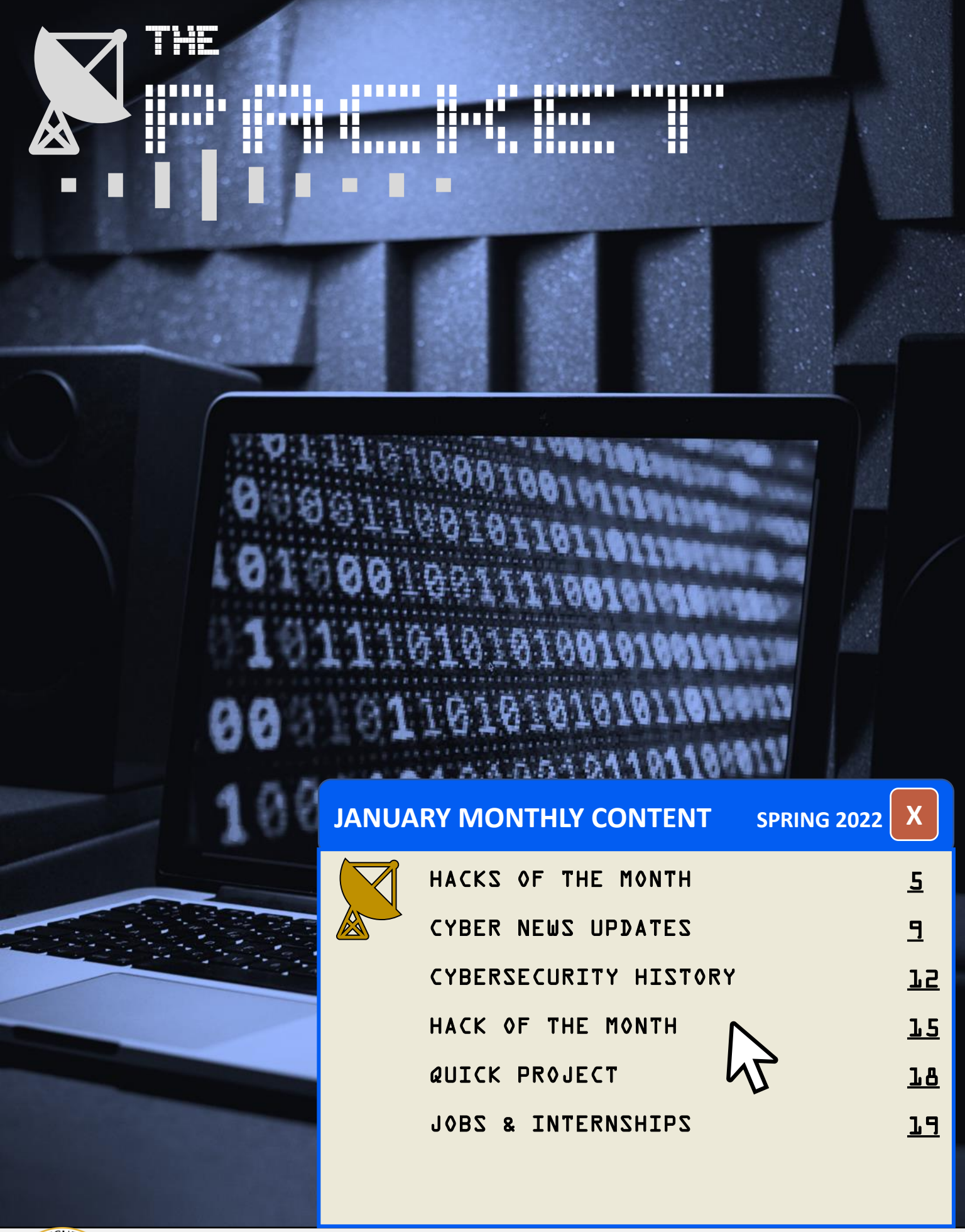
THE PACKET



JANUARY MONTHLY CONTENT

SPRING 2022

X

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

>. HELLO_WORLD_☺

≥ ----- ESTABLISHING CONNECTION -----

≥ Welcome to the JANUARY 2022 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 year 2022. Once again, the January issue is where I introduce a format change, and I welcome any comments of how you enjoy and like this new look and what changes you did not like. I hope to focus more on giving you, the student, even more information than before compared to last year's style.

≥ Last month in December, we witnessed the abuse in CVE-2021-44228 which advantage of Apache Log4j. Apache Log4j is a Java-based logging utility, and you will find this in multiple logging products. One industry where you will find this most commonly is within Managed Service Providers or MSPs. The fix is quite simple. You upgrade to the next update; however, Apache Log4j is part of many products. Therefore, it is likely to go unnoticed unless the original vendor puts out an update to fix these issues.

≥ If you would like to contribute an article, feel free to reach out and get your work published within this publication. Reach out to discover the publication criteria and what the next months topic would be. The year 2021 was almost always malware related so if you are in CYBV 454 - Malware Threats & Analysis then I want to talk to you.

