

THE

PACKET

JANUARY 2023

✦ HACKS OF THE MONTH	03
✦ CYBER NEWS UPDATES	08
✦ CYBERSECURITY HISTORY	10
✦ JOBS & INTERNSHIPS	11
✦ FACULTY CORNER	14



CAE
IN CYBERSECURITY
COMMUNITY

Check out this CactusCon 11 session!

Who's Watching Who – Hacking IP Cameras

Friday, January 27, 2023 1:00 pm



Paul Wagner



Michael Galde



Dalal Alharthi

**Cactus
CON**

FBI'S VETTED INFO SHARING NETWORK 'INFRAGARD' HACKED



The Federal Bureau of Investigations community-sharing website was compromised around December 10. The InfraGard service connects critical infrastructure owners with the FBI. This connection provides education, networking, and information-sharing on security threats and risks. The hackers responsible for this hack stripped member information from the website. The Hacker, who goes by the alias USDoD on the breached forum, used a script to collect the members' names and emails. The Hacker gained access by using the name of a CEO who is the head of a major U.S. financial cooperation. The Hacker wanted to sell the database for 50k and said the price was negotiable. As of December 18, the Hacker stated that the data was no longer available and would not be sold.

COLOMBIAN ENERGY SUPPLIER **EPM** HIT BY BLACKCAT RANSOMWARE ATTACK

Colombian energy company Empresas Públicas de Medellín suffered a BlackCat/ALPHV ransomware attack on In early December 2022, disrupting the company's operations and taking down online services. The Colombian prosecutor's office later confirmed to EL COLOMBIANO that ransomware was behind the attack on EPM that caused devices to be encrypted and data to be stolen. BlackCat ransomware, aka ALPHV, was behind the attacks, claiming to have stolen corporate data during the attacks. The ransom note created in the attack states that the threat actors stole a wide variety of data. It should be noted that this is the exact text used in all BlackCat ransom notes and is not specific to EPM. This is not the first ransomware attack that has targeted a Colombian energy company.



BLUEBOTTLE HACKERS USED SIGNED WINDOWS DRIVER IN ATTACKS ON BANKS



A signed Windows driver has been used in attacks on banks in French-speaking countries, likely from a threat actor that stole more than \$11 million from various banks. A cybercrime group dubbed Bluebottle has been linked to targeted attacks against the financial sector in Francophone countries located in Africa from at least July 2022 to September 2022. This group is also known as OPERA1ER. The attribution stems from similarities in the toolset used, the attack infrastructure, the absence of tailor-made malware, and the targeting of French-speaking nations in Africa. Three unnamed financial institutions in three African nations were breached, although it's unknown whether Bluebottle successfully monetized the attacks.

RAIL GIANT WABTEC DISCLOSES DATA BREACH AFTER LOCKBIT RANSOMWARE ATTACK



The Wabtec Corporation has disclosed a data breach that exposed personal and sensitive information. Wabtec says hackers breached their network and installed malware on specific systems as early as March 15th, 2022. On June 26th, Wabtec said they detected unusual activity on their network leading to an investigation of the attack and whether the hackers had stolen data. LockBit published samples of data stolen from Wabtec and eventually leaked all stolen data on August 20th, 2022, presumably after a ransom was not paid.

NEW LINUX MALWARE USES 30 PLUGIN EXPLOITS TO BACKDOOR **WORDPRESS** SITES



A previously unknown Linux malware has exploited 30 vulnerabilities in multiple outdated WordPress plugins and themes to inject malicious JavaScript. The main functionality of the trojan is to hack WordPress sites using a set of hardcoded exploits that are run successively until one of them works. The malware targets 32-bit and 64-bit Linux systems, giving its operator remote command capabilities. If the targeted website runs an outdated and vulnerable version, the malware automatically fetches malicious JavaScript from its command and control (C2) server and injects the script into the website. Defending against this threat requires admins of WordPress websites to update to the latest available version the themes and plugins running on the site and replace those that are no longer developed with alternatives that being supported.

