$EC ELL:

USING APPROPRIATE PROTECTION TO SECURE YOUR FINANCIAL A$$E[T]$

Russell Beauchemin | Asst. Professor of Cybersecurity & Networking @ RWU
rbeauchemin@rwu.edu

PART 01: INTRODUCTION

INTRODUCTION

- Exploits of financial security threats have existed since finance has:

Artist's Rendition of Stagecoach Robbery

Image source: True West Blog

Artist's Rendition of Bank Robbery

Image source: Shutterstock

INTRODUCTION (CONT.)

- Exploits of financial security threats have existed since finance has:

Photo of Safecracker in Army of Thieves

Image source: Chicago Sun Times

FBI Photo of Armored Car Robbery in 2019

Image source: KKTV.com

INTRODUCTION (CONT.)

- Exploits of financial security threats have existed since finance has:

Surveillance Photo 2019 Gas Station Robbery

Image source: WDUN

Artist Rendition of a Purse Snatching

Image source: Michigan Justice

INTRODUCTION (CONT.)

- In addition to these exploits, the digital transformation has created newer ones:

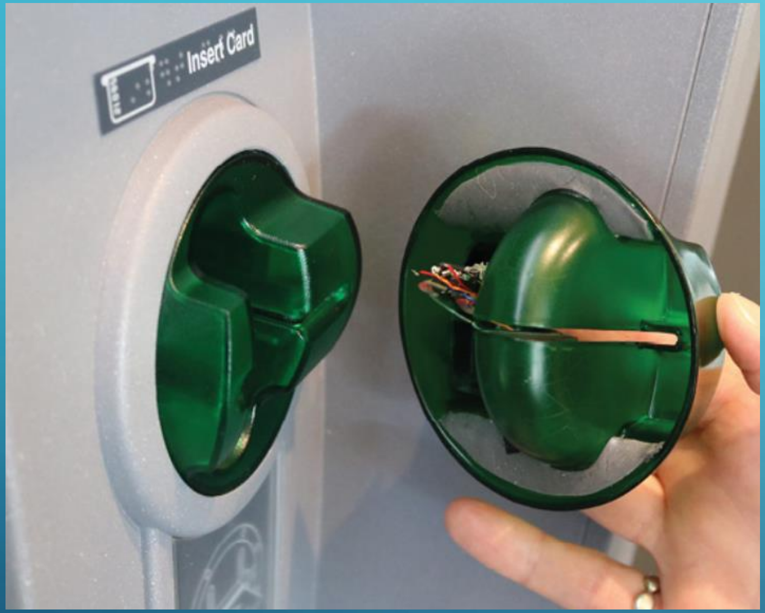


Photo of an exposed ATM Skimmer

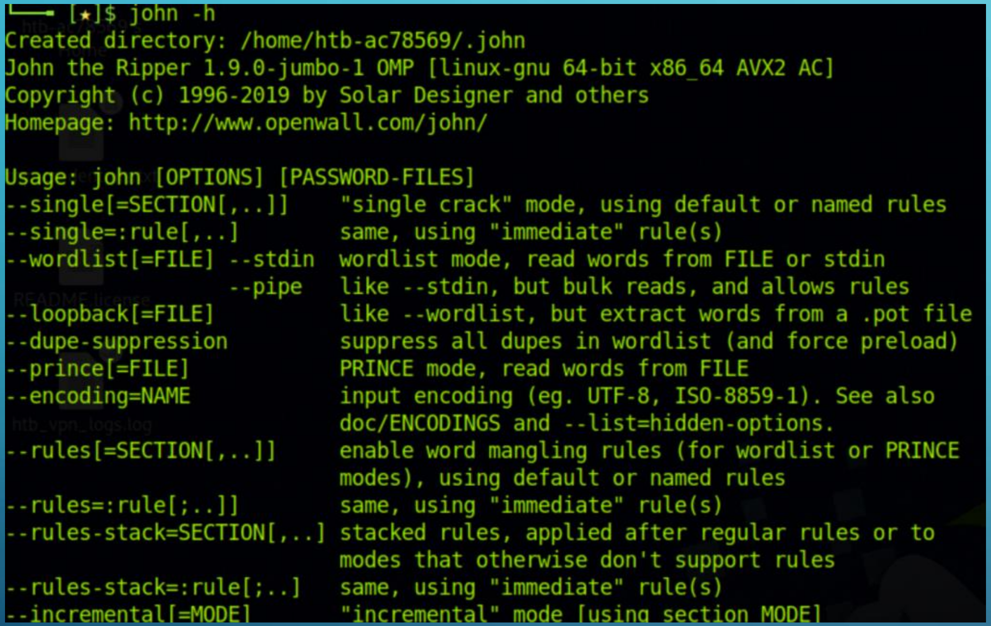
Image source: NWCU

Hardware Keylogger with WIFI

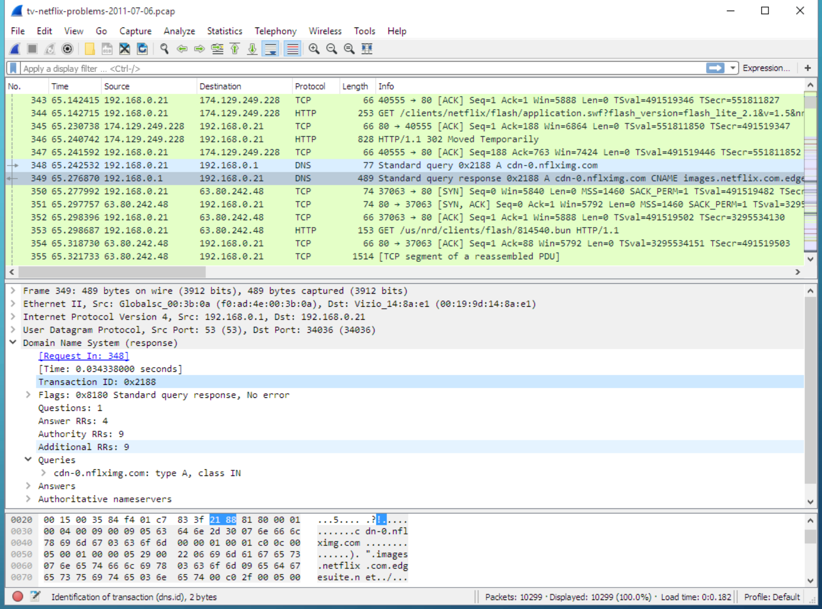
Image source: Keelog.com

INTRODUCTION (CONT.)

- In addition to these exploits, the digital transformation has created newer ones:



```
└──╼ [★]$ john -h
Created directory: /home/htb-ac78569/.john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]     "single crack" mode, using default or named rules
--single=:rule[,..]         same, using "immediate" rule(s)
--wordlist[=FILE] --stdin   wordlist mode, read words from FILE or stdin
                  --pipe    like --stdin, but bulk reads, and allows rules
--loopback[=FILE]           like --wordlist, but extract words from a .pot file
--dupe-suppression          suppress all dupes in wordlist (and force preload)
--prince[=FILE]             PRINCE mode, read words from FILE
--encoding=NAME             input encoding (eg. UTF-8, ISO-8859-1). See also
                            doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]      enable word mangling rules (for wordlist or PRINCE
                            modes), using default or named rules
--rules=:rule[;..]]         same, using "immediate" rule(s)
--rules-stack=SECTION[,..]  stacked rules, applied after regular rules or to
                            modes that otherwise don't support rules
--rules-stack=:rule[;..]    same, using "immediate" rule(s)
--incremental[=MODE]        "incremental" mode [using section MODE]
```



```
No.  Time      Source          Destination     Protocol Length Info
 343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
 344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
 345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
 346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
 347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
 348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
 349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
 350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
 351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
 352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
 353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
 354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
 355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