>. CYBER_SAGUAROS_UPDATE

- **NATIONAL CYBER LEAGUE (NCL):** I WOULD LIKE TO ONCE AGAIN CONGRATULATE THE CYBER SAGUAROS - APT 100 TEAM ON FOURTH PLACE IN THE NATIONAL CYBER LEAGUE COMPETITION.
- **NEXT EVENT CAPTURE THE FLAG CTF:**
  - CYBER SAGUAROS JUICE SHOP
    - FOR THE MONTH OF JANUARY, CYBER SAGUAROS WILL HAVE A COPY OF THE OWASP JUICE SHOP UP AND RUNNING. IF YOU HAVE NEVER SEEN THIS, BEFORE TAKE A LOOK AND GET TO HACKING. IF YOU GET STUCK THERE ARE MULTIPLE TUTORIALS AVALIABLE TO GUIDE YOU INTO ABUSING THE SITE.
  - CACTUSCON 10 (2022)
    - CACTUSCON IS EXPECTED TO PUT ON A CTF HOWEVER DETAILS ARE UNKNOWN AT THIS TIME. CYBER SAGUAROS WILL ALSO ATTEND IN-PERSON AND VIRTURALLY.
  - KRINGLECON (2021)
    - KRINGLECON 2021 FEATURED A SERIES OF FASCINATING TALKS FROM CYBERSECURITY INDUSTRY EXPERTS DISCUSSING THE LATEST INFORMATION SECURITY TOPICS. KRINGLECON 4 ALSO TOOK PLACE AND AT THE TIME OF THIS WRITING I HAVE NO IDEA HOW IT WENT. I WOULD NOT BE ABLE TO LOOK AT THIS TILL THE START OF JANUARY SO I HOPE THEY DID WELL AND I WILL UPDATE YOU IN FEBRUARY.

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.

>. HACKS_OF_THE_MONTH

RANSOMWARE ATTACK SHUTS DOWN LEWIS & CLARK COMMUNITY COLLEGE

- ARTICLE LINK
- DR. KEN TRZASKA MESSAGE
- NEWS REPORT LCCC
- BUTLER COMMUNITY COLLEGE ALSO HIT
- NEWS REPORT BCC

Lewis and Clark Community College in Godfrey closed all their campuses this week and canceled all extra-curricular activities. The director of information technology noticed suspicious activity and shut down the school's computer network. According to Ken Trzaska, hackers got into the network but never gained control. Trzaska said the college eventually received an email requesting money, but he wouldn't say how much. "That's pretty crazy for a cyber-attack to be able to shut down everything on this campus. There are no sports, no nothing this whole week," said Trey Hemminghaus, a student. According to Trzaska, the college notified police and the FBI about the ransomware attack. Trzaska said he expects the college's computer network to be back online and students back on campus by Monday.

IKEA HIT BY ONGOING EMAIL CYBERATTACK CAMPAIGN

- ARTICLE LINK
- IKEA WARNING TO EMPLOYES
- PROXYSHELL VULNERABILITY

Furniture giant IKEA confirmed that it was hit by a wave of email reply-chain cyberattacks that targeted the company's internal mailboxes, as well as those of IKEA's suppliers and business partners, Bleeping Computer reports. Attackers carry out reply-chain attacks by gaining access to genuine corporate emails via hacked employee email accounts or breached internal servers and then replying to them with malicious attachments or links. Internal IKEA emails seen by Bleeping Computer confirm that it was aware of the ongoing reply-chain campaign and warned its employees about the cyberattack. "There is an ongoing cyberattack that is targeting Inter Ikea mailboxes," IKEA said in the email sent to staff. "Other IKEA organizations, suppliers, and business partners are compromised by the same attack and are further spreading malicious emails to persons in Inter IKEA. This means that the attack can come via email from someone you work with, from any external organization, and a reply to an ongoing conversation. It is therefore difficult to detect, for which we ask you to be extra cautious." According to Bleeping Computer, the reply-chain campaign carried out against IKEA shares certain similarities with the infamous Microsoft Exchange server attack. "While IKEA has not responded to our emails about the attack and has not disclosed to employees whether internal servers were compromised, it appears that they are suffering from a similar attack," states the Bleeping Computer report.

>. HACKS_OF_THE_MONTH

SABBATH - ELUSIVE NEW RANSOMWARE DETECTED

In September 2021, Mandiant discovered a post on exploit.in seeking partners for a new ransomware affiliate program. By October 21, 2021, the **54BB47h** (**Sabbath**) ransomware shaming site and blog were created and quickly became the talk of security researchers. In contrast with most other affiliate programs, Mandiant observed two occasions where the ransomware operator provided its affiliates with pre-configured Cobalt Strike BEACON backdoor payloads. While the use of BEACON is common practice in ransomware intrusions, the use of a ransom affiliate program operator provided BEACON is unusual and offers both a challenge for attribution efforts while also offering additional avenues for detection. **UNC2190**, operating as **Arcane** and **Sabbath**, has targeted critical infrastructure including education, health, and natural resources in the United States and Canada since June 2021. The targeting of critical infrastructure by ransomware groups has become increasingly concerning as evidenced by governments moving to target ransomware actors as national security level threats with particular attention to groups that target and disrupt critical infrastructure.

Sabbath first came to light in October 2021 when the group publicly shamed and extorted a US school district on Reddit and from a now suspended Twitter account, **@54BB47h**. During this recent extortion, the threat actor demanded a multi-million-dollar payment after deploying ransomware. Media reporting indicated that the group took the unusually aggressive step of emailing staff, parents and even students directly to further apply public pressure on the school district.

- **ARTICLE LINK**
- **FIRST APPEARANCE**
- **AFFILIATE PROGRAM BREAKDOWN**
- **NEWS VIDEO – PARENTS THREATS**

LINUX REMOTE ACCESS TROJAN HIDES BEHIND THE INVALID DATE, FEBRUARY 31

Security researchers have discovered a new remote access trojan (RAT) for Linux that keeps an almost invisible profile by hiding in tasks scheduled for execution on a non-existent day, February 31st. Dubbed **CronRAT**, the malware is currently targeting web stores and enables attackers to steal credit card data by deploying online payment skimmers on Linux servers. Characterized by both ingenuity and sophistication, as far as malware for online stores is concerned, **CronRAT** is undetected by many antivirus engines.