RUSSIANS HACKED **JFK** AIRPORT'S TAXI DISPATCH SYSTEM FOR PROFIT



Two U.S. citizens were arrested for allegedly conspiring with Russian hackers to hack the John F. Kennedy International Airport (JFK) taxi dispatch system to move specific taxis to the front of the queue in exchange for a \$10 fee. The taxi dispatch system is a computer-controlled system that ensures that taxis are dispatched from the airport's holding lot to pick up the next available fare at the appropriate terminal. According to the unsealed indictment published by the U.S. Department of Justice, two men, Daniel Abayev and Peter Leyman, with the assistance of Russian hackers, breached the JFK taxi dispatch system between September 2019 and September 2021. Taxi drivers participating in the scheme had to pay \$10 to the hackers in cash or via mobile payment. Those promoting the service to their colleagues would be given waivers allowing them to skip the line for free.





CYNTHIA HETHERINGTON

FOUNDER AND PRESIDENT OF HETHERINGTON GROUP

IC CAE SPEAKER SERIES 2023

OPEN-SOURCE INTELLIGENCE OSINT

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.

**JANUARY 30TH
4:00 PM AZ**

[REGISTER HERE](#)



Intelligence Community
**Centers for
Academic
Excellence**

Diversity. Knowledge. Excellence.



College of Applied Science & Technology

Cyber Convergence Center



IC CAE SPEAKER SERIES

**THE UNIVERSITY
OF ARIZONA**

6

CYNTHIA HETHERINGTON BIO

Cynthia Hetherington, MLS, MSM, CFE, CII is the founder and president of Hetherington Group, a consulting, publishing, and training firm that leads in due diligence, corporate intelligence, and cyber investigations by keeping pace with the latest security threats and assessments. She has authored three books on how to conduct investigations, is the publisher of the newsletter, Data2know.com: Internet and Online Intelligence, and has trained over 180,000 investigators, security professionals, attorneys, accountants, auditors, military intelligence professionals, and federal, state, and local agencies on best practices.

For more than 25 years, Ms. Hetherington has led national and international investigations in corporate due diligence and fraud, personal asset recovery, and background checks. With a specialization in the financial, pharmaceutical, and telecommunications industries, her investigations have recovered millions of dollars in high profile corruption cases, assisting on the investigations of the top two Ponzi cases in United States history.

In 2015, Ms. Hetherington founded the OSMOSIS Institute, host of the annual OSMOSIS Conference. Hundreds of investigators across the nation attend to gain insights into Open Source Intelligence and receive training from the most recognized social media and open source trainers in North America.

Ms. Hetherington won the prestigious Women in IT New York's 2022 Security Leader of the Year. In 2021, Ontic Center for Protective Intelligence honored Ms. Hetherington with the Protective Intelligence Pioneer Award. In 2019, she was honored with the Enterprising Woman of the Year Award by Enterprising Women Magazine and the CybHER Warrior Award by Dakota State University Madison Cyber Labs. Also in 2019, she was shortlisted for the coveted Women in IT New York's Entrepreneur of the Year Award and named a finalist in the esteemed Ernst & Young LLP New Jersey Entrepreneur of the Year Awards. Ms. Hetherington is a recipient of the Association of Certified Fraud Examiners' James Baker Speaker of the Year Award.

FBI WARNS OF SEARCH ENGINE ADS PUSHING MALWARE, PHISHING

The FBI is warning the public that cyber criminals use search engine advertisement services to impersonate brands and direct users to malicious sites that host ransomware and steal login credentials and other financial information.

Cybercriminals purchase advertisements that appear within internet search results using a domain similar to an actual business or service. When a user searches for that business or service, these advertisements appear at the very top of search results with the minimum distinction between an advertisement and an actual search result. Additionally, these advertisements link to a webpage identical to the impersonated business's official website.

When a user searches for a program to download, the fraudulent webpage has a link to download software that is actually malware. However, the download page looks legitimate, and the download itself is named after the program the user intended to download.

These advertisements have also been used to impersonate websites involved in finances, particularly cryptocurrency exchange platforms. These malicious sites appear to be real exchange platforms and prompt users to enter login credentials and financial information, giving criminal actors access to steal funds.