```
Identification of transaction (dns.id), 2 bytes    Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182    Profile: Default
```

Screenshot of JtR Password Cracker

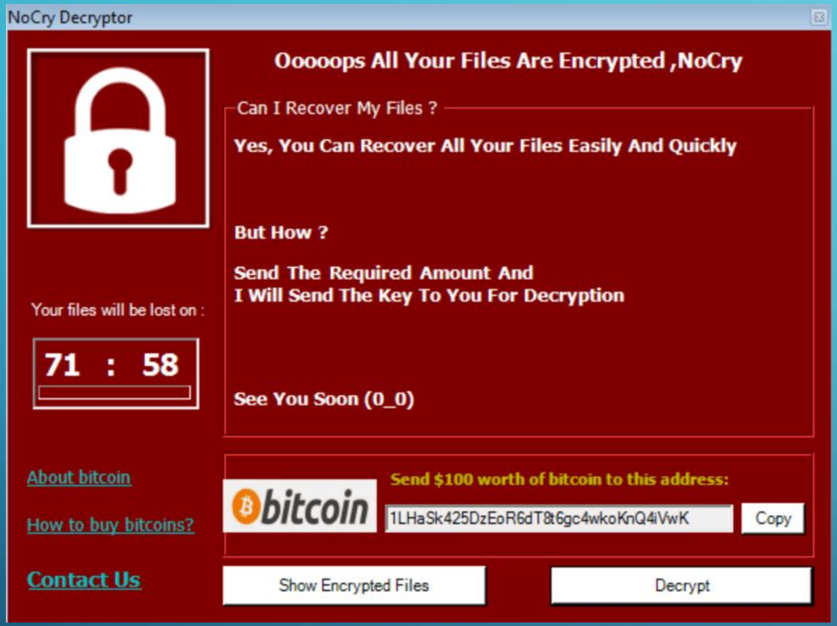
Image source: FreeCodeCamp

Screenshot of Wireshark Network Sniffer

Image source: Wireshark

INTRODUCTION (CONT.)

- In addition to these exploits, the digital transformation has created newer ones:



NoCry Decryptor

Oooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

Your files will be lost on :

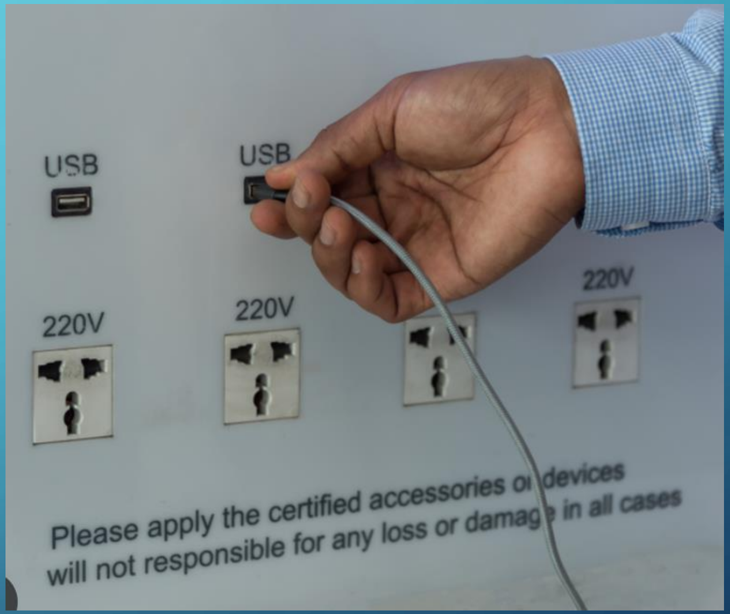
71 : 58

Send $100 worth of bitcoin to this address:

1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

Screenshot of Ransomware Attack

Image source: Heimdal Security



USB
USB
220V
220V
220V
Please apply the certified accessories or devices
will not responsible for any loss or damage in all cases

Photo of a "Juice Jacking" device

Image source: ShutterStock

INTRODUCTION (CONT.)

- And we haven’t even begun to scratch the surface of modern threats and exploits.

- This presentation is an overview of how threat actors use tools and techniques, like shown in the previous slides, to gain unauthorized access to financial systems, networks, and data, present you with ways you can protect yourself and your companies from falling prey to these threats, and speculate what the future of protection and prevention measures against these attempts will look like.

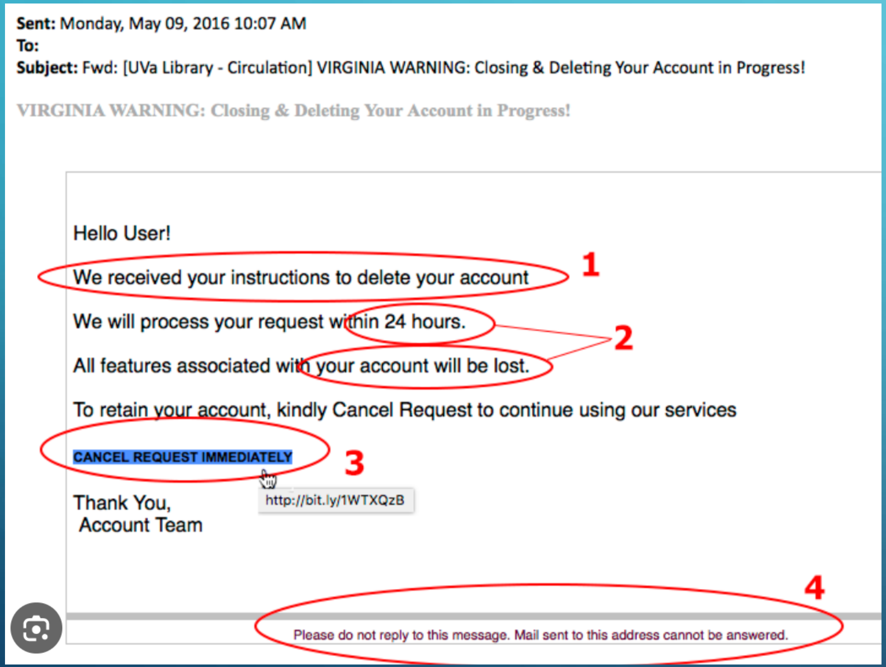
PART 02: BASIC TERMS

DEFINITIONS OF BASIC TERMS (SRC: NIST)

- **THREAT:** *Any circumstance or event with the potential to negatively impact an organization or its assets (e.g. Malware, Cybercrime, Social engineering.)*
- ***THREAT ACTOR:*** *Any individual or group posing a threat (e.g. hacker, hacktivists, nation-state.)*
- **BREACH:** *An event or series of events resulting in unwanted or unauthorized access to personally identifiable information (e.g. Equifax, Target, Capital One--more later.)*
- **ATTACK VECTOR:** *A pathway or method used by a threat actor to exploit a threat (e.g. social engineering, malware, phishing.)*
- **FIREWALL:** *A device or software that filters and restricts data communication between two connected networks (e.g. Windows Defender, Sonicwall, Cisco Firewall.)*

DEFINITIONS OF BASIC TERMS (SRC: NIST)

- **PHISHING:** *An attempt to acquire sensitive data, through a fraudulent solicitation in email or website, masquerading as a legitimate business or person.*



Sent: Monday, May 09, 2016 10:07 AM
To:
Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

We will process your request within 24 hours.

All features associated with your account will be lost.

To retain your account, kindly Cancel Request to continue using our services

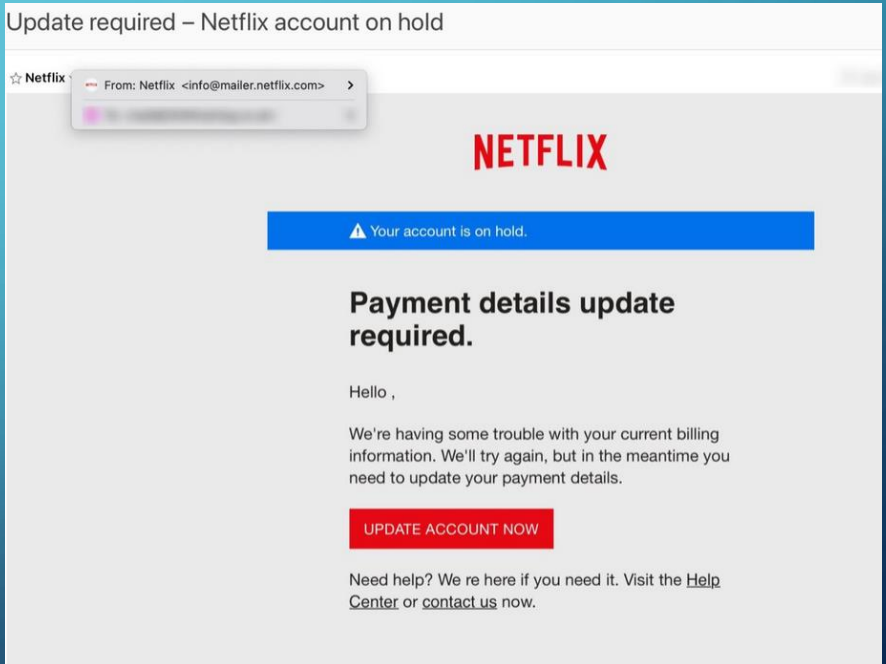
CANCEL REQUEST IMMEDIATELY

http://bit.ly/1WTXQzB

Thank You,
Account Team

Please do not reply to this message. Mail sent to this address cannot be answered.

Image source: UVA



Update required – Netflix account on hold

☆ Netflix

From: Netflix <info@mailer.netflix.com>

[redacted]

NETFLIX

Your account is on hold.

Payment details update required.

Hello ,

We're having some trouble with your current billing information. We'll try again, but in the meantime you need to update your payment details.

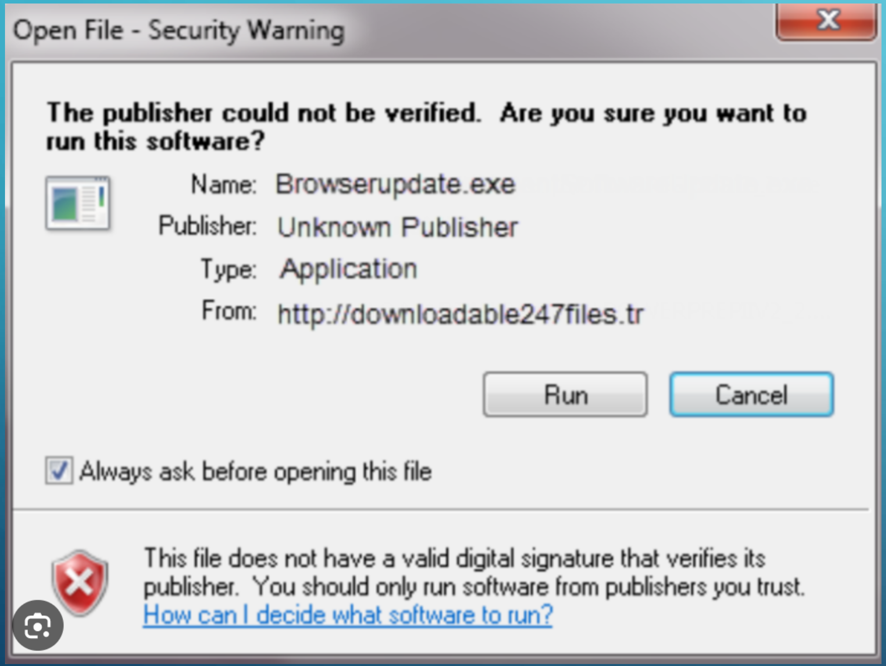
UPDATE ACCOUNT NOW

Need help? We re here if you need it. Visit the Help Center or contact us now.

Image source: Tessian.com

DEFINITIONS OF BASIC TERMS (SRC: NIST)

- **MALWARE:** *Hardware, Firmware, or Software that is intentionally included or inserted into a system for a harmful purpose.*



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: Browserupdate.exe

Publisher: Unknown Publisher

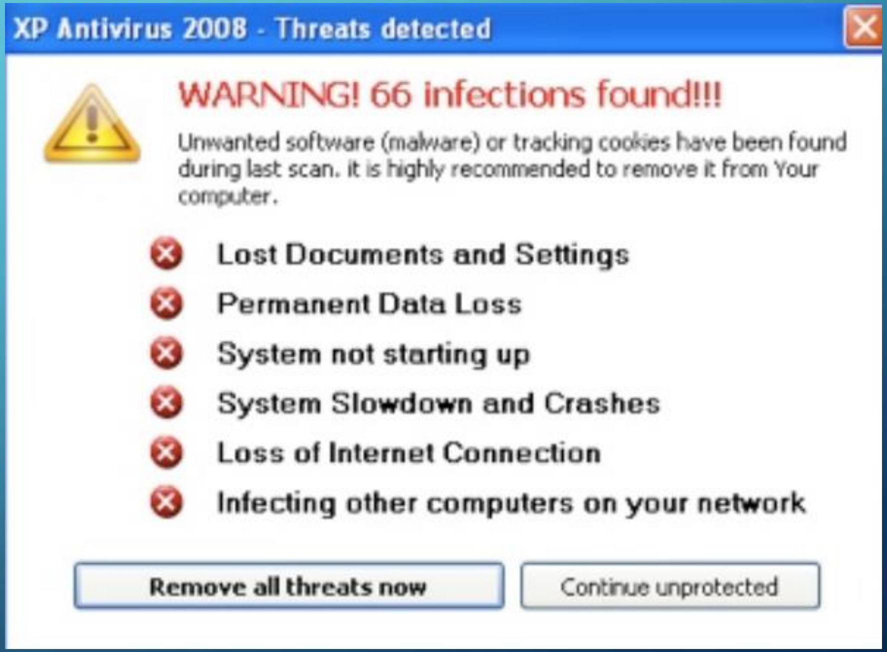
Type: Application

From: http://downloadable247files.tr

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Image source: CMU



XP Antivirus 2008 - Threats detected

WARNING! 66 infections found!!!

Unwanted software (malware) or tracking cookies have been found during last scan. it is highly recommended to remove it from Your computer.

- ☒ Lost Documents and Settings
- ☒ Permanent Data Loss
- ☒ System not starting up
- ☒ System Slowdown and Crashes
- ☒ Loss of Internet Connection
- ☒ Infecting other computers on your network

Image source: IGCSEICT

DEFINITIONS OF BASIC TERMS (SRC: NIST)

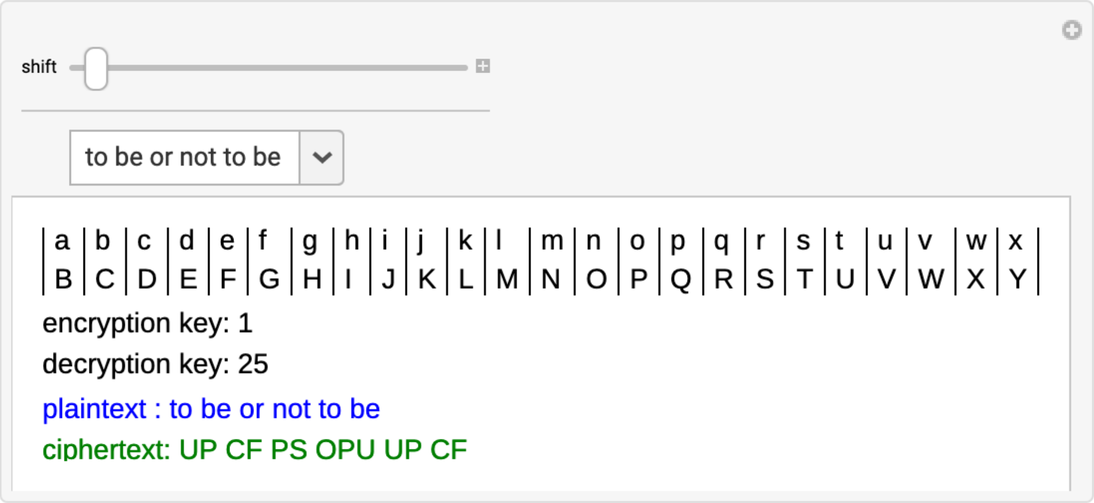
- **SOCIAL ENGINEERING:** *An attempt to trick someone into revealing information that can be used to attack systems/networks usually by telephone, email, or in-person.*

And I can't remember what email address
we used to log on to the account,
and the baby's crying-

Source: YouTube

DEFINITIONS OF BASIC TERMS (SRC: NIST)

- **ENCRYPTION:** *The transfer of data from one form into another to conceal the data's original meaning.*



shift

to be or not to be

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

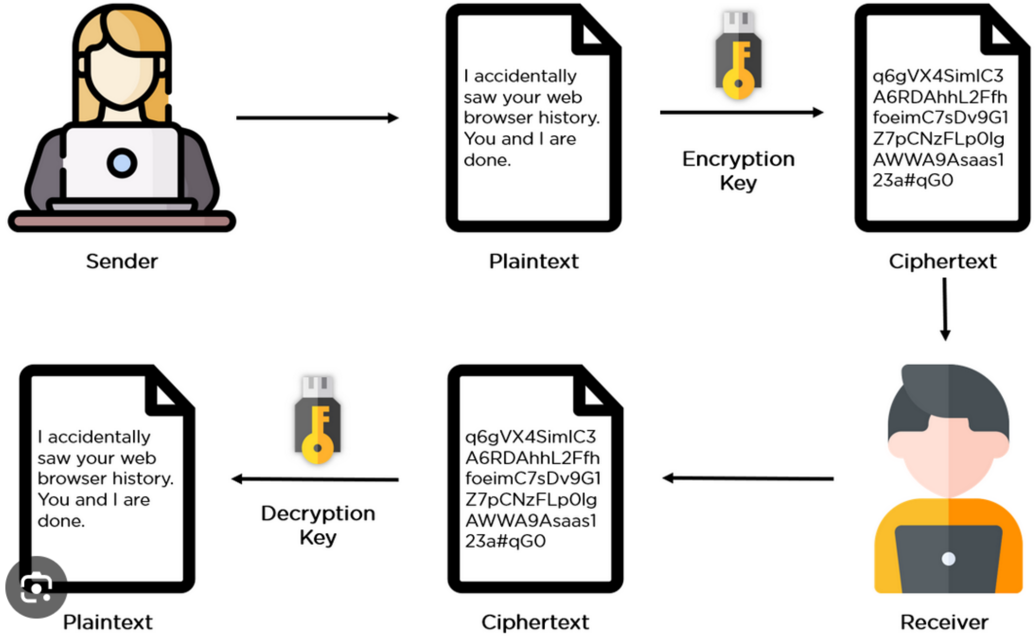
encryption key: 1

decryption key: 25

plaintext : to be or not to be

ciphertext: UP CF PS OPU UP CF

Source: Wolfram.com

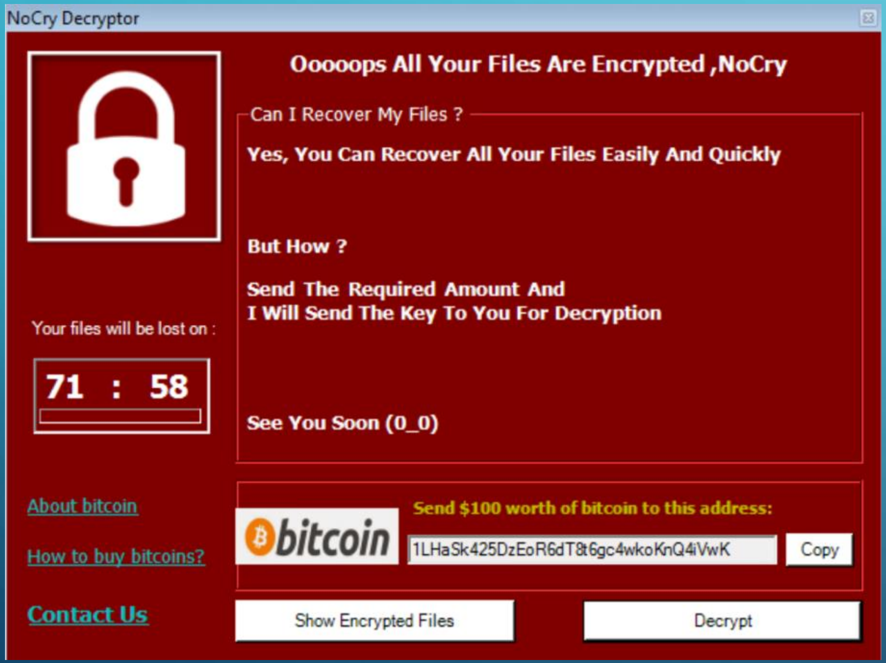


Sender
I accidentally saw your web browser history. You and I are done.
Plaintext
Encryption Key
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Ciphertext
Receiver
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Ciphertext
Decryption Key
I accidentally saw your web browser history. You and I are done.
Plaintext

Source: Simplilearn.com

DEFINITIONS OF BASIC TERMS (SRC: NIST)

- **RANSOMWARE:** Malware that *prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid.*



Ooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

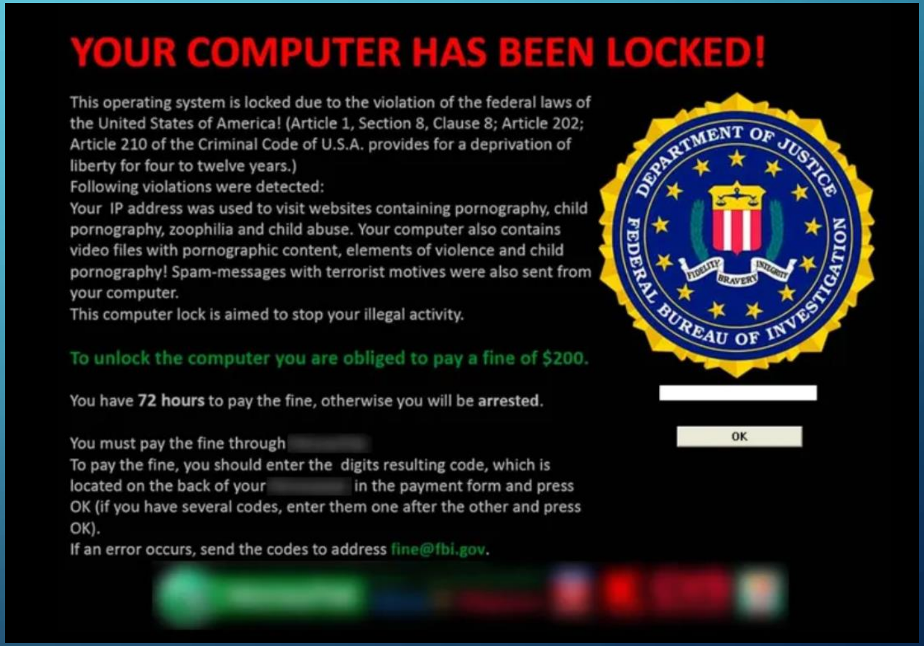
Your files will be lost on :

71 : 58

Send $100 worth of bitcoin to this address:

1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

Image source: Heimdal Security



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

[redacted]

Image source: WIRED

PART 03: BACKGROUND

BACKGROUND

- Why should we care about cybersecurity in financial sector?
- Motivation of hackers are broken down into four major categories:
  1. Financial – they want to make money and/or steal intellectual property
  2. Political/Government – They want to influence change in another state/country
  3. Hacktivism – Hacking for a “good” cause
  4. Revenge – Retaliating for something that was done to them
- Let’s look at some examples of each…

BACKGROUND (CONT.)

Examples of Financial Motives

- 04/17/2022 – Beanstalk Farms cryptocurrency heist resulting in $180 million in stolen financial assets. (Carnegie)
- 12/04/2021 – Bitmart Security Breach resulting in roughly $200 million in financial assets stolen by hackers. (Carnegie)
- 05/2019 – First American Financial had 800 million records leaked from their website including names, addresses, SS#s, bank account #s, etc… (Forbes)
- 09/2017 – Equifax data breach resulting in financial data of 40%-50% of entire US population's SS#s, names, driver's license #s, and credit card numbers. (Upguard)

BACKGROUND (CONT.)

Examples of Political/Governmental Motive

- 02/2022 – Russian military hackers launch DDos attacks against Ukrainian banks and government. (Reuters)
- 09/2022 – Russian-based hacking group took down MI5s website. (CSIS)
- 05/2022 – Iranian hacking group took down the Port of London Authority's website. (CSIS)
- 08/2014 – Sony Pictures was hacked by a North Korean government group in an effort to have the movie *The Interview* pulled from release because it was a film about their leader, Kim Jong Un, getting assassinated. (TrendMicro)

BACKGROUND (CONT.)

Examples of Hacktivism Motive

BACKGROUND (CONT.)

Examples of Revenge Motive

- 02/2022 – IT Technician working for Welland Park Academy, who was terminated, logged into the school and deleted files and blocked access to services in retaliation. (BBC)
- 02/2017 – Fired system administrator logged in to Georgia-Pacific's network and altered its industrial control systems in retaliation for being fired, costing the company $1.1 million in damages. (GRCILAW)
- 2016 – System administrator for American College of Education was terminated after which time he logged in and changed its Google Account's password blocking access to email and study materials for 2000 students. Said he would "give it back" for $200,000. (Kaspersky)

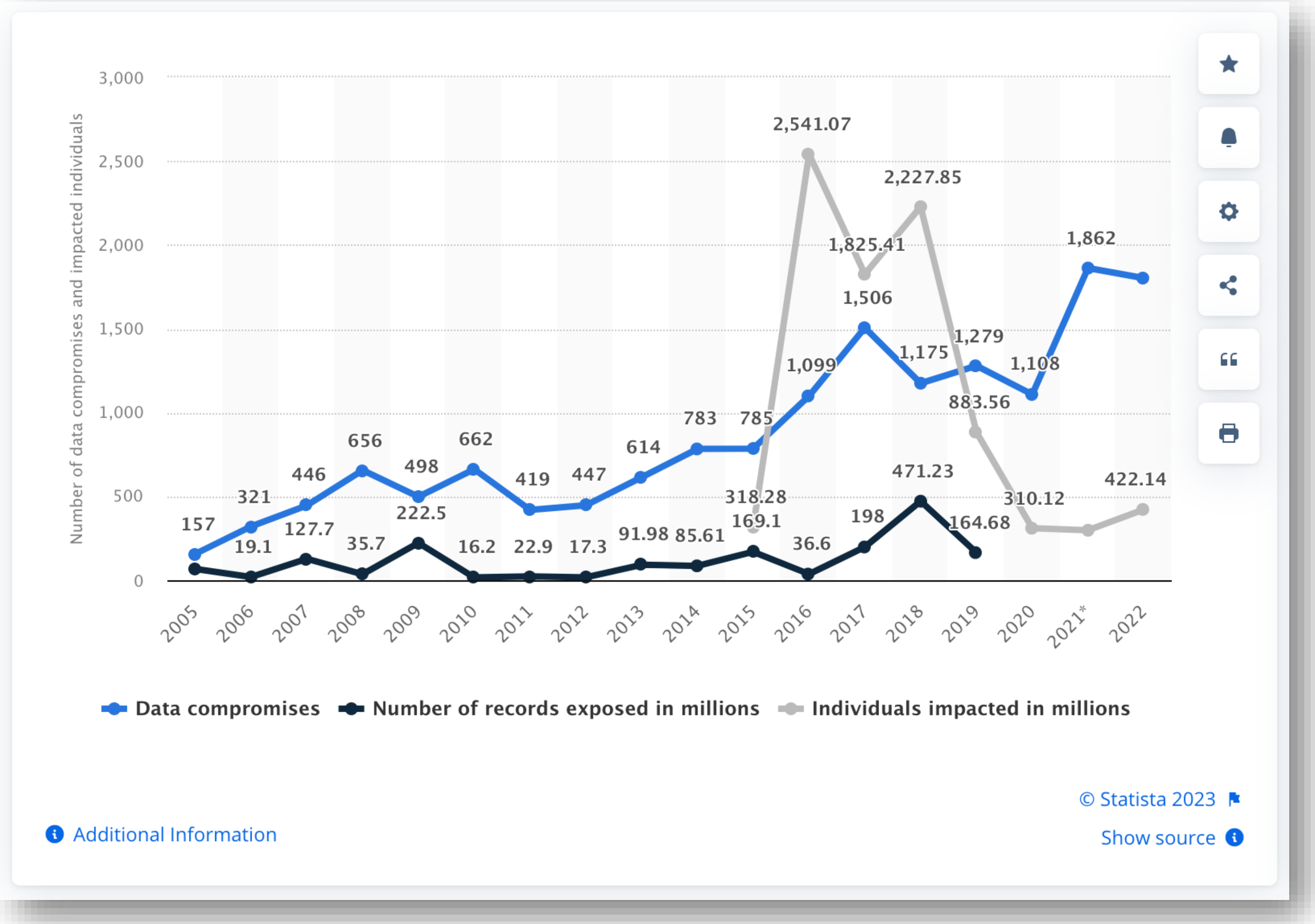
PART 04: STATISTICS

STATISTICS

- Now that we have seen some real-world examples of cyberattacks, let’s take a look at some statistics demonstrating the following:
  - Annual number of data compromises from 2005 – 2022
  - Annual amount of monetary damage caused by cybercrime in US from 2001 – 2022
  - Average cost of a data breach from 2006 – 2023
  - Distribution of cyberattacks across industries in 2022

STATISTICS (CONT.)

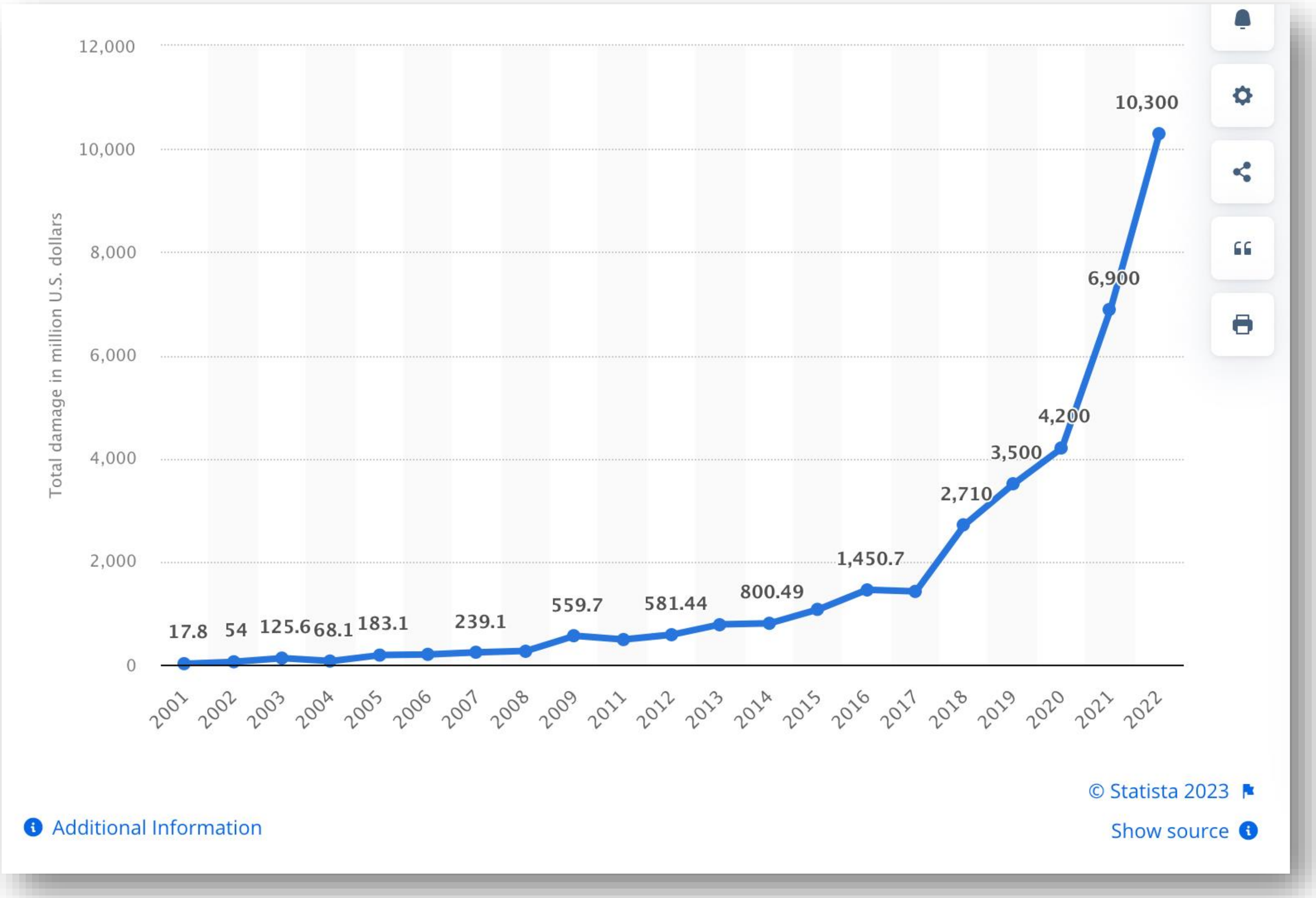
Annual number of data compromises and individuals impacted in the United States from 2005 to 2022



Source: Statista.com

STATISTICS (CONT.)

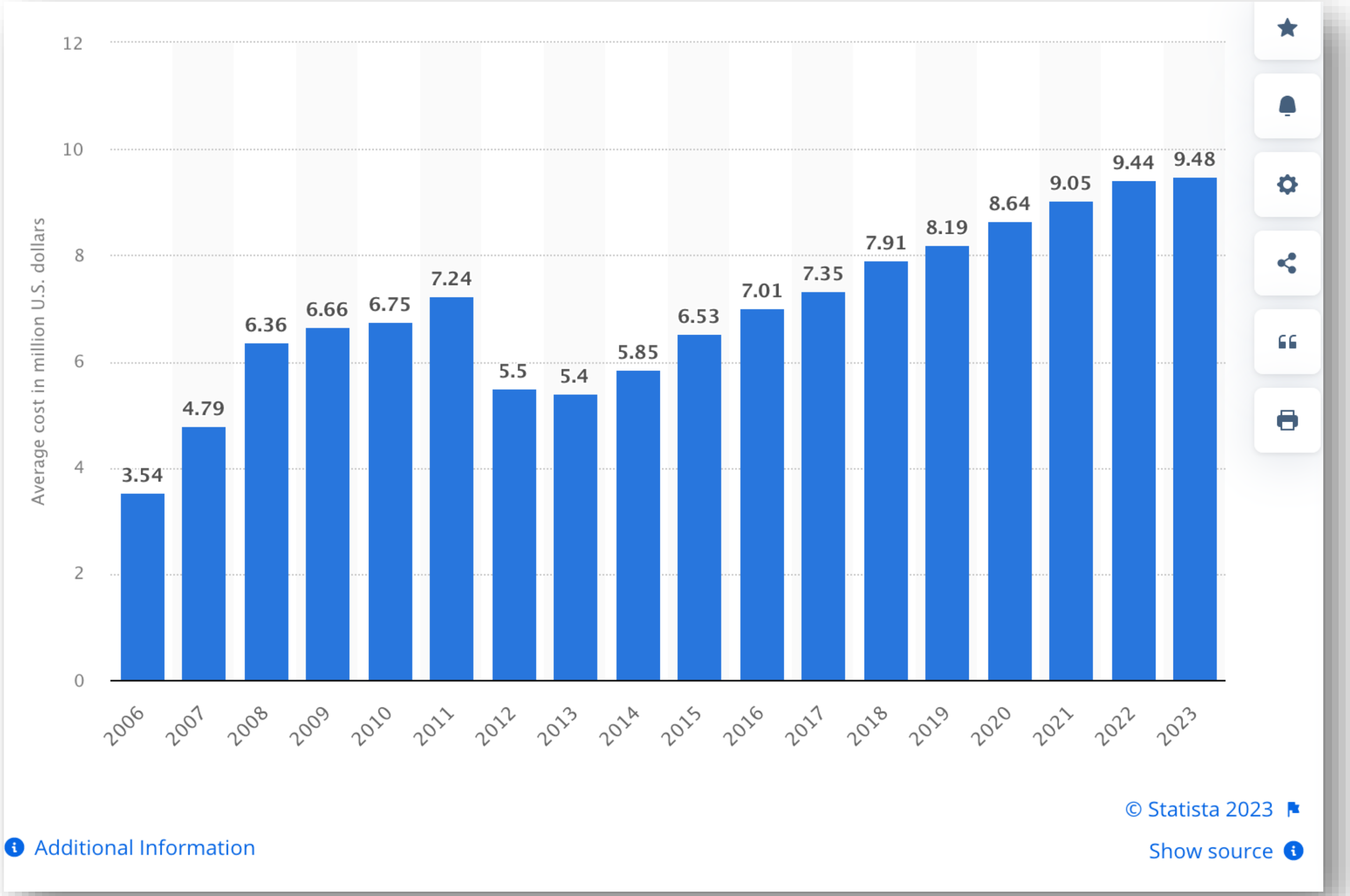
Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2022 (in million U.S. dollars)



Source: Statista.com

STATISTICS (CONT.)

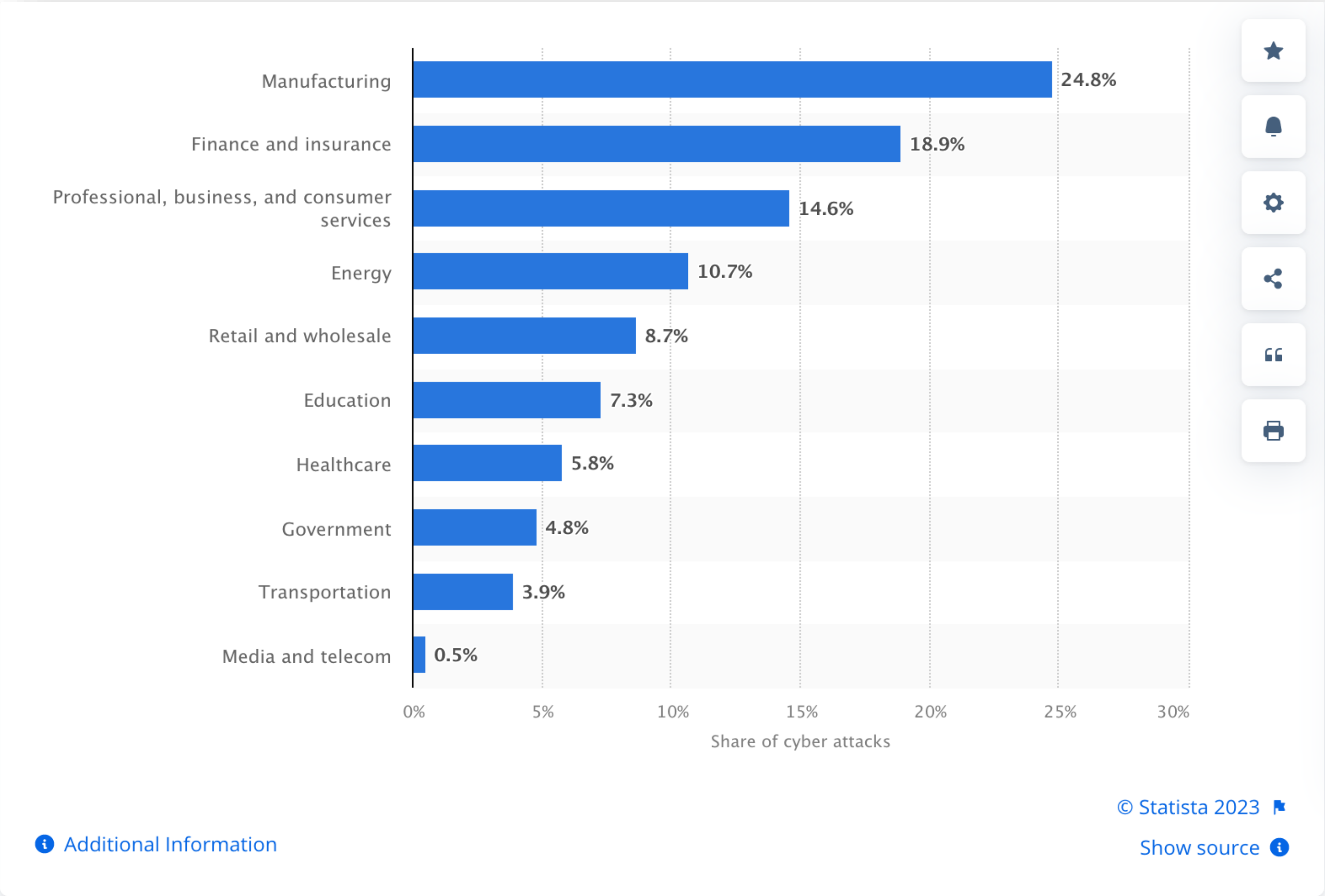
Average cost of a data breach in the United States from 2006 to 2023 (in million U.S. dollars)



Source: Statista.com

STATISTICS (CONT.)

Distribution of cyber attacks across worldwide industries in 2022

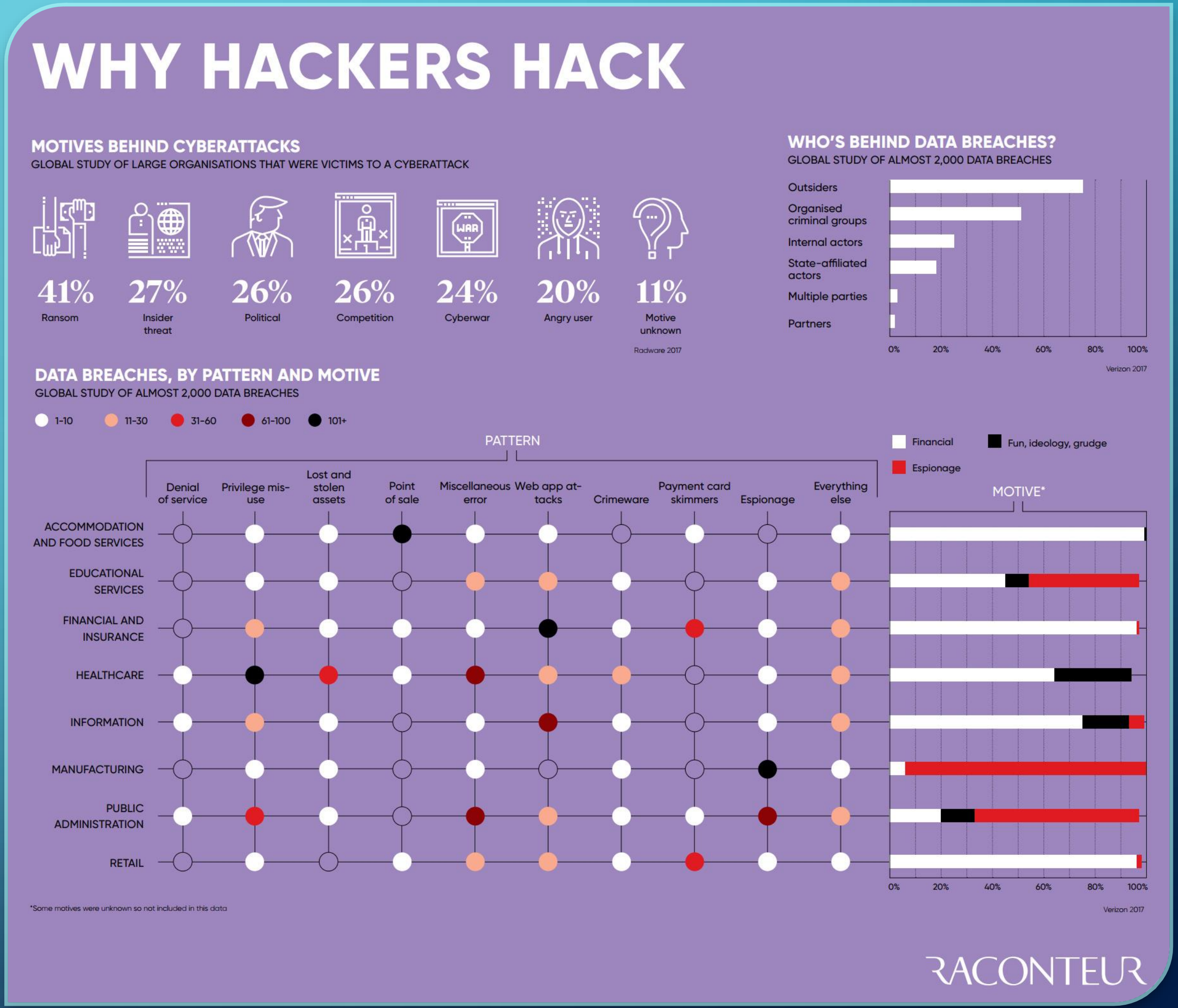


Source: Statista.com

PART 05: ATTACK ANALYSIS

ATTACK ANALYSIS

- Why do hackers hack?
- Infographic based on data from Verizon's DBIR database polled from 2017. Attack patterns and motives are still relevant today.
- Source: Visualcapitalist.com



WHY HACKERS HACK

MOTIVES BEHIND CYBERATTACKS

GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

41%	27%	26%	26%	24%	20%	11%
Ransom	Insider threat	Political	Competition	Cyberwar	Angry user	Motive unknown

Radware 2017

WHO'S BEHIND DATA BREACHES?

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES

Verizon 2017

DATA BREACHES, BY PATTERN AND MOTIVE

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES

○ 1-10 ● 11-30 ● 31-60 ● 61-100 ● 101+

PATTERN

	Denial of service	Privilege misuse	Lost and stolen assets	Point of sale	Miscellaneous error	Web app attacks	Crimeware	Payment card skimmers	Espionage	Everything else
ACCOMMODATION AND FOOD SERVICES		1-10	1-10	101+	1-10	1-10		1-10		1-10
EDUCATIONAL SERVICES		1-10	1-10		11-30	11-30	1-10		1-10	11-30
FINANCIAL AND INSURANCE		11-30	1-10	1-10	1-10	101+	1-10	31-60	1-10	11-30
HEALTHCARE	1-10	101+	31-60	1-10	61-100	11-30	11-30		1-10	11-30
INFORMATION	1-10	11-30	1-10		1-10	61-100	1-10		1-10	11-30
MANUFACTURING		1-10	1-10		1-10		1-10		101+	1-10
PUBLIC ADMINISTRATION	1-10	31-60	1-10		61-100	11-30	1-10	1-10	61-100	11-30
RETAIL		1-10		1-10	11-30	11-30	1-10	31-60	1-10	1-10

Verizon 2017

*Some motives were unknown so not included in this data

RACONTEUR

ATTACK ANALYSIS (CONT.)

- Purplesec reports that from 2019-2020:
  - 67% of financial institutions reported an increase in cyberattacks
  - 26% of financial enterprises faced a destructive attack (attack resulting in loss of financial assets)
  - 32% of financial institutions experienced “Island hopping” where an attacker leverages access to one organization to gain access to another
  - 25% of malware attacks hit banks and other financial industries—this is more than any other industry
  - Credit card compromises increased 212%
  - 47% of financial institutions reported increase in wire fraud
  - Despite these statistics, only 32% of financial institution CISOs said they conduct monthly threat hunts

ATTACK ANALYSIS (CONT.)

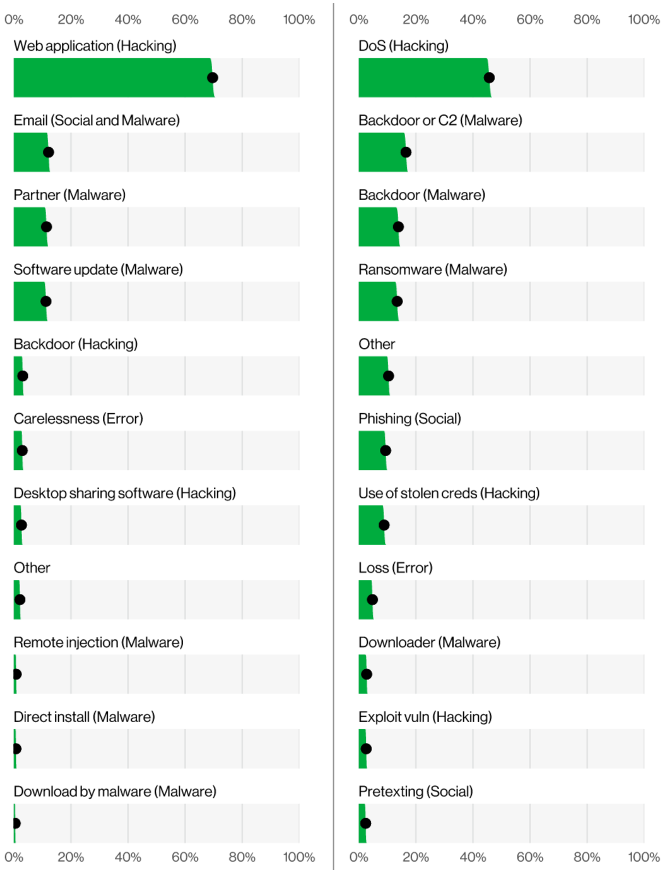


Figure 16. Top action vectors in incidents (n=18,419)

Figure 17. Top action varieties in incidents (n=18,511)

- Infographic depicting the top attack vectors hackers use to compromise systems and networks in 2022 according to Verizon's 2022 DBIR.

ATTACK ANALYSIS (CONT.)

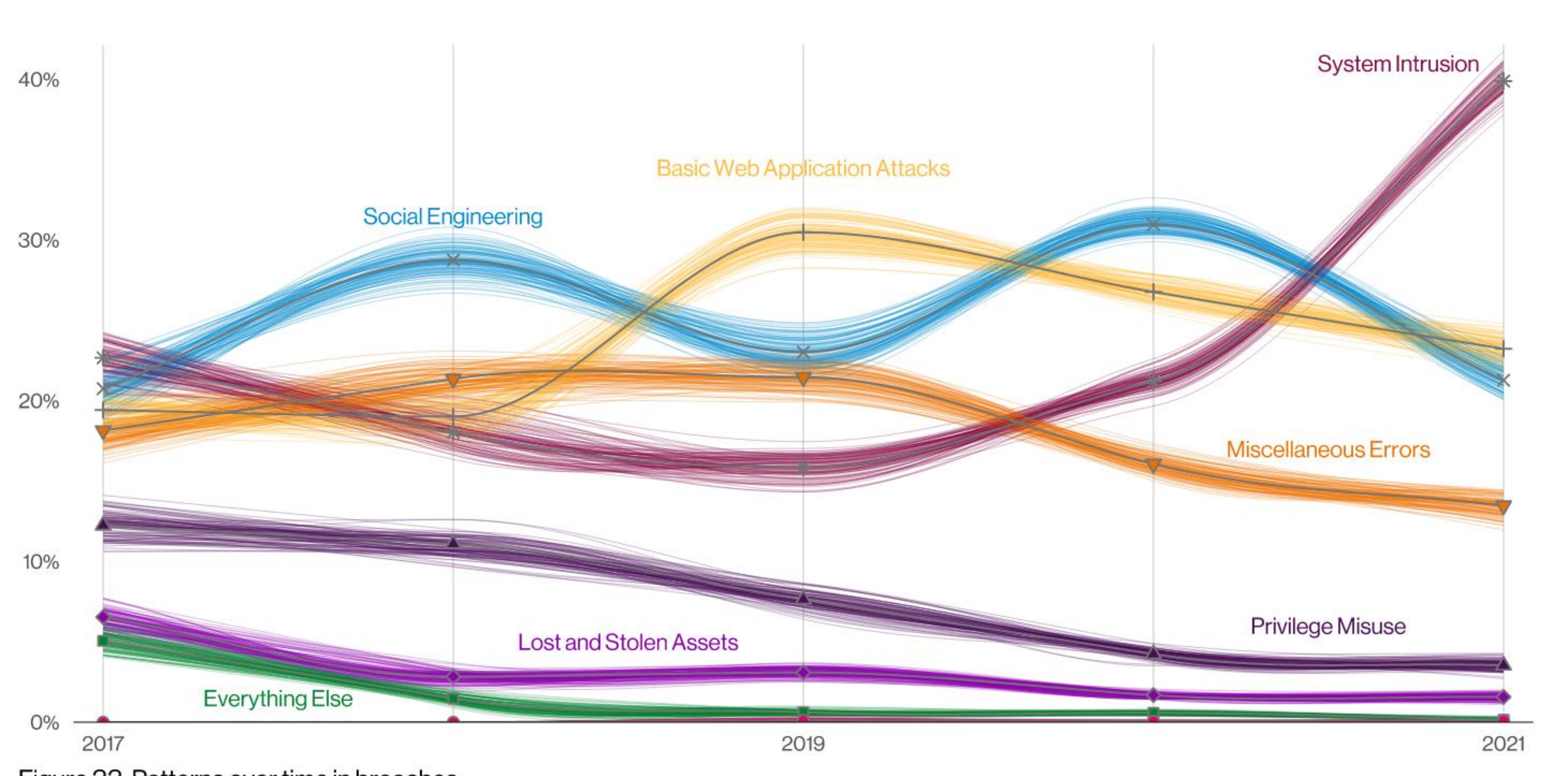


Figure 33. Patterns over time in breaches

Source: Verizon DBIR

ATTACK ANALYSIS (CONT.)

- Attack Analysis Summary:
  - Financial gain is the biggest motivation for hackers
  - Humans are the single greatest threat to security
  - Systems and applications should be kept up-to-date with latest security patches
  - Manufacturing and Financial sectors are the biggest targets worldwide
  - These numbers will only continue to rise given the scale and growth of industries and the new methods and tools hackers have access to moving forward

PART 06: PROTECTION & DEFENSE

PROTECTION & DEFENSE AGAINST ATTACKS

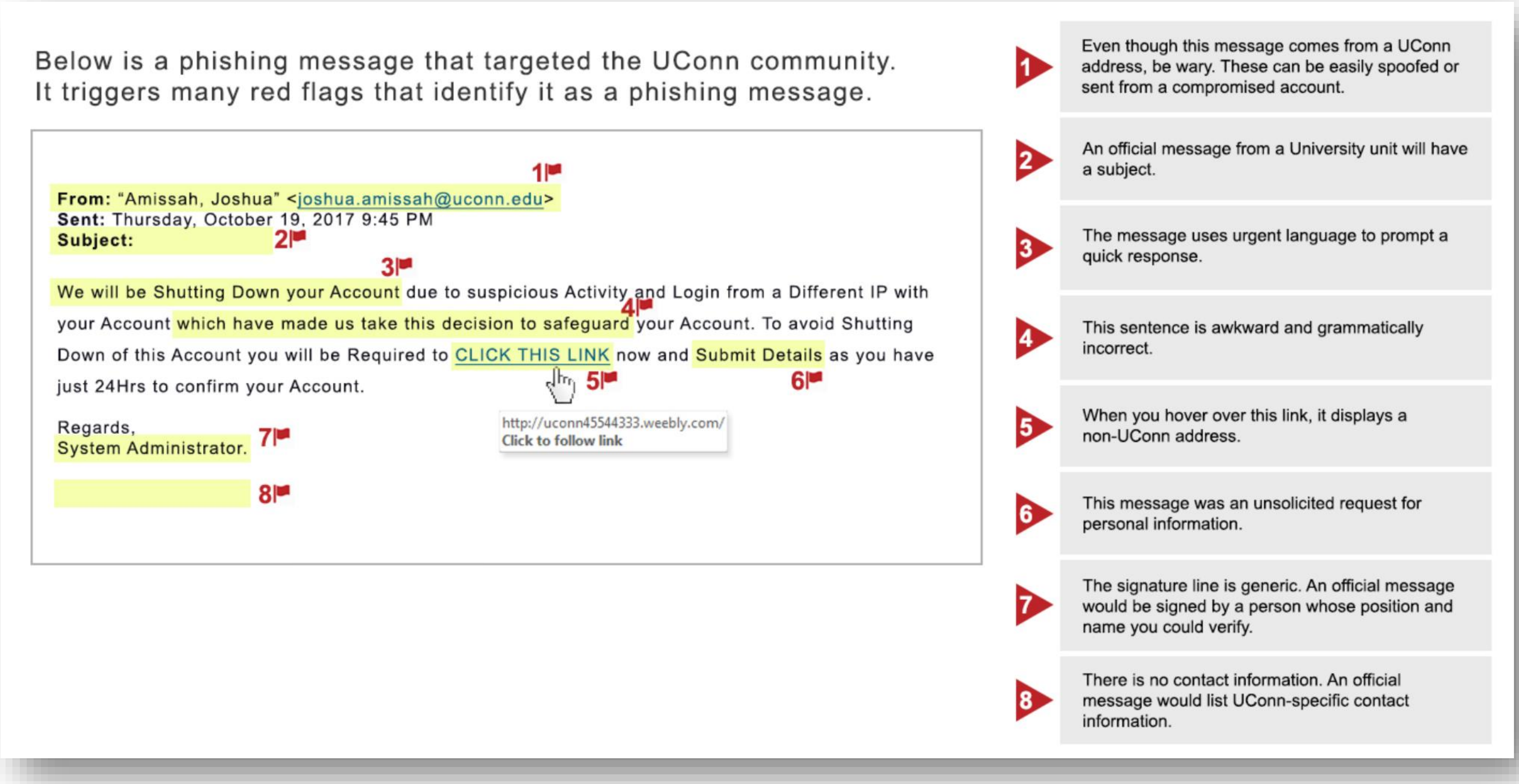
- As we learned, there are four major categories of attacks:
  - Social Engineering (e.g. pretexting, tailgating, phishing)
  - Malware (e.g. ransomware, viruses, trojan horses)
  - Hacking (e.g. brute force attacks, MITM attacks, impersonation attacks)
  - User error (e.g. incorrect configuration, lost device, poor password hygiene
- Let’s examine how to protect and defend ourselves against each of these…

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- Protection and defense against social engineering attacks:
  - User Education and Awareness
  - If you receive an email or call that seems suspicious, put them on hold or request assistance from a colleague/supervisor
  - If email, check sender and URL locations (before clicking on them) to ensure legitimacy
  - Verify everything, if you can, before responding
  - Let's look at a sample phishing attack…

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- Sample phishing attempt from UCONN.



Below is a phishing message that targeted the UConn community. It triggers many red flags that identify it as a phishing message.

