THE PACKET

FALL

DECEMBER 2021

IN THIS ISSUE

NATIONAL SECURITY AGENCY

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the DECEMBER issue of "THE PACKET" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I wish to welcome you to the last issue of the year 2021. This year was better than 2020 but not by much. We have seen an increase in ransomware events the past year and every month had what appeared to be a major security breach. The Banking industry has seen a 1,318% increase in ransomware attacks in 2021 alone. It feels like decades ago, but this year started with a major security breach under SolarWinds, and we are still discovering more about this attack. The year 2021 has been non-stop excitement if you are really into malware, you may like the idea of taking CYBV 454 to learn more about reverse engineering nasty malware samples. I hope to include some of these in my future examples as I am in the process of updating everything in the course. Every attack vector is on the table to include package managers. The package manager PyPi is used by many organizations for package management, however, it hosted 11 malicious packages that have been downloaded over 41 thousand times. Now, there is also a global shortage of workers, and this is going to stress an already stressed system that needs to have protections that need to adapt over time.

--- END MESSAGE ---

>. SYS_ALERT

>. CYBER_SAGUAROS_UPDATE

- NATIONAL CYBER LEAGUE (NCL): I WOULD LIKE TO CONGRATULATE THE CYBER SAGUAROS APT 100 TEAM ON FOURTH PLACE IN THE NATIONAL CYBER LEAGUE COMPETITION.
- NEXT EVENT CTF:
  - SANS HOLIDAY HACK CTF
    - THIS WILL BE OPEN TO EVERYONE. THE BENEFIT OF THIS CTF WILL BE THAT IT WILL HAPPEN WHILE WE ARE ON BREAK, SO IT SHOULD NOT INTERFERE WITH ANY HOMEWORK OR CLASSES! GOOD LUCK!!!
  - WRCCDC (WESTERN REGIONAL COLLEGIATE CYBER DEFENSE COMPETITION)
    - WRCCDC INVITATIONAL #2 WILL TAKE PLACE ON DECEMBER 11TH. INVITATIONAL #1 TOOK PLACE ON NOVEMBER 20.
  - KRINGLECON 2021
    - KRINGLECON 2021 FEATURES A SERIES OF FASCINATING TALKS FROM CYBERSECURITY INDUSTRY EXPERTS DISCUSSING THE LATEST INFORMATION SECURITY TOPICS. SOME OF THOSE TALKS WILL EVEN HELP YOU BUILD SKILLS TO SOLVE THIS YEAR'S HOLIDAY HACK CHALLENGES! AND SANTA'S TEAM HAS EVEN CONJURED UP A SOUNDTRACK FEATURING SOME GREAT CUSTOM HOLIDAY HACKING MUSIC FOR YOU TO ENJOY WHILE YOU PLAY AND ATTEND THE CON.

Cyber Saguaros

CYBER_SAGUAROS

SYS_ALERT.<

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

ROBINHOOD HACKERS ACCESSED INTERNAL TOOL FOR REMOVING ACCOUNT SECURITY FEATURES

The hackers behind the recent breach of customer data from app-based broker Robinhood had access to an internal tool that presented them the option of tampering with user accounts, including removing specific users' multi-factor authentication protections, according to screenshots of the tool obtained by Motherboard. The screenshots of the tool also show buttons for logging a user out of their account, adding a trusted device, and blocking certain sessions from accessing the Robinhood account. The screenshots show that as well as offering the ability to make changes to users' accounts, the tool provides notes on specific accounts generated by Robinhood's fraud team; the devices used to log into Robinhood; the user's IP addresses; whether the devices are trusted; their balances such as net cash as well as their buying power; and their phone number and whether that number is verified. Another of the screenshots shows an internal message written by a Robinhood employee discussing changes to account security practices. On Wednesday, a Robinhood spokesperson said that "As we disclosed on November 8, about 10 customers had more extensive account details and information exposed," when asked about the hackers' access to the internal tool. Robinhood told Motherboard at the time that it is required by SEC rules to keep account information for six years after an account is closed.

REVIL RANSOMWARE GROUP SERVERS HIT BY HACKING TECHNIQUE IT USES TO COMPROMISE TARGETS

REvil, the ransomware group that hacked into the U.S. Colonial Pipeline this past May, was itself hacked and shut down by a multinational cyber operation, according to an exclusive report from Reuters. The ransomware group REvil has been shut down by the government using the same technique that it uses to hack into the servers of private companies. Officials from the Federal Bureau of Investigation along with the U.S. Cyber Command, worked with several different countries to bring down REvil as well as several other cybercrime groups. The shutdown by the government used a loophole in the ransomware's backup system, allowing law enforcement agencies to access REvil's servers and shut them down. Reuters has described REvil as "One of the worst of dozens of ransomware gangs that work with hackers to penetrate and paralyze companies around the world." The hacking of the Colonial Pipeline by REvil and another ransomware group, DarkSide, led to massive gasoline shortages and caused President Joe Biden to declare a state of emergency. The White House National Security Council told Reuters that they were "Undertaking a whole of government ransomware effort, including disruption of ransomware infrastructure and actors," but declined to comment specifically on the REvil operation.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

NEW MALWARE (BOTENAGO) TARGETING MILLIONS OF IOT DEVICES WITH MORE THAN 30 EXPLOITS

AT&T Alien Labs™ has found new malware written in the open-source programming language Golang. Some AVs detect these new malware variants using Go as Mirai malware - the payload links do look similar. There is a difference between the Mirai malware and the new malware variants using Go, including differences in the language in which it is written and the malware architectures. The new malware strains Alien Labs has discovered do not have the same attack functions as Mirai malware, and the new strains only look for vulnerable systems to spread their payload. In addition, Mirai uses an "XOR table" to hold its strings and other data, as well as to decrypt them when needed - this is not the case for the new malware using Go. For this reason, Alien Labs believes this threat is new, and we have named it BotenaGo. The new BotenaGo malware exploits more than 30 vulnerabilities. Depending on the infected system, the malware uses different links, each with a different payload. At the time of analysis, all the payloads had been removed from the hosted servers by the attacker(s), and so Alien Labs could not analyze any of them. Malware authors continue to create new techniques for writing malware and upgrading its capabilities.

WATER SUPPLIER TARGETED BY MONTHS-LONG UNDETECTED CYBER BREACH

Queensland's largest regional water supplier, Sunwater, says it was targeted by hackers in a cyber security breach that went undetected for nine months. Sunwater admitted the cyber breach after the tabling of a Queensland's Audit Office report into the state's water authorities, which mentioned the incident but did not say which authority was targeted. Following questions from the ABC reporter, Sunwater confirmed it was the authority affected by the breach revealed in the Audit Office's report. The Water 2021 report stated the cyber breach had occurred between August 2020 and May 2021 and involved unauthorized access to the entity's web server that stored customer information. The report found "threat actors" had targeted an older, more vulnerable version of the system. The web server contained suspicious files that increased visitor traffic to an online video platform, the report said. The 36-page report called for immediate action to fix "ongoing security weaknesses in information systems". It noted in the case of the cyber breach, measures had been taken to fix the issue including updating software, using stronger passwords, and monitoring incoming and outgoing network traffic. Under the heading "Further Action Needs To Be Taken", the report said cyber attacks were a risk with ongoing changes in entities' working environments due to COVID-19.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

ZERO-DAY BUG IN ALL WINDOWS VERSIONS GETS FREE UNOFFICIAL PATCH

A free and unofficial patch is now available for a zero-day local privilege escalation vulnerability in the Windows User Profile Service that lets attackers gain SYSTEM privileges under certain conditions. The bug, tracked as CVE-2021-34484, was incompletely patched by Microsoft during the August Patch Tuesday. The company only addressed the impact of the proof-of-concept (PoC) provided by security researcher Abdelhamid Naceri who reported the issue. Naceri later discovered that threat actors could still bypass the Microsoft patch to elevate privileges to gain SYSTEM privileges if certain conditions are met, getting an elevated command prompt while the User Account Control (UAC) prompt is displayed. Luckily, the exploit requires attackers to know and log in with other users' credentials for exploiting the vulnerability, which means that it will likely not be as widely abused as other LPE bugs (including PrintNightmare). The bad news is that it impacts all Windows versions, including Windows 10, Windows 11, and Windows Server 2022, even if fully patched. Additionally, threat actors will only need another domain account to deploy the exploits in attacks, so it's something admins should be concerned about.

HOW TO BREAK THE CLOUD WITH TWO LINES OF CODE - CHAOSDB

In August 2021 the Wiz Research Team disclosed ChaosDB – a severe vulnerability in the popular Azure Cosmos DB database solution that allowed for complete, unrestricted access to the accounts and databases of several thousand Microsoft Azure customers, including many Fortune 500 companies. However, what the Wiz Research Team did not disclose in August was the full extent of the ChaosDB vulnerability. Not only did it effectively allow an unprivileged attacker to obtain complete and unrestricted access to the databases of several thousand Microsoft Azure customers, but by exploiting each misconfiguration in this service, and chaining them together, the Wiz Research Team obtained an excessive amount of Microsoft's internal Cosmos DB-related secrets and credentials. Using these secrets, the Wiz Research Team was able to authenticate, as admin, to over 100 Cosmos DB-related management panels (in the form of Service Fabric instances, which is the container orchestration solution being used behind the scenes to power the service). One of the things that the Wiz Research Team was able to do as admin in this interface was to obtain information regarding every Cosmos DB Account that is hosted in the regional cluster, including its authentication tokens! What this means is that with only two lines of code the Wiz Research Team was able to do what was previously thought to be impossible: escape the abstraction layers of the cloud to access the underlying internal Azure infrastructure. This was more than an account takeover vulnerability; in the wrong hands, it could have been a service takeover vulnerability.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

UKRAINE LINKS MEMBERS OF GAMAREDON HACKER GROUP TO RUSSIAN FSB

The Security Service of Ukraine or SBU is Ukraine's law-enforcement authority and main government security agency in the areas of counterintelligence activity and combating terrorism. SSU and the Ukrainian secret service say they have identified five members of the Gamaredon hacking group, a Russian state-sponsored operation known for targeting Ukraine since 2014.

This Gamaredon hacking group, tracked as Armageddon by the SSU, is allegedly operated under The Federal Security Service (FSB) of the Russian Federation which is the principal security agency of Russia and the main successor agency to the Soviet Union's KGB. The FSB is believed to be responsible for over 5,000 cyber-attacks in Ukraine since the operation began.

Over the last seven years, Ukraine says the actors targeted over 1,500 government, public and private entities in the country, aiming to collect intelligence, disrupt operations, and take control over critical infrastructure facilities.

The names of the five individuals the SSU claims are part of the Gamaredon operation are Sklianko Oleksandr Mykolaiovych, Chernykh Mykola Serhiovych, Starchenko Anton Oleksandrovych, Miroshnychenko Oleksandr Valeriovych, and Sushchenko Oleh Oleksandrovych.

All five were reportedly operating under the guidance of the 18th Center of Information Security of the FSB in Moscow. According to SSU, Pteranodon was derived from "Pterodo," a widely available malware circulating Russian hacking forums since 2016. The group continued to create new powerful DLL modules for Pteranodon, so it has evolved significantly over the past five years.