While search engine advertisements are not malicious, it is crucial to practice caution when accessing a web page through an advertised link.

The FBI recommends that individuals take the following precautions:

- Before clicking on an advertisement, check the URL to ensure the site is authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Rather than search for a business or financial institution, type the business's URL into an internet browser's address bar to access the official website directly.
- Use an ad-blocking extension when performing internet searches. Most internet browsers allow a user to add extensions, including extensions that block advertisements. These ad blockers can be turned on and off within a browser to permit advertisements on certain websites while blocking advertisements on others.

The FBI recommends that businesses take the following precautions:

- Use domain protection services to notify businesses when similar domains are registered to prevent domain spoofing.
- Educate users about spoofed websites and the importance of confirming correct destination URLs.
- Educate users about where to find legitimate downloads for the business's programs.



THIS INTERNSHIP ARMS STUDENTS WITH THE SKILLS THEY NEED TO BATTLE CYBERCRIME NOW AND, IN THE FUTURE.

By providing hands-on experience in the University's Security Operations Center, an internship program prepares students for future careers in cybersecurity and meets a real-time need to address issues that threaten information technology systems on campus.

Today, the college's Security Operations Center Internship Program gives students the opportunities they need to prepare for a future as cybersecurity professionals. The program - a joint venture between the college and the SOC, a department within the Information Security Office, which is part of University Information Technology Services - offers two internship positions and two paid student worker positions during the fall and spring semesters and the summer session.

Student worker positions are also available for students to apply for on Handshake. The internship program began in 2020 to help students develop the skills needed to move into professional roles after graduation.

"Exposing students to current security threats and giving them the hands-on experience to mitigate them is a benefit of the internship," explains Sonia Nazaroff, an information security analyst with ISO and director of the internship program for the SOC. "Giving students the training they need in college, and most notably on the job, will develop the skills they need in the real world."

The internships "Are an amazing opportunity for students to develop cybersecurity skills and experience while supporting organizations," said Paul Wagner, associate professor of practice at the College of Applied Science and Technology. Students who do well academically and complete an internship are more likely to receive job offers before graduation, Nazaroff said.

She explained that this hands-on experience helps students grow their professional resumes, experience, and connections, making them appealing candidates in the job market. "It's very important for our students to see these different incidents. It's great to apply what they've learned in CAST to their everyday tasks in the SOC," Nazaroff said. During the internship, students engage with security analysts, engineers, and other security and IT professionals and leaders on campus. Working with the students directly is essential to answering questions and providing professional development and mentoring, Nazaroff said.

"Ultimately, we want to provide a variety of opportunities for students to develop hard and soft skills so that they can become well-rounded security professionals," Nazaroff said.

"Although the program is relatively new, it demonstrates that students can easily move into new roles after graduation," Nazaroff said.



OPERATION AURORA FIRST PUBLICLY DISCLOSED BY GOOGLE

Operation Aurora was a series of cyber attacks conducted by advanced persistent threats such as the Elder wood Group based in Beijing, China, with ties to the People's Liberation Army. The attacks began in mid-2009 and continued through December 2009. According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at high-tech, security, and defense contractor companies. Technical evidence, including IP addresses, domain names, malware signatures, and other factors, show China groups behind this attack series.

JANUARY 12, 2010

DATA ENCRYPTION STANDARD (DES) PUBLISHED AS FEDERAL STANDARD (FIPS PUB 46)

The Data Encryption Standard (DES) is a symmetric-key algorithm for digital data encryption. The origins of DES date to 1972, when a National Bureau of Standards study of US government computer security identified a need for a government-wide standard for encrypting unclassified, sensitive information. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography. DES is now considered insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes. Although there are theoretical attacks, the algorithm is believed to be practically secure in Triple DES. This cipher has been superseded by the Advanced Encryption Standard (AES). DES has been withdrawn as a standard by the National Institute of Standards and Technology.

