CS 419: Computer Security

Week 1: Thinking about security

Paul Krzyzanowski

Part 1

Introduction

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**
  - Usually accomplished with access control and encryption

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.

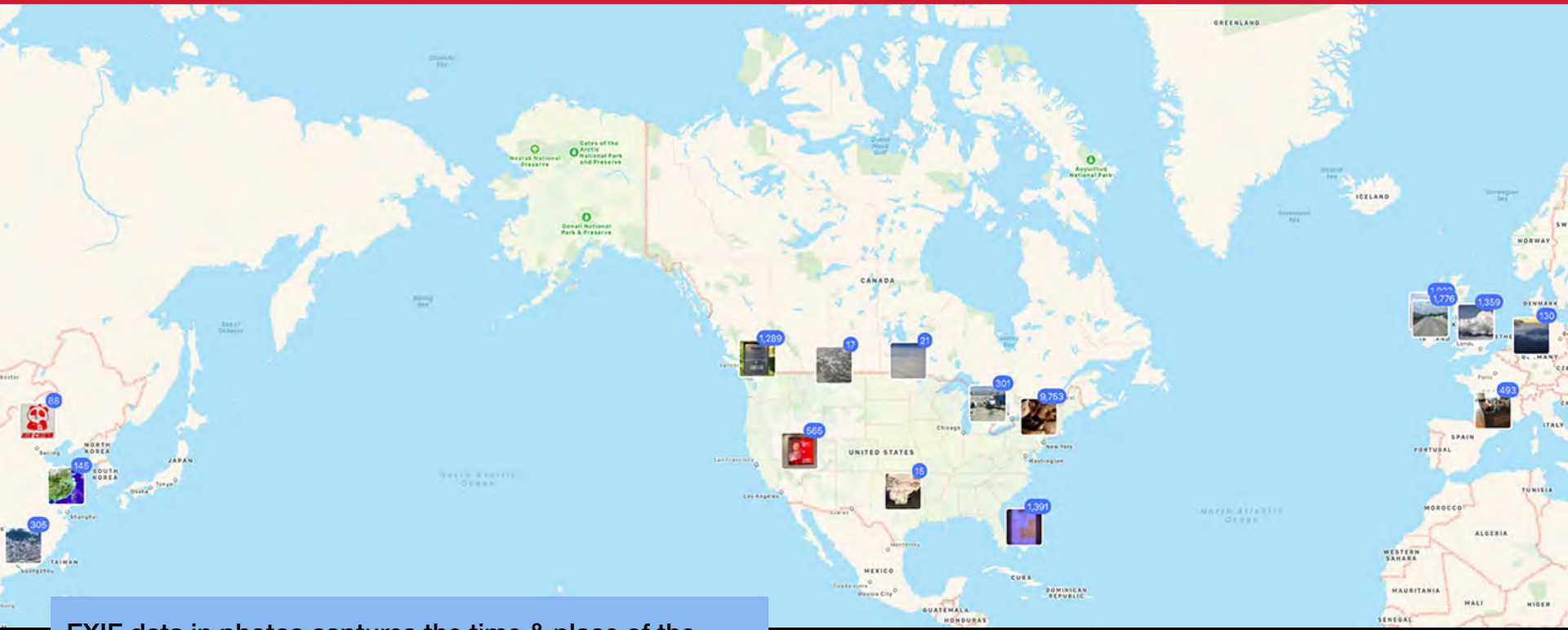
See: HIPAA, personal information, Privacy Act of 1974
RFC 4949, Internet Security Glossary

Privacy is a reason for confidentiality

Privacy is increasingly harder to attain

- **"Free services"**
  - Facebook, Google, Twitter, LinkedIn, Instagram, TikTok, …
  - Information collection, browser cookies to track web access
- **More data is online**
  - No need to go to town hall to get real estate transactions
- **Phone companies know every place you go**
- **Big data analytics**
  - It's increasingly easy to correlate data:
    Credit card spending, travel, jobs, marriages/divorces, kids, cars, …
- **This can be good and bad**

Where I've been 2019-2020



EXIF data in photos captures the time & place of the photo – creating a chronological log of your travels

Privacy & data mining … on a national level

- **U.S. credit scores**
  - Credit reporting companies track employment, spending, home ownership, loan repayment, …
  - Credit scores affect ability to borrow money, buy a home
- **China's social credit system**
  - Track trustworthiness of everyday citizens, corporations, and government officials
  - Track behavior
    - Frivolous spending, major & minor infractions (smoking in a no-smoking zone)
  - Boost public confidence and fight problems like corruption and business fraud

Integrity

- **The trustworthiness of the data or resources**
- **Preventing unauthorized changes to the data or resources**
- **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: over 200 million lines of code
    - Linux kernel: 27.8M lines of code across 66,492 files
    - Linux kernel in 2019: 74,754 commits from 4,189 different authors
    - 3,386,347 lines of new code added and 1,696,620 lines removed

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 data breaches

Exfiltration

Some big data breaches

- **Yahoo** – October 2017
  - Three billion user accounts compromised
  - Names, security questions & answers
- **Aadhaar** – March 2018
  - Personal information of more than one billion Indian citizens stored in the world's largest biometric database
  - Names, unique identity numbers, bank details, photos, thumbprints, retina scans
- **First American Financial Corp.** – May 2019
  - 885 million user's records leaked dating back more than 16 years
  - Bank accounts, social security numbers, wire transaction, mortgages

Some big data breaches

- **Facebook** – April 2019
  - Two 3rd-party app datasets exposed to public Internet
  - Contains comments, likes, reactions, account names
  - 540 million users affected
- **Verifications.io** – February 2019
  - Email validation service exposed 763 million unique addresses
  - Public MongoDB instance with no password
  - Names, phone numbers, dates of birth, genders
- **Marriott** – November 2018
  - Data from about 500 million Starwood hotel customers from 2014-2016
  - Names, contact info, passport numbers, Preferred Guest numbers, etc.
  - Credit & debit card numbers and expiration dates from 100 million customers

Some big data breaches

- **Adult Friend Finder** – October 2016
  - 20 years of data from six databases
  - Names, email addresses, passwords
- **Twitter** – May 2018
  - User passwords of 330 million users made accessible to internal network
- **Adobe** – October 2013
  - Username, email, encrypted password, and password hint from 153 million accounts
- **Equifax** – September 2017
  - One of the three largest consumer credit reporting agencies in the U.S.
  - Names, home addresses, phone numbers, dates of birth, social security numbers, driver's license numbers of 148 million Americans
  - Credit card information from 209,000 customers

Some 2020 ransomware attacks & recovery costs

- ISS World (Denmark-based facilities management) – $75-112.4M
- Cognizant (IT services) – $50-70M
- Redcar And Cleveland Council (England) – $13.6-22.2M
- Travelex (Money exchange) – $2.3M
- University of California San Francisco – $1.14M
- Communications & Power Industries (CPI) – $500,000
- La Salle County, IL – $500,000
- Grubman Shire Meiselas & Sacks (media law firm) – $365,000
- Tillamook County, OR – $300,000
- Florence, AL – $291,000
- San Miguel County, NM – $250,000

Other recent ransomware attacks

- **2019**
  - Jackson County, Georgia
  - City of Albany, New York
  - Augusta, Maine
  - Greenville, North Carolina
  - Imperial County, California
  - Baltimore, Maryland
  - Riviera Beach, Florida
- **2018**
  - City of Atlanta, Georgia
  - City of New Haven, Connecticut

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

Large-scale ransomware: 2016 – Petya

Encrypting malware that targets Microsoft Windows systems

- Ransom ~$400 & doubles after each week
- Infected millions of computers

June 2017 – NotPetya – new variant of Petya launched

- Spread via software update mechanism of a Ukrainian tax preparation program
- Disguised as ransomware
- Damages estimated to be over $10 billion
- Russian government blamed
  - Used EternalBlue exploit, believed to have been developed by the U.S. NSA

Just a few recent security attacks

Elon Musk confirms Tesla gigafactory was target of foiled cyberattack

MarketWatch

Justice Department accuses Russian man of conspiring to hack network, hold data for ransom

Mike Murphy • August 29, 2020

Elon Musk confirmed Thursday that the Tesla Inc. gigafactory in Nevada was the target of a cyberattack that was foiled by the FBI.

The blog Teslarati reported Thursday that a Russian man approached a worker at the factory in July through the WhatsApp chat app, and offered him $1 million to install malware into Tesla's internal network that would cause a distributed denial-of-service attack. While Tesla's cybersecurity team was distracted by the DDoS attack, the malware would access corporate secrets that the hackers could hold for ransom. Instead, the worker reported it to officials at Tesla, who alerted the FBI. He reportedly pretended to go along with the plan and wore a wire during future meetings with the Russian man, who was arrested Aug. 22 in Los Angeles in an apparent attempt to flee the U.S.

In a tweet replying to the Teslarati report, Musk confirmed "This was a serious attack."

https://www.marketwatch.com/story/elon-musk-confirms-tesla-gigafactory-was-target-of-foiled-cyberattack-11598576564

New Zealand Stock Trading Halted For a Third Day After Cyber Attacks

Bloomberg

Exchange battling to restore services, avoid more disruption

Tracy Withers • August 26, 2020

New Zealand's stock exchange is battling to restore services after cyber attacks shuttered the market for a third straight day, frustrating investors who were unable to trade amid a busy company earnings season.

The NZ$204 billion ($135 billion) market, which is nearing a record high, was unable to reopen Thursday after the exchange's website was again hit with a distributed-denial-of-service attack that floods a network with Internet traffic and disrupts services. Officials have declined to speculate on the source of the attack, other than saying it's coming from offshore.