PHISHING ATTACKS ARE HARDER TO SPOT ON YOUR SMARTPHONE. THAT'S WHY HACKERS ARE USING THEM MORE

There's been a surge in mobile phishing attacks targeting the energy sector as cyber attackers attempt to break into networks used to provide services including electricity and gas. The desire to break into these networks has resulted in a sharp rise in phishing attacks against the energy sector, specifically cyberattacks targeting mobile devices, warns a report by cybersecurity researchers at Lookout. According to the paper, there's been a 161% increase in mobile phishing attacks targeting the energy sector since the second half of last year. Attacks targeting energy organizations account for 17% of all mobile attacks globally, making it the most targeted sector, ahead of finance, government, pharmaceuticals, and manufacturing. Tailoring phishing emails towards mobile devices can make them more difficult to spot because the smaller screen provides fewer opportunities to double-check that links in messages are legitimate, while smartphones and tablets might not be secured as comprehensively as laptops and desktop PCs, providing attackers with a useful means of attempting to compromise networks. "By launching phishing attacks that mimic the context that the recipient expects, attackers can direct a user to a fake webpage that mimics a familiar application login page. Without thinking, the user provides credentials and data has been stolen," he added. "The majority of attacks start with phishing, and mobile presents a multitude of attack pathways. An anti-phishing solution must block any communication from known phishing sites on mobile devices, including SMS, apps, social platforms, and email".

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

U.S. OFFERS $10 MILLION REWARD IN HUNT FOR DARKSIDE CYBERCRIME GROUP

The U.S. State Department on Thursday announced a reward of up to $10 million for information leading to the identification or location of anyone with a key leadership position in DarkSide, a cybercrime organization the Federal Bureau of Investigation has said is based in Russia. The Federal Bureau of Investigation (FBI) is the domestic intelligence and security service of the United States and its principal federal law enforcement agency. The FBI has said DarkSide was responsible for the May cyber-attack targeting the Colonial Pipeline, causing a days-long shutdown that led to a spike in gas prices, panic buying, and localized fuel shortages in the U.S. Southeast. The State Department also said it is offering a reward of up to $5 million for information leading to the arrest or conviction in any country of any person attempting to participate in a DarkSide ransomware incident. "In offering this reward, the United States demonstrates its commitment to protecting ransomware victims around the world from exploitation by cybercriminals," the department said in a statement. Colonial Pipeline has said it paid the hackers nearly $5 million in Bitcoin to regain access to its systems. The U.S. Justice Department in June recovered about $2.3 million of the ransom. The State Department in July offered a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participated in malicious cyber activities against U.S. critical infrastructure.

COULD CYBER DIPLOMACY BE THE ULTIMATE ANSWER TO AMERICAN RANSOMWARE WOES

As the 117th Congress barrels toward the conclusion of its first session, American cyberspace is increasingly imperiled by two distinct but interconnected threats: the increasing frequency of ransomware attacks and other cyber events that threaten resources critical to everyday American life, and the glacial pace of the Senate's consideration of the Cyber Diplomacy Act of 2021. While international law may dictate a duty to address cyber criminality within Russian borders, there is little benefit for Moscow to do so, and few drawbacks for Russia to allow such activity to continue. The Cyber Diplomacy Act of 2021 is the third iteration of a cyber diplomacy bill since 2017, and the third attempt to create a permanent cyber diplomacy office through congressional mandate, as recommended by the Cyberspace Solarium Commission. While an imperfect proposal, the Cyber Diplomacy Act, passed with bipartisan support, would communicate American resolve in establishing and enforcing "Rules of the road" in cyberspace, one of President Biden's top priorities. If past is prologue, without the roots planted by the Cyber Diplomacy Act, this bureau could easily succumb to the winds of political expediency. Is cyber diplomacy the ultimate answer to American ransomware woes? Unlikely. It's an important step in building a foundation for layered deterrence in cyberspace, and imposing concrete costs for cyber perpetrators and the nations who enable them, thus better protecting American private industry and infrastructure, and turning a Putinesque smile into a frown.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