JANUARY 15, 1977

BRAIN BOOT SECTOR VIRUS IS RELEASED

Brain is the industry standard name for a computer virus released in its first form on January 19, 1986, and is the first computer virus for MS-DOS. Brain affects the IBM PC by replacing the boot sector of a floppy disk with a copy of the virus. The actual boot sector is moved to another sector and marked as bad. Infected disks usually have five kilobytes of bad sectors. The disk label is usually changed to ©Brain

JANUARY 19, 1986

Security Research Intern

Remote

The position will be Remote. During the 12-week internship, you'll be a full-time member of the Security Research team and paired with a mentor on your team. You will have the guidance, environment, and responsibility to execute small projects directly impacting our organization. You will work on real projects, features, and updates that will affect our customers worldwide!

QUALIFICATIONS:

- Pursuing a degree in Computer Science or a related field, with demonstrated cyber security talent and a passion for becoming a security expert.
- Must be currently enrolled in a full-time degree program and returning to the program after completing the internship.
 - Comfortable writing code in at least one programming language
 - Familiarity with relational databases (MySQL, Postgres, SQLServer, Oracle) and ease of working with UNIX or any Linux Platform
 - Knowledge of typical attacker TTPs
 - Understanding of threat intelligence and IOCs is a plus
- Understanding of Common Vulnerabilities and Exposures (CVE)
- Curious mind and eager to learn a variety of tools and technologies

PREFERRED QUALIFICATIONS:

- Experience with Python and SQL
- Working knowledge/experience with AWS, GCP, or Azure
- Working knowledge/experience with Containers
- Sharp analytical abilities and proven design skills
- Experience in data analysis



Information Security Intern

Remote

The Information Security team is looking for someone with a strong work ethic, a fantastic attitude, and comfortable tackling any challenge. We provide significant flexibility and autonomy to team members, have high expectations, and expect everyone to contribute meaningfully to our broader collective goals.

- Promptly respond to all security incidents and provide thorough post-event analysis.
- Participate in security tool tuning and improvement to minimize false positives and maximize detection and prevention of threats.
- Participate in growing and maturing SOC processes.
- Provide support for IT audits as needed.

QUALIFICATIONS:

- At a minimum, you should be a rising junior, senior, OR masters-level student in a degree/certificate-seeking accredited program
- Strong troubleshooting skills
- Ability to multi-task across multiple technologies and work both independently and in a team environment
- Ability to interact with a broad cross-section of personnel to explain complex security topics in technical and non-technical settings.
- Strong project management skills, including planning and execution
- Strong written and verbal communication skills, including presenting information
- Strong quantitative, analytical and problem-solving skills
- Strong interpersonal, leadership, and communication skills
- Ability to work in a dynamic, collaborative environment

wex™



Security Intern Program 2023

Remote

We do two things - secure Grafana Labs, the company behind the Grafana project, and build out our security observability platform and product. As a company, we are remote-first and global, and we embrace people of different experiences and backgrounds to build diverse teams where every person brings a new perspective to the software. Our backend tech stack consists of services written in Go, running on multiple Kubernetes clusters that leverage Google's Cloud Platform. On the front end, we use React, HTML, and JavaScript.



- 12-week internship embedded in our Security Engineering team
- Working on real-life projects
- Become an active part of a globally distributed group of interns
- Train on how to be successful in a global remote environment
- Regularly meet with a mentor to get all the support you need
- Take an active role in defining your objectives
- Actively participate in technical discussion
- Dive deep into a part of our codebase
- Embrace our open-source culture and be brave to contribute to open-source projects
- Gain a deeper understanding of our products and customers
- Present some of your learnings at the end of your internship

QUALIFICATIONS:

- Interest in working with security and software engineering
- Some experience with at least one programming language.
- Some experience with Git and Linux.

PREFERRED QUALIFICATIONS:

- Exposure to security tooling/scanners
- Experience with any Grafana products
- Some experience in security research / CTF / pen testing

Imagine a world where children are left entirely to their own guidance and education. One where the only instruction they ever receive is from peers. What kind of a world would that be?

When the Internet was born, it was called the ARPANET. Initially, its creators tried to maintain control over its growth and development, but that control became untenable as it grew. Eventually, a dark side emerged there.

The Internet can be subdivided into the Surface Web (that which you can Google) and the Deep Web. You may be surprised to hear that most of you regularly visit the Deep Web. Accounts such as Facebook, Twitter, or your company network that require sign-in credentials are not indexed by search engines and are a significant part of the Deep Web.

Estimates put the Deep Web as over 95% of the internet. The Dark Web is a subset of the Deep Web that is intentionally hidden, requiring a specific browser to access. No one knows the size of the Dark Web, but most estimates put it at around 5% of the total internet.

The Dark Web is best known for illegal and nefarious activities. You can buy drugs, guns, credit card numbers, credentials, and hacked Netflix accounts. You can buy malware or pay hackers to breach your competition for intellectual property. There are even illicit E-Commerce sites. These sites have the same features as any e-retail operation, including ratings/reviews, shopping carts, and forums. However, sellers have been known to disappear suddenly with their customers' crypto-coins without providing the requested service. The old saying, "There is no honor among thieves," applies. Imagine that.

Not all activities on the Dark Web are illegal. Around half of the Dark Web is used for legitimate activities. It allows political dissidents to communicate anonymously with journalists without fear of persecution.

People also go to the Dark Web for mundane activities like joining a chess club or exchanging recipes. Even Facebook occupies some space there. The app is called BlackBook. You might not be that surprised to hear that the New York Times has a Dark Web presence. In truth, the Dark Web attracts many who want to be anonymous.

The most common way to get on the Dark Web is through an anonymizing browser called Tor (the onion router). The Tor browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable (ostensibly). It is difficult to find your way around, and websites are not indexed by “normal” search engines like Google.

Popular Deep Web search engines include DeepPeep and IncyWincy. The experience is unpredictable, unreliable, and often incredibly slow.

You may think, “This is all very interesting, but I am not interested in a seedy journey to the Dark Web. Why should I care?” Here’s why. The Dark Web is full of Personally Identifiable Information (PII) and password credentials captured from breaches that are then bought and sold. Or sometimes just dumped to a site. Large identity theft companies, like Experian, offer services that search for your information on the Dark Web and notify you of their findings.

You can also look to your trusted security advisor to obtain a Dark Web monitoring service that tracks your company's domain information.

For your email address, you can check for yourself at www.haveibeenpwned.com. Enter your email address to see if your credentials have been breached. If so, it is time to change passwords and verify your account information (see my previous article on password hygiene).

In the novel *Lord of the Flies*, a group of boys is stranded on a deserted island. Their attempt at self-governance is a disaster. A dark side emerged. Civilization eroded, and chaos reigned. Kind of like the Internet.



Home

Notify me


Domain search

Who's been pwned

Passwords

API

About

Donate 

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?

Oh no — pwned!

Pwned in 80 data breaches and found 21 pastes ([subscribe](#) to search sensitive breaches)

Good news — no pwnage found!

No breached accounts and no pastes ([subscribe](#) to search sensitive breaches)



FACULTY CORNER



✉ Welcome to the JANUARY 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 if you have not noticed, this came out late. I have been busy preparing for classes and a workshop at CACTUSCON. The theme for 2023 is AI content. All images are AI-generated, and the debate around AI has been interesting. CACTUSCON is right around the corner, and Dr. Dalal Alharthi Paul Wagner will be there. We will be presenting an introductory workshop on exploiting IP cameras. The concepts apply to many categories, and the workshop is open to all age groups. Please stop by and say hello if you are in the area.

✉ Reflecting on 2022, the conflict between Russia and Ukraine has escalated in cyber. The targeting of Ukrainian and NATO infrastructure is an ongoing case study. Ransomware has developed its business model to become more resilient. Ransomware also developed a moral code of ethics that is evolving. Because of this, as we move into 2023, ransomware will be an exciting category to watch develop this year.

✉ So, welcome to the Spring semester and a new year. Over the next few months, I want to include even more cybersecurity news, events, and projects. The Packet will keep you updated and help you improve your skills.

✉ 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/>

