries?

- National intelligence organizations
  - – Huge money & long-term goals
  - – Somewhat risk averse
    - Bad public relations
    - Do not want leaks to reveal attack techniques
  - – Often have a lot of influence
    - NSA was instrumental in the adoption of 56-bit keys for DES or the Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator)
    - Lenovo computers, owned partially by the Chinese government's Academy of Sciences has been accused of "malicious circuits" built into the computers
    - NSA planted backdoors into Cisco routers built for export that allows the NSA to intercept any communications through those routers.
- Infowarriors – cyber warfare
  - – Huge money & short-term goals
  - – Disrupt power grids, commerce, transportation
  - – EMP weapons, spread selective information, misinformation, blackmail

Nation State Attacks

Microsoft notified 10,000 victims of nation-state attacks

Most of the attacks came from state-sponsored hacking groups in Iran, North Korea, and Russia.

By Catalin Cimpanu for Zero Day | July 18, 2019

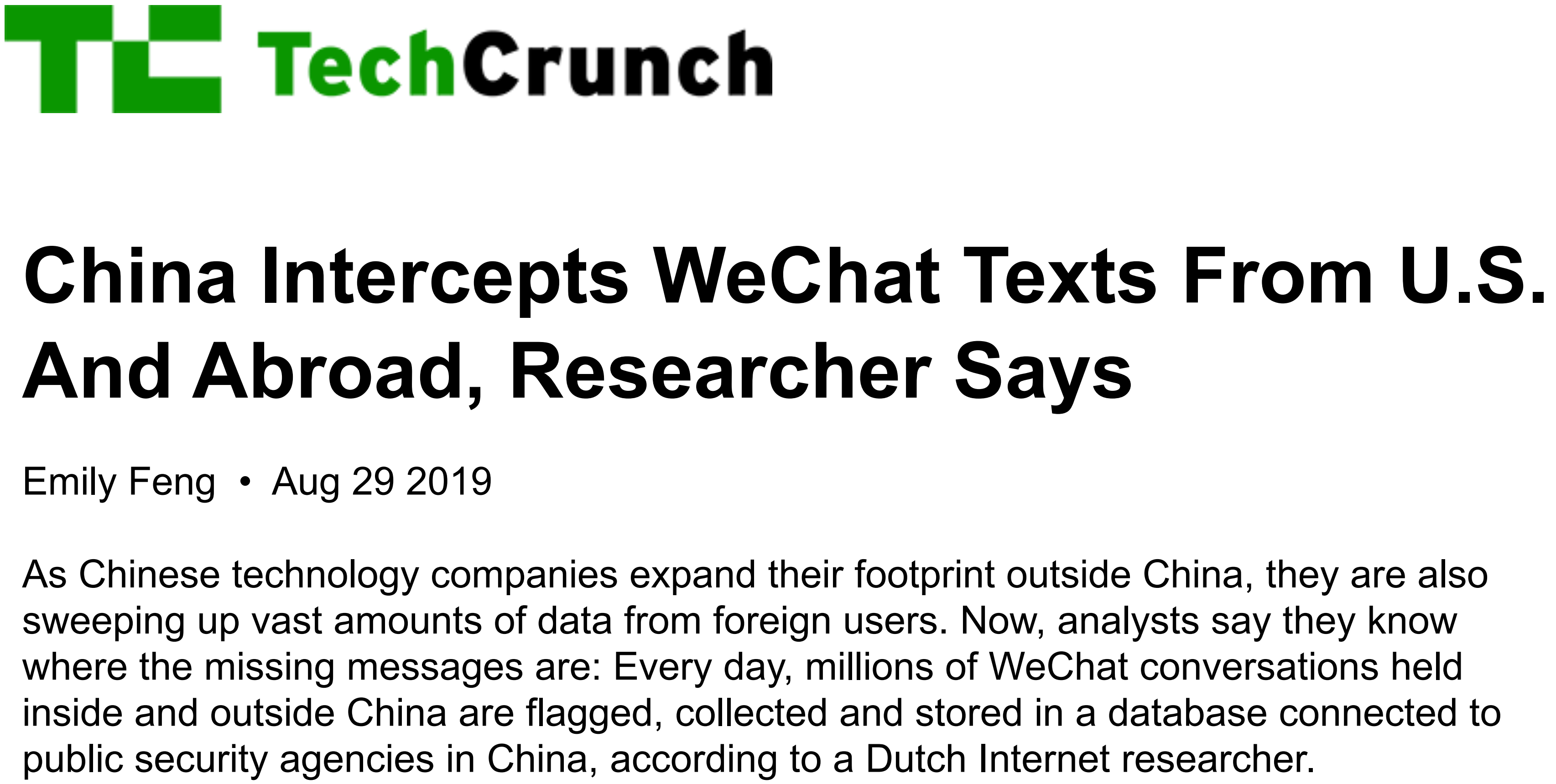
Microsoft said that over the past year it notified nearly 10,000 users that they'd been targeted or compromised by nation-state hacking groups.

The company didn't just blast out random statistics, but also named names. Microsoft said most of the attacks came from state-sponsored hackers from Iran, North Korea, and Russia.

More precisely, the Iran attacks came from groups Microsoft calls Holmium and Mercury, the North Korean attacks came from a group called Thallium, and the Russian attacks came from groups called Yttrium and Strontium.

https://www.zdnet.com/article/microsoft-notified-10000-victims-of-nation-state-attacks/

Nation state cooperation with app makers?



TechCrunch

China Intercepts WeChat Texts From U.S. And Abroad, Researcher Says

Emily Feng • Aug 29 2019

As Chinese technology companies expand their footprint outside China, they are also sweeping up vast amounts of data from foreign users. Now, analysts say they know where the missing messages are: Every day, millions of WeChat conversations held inside and outside China are flagged, collected and stored in a database connected to public security agencies in China, according to a Dutch Internet researcher.

https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says

TechCrunch

New iPhone Hack Shock For 1 Billion Apple Users As Attacker Is Revealed

Zack Whittaker • Sept 1 2019

A number of malicious websites used to hack into iPhones over a two-year period were targeting Uyghur Muslims, TechCrunch has learned.

Sources familiar with the matter said the websites were part of a state-backed attack — likely China — designed to target the Uyghur community in the country's Xinjiang state.

It's part of the latest effort by the Chinese government to crack down on the minority Muslim community in recent history. In the past year, Beijing has detained more than a million Uyghurs in internment camps, according to a United Nations human rights committee.

The websites were part of a campaign to target the religious group by infecting an iPhone with malicious code simply by visiting a booby-trapped web page. In gaining unfettered access to the iPhone's software, an attacker could read a victim's messages, passwords, and track their location in near-real time.

https://techcrunch.com/2019/08/31/china-google-iphone-uyghur/

BUSINESS INSIDER

The US hit Iran with a secret cyberattack to disrupt oil tanker attacks the same day Trump almost authorized military strikes

John Haltiwanger - Aug. 28, 2019, 5:02 PM

- A US cyberattack launched against Iran in late June in response to the downing of a US Navy drone successfully disrupted its abilities to attack oil tankers, according to a new report.
- The cyberattack "wiped out a critical database" used by Tehran to plan such attacks.
- A cybersecurity expert at Marine Corps University told Insider that the reported attack would not necessarily have been a proportional response to the downing of the drone, and was actually "deescalatory" in the sense it was "a step taken to give us options outside of war."

https://www.businessinsider.com/us-hit-iran-with-secret-cyberattack-disrupt-oil-tanker-attacks-2019-8

Are our intelligence efforts secure?

Government agencies try to develop – and pay for – the best attacking & defense techniques

But…

The American Military Sucks at Cybersecurity

A new report from US military watchdogs outlines hundreds of cybersecurity vulnerabilities.

Matthew Gault • January 23, 2019

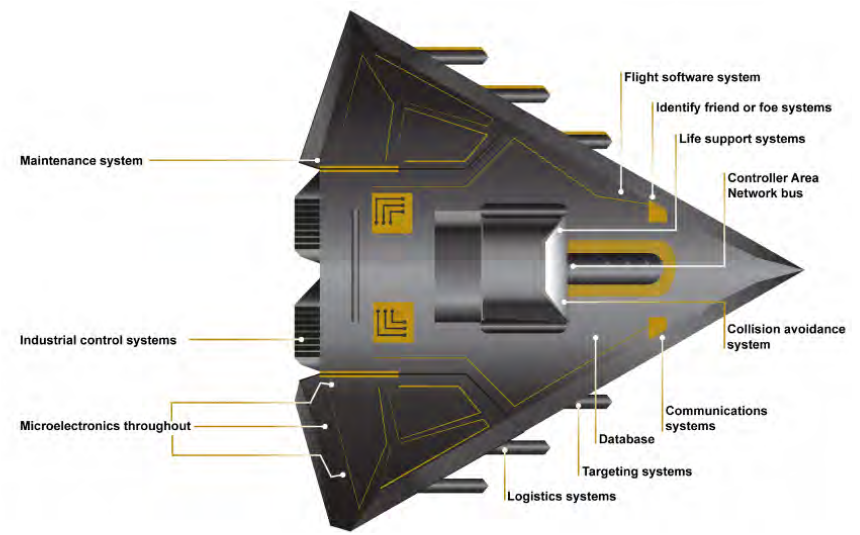
The Department of Defense is terrible at cybersecurity. That's the assessment of the Pentagon's Inspector General (IG), who did a deep dive into the American military's ability to keep its cyber shit on lockdown. The results aren't great. "As of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008," the Inspector General said in a new report.

The new report is a summary of the IG's investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they'd been addressed. Previously, the IG had recommended the Pentagon take 159 different steps to improve security. It only took 19 of them.

https://motherboard.vice.com/en_us/article/7xy5ky/the-american-military-sucks-at-cybersecurity

BLEEPINGCOMPUTER

US Advanced Weaponry Is Easy to Hack, Even by Low-Skilled Attackers


Flight software system
Identify friend or foe systems
Life support systems
Maintenance system
Controller Area Network bus
Industrial control systems
Collision avoidance system
Microelectronics throughout
Communications systems
Database
Targeting systems
Logistics systems

By Ionut Ilascu • October 9, 2018

Major weapon systems developed by the US Department of Defense are riddled with vulnerabilities that make them an easy target for adversaries trying to control them or disrupt their functions.

As the DoD plans to spend about $1.66 trillion to advance its weapons arsenal, the US Government of Accountability Office (GAO) finds reports from various development stages of the systems showing that mission-critical vulnerabilities are a regular find in "nearly all weapon systems that were under development."

Testing teams charged with probing the resilience to cyber attacks were able to take control or disable the target using basic tools and techniques. Sometimes, just scanning the system caused parts of it to shut down.

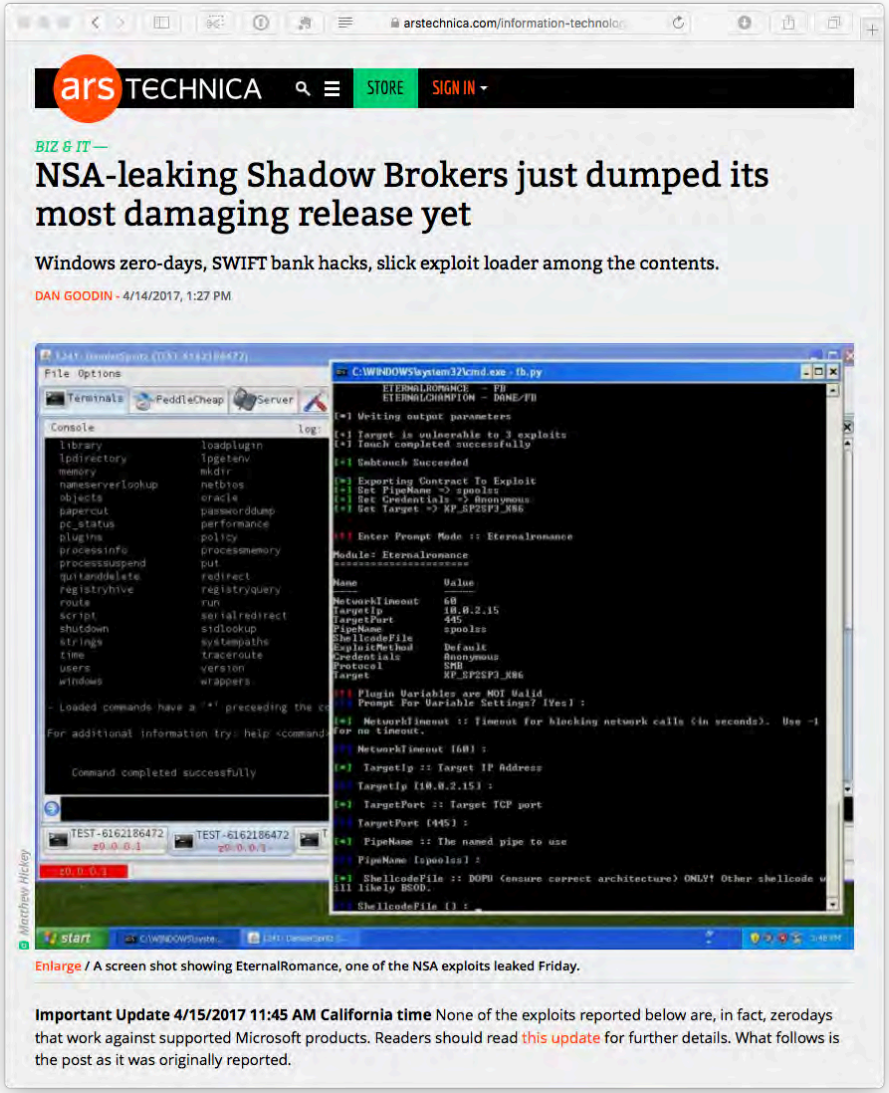
https://www.bleepingcomputer.com/news/security/us-advanced-weaponry-is-easy-to-hack-even-by-low-skilled-attackers/

March 2017 – Wikileaks publishes CIA Vault 7

- 8,761 documents stolen from the CIA
- Document spying operations & hacking tools
- iOS and Android vulnerabilities
- Bugs in Windows
- Ability to turn some smart TVs into listening devices

April 2017 – Theft from the NSA

- Shadow Brokers – the group that leaked a gigabyte of the National Security Agency's weaponized software exploits over an eight-month period
- Most vulnerabilities were patched … but lots of systems never get updated



BIZ & IT —

NSA-leaking Shadow Brokers just dumped its most damaging release yet

Windows zero-days, SWIFT bank hacks, slick exploit loader among the contents.

DAN GOODIN - 4/14/2017, 1:27 PM

```
  library                 loadplugin
  lpdirectory             lpgetenv
  memory                  mkdir
  nameserverlookup        netbios
  objects                 oracle
  papercut                passworddump
  pc_status               performance
  plugins                 policy
  processinfo             processmemory
  processsuspend          put
  quitanddelete           redirect
  registryhive            registryquery
  route                   run
  script                  serialredirect
  shutdown                sidlookup
  strings                 systempaths
  time                    traceroute
  users                   version
  windows                 wrappers

- Loaded commands have a '*' preceeding the co

For additional information try: help <command>

   Command completed successfully
```

C:\WINDOWS\system32\cmd.exe - fb.py

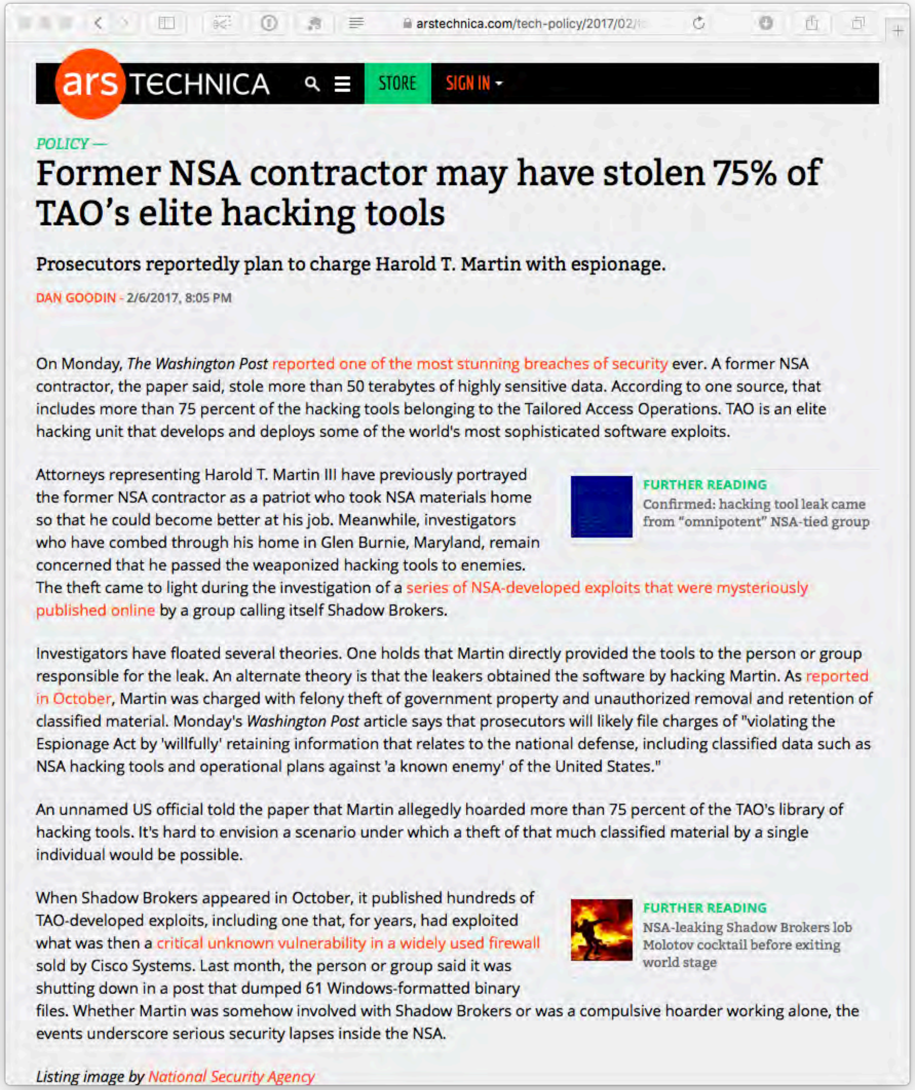
```
        ETERNALROMANCE   - FB
        ETERNALCHAMPION  - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 3 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded

[*] Exporting Contract To Exploit
[+] Set PipeName => spoolss
[+] Set Credentials => Anonymous
[+] Set Target => XP_SP2SP3_X86


[!] Enter Prompt Mode :: Eternalromance

Module: Eternalromance
======================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            10.0.2.15
TargetPort          445
PipeName            spoolss
ShellcodeFile
ExploitMethod       Default
Credentials         Anonymous
Protocol            SMB
Target              XP_SP2SP3_X86

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [10.0.2.15] :

[*]  TargetPort :: Target TCP port

[?] TargetPort [445] :

[*]  PipeName :: The named pipe to use

[?] PipeName [spoolss] :

[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] : _
```

Enlarge / A screen shot showing EternalRomance, one of the NSA exploits leaked Friday.

Important Update 4/15/2017 11:45 AM California time None of the exploits reported below are, in fact, zerodays that work against supported Microsoft products. Readers should read this update for further details. What follows is the post as it was originally reported.

Sept 2017 – TAO tools theft from NSA

- Former NSA contractor stole >50 TB of highly sensitive data
- Includes 75% of hacking tools belonging to NSA's Tailored Access Operations
- "took NSA materials home so that he could become better at his job"
- "Theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers."



POLICY —

Former NSA contractor may have stolen 75% of TAO's elite hacking tools

Prosecutors reportedly plan to charge Harold T. Martin with espionage.

DAN GOODIN - 2/6/2017, 8:05 PM

On Monday, *The Washington Post* reported one of the most stunning breaches of security ever. A former NSA contractor, the paper said, stole more than 50 terabytes of highly sensitive data. According to one source, that includes more than 75 percent of the hacking tools belonging to the Tailored Access Operations. TAO is an elite hacking unit that develops and deploys some of the world's most sophisticated software exploits.

Attorneys representing Harold T. Martin III have previously portrayed the former NSA contractor as a patriot who took NSA materials home so that he could become better at his job. Meanwhile, investigators who have combed through his home in Glen Burnie, Maryland, remain concerned that he passed the weaponized hacking tools to enemies. The theft came to light during the investigation of a series of NSA-developed exploits that were mysteriously published online by a group calling itself Shadow Brokers.

FURTHER READING
Confirmed: hacking tool leak came from "omnipotent" NSA-tied group

Investigators have floated several theories. One holds that Martin directly provided the tools to the person or group responsible for the leak. An alternate theory is that the leakers obtained the software by hacking Martin. As reported in October, Martin was charged with felony theft of government property and unauthorized removal and retention of classified material. Monday's *Washington Post* article says that prosecutors will likely file charges of "violating the Espionage Act by 'willfully' retaining information that relates to the national defense, including classified data such as NSA hacking tools and operational plans against 'a known enemy' of the United States."

An unnamed US official told the paper that Martin allegedly hoarded more than 75 percent of the TAO's library of hacking tools. It's hard to envision a scenario under which a theft of that much classified material by a single individual would be possible.

When Shadow Brokers appeared in October, it published hundreds of TAO-developed exploits, including one that, for years, had exploited what was then a critical unknown vulnerability in a widely used firewall sold by Cisco Systems. Last month, the person or group said it was shutting down in a post that dumped 61 Windows-formatted binary files. Whether Martin was somehow involved with Shadow Brokers or was a compulsive hoarder working alone, the events underscore serious security lapses inside the NSA.

FURTHER READING
NSA-leaking Shadow Brokers lob Molotov cocktail before exiting world stage

Listing image by National Security Agency

Some Nation-State Attacks (probably)

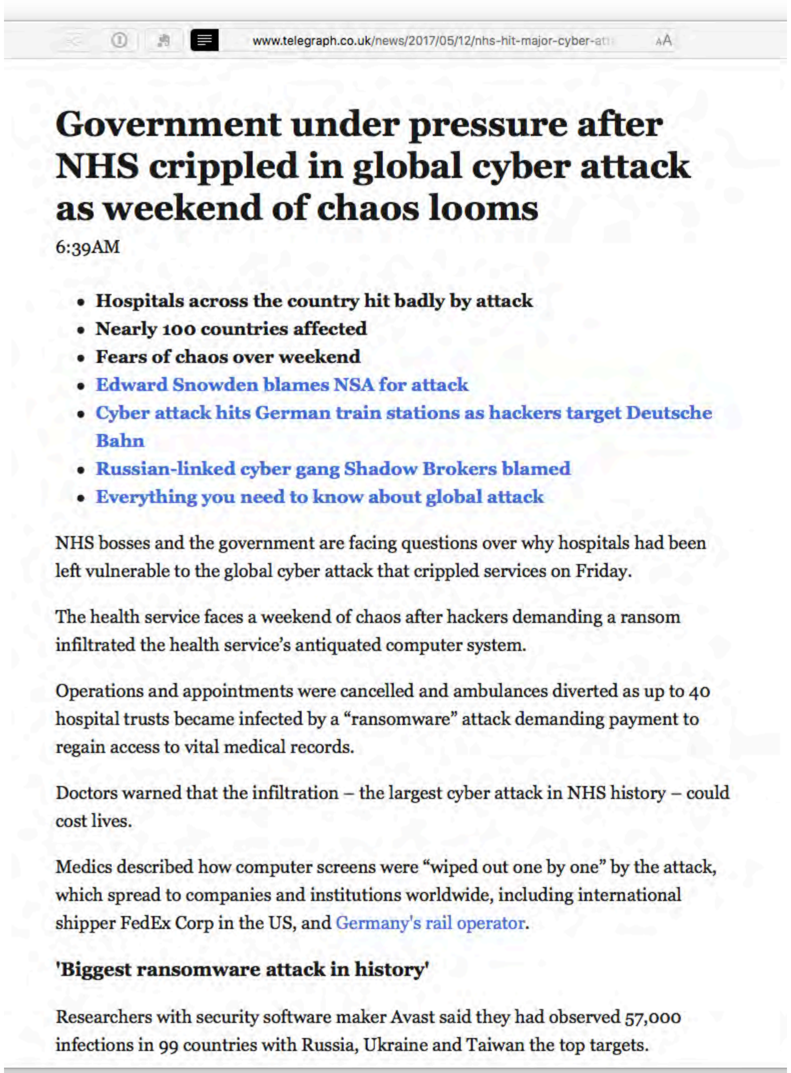
- **2005-2010: Stuxnet** (U.S., Israel against Iran)
  - Attack on Iran's nuclear power program
  - Malware designed to target Siemens SCADA systems and damage 984 uranium enrichment centrifuges
  - Demonstrates capabilities of a nation state attack on infrastructure
  - Israel & the U.S. allegedly responsible
- **2015: First known successful cyber attack on a power grid** (Russia against Ukraine)
  - 30 substations were switched off and 230,000 people were without power for 1-6 hours
  - Attacks carried out from computers with Russian IP addresses
- **2018 and earlier: Russian accesses U.S. infrastructure** (Russia against U.S.)
  - Russian hackers had direct access to an American power company's control systems
  - Lays groundwork for future attacks
- **2017: NotPetya malware attacks on Ukraine (and other places): >$10B damages**
  - Banks, ministries, newspapers, and electricity firms affected
  - Originated from an update to a Ukrainian tax accounting package called MeDoc
- **U.S. & UK governments identify China's ZTE and Huawei as national security risks**

https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Nation-State Attacks: WannaCry ransomware

2017

- Hits 100s of thousands of computers
  - Mostly in the UK's NHS
- Ransomware
  - Encrypted contents of data
  - Demanded bitcoin payment
- Attributed to North Korea
- Exploited leaked Shadow Brokers Windows vulnerabilities



www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-att

Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms

6:39AM

- **Hospitals across the country hit badly by attack**
- **Nearly 100 countries affected**
- **Fears of chaos over weekend**
- **Edward Snowden blames NSA for attack**
- **Cyber attack hits German train stations as hackers target Deutsche Bahn**
- **Russian-linked cyber gang Shadow Brokers blamed**
- **Everything you need to know about global attack**

NHS bosses and the government are facing questions over why hospitals had been left vulnerable to the global cyber attack that crippled services on Friday.

The health service faces a weekend of chaos after hackers demanding a ransom infiltrated the health service's antiquated computer system.

Operations and appointments were cancelled and ambulances diverted as up to 40 hospital trusts became infected by a "ransomware" attack demanding payment to regain access to vital medical records.

Doctors warned that the infiltration – the largest cyber attack in NHS history – could cost lives.

Medics described how computer screens were "wiped out one by one" by the attack, which spread to companies and institutions worldwide, including international shipper FedEx Corp in the US, and Germany's rail operator.

'Biggest ransomware attack in history'

Researchers with security software maker Avast said they had observed 57,000 infections in 99 countries with Russia, Ukraine and Taiwan the top targets.

Attacks & threats: Criminal attacks

- Fraud
- Theft (financial)
- Scams
  - Pay $$ and get little or nothing back: pyramid schemes, fake auctions
- Destruction
  - Sometimes we want to make data accessible but keep control of its distribution: software, music, movies, photos, books
- Intellectual property theft
- Identity theft
- Brand theft

Attacks & threats: Privacy violations

- Surveillance
- Databases
- Traffic analysis
- Large-scale surveillance
  - E.g., ECHELON

Other attacks & threats

- Publicity attacks
- Availability attacks
  - DoS, DDoS

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

Threat models

- Set of assumptions about the abilities of an adversary
- A way to identify & prioritize potential threats from an attacker’s point of view
  - Think about things that could go wrong
  - Bad guys don’t follow rules: they don’t care about your policies
  - We need to understand what types of attacks are possible
- Assess
  - What’s valuable?
  - Where will you be likely to be attacked?
  - What are the most significant threats?
- Think about entities in the system, how they communicate & store data
  - Where are the trust boundaries?
  - Where and how is protection enforced?

Trusted Computing Base (TCB)

TCB = All hardware & software of a computing system critical to its security

> "The totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy."
>
> – *Orange* Book
> *U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*

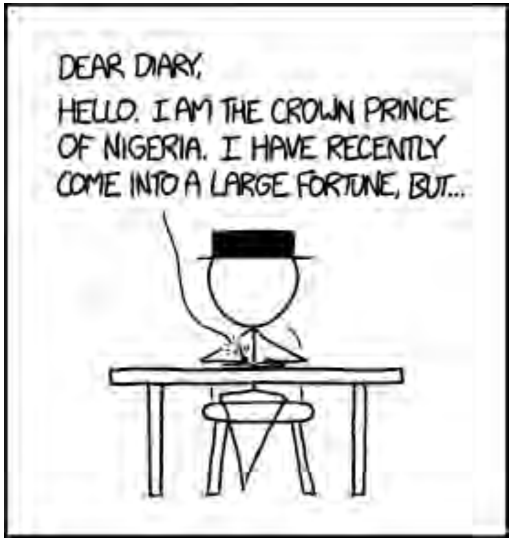
- If the TCB is compromised, we can no longer guarantee the security of a system
- Software that is part of the TCB must protect itself against tampering
  - Operating system memory protection is an example of this: an application may be compromised but the operating system is still intact and unaffected

Don’t underestimate the human element

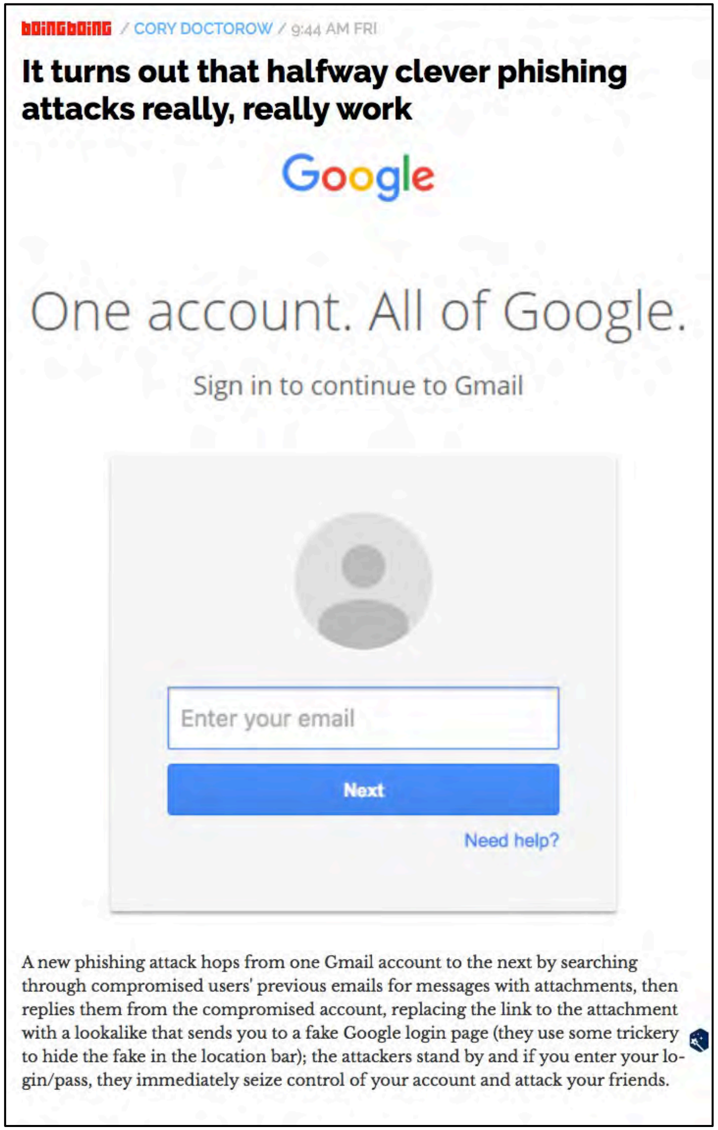
Humans are

- Bad at storing keys
- Poor at estimating risk
- Not accurate
- Careless
- Gullible

Social engineering is a top threat


DEAR DIARY,
HELLO. I AM THE CROWN PRINCE OF NIGERIA. I HAVE RECENTLY COME INTO A LARGE FORTUNE, BUT...

https://xkcd.com/1777/



boingboing / CORY DOCTOROW / 9:44 AM FRI

It turns out that halfway clever phishing attacks really, really work

Google

One account. All of Google.

Sign in to continue to Gmail

Enter your email

Next

Need help?

A new phishing attack hops from one Gmail account to the next by searching through compromised users' previous emails for messages with attachments, then replies them from the compromised account, replacing the link to the attachment with a lookalike that sends you to a fake Google login page (they use some trickery to hide the fake in the location bar); the attackers stand by and if you enter your login/pass, they immediately seize control of your account and attack your friends.

The end