VIEWING WEBSITE HTML CODE IS NOT ILLEGAL OR "HACKING," PROF. TELLS MISSOURI GOV

As we reported on October 14, Missouri Gov. Mike Parson threatened to prosecute and seek civil damages from a St. Louis Post-Dispatch journalist who identified a security flaw that exposed the Social Security numbers of teachers and other school employees. This is all happening even though the state government made teachers' Social Security numbers available in an unencrypted form in the HTML source code of a publicly accessible website. "No statute in Missouri or on the federal level prohibits members of the general public from viewing publicly available websites or viewing the website's unencrypted source code. No reasonable person would think they were unauthorized to view a publicly available website, its unencrypted source code, or any of the unencrypted translations of that source code. There is no probable cause to investigate Professor Khan, and instigation or continuation of any proceeding against him would therefore be prohibited." The letter notes that Post-Dispatch reporter Josh Renaud asked Khan to verify the security flaw in a Missouri government website that allowed the public to search teacher certifications and credentials. Due to a major security flaw present in its design, the website was programmed to send the full Social Security number of Missouri teachers to every visitor to the website, whether the visitor was aware or not. None of the data was encrypted, no passwords were required, and no steps were taken by the State of Missouri to protect the Social Security numbers of its teachers that the State automatically sent to every website visitor. "The State of Missouri automatically transmitted teacher Social Security numbers to every website visitor. No one who discovered and reported this security flaw attempted to gain unauthorized access to or 'hack' the website."

MANITOBA CANADA PROVINCE SUED OVER PRIVACY BREACH INVOLVING 9,000 CHILDREN

A class-action lawsuit will proceed against the province after confidential information about nearly 9,000 children with disabilities was mistakenly sent to agencies that provide services to them and community advocates. "The breach demonstrated that the defendant had inadequate policies for the protection of sensitive information and was blatantly careless in protecting such information," the lawsuit alleges. Data included in the misdirected email was requested by the children's advocate for a review into the delivery of children's disability services in the province. Manitoba Families, at the time, attributed the blunder to "Human error." In a statement of defense filed in June, the province said the children's advocate was "Entitled to compel the disclosure of the information" contained in the email, and Children's Disability Services was authorized under the Personal Health Information Act to disclose the requested information. Many of the recipients of the email were under contract with the province to provide services to children with disabilities and "Were accustomed to managing personal information which was similar in nature," says the statement of defense. "Child Disability Services never explained to the class why the child-specific information of 9,000 children had to be delivered to any organization in spreadsheet format without any anonymization or encryption," the lawsuit alleges. "The defendant's actions and inactions related to the privacy breach caused humiliation, and extreme distress and anguish about the potential future uses of class members' most sensitive information," the lawsuit alleges.

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

SPRING SCHEDULE 2022

FALL

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	BOOK
CYBV 303	WINDOWS SECURITY ESSENTIALS	BOOK
CYBV 310	INTRODUCTION TO SECURITY PROGRAMMING I	PENDING BOOK SELECTION
CYBV 311	INTRODUCTION TO SECURITY PROGRAMMING II	PENDING BOOK SELECTION
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 351	SIGNALS INTELLIGENCE AND ELECTRONIC WARFARE	PENDING BOOK SELECTION
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
CYBV 381	FROM INCIDENT TO DIGITAL FORENSICS	PENDING BOOK SELECTION
CYBV 382	NETWORK FORENSICS	PENDING BOOK SELECTION
CYBV 385	INTRODUCTION TO CYBER OPERATIONS	BOOK
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	BOOK 1, BOOK 2
CYBV 400	ACTIVE CYBER DEFENSE	BOOK 1, BOOK 2
CYBV 435	CYBER THREAT INTELLIGENCE	BOOK 1, BOOK 2

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

SPRING SCHEDULE 2022

FALL

CAT #	COURSE	BOOKS
CYBV 436	COUNTER CYBER THREAT INTEL	BOOK 1, BOOK 2
CYBV 437	DECEPTION & COUNTER-DECEPTION	BOOK
CYBV 440	DIGITAL ESPIONAGE	PENDING BOOK SELECTION
CYBV 441	CYBER WAR, TERROR AND CRIME	PENDING BOOK SELECTION
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	BOOK
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	BOOK
CYBV 473	VIOLENT PYTHON	BOOK 1, BOOK 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	BOOK 1, BOOK 2
CYBV 475	CYBER DECEPTION DETECTION	PENDING BOOK SELECTION
CYBV 479	WIRELESS NETWORKING AND SECURITY	BOOK 1, BOOK 2
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION
CYBV 498	SENIOR CAPSTONE IN CYBER OPERATIONS	BOOK
CYBV 499	INDEPENDENT STUDY	PENDING BOOK SELECTION

CHRISTMAS MOVIES – OR ITS TIME FOR HACKER MOVIES

The holidays are coming and now it is time to cuddle up and watch a few movies to escape the snow and enjoy more time with family. Trying to discover what to watch is today's goal, so load up your Netflix account and get to watching!

SNEAKERS

This would be my very first technically accurate movie when I was younger, it had the feeling that the creators put more time into making this world believable, even if it does have some fantasy elements. Sneakers came out in 1992 and does not have the respect that it deserves. This is a great movie, and I am going to place it at my #1 because I think more people need to see it. The world of penetration testing is a big part of this movie and I love that.

HBO max hulu

THE MATRIX

So, the first Matrix movie was a game-changer, the story was great, the action was some of the best and it made you want to watch the sequels. I don't remember any movie where I was excited to watch part 2. I don't think any of the sequels matched the excitement from the first movie, but this movie defined my world of entertainment. Also, in a later movie, they feature Nmap which was fun to see.

hulu

CHRISTMAS MOVIES – OR ITS TIME FOR HACKER MOVIES

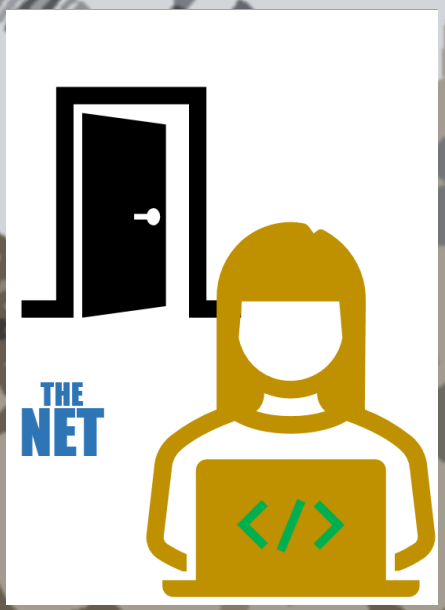
The holidays are coming and now it is time to cuddle up and watch a few movies to escape the snow and enjoy more time with family. Trying to discover what to watch is today's goal, so load up your Netflix account and get to watching!

HACKERS

So, this movie is not something I would call technically accurate, or even a little bit accurate but what this movie is can be defined as just simply entertaining. It is way over the top and this movie is at some points hard to watch. I guess the beginning court scene is accurate enough but everything else is hard to justify. With all of that, I find this movie to be entertaining, something to watch with friends and make fun of it while you go along. Maybe something like a hate-watch party and then quote every scene later on. This is the movie for friends for sure.

THE NET

This was my very first Bullock moviue and overall, I think she played the role very well. There is nothing technically accurate here outside of predicting the rise of food delivery, work-from-home situations, and how an introvert could make a good living as a computer security researcher but everything else is just simply fantastic. This movie got a few things right in its predictions of the internet, but it also got so much wrong, but that is one of the reasons I keep coming back to this movie. The drama and action in this movie save it and I love this movie so much. This is another movie to watch with friends.



BEFORE YOU KNOW WHERE YOU GO, YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

TROY HUNT LAUNCHES HAVE I BEEN PWNED? (HIBP)

HAVE I BEEN PWNED, is by far one of the most influential advances in cyber security because it made user education easy and straight forward. All you do is go to the HAVE I BEEN PWNED website, enter your email and then it will inform a user if a breach has been detected. User education is one of the hardest to push and this site made it easy and pushed cybersecurity forward.

DECEMBER 4, 2013

THE BIRTH OF RANSOMEWARE AND OTHER MISGUIDED ADVENTURES

Joseph Lewis Popp allegedly mailed floppy disks to the UK which were labeled "AIDS Information Introductory Diskette" but contained the AIDS trojan which demanded $189 to "renew the license" by sending payment to a post office box in Panama.

DECEMBER 11, 1989

TRAKE DOWN VS. GHOST IN THE WIRES – FUN HACKER LORE

Kevin Mitnick allegedly performed a remote attack against Tsutomu Shimomura's personal computer, gaining access by using source address spoofing and TCP sequence prediction. But there's no proof he did it and it's generally accepted he lacked the required technical skills. Tsutomu Shimomura is a Japanese-born American physicist and computer security expert. He is known for helping the FBI track and arrest hacker Kevin Mitnick. Takedown, his 1996 book on the subject with journalist John Markoff, was later adapted for the screen in Take Down in 2000. So, in December 1994, when someone broke into Tsutomu Shimomura's elaborate computer system in his San Diego home using a never-before-seen, sophisticated hacking method and then stole some fancy cellular phone tools, Shimomura took it as a personal challenge. When the trail led to Mitnick, Shimomura became a cybersleuth, on a mission to catch Kevin

DECEMBER 25, 1994

RELEASE OF BACKUPHDDVD AND THE END OF

BackupHDDVD and its source code were published to the website Doom9. The utility could be used to decrypt AACS protected content. BackupHDDVD is a tool to decrypt a AACS protected movie that you own, so you can play it back later using an HDDVD player software.

DECEMBER 26, 2006

DOD CYBER SCHOLARSHIP PROGRAM (DOD CYSP)

The Department of Defense (DoD) Cyber Scholarship Program (CySP) is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA).

The objectives of the program:

- Promote higher education in all disciplines of cybersecurity
- Enhance the Department's ability to recruit and retain cyber and IT specialists,
- Increase the number of military and civilian personnel in the DoD with this expertise, and ultimately
- Enhance the nation's cyber posture.

- The DoD is working with universities like the University of Arizona and other defined National Centers of Academic Excellence (CAE). Interested students need to apply directly with the University of Arizona at CYSP@EMAIL.ARIZONA.EDU

- Minimum cumulative GPA of 3.2 (undergraduate)
- Must be entering junior or senior year.
- Must be a U.S. Citizen.
- Must agree to work for the DoD as a civilian for one year for each year of scholarship received.

- **LINK TO APPLY**

THE DEADLINE IS TUESDAY, FEBRUARY 1, 2022 AT 11:59 P.M. EASTERN TIME. YOU MUST HAVE YOUR APPLICATION AND ALL MATERIALS SUBMITTED BY THAT DATE AND TIME.

CAE IN CYBERSECURITY COMMUNITY

The NSA CAE–CO designation provides UA graduates access to the CAE Community and all of its resources.

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

INTERN, INFORMATION SECURITY - SUMMER 2022

freedom

Freedom Financial Network is looking for a talented Information Security Intern for the summer of 2022. You'll work with other members of the Information Security team to influence business performance and make an impact through meaningful project work. You will develop professionally and enhance your skills at workshops and business overviews. You will foster connection by growing your network as you meet and learn from the broader team. You'll have an opportunity to interact with every facet of our business.

- Gain an understanding of and contribute to the design and implementation of IAM functions, including User and system account provisioning Role-Based Access Control.
- Learn to Protect against unauthorized access, modification, or destruction of data
- Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization.
- Gain understanding of Planning, implementing and Monitoring of various security tooling in a layered defense architecture
- Update and Maintain Security documentation - Policies, Processes and Procedures
- Work closely with compliance team members to aid in regulatory tracking and compliance.
- Participate in end user Security Awareness Train end users and promote security awareness to ensure system security and to improve server and network efficiency.
- Learn Data Security protection strategies such as Data Loss Prevention - help develop plans to safeguard sensitive information in motion and at rest for both digital and non-digital against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.

CYBER SECURITY INTERN - SUMMER 2022

icims

The Cyber Security Intern will support our Information Security team and assist with diverse security-related tasks and issues for our rapidly growing company. This is a great opportunity for a passionate student and security enthusiast to work with our Security Operations team to address security concerns across the iCIMS environment!

- Work closely with our Security Analysts to monitor, detect, and investigate security events across the organization.
- Interpret and respond to alerts from various security technologies (SIEM, IDS/IPS, anti-virus, DLP, etc.).
- Optimize and tune security monitoring and detection tools to improve the fidelity of events.
- Assist in penetration testing and the vulnerability management program to identify, evaluate, and report on security vulnerabilities in systems and applications.

THANK YOU

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/

NATIONAL SECURITY AGENCY

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY