Understanding Dark Web Operations

Willie Harris & Ryan McPhee

Who are we?

Willie Harris

Senior
CS + Cyber Conc.
ISC^2 CC
wdharri2@ncsu.edu

Ryan McPhee

Junior
CS + Cyber Conc.
ISC^2 CC, CompTIA Security+
rcmcphee@ncsu.edu

NC STATE UNIVERSITY

College of Education
Friday Institute for Educational Innovation

The comprehensive NCDPI K-12 Cybersecurity Program encompasses a multidimensional approach to safeguarding PSU across North Carolina and their stakeholders from threat actors. The Friday Institute is involved in 7 distinct workstreams that collectively create and support a robust defense against cyber risks. These workstreams encompass overall program management engagement and support, cybersecurity awareness and skills training, vulnerability management, asset discovery and identification, incident response, cybersecurity consulting, and identity and access management. Along with the other program services and resources, the Friday Institute plays an instrumental part in the protection, detection, and responses for K-12 institutions across North Carolina.

Presentation Scope:

- NOT a deep dive into everything the dark web is and has to offer
- A general understanding of the dark web is valuable to organizations
- Operationalizing this understanding can grant benefits to the organization and those who are a part of it.

Today's agenda

01

Dark Web Introduction

02

Accessing the Dark Web Securely

03

Monitoring Unauthorized Data Disclosure

04

Verifying Data Authenticity & Reporting Protocols

05

Statistics and Results

06

Today's Summary

01

Dark Web Introduction

What is the Dark Web?

Different Internet Layers

Surface

Google	YouTube
Edge	Amazon
Bing	Wikipedia

Deep

Banking Sites
Medical Portals
Insurance Pages
Cloud Storage Sites

Dark

Tor Exclusive Forums
Anonymous PasteBins

Relative Proportions

~90%

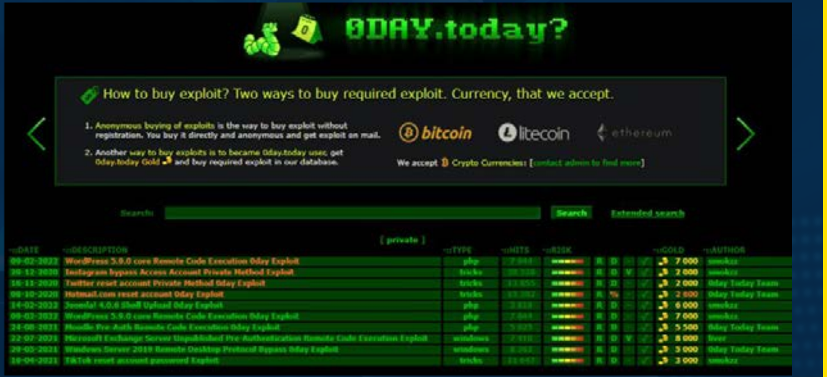
Deep + Dark Web

~0.01%

Dark Web

VIRUS
PASSWO
LOGIN

MICHIGAN
STATE



0DAY.today?

How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.