- **ARTICLE LINK**
- **SOURCE CODE**
- **MALWARE RESEARCH**

SOLARWINDS HACKERS HAVE A WHOLE BAG OF NEW TRICKS FOR MASS COMPROMISE ATTACKS

Almost exactly a year ago, security researchers uncovered one of the worst data breaches in modern history, if not ever: a Kremlin-backed hacking campaign that compromised the servers of network management provider SolarWinds and, from there, the networks of 100 of its highest-profile customers, including nine US federal agencies. Rather than breaking into each target one by one, the group hacked into the web of SolarWinds. It used the access and the trust customers had in the company to push a malicious update to roughly 18,000 of its customers. Almost instantly, the hackers could intrude into the networks of all of those entities. Since last year, company researchers say the two hacking groups linked to the SolarWinds hack-one called **UNC3004** and the other **UNC2652** have continued to devise new ways to compromise large numbers of targets efficiently. Now, instead of poisoning the supply chain of SolarWinds, the groups have compromised the networks of cloud solution providers and managed service providers, or CSPs and MSPs, which many large companies rely on for a wide range of IT services. The groups then found clever ways to use those compromised providers to intrude upon their customers.

- Use of credentials stolen by Cryptbot, an information stealer that harvests system and web browser credentials and cryptocurrency wallets.
- Once the hacker groups were inside a network, they compromised enterprise spam filters or other software with “application impersonation privileges,”
- Abuse of legitimate residential proxy services or geo-located cloud providers such as Azure to connect to end targets.
- Clever ways to bypass security restrictions, such as extracting virtual machines to determine internal routing configurations of the networks they wanted to hack.
- Gaining access to an active directory stored in a target’s Azure account and using this all-powerful administration tool to steal cryptographic keys that would generate tokens that could bypass two-factor authentication protections.
- Use of a custom downloader dubbed Ceeloader.

- **ARTICLE LINK**
- **CRYPTOBOT DETAILS**
- **NEW GROUP RESEARCH**
- **SOLARWINDS RESEARCH**
- **MITIGATION RECOMMENDATIONS**

CUBA RANSOMWARE BREACHED 49 US CRITICAL INFRASTRUCTURE ORGS

Today I learned there is a Cuban group named as the **Cuba Ransomware** group and yes that is their real name. The Federal Bureau of Investigation has revealed that the **Cuba ransomware** gang has compromised the networks of at least 49 organizations from US critical infrastructure sectors, including but not limited to the financial, government, healthcare, manufacturing, and information technology sectors. The FBI also added that this ransomware group had made over $40 million since it started targeting US companies. "**Cuba ransomware** actors have demanded at least US $74 million and received at least US $43.9 million in ransom payments," the FBI added.

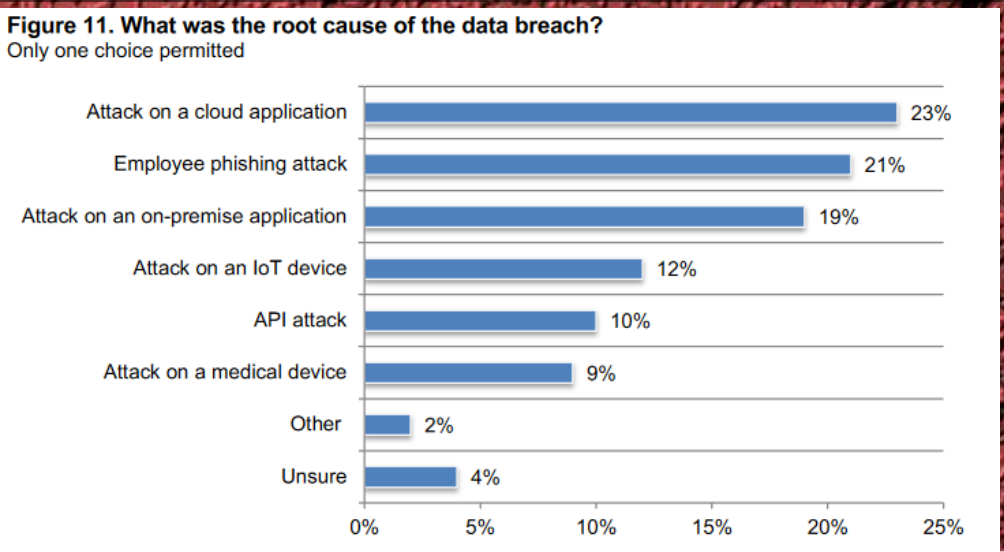
- **Cuba ransomware** is delivered on victims' networks through the Hancitor malware downloader, which allows the ransomware gang to gain easier access to previously compromised corporate networks
  - Hancitor (Chancitor) is known for delivering information stealers, Remote Access Trojans (RATs), and other types of ransomware
- Once in, using the key provided by Hancitor, **Cuba ransomware** operators will use legitimate Windows services to deploy their ransomware payloads remotely and encrypt files using the ".cuba" extension.