From: “Amissah, Joshua” <joshua.amissah@uconn.edu> 1
Sent: Thursday, October 19, 2017 9:45 PM
Subject: 2

3 We will be Shutting Down your Account due to suspicious Activity and Login from a Different IP with your Account which have made us take this decision to safeguard 4 your Account. To avoid Shutting Down of this Account you will be Required to CLICK THIS LINK 5 now and Submit Details 6 as you have just 24Hrs to confirm your Account.

http://uconn45544333.weebly.com/
Click to follow link

Regards,
System Administrator. 7

8

1 Even though this message comes from a UConn address, be wary. These can be easily spoofed or sent from a compromised account.

2 An official message from a University unit will have a subject.

3 The message uses urgent language to prompt a quick response.

4 This sentence is awkward and grammatically incorrect.

5 When you hover over this link, it displays a non-UConn address.

6 This message was an unsolicited request for personal information.

7 The signature line is generic. An official message would be signed by a person whose position and name you could verify.

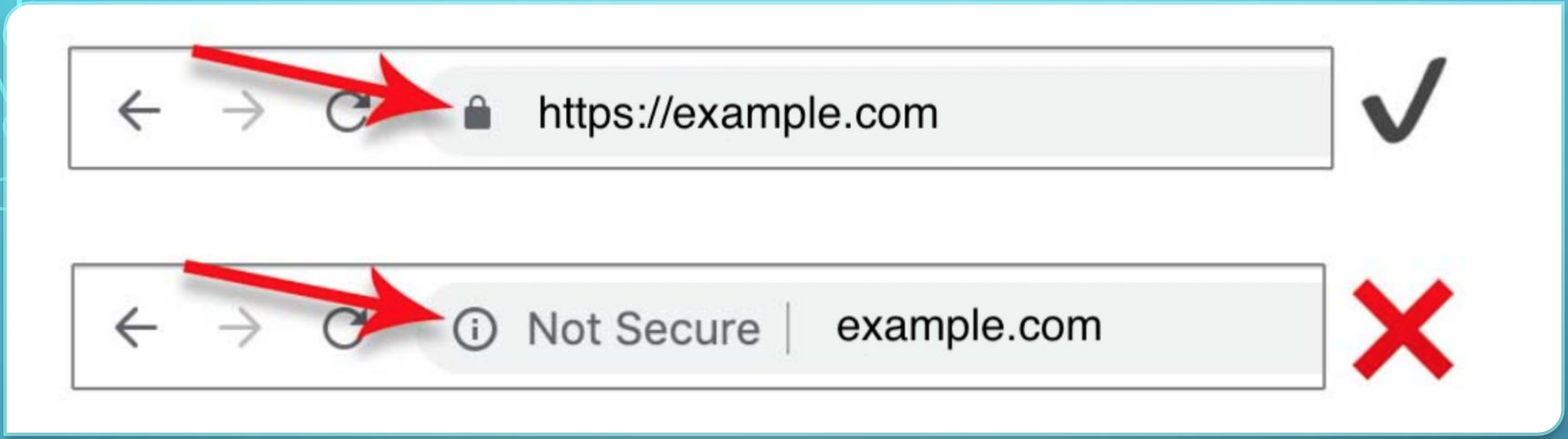
8 There is no contact information. An official message would list UConn-specific contact information.

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- Protection and defense against malware attacks:
  - Properly configured and updated anti-malware software
  - User education and awareness (don't plug in rogue hardware devices, look for strange devices plugged into your computer, don't download software from links in email)
  - Run regular scans on your computer (at least once per week, if not more frequently)
  - Report any and all anomalies to your IT/IS team as directed
  - Ask your IT department to regularly audit your computer to check for unauthorized/unexpected network traffic
  - Lock your computer (Windows key + L) if you are going to be away from it for more than 30 seconds

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- Protection and defense against hacking attempts:
  - User education and awareness (notice a theme here?)
  - Don't join wi-fi networks unless you are 100% positive they belong to your company
  - Don't access websites unless you are 100% sure they belong to your company and are secure
  - Ask your IT/IS team (or do it yourself, if your comfortable) to regularly monitor your system log files to determine if someone is trying to use brute-force attack to access your system
  - Ask your IT/IS team to monitor network traffic coming into/out of your machine (if they aren't already) and look for anomalies



https://example.com

✓

Not Secure | example.com

✗

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

SAMPLE OF UNSECURED WEBSITE

PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- Protection and defense against user error:
  - User education and awareness
  - Don’t write passwords down on Post-It notes or put them on/around your workspace
  - If you don’t know what you’re doing, don’t be afraid to ask
  - Always use strong passwords (eight+ characters, mix of upper and lower cases, numbers, and special characters.) Example strong password: N0d3@l$us%
  - Use Multi-Factor Authentication
  - Familiarize yourself with your company’s security policy and stay vigilant
  - Always use VPN when connecting from outside office

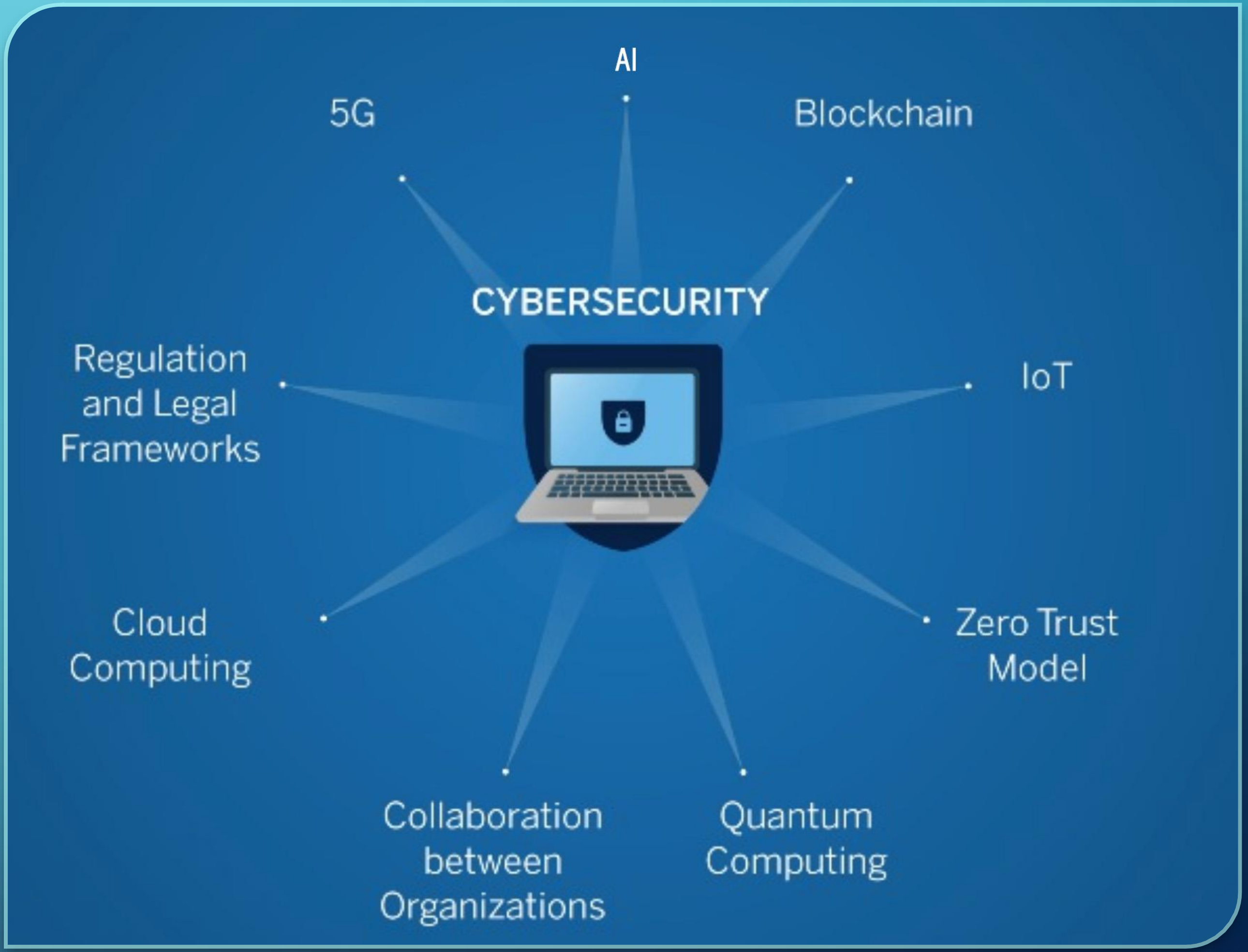
PROTECTION & DEFENSE AGAINST ATTACKS (CONT.)

- What can you do?
  - Encrypt, Encrypt, Encrypt!
  - Use VPN whenever you are on a public network (or use your mobile hotspot)
  - Minimum of 3 backups (1 cloud, 1 removable, 1 solid state) all stored in separate loc.
  - Ask your IT department, if it doesn't do so already, to run quarterly/semi-annul penetration tests on your device/devices
  - Use MFA for EVERYTHING!
  - Lock/Freeze all three of your credit reports (Experian, Equifax, TransUnion)

PART 07: THE FUTURE OF CYBERATTACKS

THE FUTURE OF CYBERATTACKS

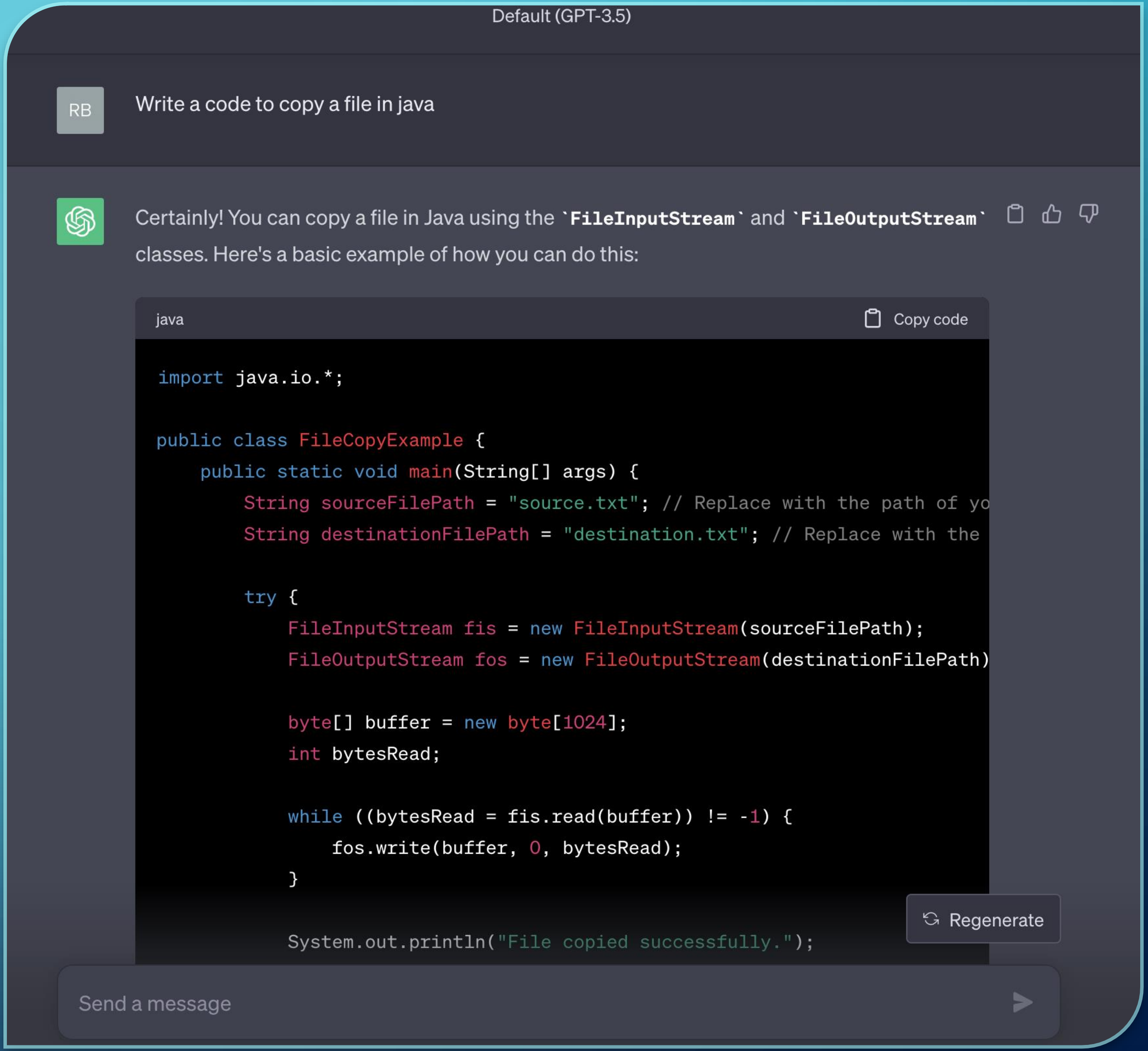
- What are some things to look for in the future?
  - Artificial Intelligence (AI)
  - Continued advancement of IoT attacks
  - Emerging Technologies (VAMR exploits, Metaverse Microtransactions, Drone technology)



Source: BBVAOpenmind

THE FUTURE OF CYBERATTACKS (CONT.)

- Artificial Intelligence (AI)
- Sample of code I asked CHATGPT to generate to copy a file using JAVA.



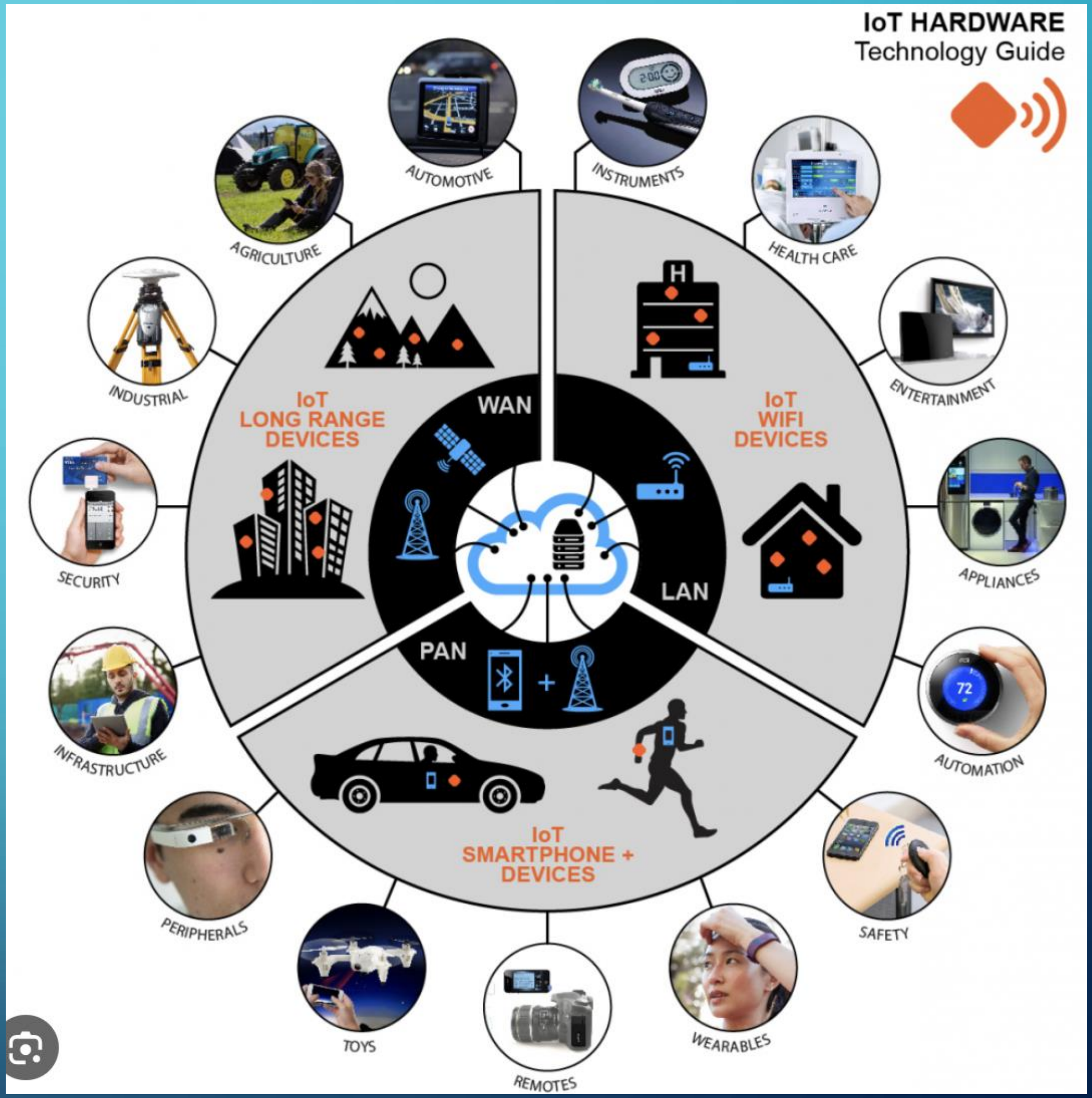
Write a code to copy a file in java

Certainly! You can copy a file in Java using the `FileInputStream` and `FileOutputStream` classes. Here's a basic example of how you can do this:

```java
import java.io.*;

public class FileCopyExample {
    public static void main(String[] args) {
        String sourceFilePath = "source.txt"; // Replace with the path of yo
        String destinationFilePath = "destination.txt"; // Replace with the

        try {
            FileInputStream fis = new FileInputStream(sourceFilePath);
            FileOutputStream fos = new FileOutputStream(destinationFilePath)

            byte[] buffer = new byte[1024];
            int bytesRead;

            while ((bytesRead = fis.read(buffer)) != -1) {
                fos.write(buffer, 0, bytesRead);
            }

            System.out.println("File copied successfully.");
```

THE FUTURE OF CYBERATTACKS (CONT.)

- IoT Advancement
- Zero-day exploits



THE FUTURE OF CYBERATTACKS (CONT.)

- VAMR/Metaverse
- Drones/Spying

QUESTIONS/COMMENTS

THANK YOU!

RUSSELL BEAUCHEMIN

RBEAUCHEMIN@RWU.EDU