…

Cyber-security experts appear baffled by the attacks, saying New Zealand isn't typically a target and that it's unclear whether the hackers are criminals or state-based actors.

https://www.bloomberg.com/news/articles/2020-08-27/n-z-stock-trading-halted-for-a-third-day-after-cyber-attacks

Intel investigating breach after 20GB of internal documents leak online

Leak confirmed to be authentic. Many files are marked "confidential" or "restricted secret."

Catalin Cimpanu • August 7, 2020

US chipmaker Intel is investigating a security breach after earlier today 20 GB of internal documents, with some marked "confidential" or "restricted secret," were uploaded online on file-sharing site MEGA.

The data was published by Till Kottmann, a Swiss software engineer, who said he received the files from an anonymous hacker who claimed to have breached Intel earlier this year.

Kottmann received the Intel leaks because he manages a very popular Telegram channel where he regularly publishes data that accidentally leaked online from major tech companies through misconfigured Git repositories, cloud servers, and online web portals.

https://www.zdnet.com/article/intel-investigating-breach-after-20gb-of-internal-documents-leak-online/

Ongoing Meow attack has nuked >1,000 databases without telling anyone why

Ongoing attack hitting unsecured data leaves the word "meow" as its calling card.

Dan Goodin • July 22, 2020

More than 1,000 unsecured databases so far have been permanently deleted in an ongoing attack that leaves the word "meow" as its only calling card, according to Internet searches over the past day.

The attack first came to the attention of researcher Bob Diachenko on Tuesday, when he discovered a database that stored user details of the UFO VPN had been destroyed. …

Since then, Meow and a similar attack have destroyed more than 1,000 other databases. At the time this post went live, the Shodan computer search site showed that 987 ElasticSearch and 70 MongoDB instances had been nuked by Meow. A separate, less-malicious attack tagged an additional 616 ElasticSearch, MongoDB, and Cassandra files with the string "university_cybersec_experiment." The attackers in this case seem to be demonstrating to the database maintainers that the files are vulnerable to being viewed or deleted.

It's not the first time attackers have targeted unsecured databases, which have become increasingly common with the growing use of cloud computing services from Amazon, Microsoft, and other providers.

https://arstechnica.com/information-technology/2020/07/more-than-1000-databases-have-been-nuked-by-mystery-meow-attack/

Three days later …

BLEEPINGCOMPUTER

New ‘Meow’ attack has deleted almost 4,000 unsecured databases

Ionut Ilascu • July 25, 2020

Hundreds of unsecured databases exposed on the public web are the target of an automated 'meow' attack that destroys data without any explanation.

The activity started recently by hitting Elasticsearch and MongoDB instances without leaving any explanation, or even a ransom note. Attacks then expanded to other database types and to file systems open on the web.
…
At the time of writing, BleepingComputer saw that 'meow' attacks impacted mostly Elasticsearch databases (1,395), followed by MongoDB (383), and Redis (54). This amounts to 1,832 but the real figure is higher as search engines start indexing the other database types. We will update the numbers when we get result for other database types.

According to LeakIX, a project that indexes open services, Apache ZooKeeper has been added on the list of "meow" attacks.

07/25 Update: The Meow attacks continue to escalate with almost 4,000 databases deleted as of Saturday, July 25th.

https://www.bleepingcomputer.com/news/security/new-meow-attack-has-deleted-almost-4-000-unsecured-databases/

Nintendo now says that the accounts of 300,000 Switch users have been hacked

BUSINESS INSIDER

Nintendo revealed a major breach in April, saying that "about 160,000 accounts" of Nintendo Switch users were affected. As it turns out, the actual number was closer to 300,000, Nintendo said this week.

Ben Gilbert • June 9, 2020

Do you have a Nintendo Switch? Did you also have a Nintendo 3DS or Wii U?

If you answered yes to both of those questions, there's a possibility your Nintendo Switch account was one of about 300,000 that was breached by hackers.

Nintendo announced the breach in April, but it doubled the number of affected accounts in an update this week "as a result of continuing the investigation."

https://www.businessinsider.com/nintendo-switch-account-hack-update-2020-6

Cyberattack forces Honda to suspend global production for a day

engadget

The company detected a virus on internal servers in Tokyo.

Christine Fisher • June 9, 2020

Honda was forced to suspend global production for a day due to a cyberattack that infiltrated the company's internal servers in Tokyo, Financial Times reports. Honda detected the virus on Monday and was forced to send some employees home for the day as the attack impacted email and other systems in plants around the world.

According to FT, production at some US plants was halted on Monday. While most work has resumed, car plants in Ohio and Turkey and motorcycle factories in Brazil and India reportedly remain closed. At this point, it does not appear that any customer or employee info was exposed. The attack may have also impacted a car inspection system.

https://www.engadget.com/honda-cyberattack-suspends-global-production-140545697.html

Mercedes-Benz onboard logic unit (OLU) source code leaks online

Daimler allowed anyone to register on one of its on-premise GitLab servers.

Catalin Cimpanu • May 18, 2020

The source code for "smart car" components installed in Mercedez-Benz vans has been leaked online over the weekend, ZDNet has learned.

The leak occurred after Till Kottmann, a Swiss-based software engineer, discovered a Git web portal belonging to Daimler AG, the German automotive company behind the Mercedes-Benz car brand.

Kottmann told ZDNet that he was able to register an account on Daimler's code-hosting portal, and then download more than 580 Git repositories containing the source code of onboard logic units (OLUs) installed in Mercedez vans.

WHAT'S AN OLU?
According to the Daimler website, the OLU is a component that sits between the car's hardware and software, and "connects vehicles to the cloud."

Daimler says the OLU "simplifies technical access and the management of live vehicle data" and allows third-party developers to create apps that retrieve data from Mercedes vans.

https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/

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

A huge database of Facebook users' phone numbers found online

TechCrunch

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/

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

THE WALL STREET JOURNAL.

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

Security Companies Get Hacked

Cybersecurity Firm Imperva Discloses Breach

August 19 2019

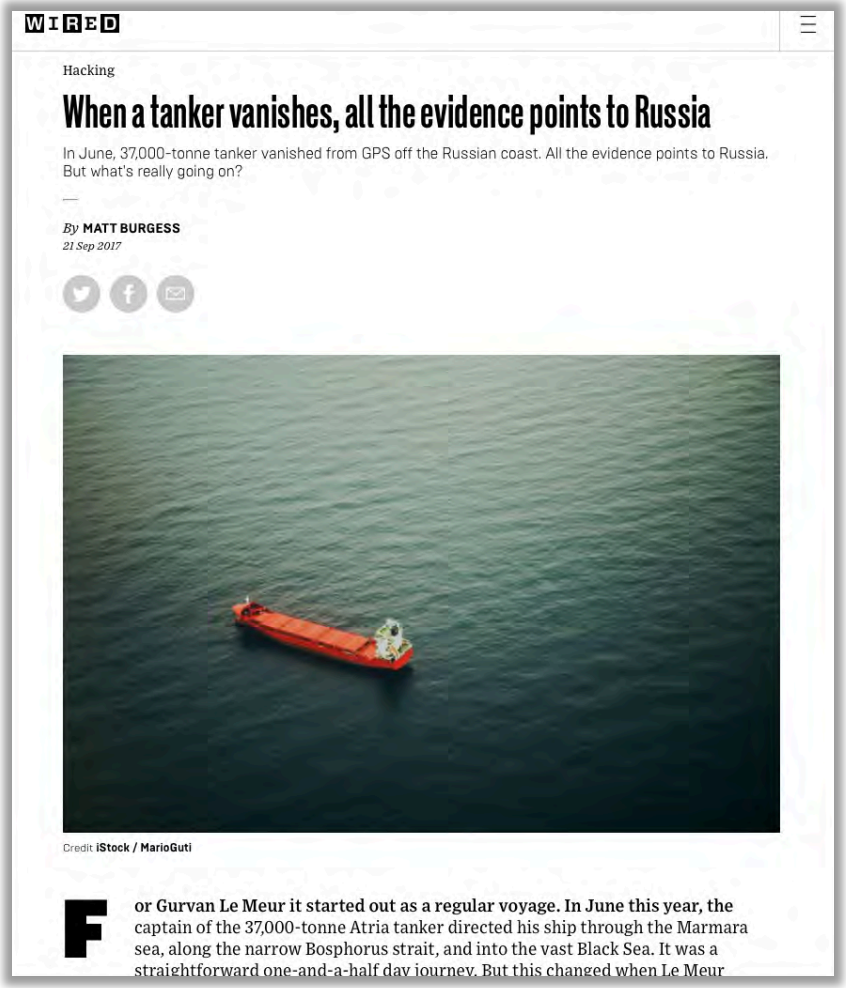
Imperva, a leading provider of Internet firewall services that help Web sites block malicious cyberattacks, alerted customers on Tuesday that a recent data breach exposed email addresses, scrambled passwords, API keys and SSL certificates for a subset of its firewall users.

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/

Some more things to worry about

2017 – GPS hacking



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?

—

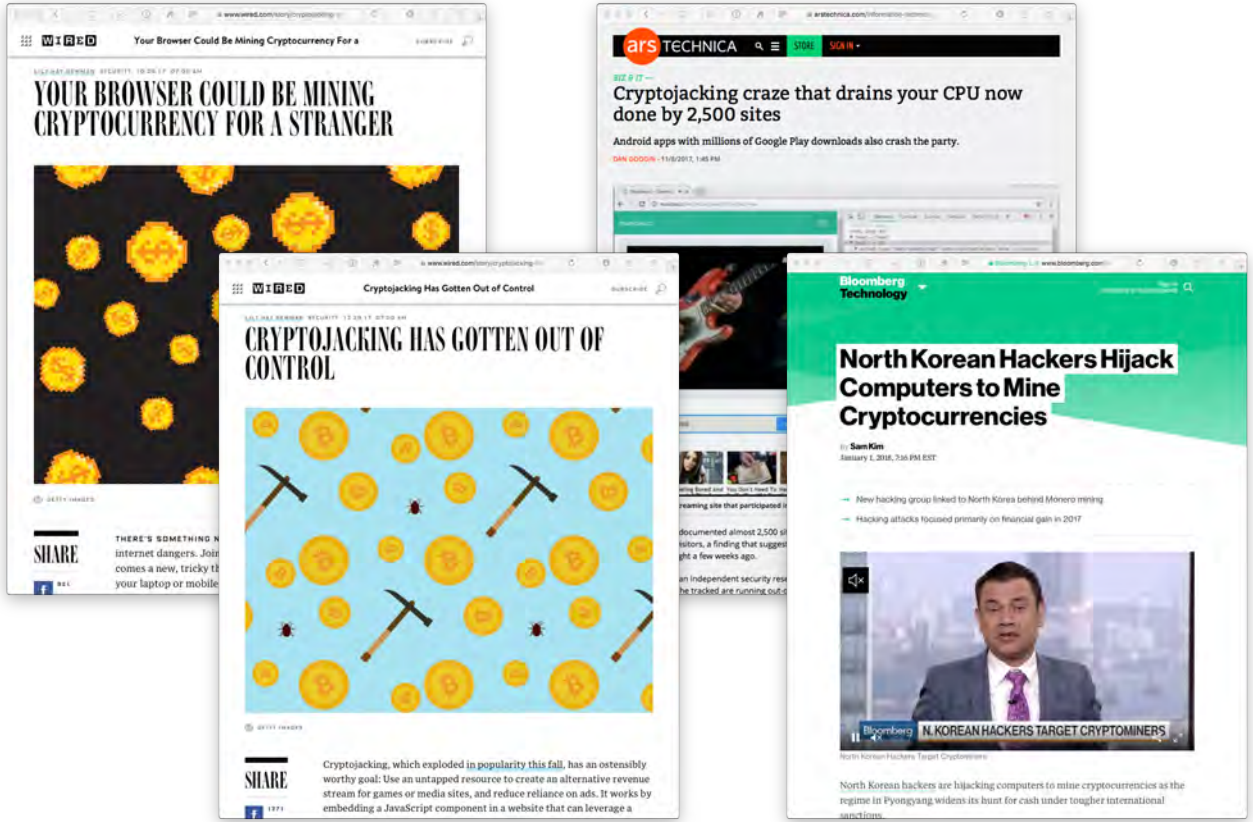
By **MATT BURGESS**
21 Sep 2017

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 Coming From Government Servers

Fall 2018-now – Cryptojacking



Supercomputers hacked across Europe to mine cryptocurrency

Confirmed infections have been reported in the UK, Germany, and Switzerland. Another suspected infection was reported in Spain.

Catalin Cimpanu • May 16, 2020

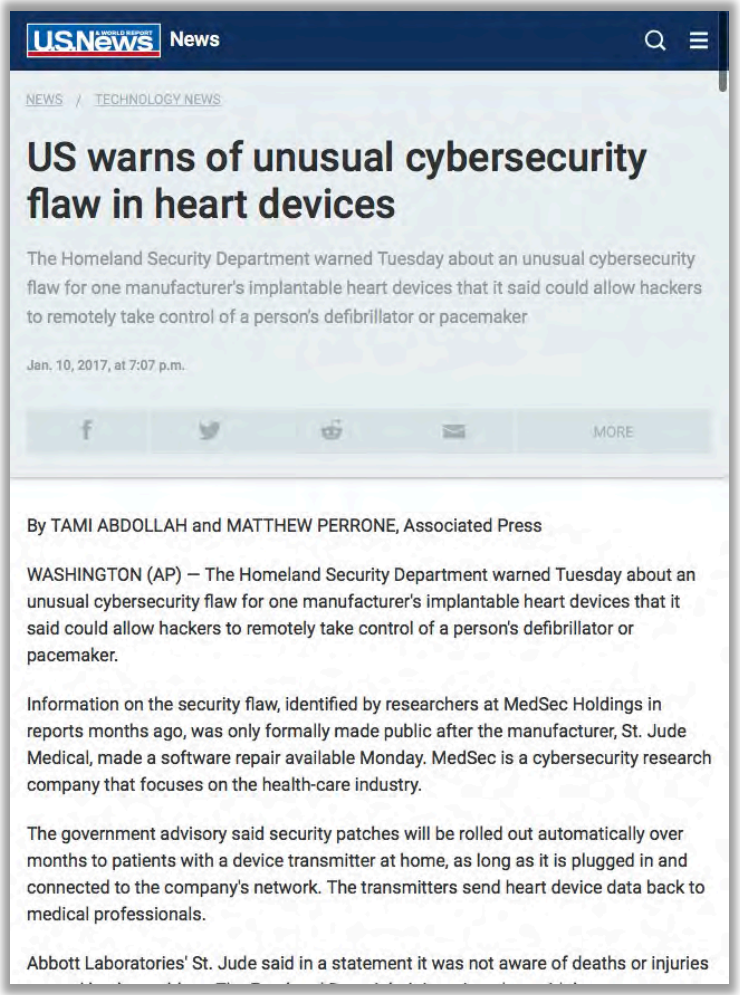
Multiple supercomputers across Europe have been infected this week with cryptocurrency mining malware and have shut down to investigate the intrusions.

Security incidents have been reported in the UK, Germany, and Switzerland, while a similar intrusion is rumored to have also happened at a high-performance computing center located in Spain.

The first report of an attack came to light on Monday from the University of Edinburgh, which runs the ARCHER supercomputer. The organization reported "security exploitation on the ARCHER login nodes," shut down the ARCHER system to investigate, and reset SSH passwords to prevent further intrusions.

Link

Potential for bodily harm



U.S.News News

NEWS / TECHNOLOGY NEWS

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.

MORE

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.

The government advisory said security patches will be rolled out automatically over months to patients with a device transmitter at home, as long as it is plugged in and connected to the company's network. The transmitters send heart device data back to medical professionals.

Abbott Laboratories' St. Jude said in a statement it was not aware of deaths or injuries

The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy

electrek

Fred Lambert • August 27, 2020

A few years ago, a hacker managed to exploit vulnerabilities in Tesla's servers to gain access and control over the automaker's entire fleet.

In July 2017, Tesla CEO Elon Musk got on stage at the National Governors Association in Rhode Island and confirmed that a "fleet-wide hack" is one of Tesla's biggest concerns as the automaker moves to autonomous vehicles.

He even presented a strange scenario that could happen in an autonomous future:

> *"In principle, if someone was able to say hack all the autonomous Teslas, they could say – I mean just as a prank – they could say 'send them all to Rhode Island' [laugh] – across the United States… and that would be the end of Tesla and there would be a lot of angry people in Rhode Island."*

What Musk knew that the public didn't was that Tesla got a taste of that actually happening just a few months prior to his talk.

https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/

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.

Hack-back

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

For six months, security researchers have secretly distributed an Emotet vaccine across the world

Binary Defense researchers have identified a bug in the Emotet malware and have been using it to prevent the malware from making new victim

Catalin Cimpanu • August 14, 2020

Most of the time, fighting malware is a losing game. Malware authors create their code, distribute payloads to victims via various methods, and by the time security firms catch up, attackers make small changes in their code to quickly regain their advantage in secrecy. …

However, not all malware operations can be hurt this way. Some cyber-criminals either reside in countries that don't extradite their citizens or have a solid knowledge of what they're doing.

Emotet is one of the gangs that check both boxes. Believed to operate from the territories of the former Soviet States, Emotet is also one of today's most skilled malware groups, having perfected the infect-and-rent-access scheme like no other group.

The malware, which was first seen in 2014, evolved from an unimportant banking trojan into a malware swiss-army knife that, once it infects victims, it spreads laterally across their entire network, pilfers any sensitive data, and turns around and rents access to the infected hosts to other groups.

https://www.zdnet.com/article/for-six-months-security-researchers-have-secretly-distributed-an-emotet-vaccine-across-the-world/

Part 2

Security Goals & Threats

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
  - Cost-benefit analysis
    - Is it cheaper to prevent an attack or recover?
    - Who pays & who gets punished?

> Microsoft and the device manufacturer and installer exclude all implied warranties and conditions, including those of merchantability, fitness for a particular purpose, and non-infringement. …. you may not under this limited warranty, under any other part of this agreement, or under any theory, recover any damages or other remedy, including lost profits or direct, consequential, special, indirect, or incidental damages.
>
> *Microsoft Windows 10 End-User License Agreement*

Protection: Know Your Enemy!

Different attackers

… who have different goals

… and different skill levels

Who do 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: a bad policy or a bug
- **Attack Vector**
  - The type of attack – the component that's used to break into the system
- **Exploit**
  - Software, commands, or instructions to take advantage of a vulnerability
- **Attack (cyber attack)**
  - The use of an exploit to subvert security policies and mechanisms
- **Threat**
  - an adversary that is capable of attacking
- **Attack surface**
  - All the attack vectors in the system

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

Vulnerabilities

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

What if a system had no vulnerabilities?

Would you not worry about threats?

Some vulnerabilities can be really old

Hack Brief: Microsoft Warns of a 17-Year-Old 'Wormable' Bug

WIRED

The SigRed vulnerability exists in Windows DNS, used by practically every small and medium-sized organization in the world.

Andy Greenberg • July 14, 2020

Since Wannacry and NotPetya struck the internet just over three years ago, the security industry has scrutinized every new Windows bug that could be used to create a similar world-shaking worm. Now one potentially "wormable" vulnerability—meaning an attack can spread from one machine to another with no human interaction—has appeared in Microsoft's implementation of the domain name system protocol, one of the fundamental building blocks of the internet.

As part of its Patch Tuesday batch of software updates, Microsoft today released a fix for a bug discovered by Israeli security firm Check Point, which the company's researchers have named SigRed. The SigRed bug exploits Windows DNS, one of the most popular kinds of DNS software that translates domain names into IP addresses. Windows DNS runs on the DNS servers of practically every small and medium-sized organization around the world. The bug, Check Point says, has existed in that software for a remarkable 17 years.

Check Point and Microsoft warn that the flaw is critical, a 10 out of 10 on the common vulnerability scoring system, an industry-standard severity rating.

Vulnerabilities are on the rise

Vulnerabilities in popular open source projects doubled in 2019

ZDNet

Jenkins and MySQL vulnerabilities have had the most weaponized vulnerabilities in the past five years.

Catalin Cimpanu • June 8, 2020

A study that analyzed the top 54 open source projects found that security vulnerabilities in these tools doubled in 2019, going from 421 bugs reported in 2018 to 968 last year.

According to RiskSense's "The Dark Reality of Open Source" report, released today, the company found 2,694 bugs reported in popular open source projects between 2015 and March 2020.

The report didn't include projects like Linux, WordPress, Drupal, and other super-popular free tools, since these projects are often monitored, and security bugs make the news, ensuring most of these security issues get patched fairly quickly.

Instead, RiskSense looked at other popular open source projects that aren't as well known but broadly adopted by the tech and software community. This included tools like Jenkins, MongoDB, Elasticsearch, Chef, GitLab, Spark, Puppet, and others.

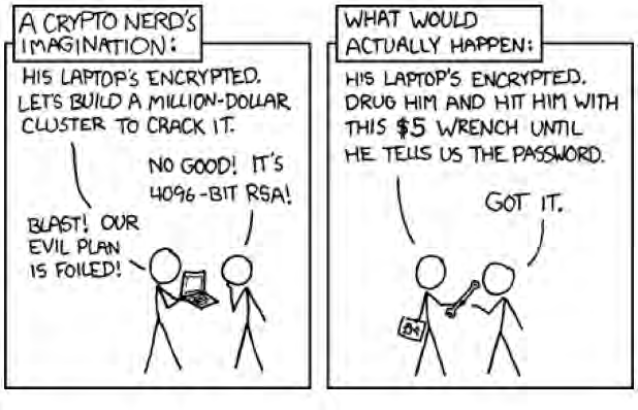
RiskSense says that one of the main problems they found during their study was that a large number of the security bugs they analyzed had been reported to the National Vulnerability Database (NVD) many weeks after they've been publicly disclosed. … It also allowed threat actors to create and deploy exploits -- resulting in the "weaponization" of a security bug.

https://www.zdnet.com/article/vulnerabilities-in-popular-open-source-projects-doubled-in-2019/

Threats

Threats – the potential attackers

- Who are the adversaries?
- 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



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

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.

July 2020 Twitter Breach

- **Hackers targeted 130 users**
- **Tweeted cryptocurrency scam from 45 accounts they were able to access**
  - Changing the email address & login credentials
- **Brought in $120,000**
- **Not a big deal … but could have been a lot worse**
  - Twitter is used by political & business leaders
  - The right tweet can move markets or start conflicts

What happened?

Internal employee changed email addresses and turned off security features of certain high-profile accounts.

It wasn't social engineering, it was bribery — a Twitter employee was paid.

Insider threat problem. Twitter has almost 5,000 employees.

https://www.theverge.com/2020/7/15/21326656/twitter-hack-explanation-bitcoin-accounts-employee-tools

Exclusive: More than 1,000 people at Twitter had ability to aid hack of accounts

REUTERS®

Joseph Menn, Katie Paul, Raphael Satter • July 23, 2020

SAN FRANCISCO (Reuters) - More than a thousand Twitter employees and contractors as of earlier this year had access to internal tools that could change user account settings and hand control to others, two former employees said, making it hard to defend against the hacking that occurred last week.

Twitter said on Saturday that the perpetrators "manipulated a small number of employees and used their credentials" to log into tools and turn over access to 45 accounts. here On Wednesday, it said that the hackers could have read direct messages to and from 36 accounts but did not identify the affected users.

The former employees familiar with Twitter security practices said that too many people could have done the same thing, more than 1,000 as of earlier in 2020, including some at contractors like Cognizant.

https://www.reuters.com/article/us-twitter-cyber-access-exclusive/exclusive-more-than-1000-people-at-twitter-had-ability-to-aid-hack-of-accounts-idUSKCN24O34E

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

Threat actions – what might an attacker do?

- **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

Threat actions – what might an attacker do?

- **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

Part 3

Internet-Enabled Threats

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!**

How the Internet Creates Vulnerabilities

- **Action at a distance**
- **Asymmetric force**
- **Actors can be anonymous**
- **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

Action at a Distance

People can now be beyond our control or visibility.

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**

Asymmetric Force

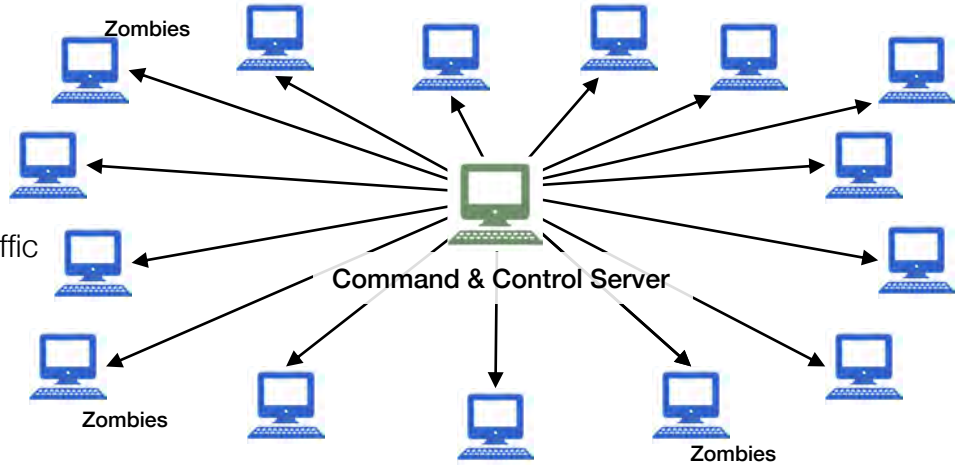
- Actors can project or harness greater force. Low barriers to entry. Offense can be more effective than defense. A small number of actors can have a large effect.
- E.g., The Anonymous hacking group that tries to take down corporations or governments, people who send fraud or spam email, or those who send Facebook requests for money.
- Sending millions of messages costs almost nothing
- Small counties can now inflict damage on countries like the US or China

WannaCry Ransomware

Botnets

- **Botnet = collection of computers owned by innocent people but infected with malicous software**
  - The botnet program periodically contacts a command & control server for directions on what additional software to download and what to run and whom to attack

- **Three common uses are:**
  1. Distributed Denial of Service (DDoS) attacks
     - One company has only so many servers
     - Send too much traffic to the servers and the server gets overloaded
     - Now nobody can get through – even legitimate traffic
     - Data is not destroyed but service is disrupted
     - Attacks come from the network of zombies
  2. Spam mailing
     - Send of tens of millions of malicious emails
  3. Cryptocurrency mining
     - Use the computing power of the zombies



Necurs Botnet

2008 Cyberattack on the U.S. Military

- **Significant compromise of classified military computer networks**
- **Started with an infected USB flash drive inserted into a U.S. military laptop at a base in the Middle East**
- **Malicious code uploaded to a network run by U.S. Central Command**
  - Spread onto other systems, allowing data to be transferred under foreign control via a remote **command and control** server
- **Served as an important wake-up call for the U.S. Department of Defense**
- **Author unknown – suspected Russian hackers because of common code from previous attacks**

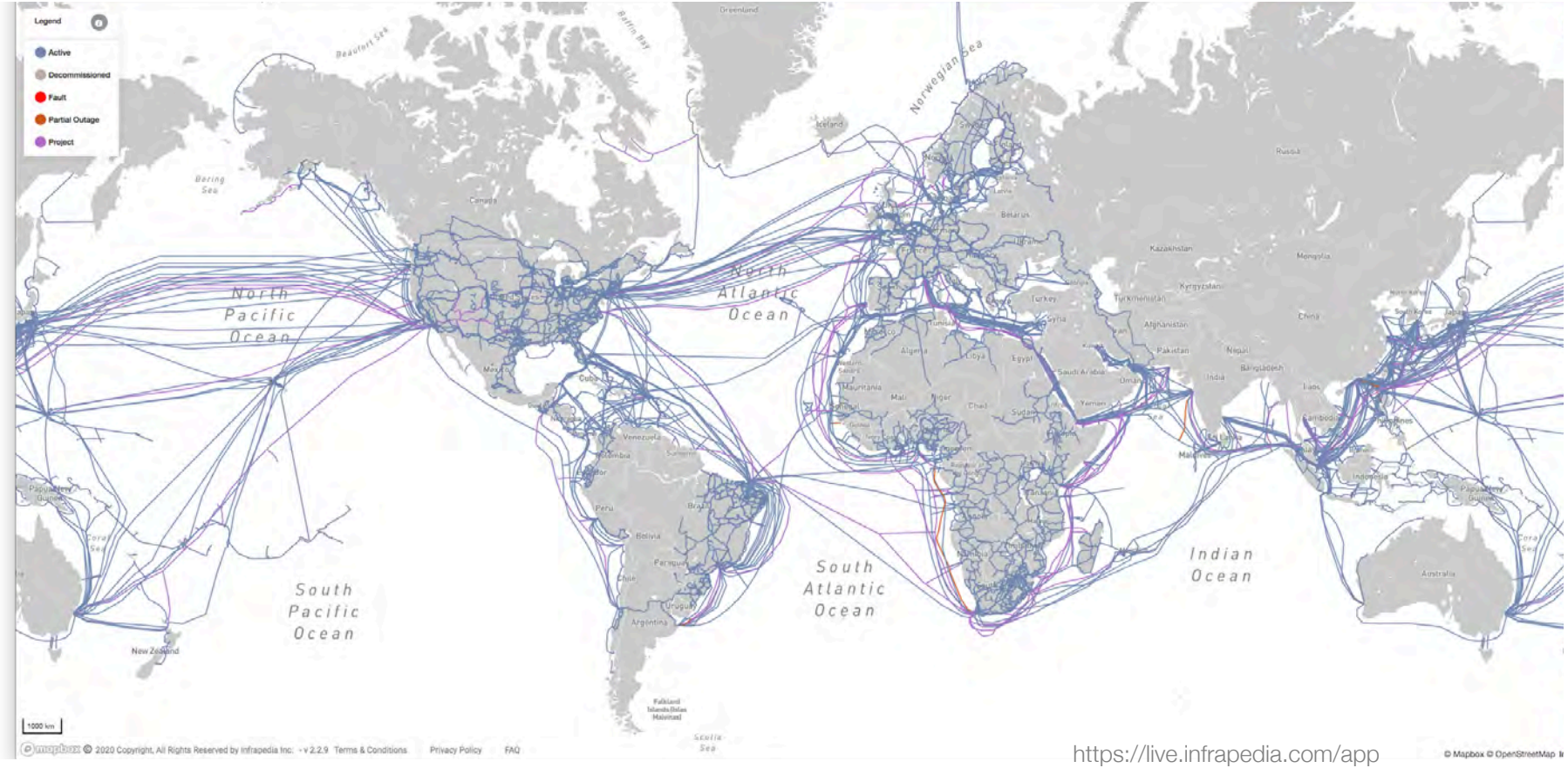
http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html

Anonymity

- **Internet protocols don't require identification**
- **We often can't identify the attacker**
  - Nobody knows who ran some of the biggest botnets or cyber attacks.
  - Identifying a source can be difficult.
  - Attack with impunity. We don't know who fired the missile.
- **Make guesses**
  - Reverse engineer the code, compare to other malware
  - Identify location of command & control server & who is accessing it
  - Trace packets & propagation
- **Sometimes we will never know**
- **Trust becomes a challenge**
  - Are you really communicating with your bank?

https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/

Lack of Borders & Checkpoints



https://live.infrapedia.com/app

We expect you to show up in court…

WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

REMARKS

CAUTION

Allegedly part of hacking team responsible for WannaCry ransomware, attack on Sony Pictures, and others

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a

Allegedly responsible for stealing terabytes of data, including coronavirus research, from western companies in 11 nations

Lack of Distinction in Data

- **All bits look the same**
- **How can you tell which data is malicious?**

Attacks

Attack Techniques

Social engineering

- **Manipulating or deceiving targets to get them to take some action that isn't in their best interest.**
  - Example: 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 with with a malicious link or attachment
  - Spear Phishing
    - Focused attack via email on a particular person or organization
- **Social Media or public (or leaked) databases**
  - Not always an attack but a great source of information for hackers: vacation schedules, employment info, family, …
  - Adversary can use this info for impersonation or spear phishing
- **Deceptive software: file, scripts**
  - 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

Areas of Attack

- **Compromised access, code/command injection**
  - Exploit known (often stolen) credentials – you can buy these
  - Take advantage of coding errors to provide input to execute arbitrary code
  - Includes keystroke logging, camera monitoring, content upload, ransomware
- **Eavesdropping & Man-in-the-middle (MitM) attacks**
  - Intercept traffic to gather login credentials, snoop on data, manipulate data, or take over a communication session
- **Web sites**
  - Offer free downloads: software, books, movies … which will contain malware
  - Reputable sites can get infected … or have ads that take you to malware
  - Drive-by downloads – malicious programs that get installed without your consent

Networked Computer vs. Real-World Risks

- **Attacking in the computer world via networks 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

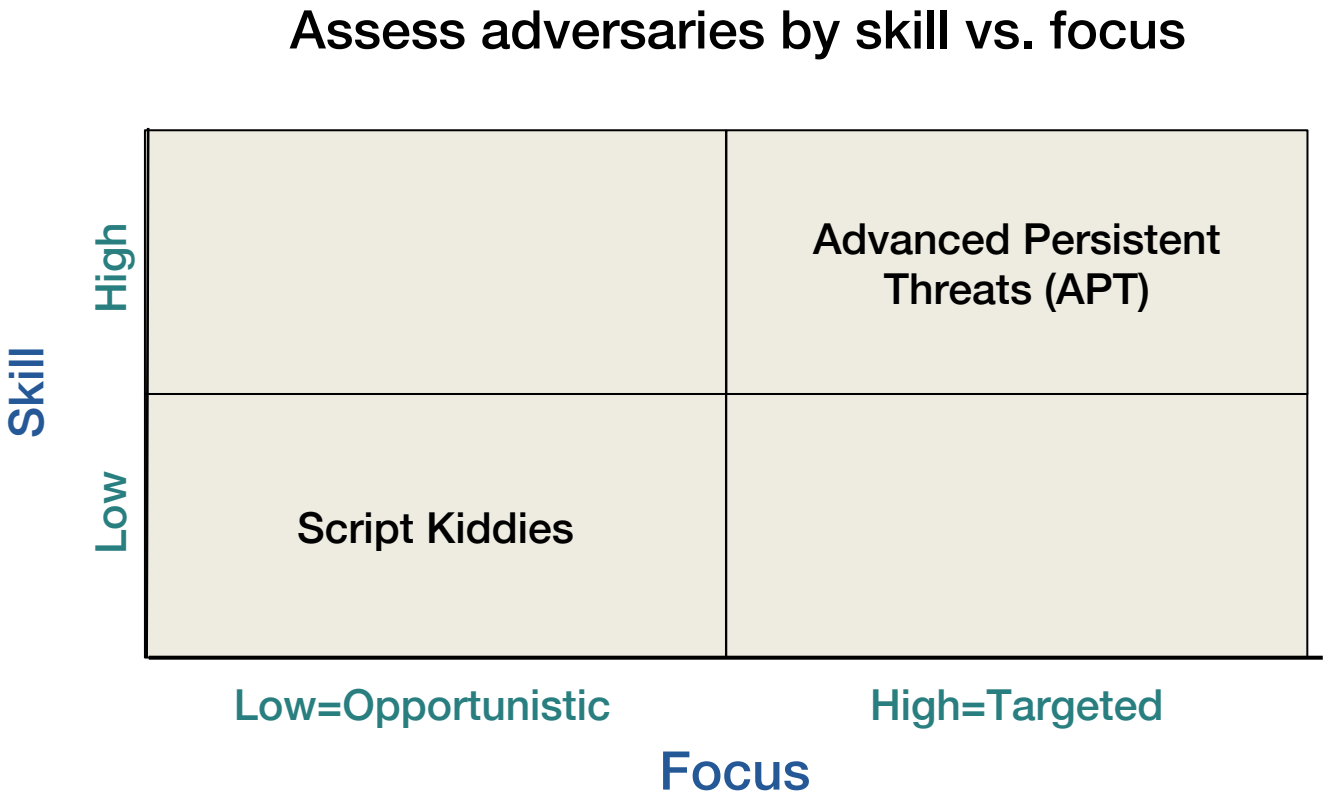
Networked Computer vs. Real-World Risks

- **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

Part 4

Attacks & Motives

Threat Matrix



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 to tailor the attacks to 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 (often identified as a group, e.g., APT22)

Teen Hacker Charged with Paralyzing Miami Schools in Embarrassingly Simple Cyberattack

GIZMODO

Alyse Stanley • September 5, 2020

A Florida teenager allegedly used an embarrassingly simple program to launch a series of DDoS attacks that helped shut down one of the nation's largest school districts for its first three days of virtual classes, the Miami Herald reported this week.

…

"The student admitted to orchestrating eight Distributed Denial-of-Service cyberattacks, designed to overwhelm district networks," the district said in a statement. More than 345,000 students attend public schools in Miami-Dade County, making it the fourth-largest district in the U.S.

…

Even more embarrassing still, the student admitted that he broke the network using a decade-old, open-source tool that most bare-bones firewall software can catch, the Herald reported Saturday.

The application's called LOIC, which stands for Low Orbit Ion Cannon. Developed by 4Chan-affiliated hackers, it basically did for DDoS attacks what Microsoft Word did for word processors by streamlining the process into an easy-to-download program that even an idiot can't mess up. No hacking experience needed, just point, click, and boom! You're on your way to committing a felony. LOIC makes it easy to coordinate thousands of anonymous users to overwhelm servers by submitting tons of garbage requests en masse.

https://gizmodo.com/teen-hacker-charged-with-paralyzing-miami-schools-in-em-1844968182

Group of unskilled Iranian hackers behind recent attacks with Dharma ransomware

Security firm Group-IB says the hackers have been targeting companies in Russia, Japan, China, and India.

Catalin Cimpanu • August 24, 2020

Cyber-security firm Group-IB says it identified a group of low-skilled hackers operating out of Iran that has been launching attacks against companies in Asia and attempting to encrypt their networks with a version of the Dharma ransomware.

The attacks have targeted companies located in Russia, Japan, China, and India, according to a report Group-IB researchers published Aug. 24.

The security firm described the group as "newbie hackers" based on the low level of sophistication and simple tactics and tools employed during attacks.

Per the report, the group used only publicly-available hacking tools, either open-sourced on GitHub or downloaded from Telegram hacking channels.

This included the likes of Masscan, NLBrute, Advanced Port Scanner, Defender Control, or Your Uninstaller.

https://www.zdnet.com/article/group-of-unskilled-iranian-hackers-behind-recent-attacks-with-dharma-ransomware/

Chinese hackers targeted major UK companies as coronavirus raged

WIRED

Hackers alleged to be working on behalf of the Chinese government have been busy throughout the coronavirus crisis – including attacking targets in the UK

Matt Burgess • July 23, 2020

As coronavirus tore through Europe in March and April, so did hackers acting on behalf of the Chinese government. Looking to make the most of organisations scrambling to respond to the health crisis, criminals working for China attacked private companies, research institutions, and governments across the world.

… Hackers working for the group known as Advanced Persistent Threat 41 (ATP41) compromised a major private provider of social care services in the UK and in the process disrupted its systems, a cybersecurity expert with knowledge of China's actions says. The attack took place in March as the UK was hurtling towards the most serious weeks of its Covid-19 outbreak.

On another occasion, state-sponsored hackers from a different Chinese group are thought to have targeted two technical companies, one in the UK and one in the US, that handle anonymised patient data. The attackers conducted reconnaissance on the firms but, the source says, there is no evidence they were actually compromised. They add that during April and May Chinese cyber actors based in Wuhan, where Covid-19 first emerged, targeted a number of European governments and their systems.

https://www.wired.co.uk/article/china-coronavirus-hacking-uk-us

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)
  - Netscout reports 26% of organizations reported they experienced an attack by a malicious insider in 2018
    - (Japan lowest at 14% and France highest at 37%).

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.
- **Nation-states: Infowarriors – cyber warfare**
  - Huge money & short-term goals
  - Disrupt power grids, commerce, transportation
  - EMP weapons, spread selective information, misinformation, blackmail

Organized Crime: Russian Business Network (RBN)

- **Operates on numerous ISPs worldwide**
- **Internet service provider run by criminals for criminals**
  - Host platform for illegal businesses
- **Domains registered to anonymous addresses**
  - Does not advertise
  - Trades in untraceable electronic transactions
- **Known for delivering fake anti-spyware & anti-malware software**
  - Used for PC hijacking and personal identity theft
- **One of the world's worst spammer, malware, and phishing networks**

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/

North Korean hackers ramp up bank heists: U.S. government cyber alert

Christopher Bing • August 26, 2020

North Korean hackers are tapping into banks around the globe to make fraudulent money transfers and cause ATMs to spit out cash, the U.S. government warned on Wednesday.

A technical cybersecurity alert jointly written by four different federal agencies, including the Treasury Department and FBI, said there had been a resurgence in financially motivated hacking efforts by the North Korean regime this year after a lull in activity.

"Since February 2020, North Korea has resumed targeting banks in multiple countries to initiate fraudulent international money transfers and ATM cash outs," the warning reads.

U.S. law enforcement titled the hacking campaign "Fast Cash" and blamed North Korea's Reconnaissance General Bureau, a spy agency, for it. They described the operation as going on since at least 2016 but ramping up in sophistication and volume recently.

Over the last several years, North Korea has been blamed by U.S. authorities and private sector cybersecurity companies for hacking numerous banks in Asia, South America and Africa.

https://www.reuters.com/article/us-cyber-usa-north-korea/north-korean-hackers-ramp-up-bank-heists-u-s-government-cyber-alert-idUSKBN25M2FU

The Vatican Is Said to Be Hacked From China Before Talks With Beijing

The New York Times

In one attack, the hackers weaponized an electronic file with a letter that had a note of condolence from Cardinal Pietro Parolin, the Vatican's secretary of state.

David E. Sanger, Edward Wong and Jason Horowitz • July 28, 2020

Chinese hackers infiltrated the Vatican's computer networks in the past three months, a private monitoring group has concluded, in an apparent espionage effort before the beginning of sensitive negotiations with Beijing.

The attack was detected by Recorded Future, a firm based in Somerville, Mass. The Chinese Communist Party has been waging a broad campaign to tighten its grip on religious groups, in what government leaders have periodically referred to as an effort to "Sinicize religions" in the country.

… But this appears to be the first time that hackers, presumed by cybersecurity experts at Recorded Future to be working for the Chinese state, have been publicly caught directly hacking into the Vatican and the Holy See's Study Mission to China, the Hong Kong-based group of de facto Vatican representatives who have played a role in negotiating the Catholic Church's status.

https://www.nytimes.com/2020/07/28/us/politics/china-vatican-hack.html

Hackers Broke Into Real News Sites to Plant Fake Stories

WIRED

A disinfo operation broke into the content management systems of Eastern European media outlets in a campaign to spread misinformation about NATO.

Andy Greenberg • July 29, 2020

OVER THE PAST few years, online disinformation has taken evolutionary leaps forward, with the Internet Research Agency pumping out artificial outrage on social media and hackers leaking documents—both real and fabricated—to suit their narrative. More recently, Eastern Europe has faced a broad campaign that takes fake news ops to yet another level: hacking legitimate news sites to plant fake stories, then hurriedly amplifying them on social media before they're taken down.

On Wednesday, security firm FireEye released a report on a disinformation-focused group it's calling Ghostwriter. The propagandists have created and disseminated disinformation since at least March 2017, with a focus on undermining NATO and the US troops in Poland and the Baltics; they've posted fake content on everything from social media to pro-Russian news websites. In some cases, FireEye says, Ghostwriter has deployed a bolder tactic: hacking the content management systems of news websites to post their own stories. They then disseminate their literal fake news with spoofed emails, social media, and even op-eds the propagandists write on other sites that accept user-generated content.

https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/

Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack

19 June 2020

Australia's government and institutions are being targeted by ongoing sophisticated state-based cyber hacks, Prime Minister Scott Morrison says.

Mr Morrison said the cyber attacks were widespread, covering "all levels of government" as well as essential services and businesses.

He declined to identify a specific state actor and said no major personal data breaches had been made.
The attacks have happened over many months and are increasing, he said.

The prime minister said his announcement on Friday was intended to raise public awareness and to urge businesses to improve their defences.

But he stressed that "malicious" activity was also being seen globally, making it not unique to Australia.

Who has been targeted?

Mr Morrison did not name specific cases but said it had spanned "government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure".
He did not give further details. Previously, defence manufacturers, government contractors and accounting firms have been among those to report data breaches.

Link
https://www.bbc.com/news/world-australia-46096768

NSA: Russia's Sandworm Hackers Have Hijacked Mail Servers

WIRED

In a rare public warning, the US spy agency says the notorious arm of Russian military intelligence is targeting a known vulnerability in Exim.

Andy Greenberg • May 28, 2020

A WARNING THAT hackers are exploiting vulnerable email servers doesn't qualify as an unusual event in general. But when that warning comes from the National Security Agency, and the hackers are some of the most dangerous state-sponsored agents in the world, run-of-the-mill email server hacking becomes significantly more alarming.

On Thursday, the NSA issued an advisory that the Russian hacker group known as Sandworm, a unit of the GRU military intelligence agency, has been actively exploiting a known vulnerability in Exim, a commonly used mail transfer agent—an alternative to bigger players like Exchange and Sendmail—running on email servers around the world. The agency warns that Sandworm has been exploiting vulnerable Exim mail servers since at least August 2019, using the hacked servers as an initial infection point on target systems and likely pivoting to other parts of the victim's network. And while the NSA hasn't said who those targets have been, or how many there are, Sandworm's history as one of the most aggressive and destructive hacking organizations in the world makes any new activity from the group worth noting.

"We still consider this to be one of the most, if not the most aggressive and potentially dangerous actor that we track," says John Hultquist, the director of intelligence at FireEye, who also led a team at iSight Partners when that company first discovered and named Sandworm in 2014.

https://www.wired.com/story/nsa-sandworm-exim-mail-server-warning

Trump confirms US conducted cyberattack against Russia in 2018

Kevin Bohn • July 10, 2020

President Donald Trump, for the first time, confirmed the US conducted a covert cyberattack in 2018 against Russia's Internet Research Agency. The Internet Research Agency is a troll farm blamed by the US for helping to facilitate interference both in the 2016 presidential election and the 2018 midterms.

Trump gave the confirmation during an interview conducted by Marc Thiessen, a Washington Post columnist and former speechwriter for President George W. Bush and Defense Secretary Donald Rumsfeld.

Thiessen writes in the Post that during his interview he asked Trump whether he had launched a cyberattack. Thiessen said Trump replied, "Correct."

https://www.cnn.com/2020/07/10/politics/donald-trump-us-russia-cyberattack/index.html

U.S. Escalates Online Attacks on Russia's Power Grid

The New York Times

By David E. Sanger and Nicole Perlroth • June 15, 2019

The United States is stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively, current and former government officials said.

In interviews over the past three months, the officials described the previously unreported deployment of American computer code inside Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.

Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States.

https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

More than half of foreign cyberattacks against China in 2019 originated in the US, China report says

South China Morning Post

China recently tightened its cybersecurity rules, requiring "critical information infrastructure" to undergo a more rigorous review process

Coco Feng • August 12, 2020

More than half of computer malware attacks in China from overseas entities in 2019 originated in the US, according to data from a government-affiliated cybersecurity team.

The total amount of computer malware attacks captured by the National Computer Network Emergency Response Technical Team (CNCERT) was over 62 million in 2019, and around 53.5 per cent of foreign attacks were from the US, lower than a year before when there were in excess of 100 million incidents, the Team said.

Russia and Canada were the second and third largest contributors to computer malware attacks against China, accounting for 2.9 and 2.6 per cent respectively of the total number of foreign attacks.

The number of new malicious attacks directed against mobile networks was nearly 2.8 million in 2019, 1.4 per cent lower than a year earlier, the first decline in such attacks in five years, according to CNCERT.

https://www.scmp.com/tech/policy/article/3097070/more-half-foreign-cyberattacks-against-china-2019-originated-us-china

Stuxnet – 2010, U.S. & Israel (?)

- **Targeted centrifuges used to purify uranium in Iran**
- **Attacked Siemens centrifuges via a SCADA interface**
  - Phase 1
    - Possible initial installation via thumb drive
      Air gapped systems – systems physically separated from other networks
    - Propagated among Microsoft Windows Systems
    - Searched for systems running Siemens Step7 control software
  - Phase 2
    - Altered the spin of the centrifuges while making it look like everything was fine
- **Showed that cyber attacks can cause real-world damage**
- **Pipelines, electric grids, banking, … are at risk**

Regin – 2003(?), U.S.(?)

- **Reputed to be the most advanced malware & hacking toolkit**
- **Developed by the NSA & GCHQ (maybe)**
- **Modular design – goal is to stay hidden and collect information**
- **Target**
  - Individuals, telecom, energy, hospitality, and research companies
  - Surveillance on European Union citizens and companies

Shamoon – 2012, Iran

- **Developed by Iran's state hackers (allegedly)**
- **Deployed in 2012 on the network of Saudi Aramco**
  - Wiped data on over 30,000 computers
  - Deployed again in 2016
- **2018: attacked computers of Saipem, an Italian oil & gas company**
  - Infected about 10% of the company's systems

Some Nation-State Attacks (probably)

- **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 regions (Russia against Ukraine)**
  - >$10B damages
  - Banks, ministries, newspapers, and electricity firms affected
  - Originated from an update to a Ukrainian tax accounting package called MeDoc
- **2019: 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 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/

Preemptory Attacks

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

BUSINESS INSIDER

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.

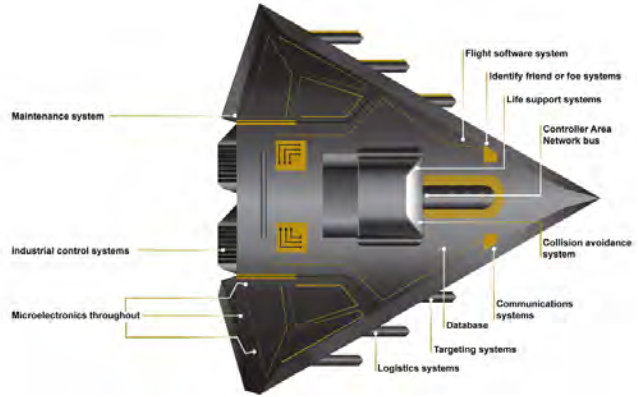
The new report is a summary of the IG's investigations into Pentagon cybersecurity over the previous year. It looked at 20 unclassified and four classified reports that detailed problems with cybersecurity and followed up to see if they'd been addressed. Previously, the IG had recommended the Pentagon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

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.

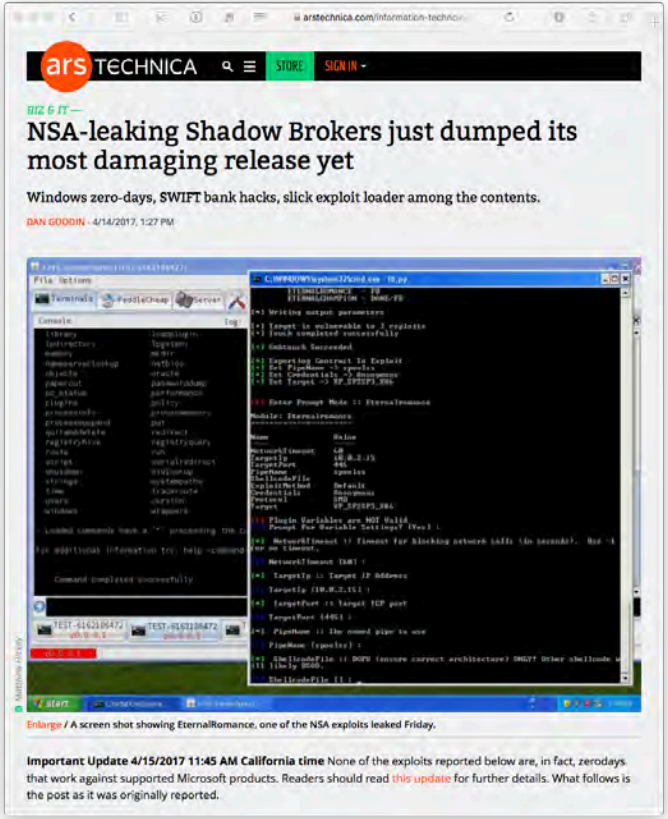
https://www.bleepingcomputer.com/news/security/us-advanced-weaponry-is-easy-to-hack-even-by-low-skilled-attackers/

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**
  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**



arstechnica.com/information-technol...

ars TECHNICA STORE SIGN IN

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

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."*

arstechnica.com/tech-policy/2017/0...

ars TECHNICA STORE SIGN IN

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.

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

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.

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.

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

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.

Listing image by National Security Agency

Attack Motives

Attack Motives: Criminal attacks

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

Attack Motives: Privacy violations

- **Surveillance**
  - Databases
  - Installation of surveillance software
  - Traffic analysis
  - Large-scale surveillance
    - E.g., ECHELON

Attack Motives: Finding vulnerabilities is a business

- **Dozens of companies have bug bounty programs**
  - They'll pay you if you find security vulnerabilities or come up with exploits
- **Some companies specialize in acquiring exploits**
  - And sell them to institutions, including government agencies

The Washington Post

The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities

Brian Fung • August 31, 2013

https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/

Paying for exploits – supply & demand

Zerodium Expects iOS Exploit Prices to Drop as It Announces Surplus

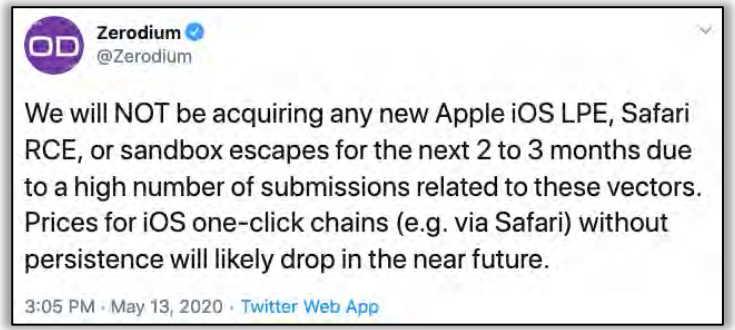
SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Exploit acquisition firm Zerodium announced this week that it's no longer buying certain types of iOS exploits due to surplus, and the company expects prices to drop in the near future.

Eduard Kovacs • May 14 2020

Zerodium said on Twitter it would no longer acquire iOS local privilege escalation, Safari remote code execution, and sandbox escape exploits in the next 2-3 months "due to a high number of submissions related to these vectors."

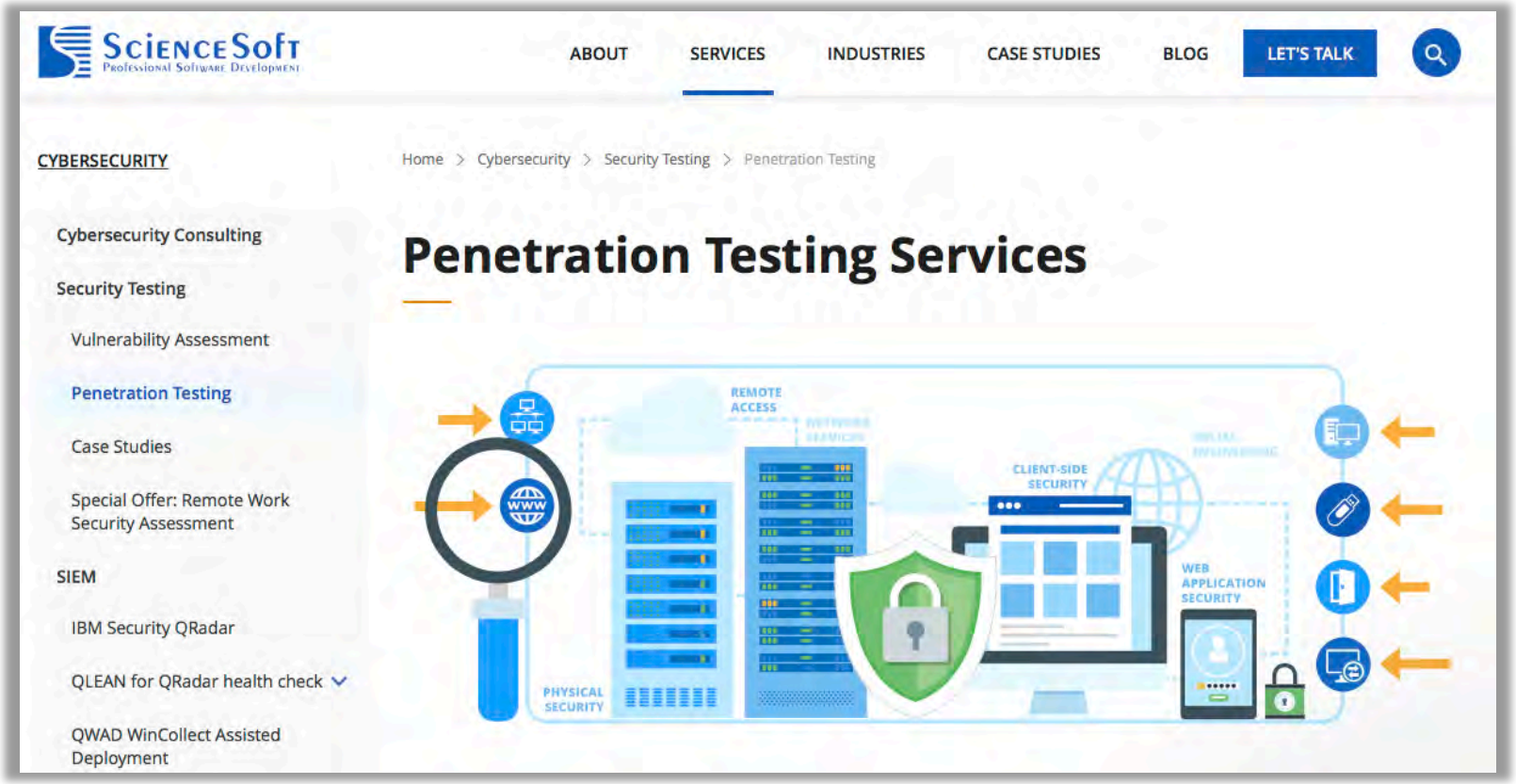
The company says it expects prices to drop for one-click exploit chains that do not provide persistence.



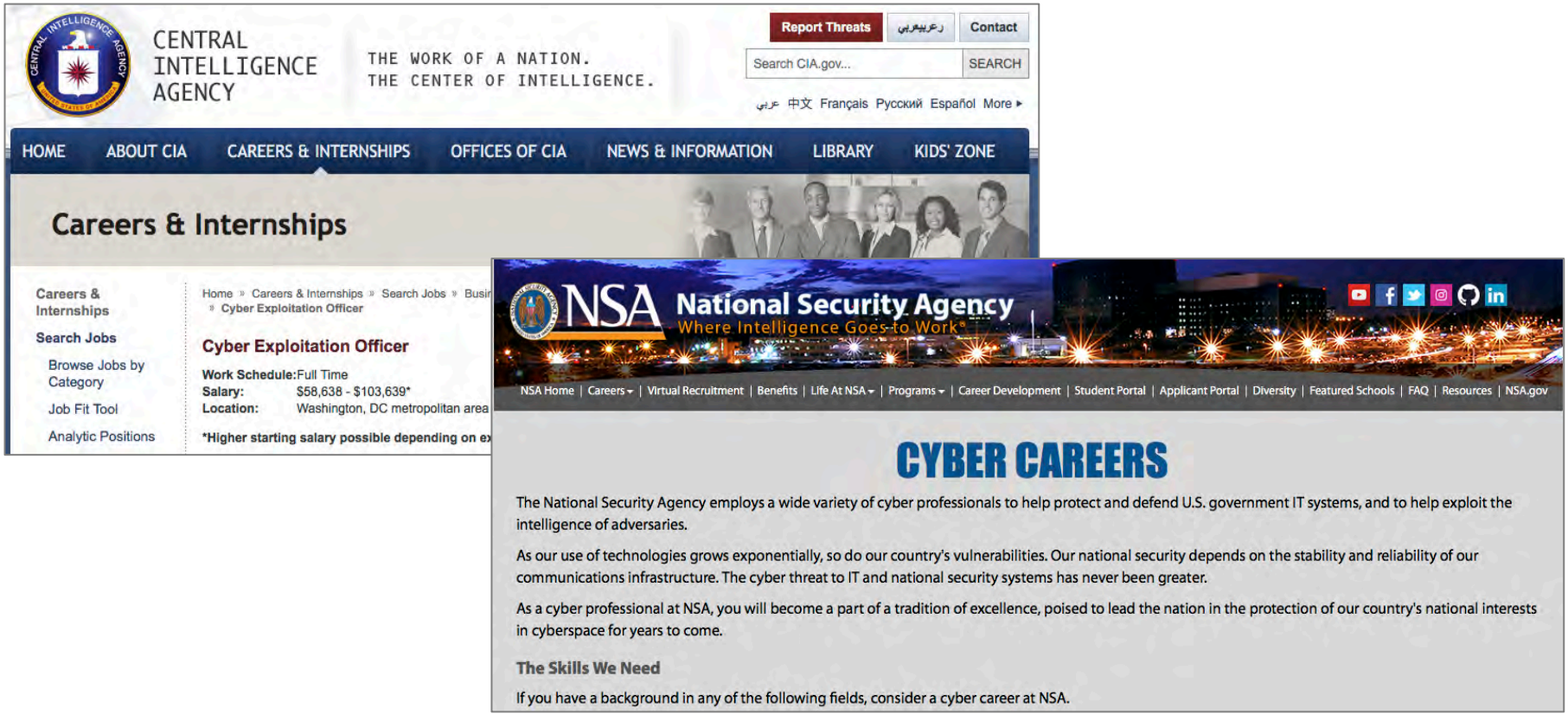
Chaouki Bekrar, CEO and founder of Zerodium, said on Twitter that only pointer authentication codes (PACs) — they provide protection against unexpected changes to pointers in memory — and the difficulty to achieve persistence "are holding [iOS security] from going to zero."

https://www.securityweek.com/zerodium-expects-ios-exploit-prices-drop-it-announces-surplus

Attack Motives: Finding exploits is a career



Attack Motives: Building exploits is a career



Other motives

- **Publicity attacks**
- **Availability attacks**
  - Denial of Service (DoS), Distributed Denial of Service (DDoS)

Threat Models

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

Trusted Computing Base (TCB)

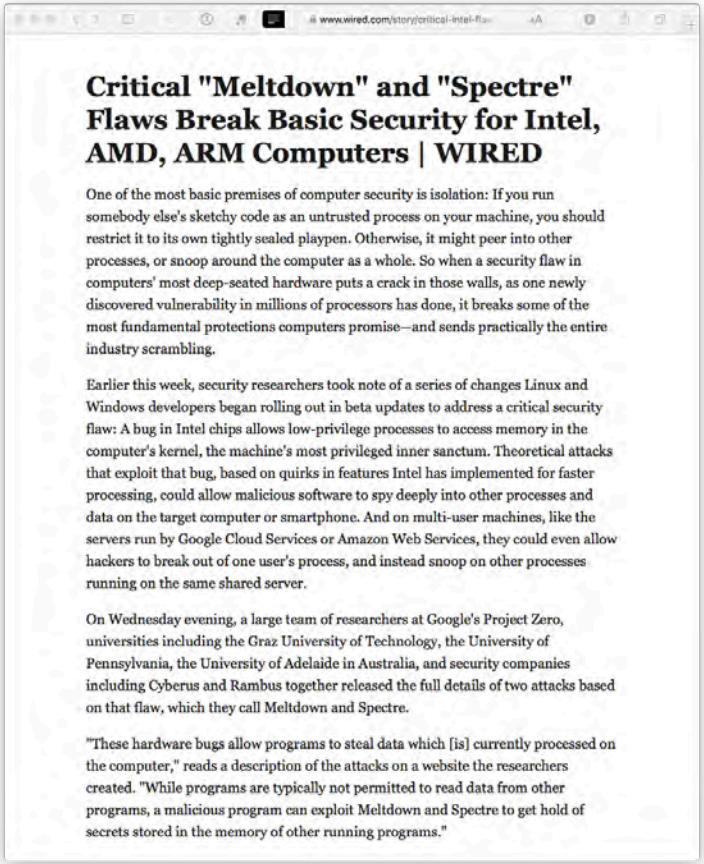
TCB = All hardware & software of a computing system critical to its security

> "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

Jan 2018 – Meltdown & Spectre

- **Intel chips do not have 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**



www.wired.com/story/critical-intel-fla...

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."

Cisco's warning: Critical flaw in IOS routers allows 'complete system compromise'

Cisco has delivered updates to address four critical flaws affecting its industrial routers.

Liam Tung • June 4 2020

Cisco has disclosed four critical security flaws affecting router equipment that uses its IOS XE and IOS software.

The four critical flaws are part of Cisco's June 3 semi-annual advisory bundle for IOS XE and IOS networking software, which includes 23 advisories describing 25 vulnerabilities.

The 9.8 out of 10 severity bug, CVE-2020-3227, concerns the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software, which allows a remote attacker without credentials to execute Cisco IOx API commands without proper authorization.

IOx mishandles requests for authorization tokens, allowing an attacker to exploit the flaw with a specially crafted API call to request the token and then execute Cisco IOx API commands on the device, according Cisco.

https://www.zdnet.com/article/ciscos-warning-critical-flaw-in-ios-routers-allows-complete-system-compromise/

Do you trust the entire supply chain?

- Alter the circuit design
- Add components after the fact
- Modify the CPU
- Modify the bootloader, firmware, or pre-installed software
- Add malware to the compiler used to build the software
- Add malware to libraries used by the apps