- **ARTICLE LINK**
- **HANCITOR MALWARE**
- **FBI ALERT**
- **CUBA RANSOMEWARE**

HOSPITAL RANSOMWARE ATTACKS GO BEYOND HEALTH CARE DATA

In a 2021 survey conducted of 597 health delivery organizations, 42% had faced two ransomware attacks in the past couple of years. Ransomware attacks undermine health care organizations' mission of providing their patients with timely care. Consider the following findings from the Ponemon study: Nearly three-quarters of respondents reported that a successful cyber attack had resulted in longer stay lengths for patients. About the same proportion said that ransomware attacks had created delays in medical procedures and tests, resulting in poor outcomes for patients who needed them. Slightly fewer noted that the attacks had yielded an increase in the number of patients diverted to or transferred to other facilities. More than a quarter of respondents had witnessed a rise in complications from medical procedures following a ransomware attack. About a fifth said cyberattacks had increased their patients' mortality rate. Hospital Cyber Attacks go beyond health care data, too. In September 2020 for an example, German authorities investigated the death of a woman following a ransomware attack against a hospital to determine if the attack allowed her death to take place. Health care is one of those sectors where a ransomware attack could affect someone's physical safety and well-being. No one wants the reputation damage and other costs that such an incident might bring. That's in addition to the possible breach of health care data.

- **PONEMON RESEARCH REPORT - The Impact of Ransomware on Healthcare During COVID-19 and Beyond**
- **SUPPLY CHAIN ATTACK THROUGH KASEYA - REvil Ransomware Gang Launches Major Supply Chain Attack Through Kaseya**
- **RANSOMEWARE BLAMED FOR CAUSE OF DEATH - Baby died because of ransomware attack on hospital claims lawsuit**



A MYSTERIOUS THREAT ACTOR IS RUNNING HUNDREDS OF MALICIOUS TOR RELAYS

Since at least 2017, a mysterious threat actor has run thousands of malicious servers in entry, middle, and exit positions of the Tor network in what a security researcher has described as an attempt to deanonymize Tor users. Tracked as **KAX17**, the threat actor ran at its peak more than 900 malicious servers' part of the Tor network, which typically tends to hover around a daily total of up to 9,000-10,000. Some of these server's work as entry points (guards), others as middle relays, and others as exit points from the Tor network. Their role is to encrypt and anonymize user traffic as it enters and leaves the Tor network, creating a giant mesh of proxy servers that bounce connections between each other and provide the much-needed privacy that Tor users come for. Servers added to the Tor network typically must have contact information included in their setup, such as an email address, so Tor network administrators and law enforcement can contact server operators in the case of a misconfiguration or file an abuse report. However, despite this rule, servers with no contact information are often added to the Tor network, which is not strictly policed, mainly to ensure there's always a sufficiently large number of nodes to bounce and hide user traffic.

- **MALICIOUS TOR NETWORKS – Understanding the problem with malicious TOR networks**
- **TOR HACKING HISTORY – Thousands of Tor exit nodes attacked cryptocurrency users over the past year**
- **KAX17 – Is "KAX17" performing de-anonymization Attacks against Tor Users?**
- **TOR RELAY – Recent rejection of relays**

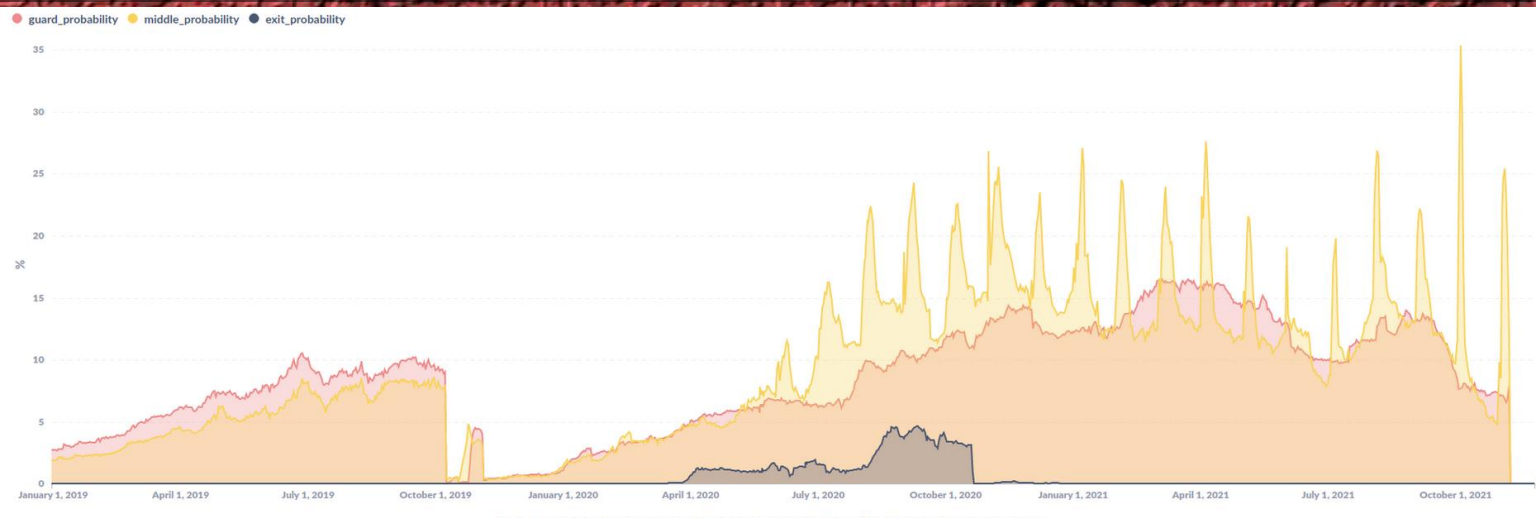


Figure 1: Guard, middle and exit probability by KAX17's relays between 2019–01–01 and the removal event on

>. CLASS_SCHEDULE

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	BOOK
CYBV 303	WINDOWS SECURITY ESSENTIALS	BOOK
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	INCIDENT RESPONSE 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
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 & 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