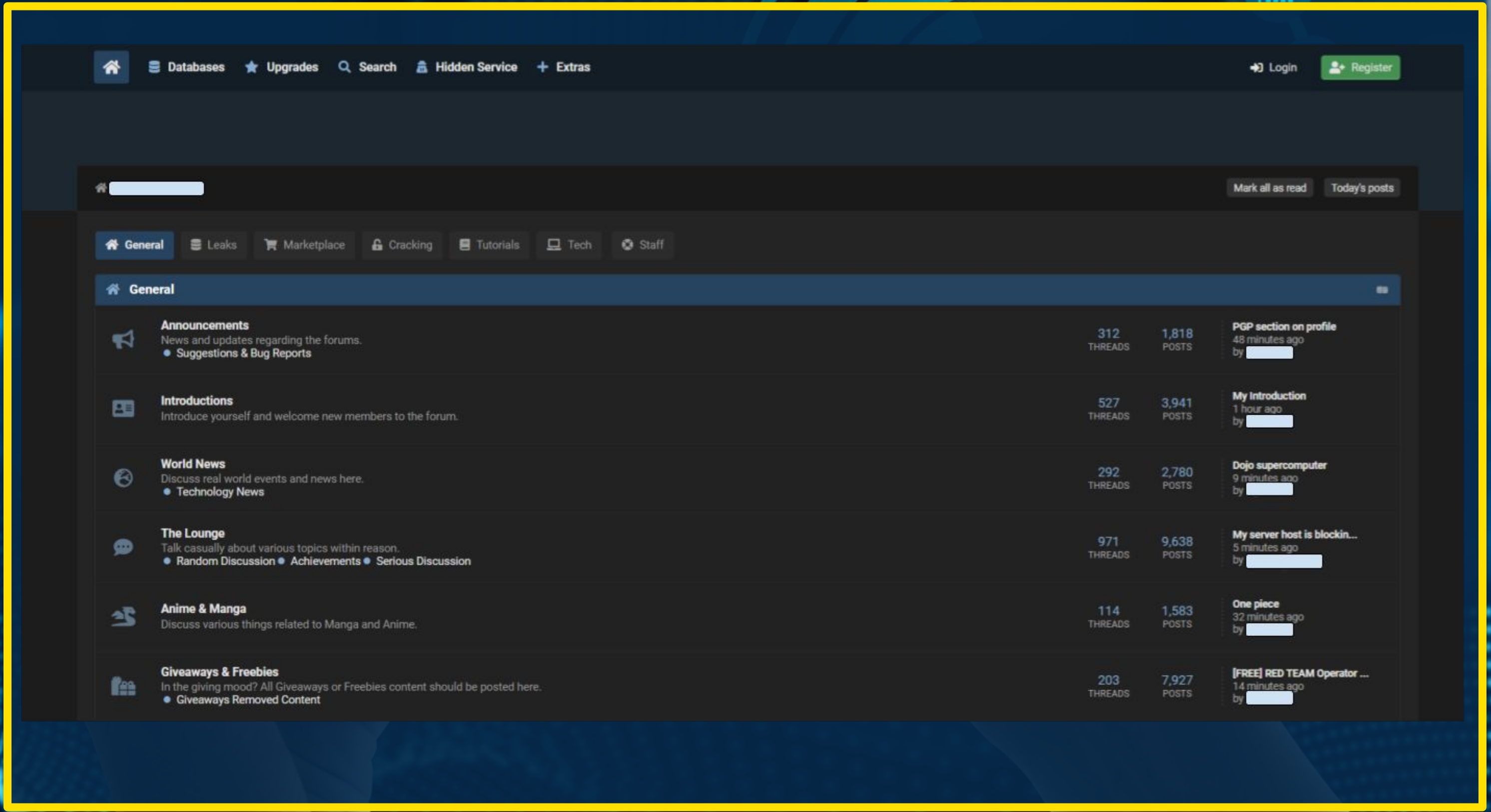
bitcoin litecoin ethereum

We accept Crypto Currencies: [contact admin to find more]

Search: Search Extended_search

[private]

DATE	DESCRIPTION	TYPE	HITS	RISK					GOLD	AUTHOR
09-02-2022	WordPress 5.9.0 core Remote Code Execution 0day Exploit	php	[illegible]	▬▬▬▬▬	R	D	-	✓	7 000	smokzz
29-12-2020	Instagram bypass Access Account Private Method Exploit	tricks	[illegible]	▬▬▬▬▬	R	D	V	✓	2 000	smokzz
16-11-2020	Twitter reset account Private Method 0day Exploit	tricks	[illegible]	▬▬▬▬▬	R	D	-	✓	2 000	0day Today Team
08-10-2020	Hotmail.com reset account 0day Exploit	tricks	[illegible]	▬▬▬▬▬	R	%	-	✓	2 000	0day Today Team
14-02-2022	Joomla! 4.0.6 Shell Upload 0day Exploit	php	[illegible]	▬▬▬▬▬	R	D	-	✓	6 000	smokzz
09-02-2022	WordPress 5.9.0 core Remote Code Execution 0day Exploit	php	[illegible]	▬▬▬▬▬	R	D	-	✓	7 000	smokzz
24-08-2021	Moodle Pre-Auth Remote Code Execution 0day Exploit	php	[illegible]	▬▬▬▬▬	R	D	-	✓	5 500	0day Today Team
22-07-2021	Microsoft Exchange Server Unpublished Pre-Authentication Remote Code Execution Exploit	windows	[illegible]	▬▬▬▬▬	R	D	V	✓	8 000	liver
29-05-2021	Windows Server 2019 Remote Desktop Protocol Bypass 0day Exploit	windows	[illegible]	▬▬▬▬▬	R	D	-	✓	5 000	0day Today Team
18-04-2021	TikTok reset account password Exploit	tricks	[illegible]	▬▬▬▬▬	R	D	-	✓	3 000	smokzz



[redacted]

General

Forum	Threads	Posts	Last post
Announcements News and updates regarding the forums. ● Suggestions & Bug Reports	312 THREADS	1,818 POSTS	PGP section on profile 48 minutes ago by [redacted]
Introductions Introduce yourself and welcome new members to the forum.	527 THREADS	3,941 POSTS	My Introduction 1 hour ago by [redacted]
World News Discuss real world events and news here. ● Technology News	292 THREADS	2,780 POSTS	Dojo supercomputer 9 minutes ago by [redacted]
The Lounge Talk casually about various topics within reason. ● Random Discussion ● Achievements ● Serious Discussion	971 THREADS	9,638 POSTS	My server host is blockin... 5 minutes ago by [redacted]
Anime & Manga Discuss various things related to Manga and Anime.	114 THREADS	1,583 POSTS	One piece 32 minutes ago by [redacted]
Giveaways & Freebies In the giving mood? All Giveaways or Freebies content should be posted here. ● Giveaways Removed Content	203 THREADS	7,927 POSTS	[FREE] RED TEAM Operator ... 14 minutes ago by [redacted]

02

Accessing the Dark Web Securely

Tools for secure operations

VPN

Tor

Tails/VM

Tails

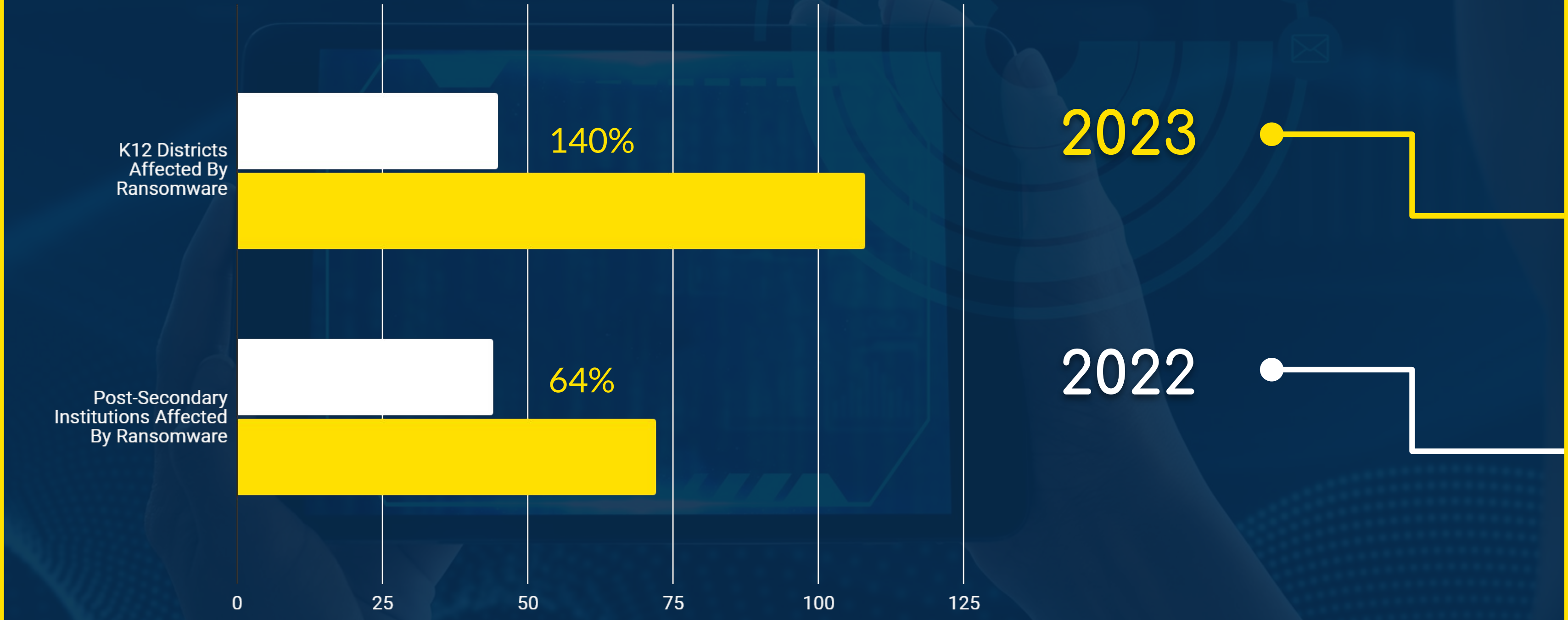
Aliases

A key way to develop trust, credibility, and relationships within the dark web environment

03

Monitoring Unauthorized Data Disclosure

Ever Growing Threat



*Figures represent minimum number

$3,650,000

Average cost of a data breach in the education industry between March 2022-2023

180

Total minimum number of K-12 Districts and Post-Secondary schools impacted by ransomware in 2023

~$675,000,000

Estimated total cost in damages from education industry breaches

What Can We Do?

+

“NCSU”
“University”
“North Carolina”
“School(s)”
“Students”
“Teachers”
“K12”

04

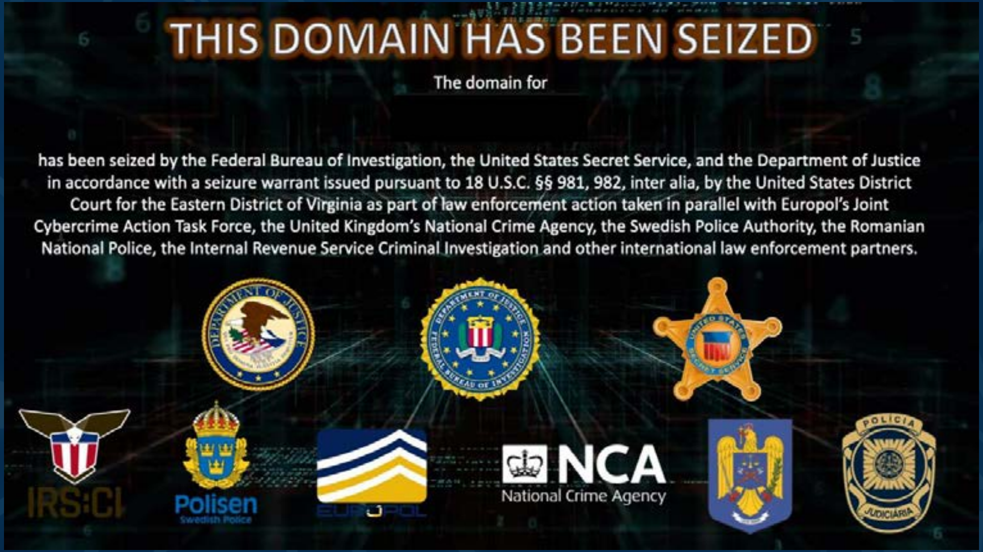
Verifying Data Authenticity & Reporting Protocols

Authenticity Verification

Public Key Signatures

Community-Verified Forums

Doe, John : 987654321098@students.psu.k12.nc.us, (555) 123-4567, Student, 10th Grade, Parkwood High School
Smith, Jane : jane.smith@psu.k12.nc.us, (555) 555-5555, Teacher, Oakwood Middle School
Brown, David : 987654321@students.psu.k12.nc.us, (555) 789-1234, Student, 8th Grade, Crestview Junior High
Wilson, Sarah : sarah.wilson@psu.k12.nc.us, (555) 234-5678, School Counselor, Elmwood Elementary School
Johnson, Michael : 55555555555@students.psu.k12.nc.us, (555) 987-6543, Student, 11th Grade, Lakeview High School
Lee, Lisa : 444555666777@students.psu.k12.nc.us, (555) 345-6789, Student, 9th Grade, Westfield High School
Davis, Jessica : 987654321012@students.psu.k12.nc.us, (555) 456-7890, Student, 10th Grade, Brookside High School
Anderson, Robert : robert.anderson@psu.k12.nc.us, (555) 234-5678, Principal, Crestwood Elementary School
Martinez, Maria : 9998887771234@students.psu.k12.nc.us, (555) 567-8901, Student, 12th Grade, Oakville High School
Hernandez, Carlos : carlos.hernandez@psu.k12.nc.us, (555) 678-9012, Custodian, Parkside Elementary School
Gonzalez, Laura : 555444333012@students.psu.k12.nc.us, (555) 789-0123, Student, 10th Grade, Hillside Junior High
Taylor, William : william.taylor@psu.k12.nc.us, (555) 890-1234, School Nurse, Maplewood Middle School
Adams, Susan : 122233301234@students.psu.k12.nc.us, (555) 901-2345, Student, 11th Grade, Lakewood High School
Scott, Brian : 888777012345@students.psu.k12.nc.us, (555) 123-4567, Student, 4th Grade, Elmwood Elementary School
Turner, Jennifer : jennifer.turner@psu.k12.nc.us, (555) 234-5678, Librarian, Crestview Elementary School
White, Richard : richard.white@psu.k12.nc.us, (555) 345-6789, Janitor, Oakwood Elementary School
Allen, Karen : 544433301234@students.psu.k12.nc.us, (555) 456-7890, Student, 10th Grade, Brookside Junior High
Baker, Timothy : timothy.baker@psu.k12.nc.us, (555) 567-8901, School Administrator, Crestwood Middle School
Carter, Michelle : 555660123456@students.psu.k12.nc.us, (555) 678-9012, Student, 8th Grade, Lakeview Junior High
Clark, Daniel : daniel.clark@psu.k12.nc.us, (555) 890-1234, School Psychologist, Hillside Elementary School



THIS DOMAIN HAS BEEN SEIZED

The domain for

has been seized by the Federal Bureau of Investigation, the United States Secret Service, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with Europol's Joint Cybercrime Action Task Force, the United Kingdom's National Crime Agency, the Swedish Police Authority, the Romanian National Police, the Internal Revenue Service Criminal Investigation and other international law enforcement partners.

05

Statistics and Results

~350,000

Unique emails
discovered on dark web forums

Additional Metrics

9

Forum Posts Discovered

12

NC K12 Districts Impacted

7

Net-New Breaches Found

06

Today's Summary

NOT
encouragement to
surf the dark web
without purpose

Data breaches and leaks are a constant and real threat to any organization

Dark web scanning is valuable to catch unknown exposures

“Biggest Leak in History”

Hackers Online Club (HOC)

“Mother of All Breaches” (MOAB)

Contained 26 billion records/emails/credentials

12 Terabytes (TB) of Data

Aggregation of already existing and exposed data

Potential Biggest Net-New Leak in History

Ars Technica

319 Files

Totaling around 104 GB of data

~71,000,000 Unique Emails

Approximately 430,000 “Have I Been Pwned” subscribers included

~35% Not Seen Before

Based on random sample. Results in approximately <u>25,000,000</u> new credentials

Best Practices ✓

- Ensure digital protection measures
  - Tor, VPNs
- Develop an online persona when necessary - alias
- Verify data for authenticity and safety
  - Scanners, Sandboxes
- Follow proper reporting procedures per organization standards
- Maintain healthy separation

Worst Practices

- Give away personally identifiable information (PII)
  - First & Last Name
  - Location
- Open raw data files without safety verification
- Access and scout sites without a formulated plan
- Make payments with identifiable transaction methods

Questions?

Resources

https://www.ibm.com/downloads/cas/E3G5JMBP

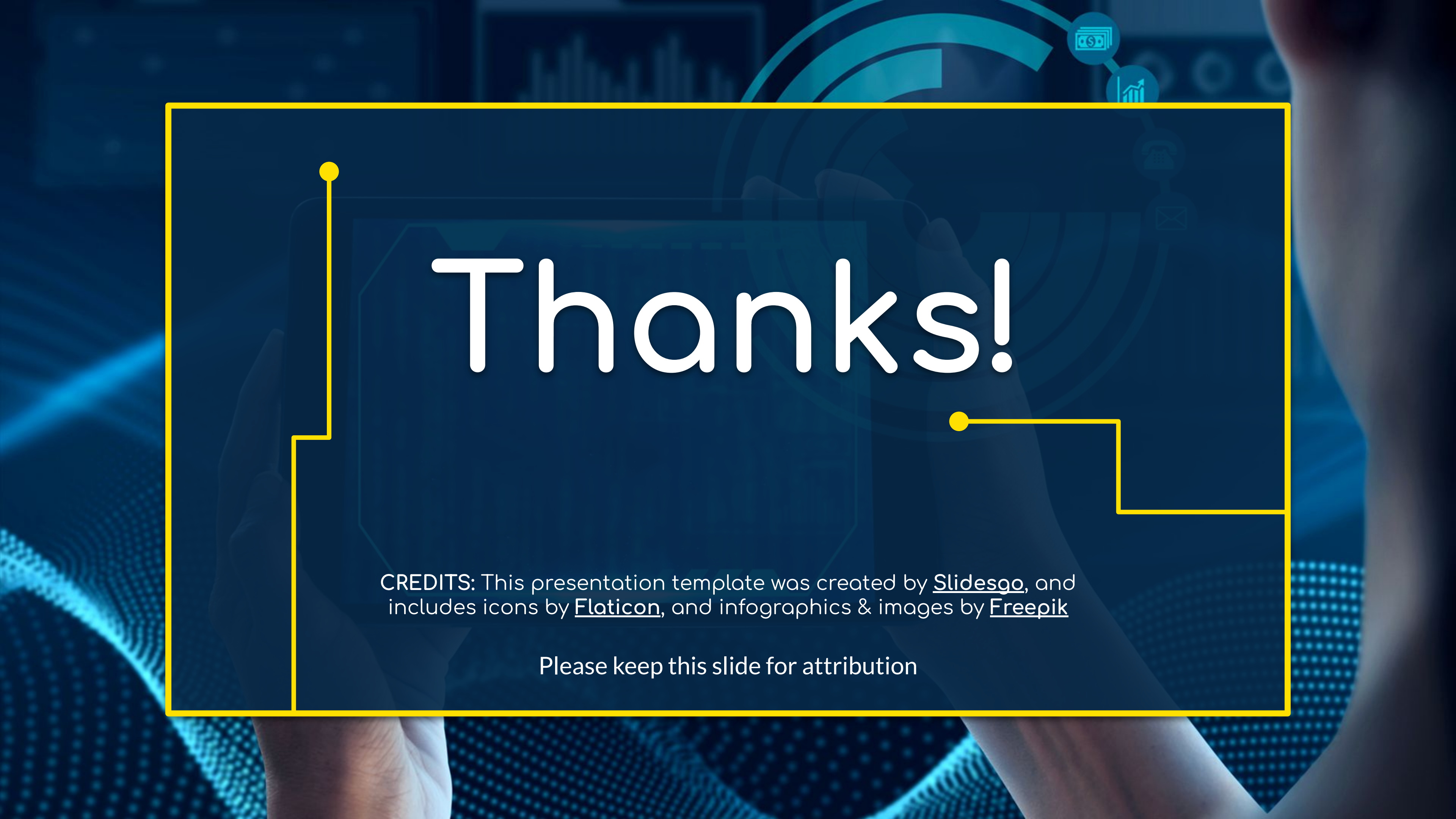
https://oit.ncsu.edu/2023/10/16/what-is-the-cost-of-a-data-breach/

https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/#:~:text=K%2D12%20schools,the%20107%20had%20data%20stolen.

https://blackdotsolutions.com/blog/dark-web-vs-deep-web/

https://hackersonlineclub.com/mother-of-all-breaches-billion-records-leaked-in-largest-data-breach/

https://arstechnica.com/security/2024/01/71-million-passwords-for-facebook-coinbase-and-others-found-for-sale/



Thanks!

CREDITS: This presentation template was created by Slidesgo, and includes icons by Flaticon, and infographics & images by Freepik

Please keep this slide for attribution