>. CYBER_SECURITY_HISTORY

OPERATION AURORA FIRST PUBLICLY DISCLOSED BY GOOGLE

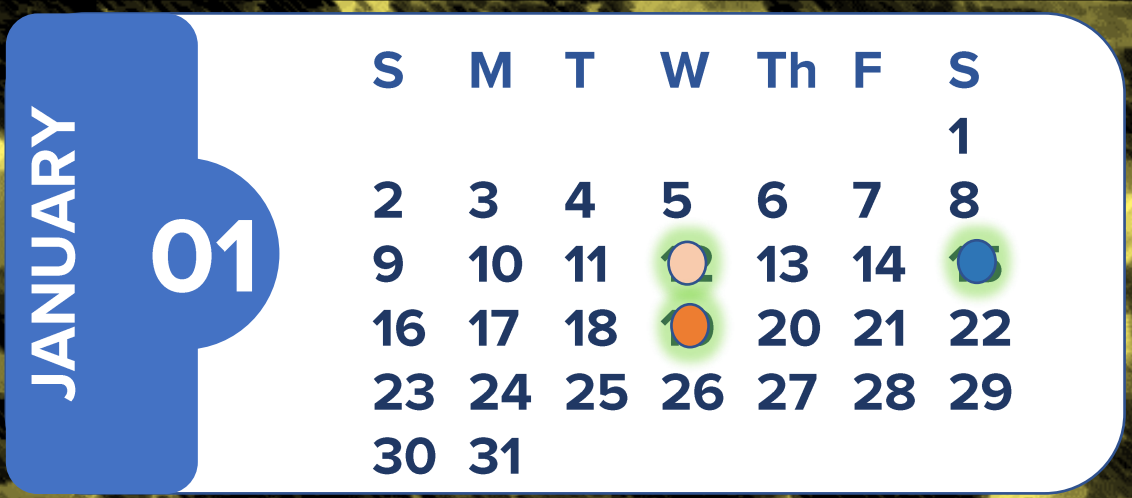
Operation Aurora was a series of cyber attacks conducted by advanced persistent threats such as the Elder wood Group based in Beijing, China, with ties to the People's Liberation Army, the attacks began in mid-2009 and continued through December 2009. According to McAfee, the primary goal of the attack 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 the encryption of digital data. 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. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. 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 that was 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 real 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

JANUARY 01

S	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

≥ February 4-5, 2022

≥Mesa Convention Center, AZ

≥Hybrid Talks and Local Workshops

≥ CactusCon is back at the Mesa Convention Center in lovely Mesa, AZ, on February 4-5, 2022! There is ample parking at the venue, with potential overflow lots north of MLK Jr. Avenue. If you book at the extremely nearby Delta Hotel Marriott, your parking will be just as close as convention center parking.

≥ CactusCon is the most prominent annual hacker and security conference in Arizona. Our last event attracted just shy of 1,500 attendees from throughout the country. However, in the previous nine (9) years, our event has established itself as a top-tier security conference and has quickly become a must-attend learning and networking event.

≥ CactusCon is constantly evolving, striving to meet the changing needs and expectations of the InfoSec community. We attract sought-after industry leaders, offer cutting-edge workshops, and provide ample opportunities for mingling and networking with people who share a passion for information security.

≥ JOIN THE DISCORD https://www.cactuscon.com/cc10

ABUSING A SYSTEM THROUGH PROCESS HERPADERPING

Last semester, the Fall of 2021, was my first-semester teaching CYBV 454 Malware Threats & Analysis. As I was finding my footing, I recall a technique of obscuring malicious programs from Anti-Virus and the host operating system. The method we will be discussing is called Process Herpaderping, which is very similar to Process Doppelgänging, Process Hollowing or Process Ghosting. Process Herpaderping is a method of obscuring a malicious process by modifying the file on a disk after the image has been mapped for the OS to execute it. In a simplistic explanation, when you begin running an executable, the operating system needs to link to it to be referenced by other programs and gather resources for it to run, access to hardware, and link it to memory. However, by creating these callbacks, these are not invoked upon the creation of the process but rather upon the creation of the first threads within the process. This method creates a gap between when a process is created and when security products are notified of its design. It also gives malware authors a window to tamper with the backing executable before security products can scan it. Microsoft provides security vendors with the ability to register callbacks that will be invoked upon the creation of processes and threads on the system. Driver developers can call APIs to receive such events, but this gap is what a malware author can use to abuse the systems' defenses.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. HACKING_POC IS 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!!

ABUSING A SYSTEM THROUGH PROCESS HERPADERPING

From an Operating Systems perspective, herpaderp attacks are often categorized as unintentional activity. But from a software developer's point of view, it's a clear security threat, and a potent one at that.

To start off our example we are going to run a program that is on one hand innocent and on the other hand a huge red flag that every Anti-Virus and Windows protection will flag as a known threat, and this is the program Mimikatz. Mimikatz is an open-source program used by hackers and security professionals like penetration testers to gather credentials on Windows computers. Coded by Benjamin Deply in 2007, mimikatz was originally created to be a proof of concept as an example framework to learn about Microsoft authentication protocol vulnerabilities. From a System Administration standpoint this is not a file you want on your network, as a network security engineer this is not something you want being transmitted on your network and the reason why is because oh how easily it can extract credentials. You want every piece of protection to alert on this program.

Well by using Process Herpaderping, we can load mimikatz into the system but make it appear as if it is a validly signed file by something the system trusts. Think of a trusted file from Microsoft, Google or Cisco. Something your system would interact with as a trusted source.

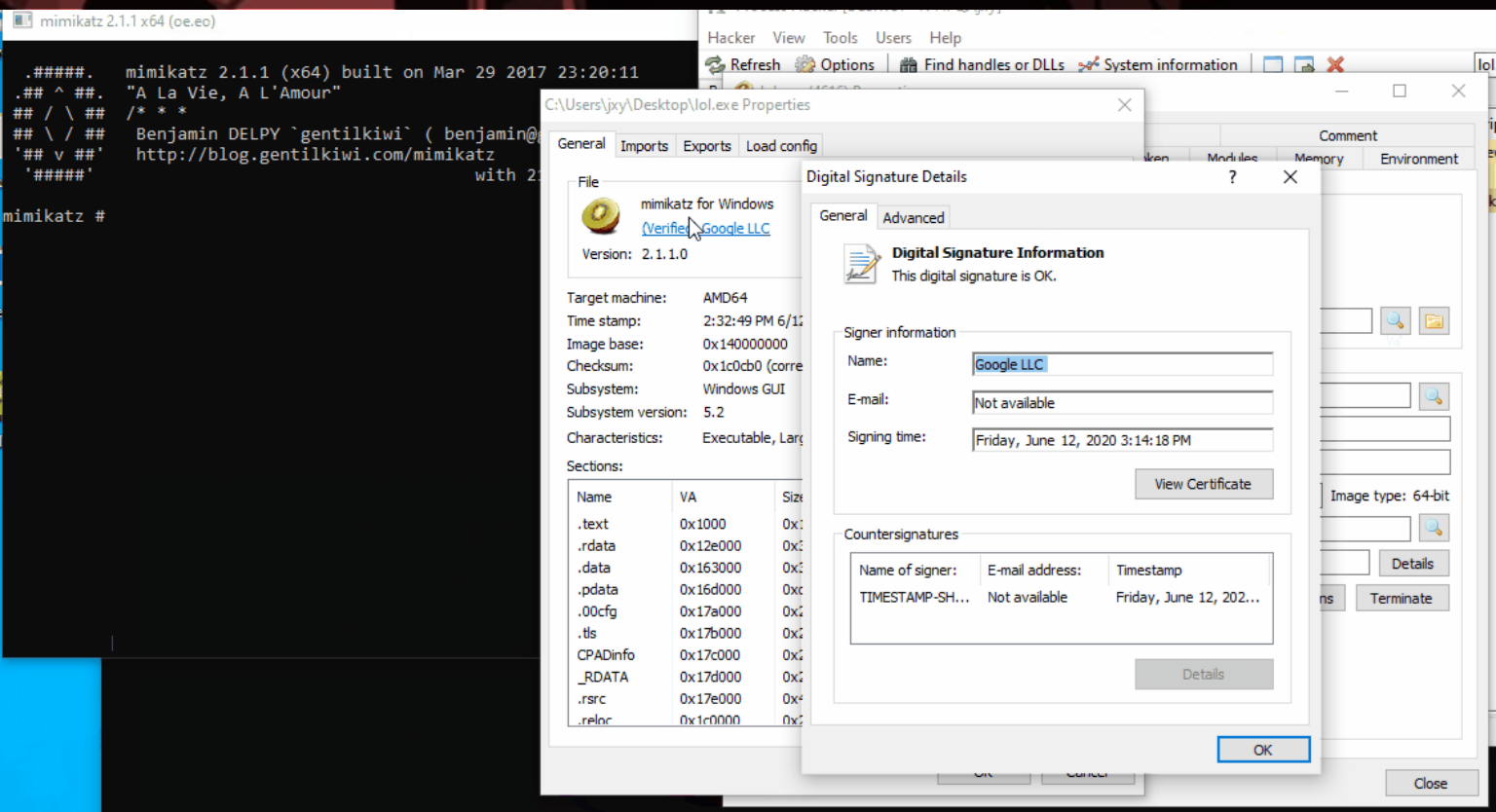
TYPE	TECHNIQUE
Hollowing	map -> modify section -> execute
Doppelganging	transact -> write -> map -> rollback -> execute
Herpaderping	write -> map -> modify -> execute -> close

ABUSING A SYSTEM THROUGH PROCESS HERPADERPING

By using the process at this GitHub page, we could run a copy of mimikatz as if it was signed by Google itself. This example goes over the Herpaderping technique which is like Hollowing and Doppelgänging however there are some key differences. In order to try this on your own make sure to build your environment correctly by using the following commands.

```
git clone https://github.com/jxy-s/herpaderping.git
cd .\herpaderping\
git submodule update --init --recursive
MSBuild .\herpaderping.sln
```

This vulnerability was disclosed to the Microsoft Security Response Center (MSRC) on 7/17/2020 and a case was opened by MSRC on 7/22/2020. MSRC concluded their investigation on 8/25/2020 and determined the findings are valid but do not meet their bar for immediate servicing. At this time their case is closed, without resolution, and is marked for future review, with no timeline.



>. QUICK_PROJECT

PROTECT YOUR SELF AT THE DNS LEVEL

If there is one thing I hate about modern technology, it is the absolute need to take every little bit of value from consumers. One of these specialized techniques, which I hate the most, is targeted advertisements and tracking user activity. These items are then packaged together and gain value as a sellable product for other companies to sell products to these data sets.
A research paper from the University of Science and Technology Beijing makes a claim "With the integration of various smart devices (smartphones, laptops, desktops, etc.) into people's lives, some traditional user tracking methods such as cookies, browser fingerprints, etc. have become ineffective. There is an urgent need for a new tracking paradigm that can track users across browsers and devices." The article published in Procedia computer science, 2021, Vol.187, p.83-88, and the model presented takes a cross-device user tracking method to solve this user tracking problem. While there are many ways that I would like to improve on this research, there is no real motivation to change from the current information collection methods because it requires little to no investment with perceived returns for the business. If it was not clear in my writing, I say perceived returns very sarcastically. So, my way of fighting the system is to just block the low effort level of collection. We will do this by installing Pi-Hole The first thing we will do is start with a fresh Raspberry Pi with a current version of Raspberry Pi OS. Once that has been set up, navigate to a terminal window and type

```
curl -sSL https://install.pi-hole.net | bash
```

This will take some time to complete and once it is done make a note of your Raspberry Pi's IP address. The next step would be going to your home router and logging in to it. Find where the DNS settings are located and simply change your DNS settings to match the IP address of your Raspberry Pi.
Now you have your own DNS server,

>. JOBS/INTERNSHIPS

INTERN - IT SPECIALIST Tempe AZ

The US Foods Summer Internship Program provides a forum for students to apply classroom skills and academic training in a real-world business environment. In addition to being assigned business-impacting projects throughout the summer, students will be matched with a manager who will meet with them on a regular basis to provide direction on assignments as well as deliver performance feedback and a mentor who will be available to offer day-to-day guidance and support. Interns will also get exposure to US Foods executive leadership; have an opportunity to participate in learning and social events with other interns across business functions and have an opportunity to deliver an end of summer presentation to showcase their accomplishments with key business leaders. US Foods internships are full-time paid positions (40 hours per week from May - August) with the possibility of transitioning to a full-time position post-graduation dependent on availability and overall performance. This position has been segmented as Blended meaning the work is a combination of onsite and remote/virtual.

- Identify, manage, escalation, and resolve technical issues
- Install and configure software, print drivers, utilities, etc. to be utilized on workstations and computer networks
- Troubleshoot all information technology issues, including software, hardware, and networking
- Monitor installed systems, identify problems, and take corrective action

- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

>. JOBS/INTERNSHIPS

IT INFORMATION SECURITY INTERNSHIP (UNDERGRADUATE) — Scottsdale AZ

This program is a 10-week full-time opportunity that starts on June 6th, 2022 and will end on August 12, 2022.
During the internship, you'll work with teams to deliver leading-edge information security controls and capabilities across the enterprise. Opportunities are available in functions such as third-party risk governance, security architecture, risk management, identity & access management, software security, vulnerability management, fraud detection, and other areas.
You will gain valuable work experience and participate in:

- Projects that contribute to the success of our business
- Community service activities
- Professional development workshops
- Mentorship and networking opportunities
- Interaction with senior leaders

And our corporate interns have an increased likelihood to receive an offer for a future role with CVS Health.

- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

INFORMATION SYSTEM SECURITY OFFICER (ISSO) ENTRY-LEVEL — Tucson AZ

Whether you're just starting out on your career journey or are an experienced professional, we offer a robust total rewards package that goes above and beyond with compensation; healthcare, wellness, retirement and work/life benefits; career development and recognition programs. Some of the superior benefits we offer include parental (including paternal) leave, flexible work schedules, achievement awards, educational assistance and child/adult backup care. You will be primarily responsible for system compliance, auditing, security plan development and delivering information systems security education and awareness. You will also assist in investigating information system security violations and help prepare reports specifying corrective and preventative actions. The position routinely collaborates with the facility security team, program personnel, and government representatives.

- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

>. JOBS/INTERNSHIPS

CYBER INFORMATION SYSTEM SECURITY OFFICER ENTRY-LEVEL — Tucson AZ

Raytheon Missiles & Defense

At Raytheon Missiles & Defense, by combining our vast resources and investments, we can dedicate ourselves to solving mission-level vs. product-level customer challenges – together we can anticipate more, move faster and make a bigger impact on the big picture. You will be primarily responsible for system compliance, auditing, security plan development and delivering information systems security education and awareness. You will also assist in investigating information system security violations and help prepare reports specifying corrective and preventative actions. The position routinely collaborates with the facility security team, program personnel, and government representatives.

- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

IT SUMMER INTERNSHIP — Phoenix AZ

P&G

IT at Procter & Gamble is where business, innovation and technology integrate to build an ambitious advantage for us. Our professionals are diverse leaders who apply deep IT understanding to deliver business models and capabilities. Whether your role is to craft an IT innovation strategy, protect our critical information systems and assets, or lead a strategic supplier, you will increase your technical mastery. Your passion for the industry will be nurtured by our culture of continued learning and growth. Your internship in IT builds change leadership and influence skills, breadth of experience across multiple businesses, and depth of expertise in one of our three IT areas:

- **Application & Integration** – The largest IT area focuses on Strategy, development, implementation, maintenance and business applications. Roles include Application Manager, IT Operations Manager, Solution Manager and Project Manager.
- **Infrastructure** – Strategy, governance and management of the hardware, software platforms and networks needed to support the development, delivery and ongoing maintenance of our applications and information. Roles include Systems, Network, and Data Center Governance and Management.
- **Data & Analytics** -Strategy of data and breaking it down into impactful results. Roles include Data and Insights, Marketing Technology and Product Management, Data and Analytics

- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

CENTER OF ACADEMIC EXCELLENCE

Cyber Operations

NOW HIRING

Student Worker

The Cyber Operations Program at the College of Applied Science & Technology is hiring a student worker. The position allows you to work remotely, up to 20 hours a week at $12.15/hour.

Duties:

- Assist students with CYBV 310 and CYBV 311
- Respond to students to clarify questions
- Assist students with technical issues
- Develop scripting to be used for automation
- Help with CSCV 452 might be needed (not a requirement)

Requirements:

- Experience programming outside of CYBV 310 and CYBV 311
- Experience with Windows for CYBV 310 and CYBV 311, including command prompt, remote desktop connections, and Visual Studio
- Experience with Linux or OSX for 452, including use of terminal, gcc, and lldb or gdb (if help with 452 is needed

Applying students must be:

- A current University of Arizona student
- Enrolled in a minimum of 6 units
- Must have completed CYBV 310 and CYBV 311
- Comfortable working with peers via Zoom and/or Discord
- Experience tutoring is not required, but would be a huge plus

THE UNIVERSITY OF ARIZONA

Email your cover letter and resume to

cbuldrini@arizona.edu

Deadline: January 12, 2022

College of Applied Science & Technology

NOW HIRING

Student Worker

The Cyber Operations Program at the College of Applied Science & Technology is hiring a student worker! The position allows you to work remotely, up to 20 hours a week at $12.15/hour.

DUTIES:

- Assisting students with fundamental python issues without solving assignment, specific challenges.
- Respond to students to clarify questions.
- Assist students with any issues related to access or operations within the VLE.
- Work with the course Professor to expand content off of the course.

REQUIREMENTS:

- Reliable computer access and ability to work remotely.
- Excellent communication skills and ability to work within a team

Applying students must be:

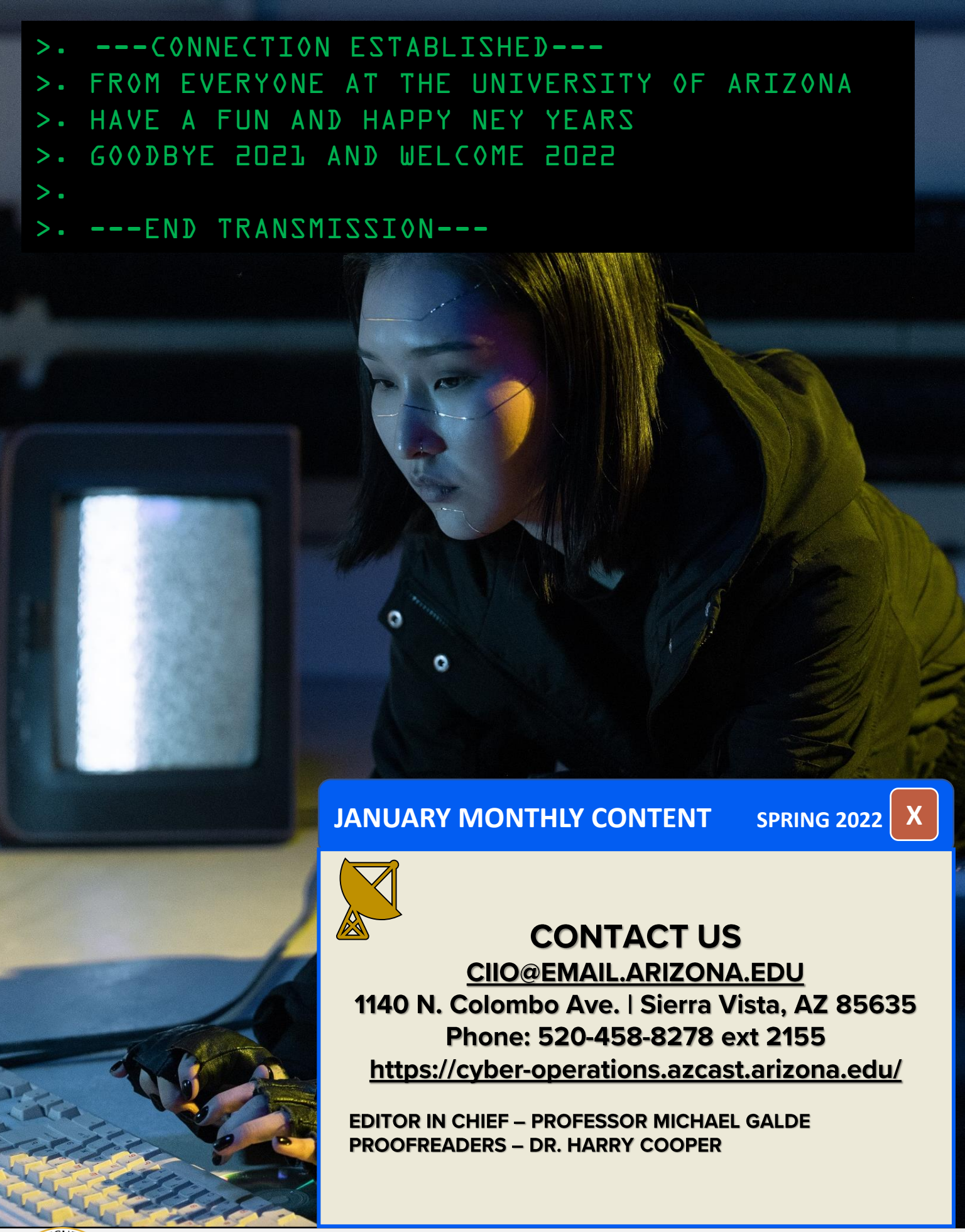
- A current University of Arizona Student
- Enrolled in a minimum of 6 UA units during the Fall and Spring Semesters
- Must have completed CYBV473.
- Must have received on "A" in CYBV473.
- Must have a desire to learn more about Python and share that knowledge with other students.

THE UNIVERSITY OF ARIZONA

Email your cover letter and resume to

cbuldrini@arizona.edu

Deadline: January 12, 2022



JANUARY MONTHLY CONTENT **SPRING 2022** X

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/

EDITOR IN CHIEF – PROFESSOR MICHAEL GALDE
PROOFREADERS – DR. HARRY COOPER

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY