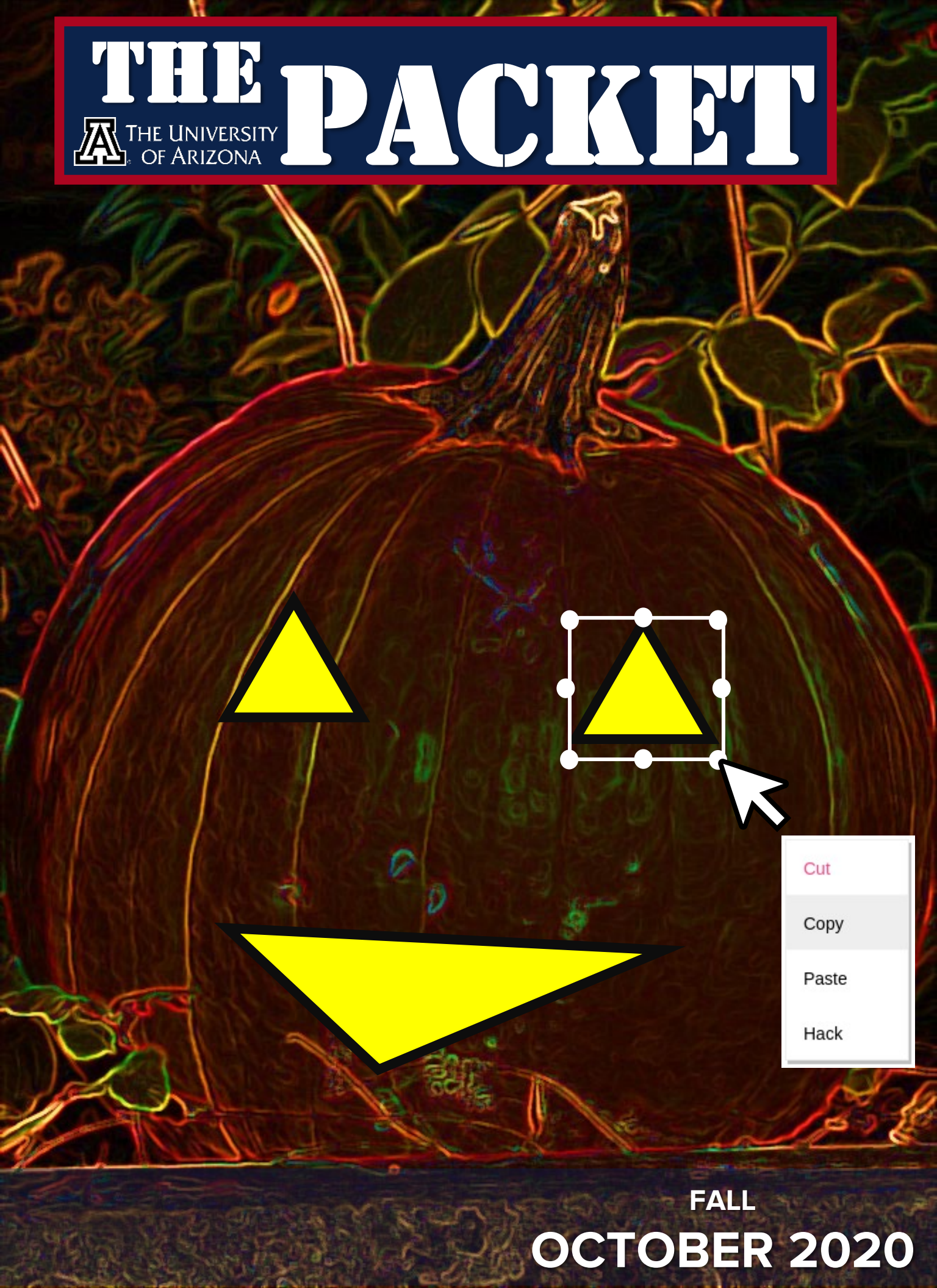
THE PACKET

THE UNIVERSITY OF ARIZONA



FALL

OCTOBER 2020

IN THIS ISSUE

--- BEGIN MESSAGE ---

Welcome to the **OCTOBER** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde and the fall semester has been going along swimmingly. A major vulnerability for Windows was published named Zero logon or CVE-2020-1472. This vulnerability allows a malicious user on a network to gain domain controller access in unpatched environments. In this edition we take a look the Proof of Concept and break it down for you. This year Halloween falls on a weekend and with current events this may end up being canceled this year. There is no need to worry about loosing out on some fun as we can adopt something as simple as a facemask and make it into something that will allow you to show off some style this fall. The global population is adapting to this ongoing pandemic and so are many of you as you adjust to learning online as you prepare to take on your future without backing down. As the global workforce moves to a remote work structure the need to cyber security professionals are necessary as the economic models adjust to our new reality. So, once again welcome to October, the year 2020 is now over 70% complete. So strap in, we are almost into 2021, and it can't be that bad right?

--- END MESSAGE ---

CYBER CLASSIFIED BY: PROFESSOR GALDE
REASON: CYBER OPERATION PROGRAM
DECYBER ON: OCTOBER 2060

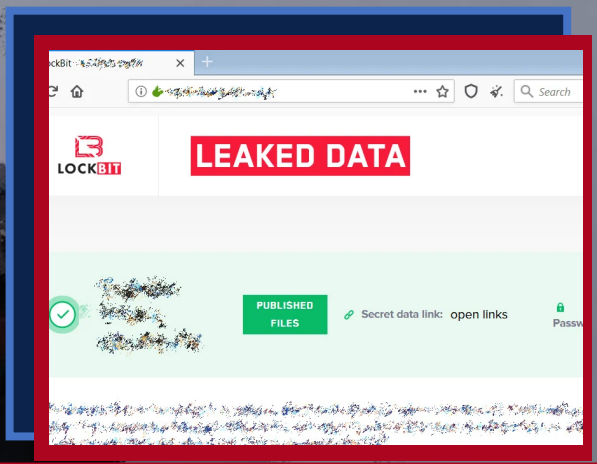
HACKS OF THE MONTH

Admin, Admin who has the admin …

CVE-2020-1472 looks innocent enough but if a malicious user is inside the network, they can easily gain admin access to an organization's domain controller. The python code that is less then 150 lines is simple enough and Microsoft has released a patch. Now how wide it has been deployed is the question. The CVE is listed as critical and is urged to be patched by all organizations with a domain controller.

Who needs a cyber attack when the company will do it for FREE!

Razer is in the news because of a misconfigured data base that just told everyone what you purchased. The data leaked contained records of customer orders and included information such as item purchased, customer email, customer (physical) address, phone number and everything but credit card details… so at least that is the silver lining in this mess. Sorry 100,000 customers who lost data.



The evolution of ransomware, the digital money press

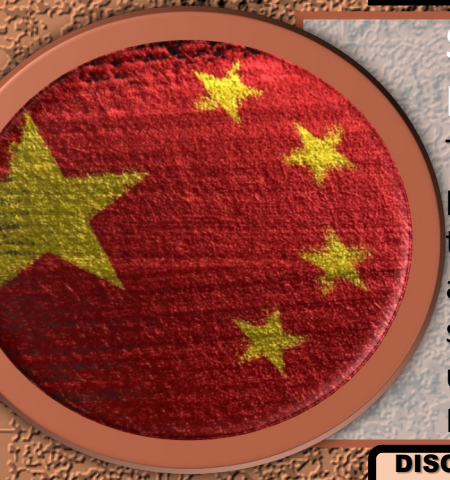
Do not pay ransomware, the best piece of advice I think anyone can offer, well the developers for LockBit is taking a page from the nasty Maze ransomware and are also hosting files of users that don't pay up. So if you refuse to pay then someone else might pay to get access to your files. Lockbit is likely seeing the success from Maze and soon all ransomware will follow this same path.

CYBER NEWS UPDATES

RANSOMWARE TO BLAME FOR NEARLY HALF THE CYBER-INSURANCE CLAIMS FILED IN EARLY 2020

Ransomware attacks were the cause of 41% of the cyber-insurance claims filed over the first six months of 2020, according to a report published by Coalition, a cyber-insurance vendor that compiled the data based on findings from 25,000 small and medium-sized companies in the U.S. and Canada. Coalition reported a 47% increase in the number of ransomware attacks, with the average size of the demand jumping by 46% over the time period in question.

DISCOVER MORE | CYBV 480 CYBER WARFARE | CYBV 435 Cyber Threat Intelligence | CYBV 385 INTRODUCTION TO CYBER OPERATIONS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY



SEVEN CHARGED IN CONNECTION WITH GLOBAL HACKING CAMPAIGN APT41

The accused Chinese hackers allegedly compromised technology providers and installed software backdoors in their networks, giving themselves a portal to collect information. The operation is linked to an advanced persistent threat group known as APT41, which private security firms have tied to the Chinese government. U.S. indictments unsealed September 16 alleged that the activity is tied to China's Ministry of State Security (MSS), a civilian intelligence agency.

DISCOVER MORE | CYBV 454 MALWARE THREATS & ANALYSIS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 388 CYBER INVESTIGATIONS AND FORENSICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

PAN-OS VULNERABILITIES ADD TO A TORRID YEAR FOR ENTERPRISE SOFTWARE BUGS

The bugs in the PAN operating system (PAN-OS) made by Palo Alto Networks add to a growing list of vulnerabilities in widely used corporate software that researchers have uncovered in 2020. One of the more critical vulnerabilities could allow a hacker who first accesses the software's management interface to plant malicious code in the operating system and obtain "maximum privileges" on the system.

DISCOVER MORE | CYBV 436 COUNTER CYBER THREAT INTELLIGENCE | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 329 CYBER ETHICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

CYBER OPERATIONS SPRING 2021

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 326	INTRO METHODS OF NTWK ANALYSIS	Book
CYBV 329	CYBER ETHICS	Book
CYBV 351	SIGINT AND EW	Book 1, Book 2, Book 3
CYBV 354	PRINCIPLES OPEN SOURCE INTEL	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	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
CYBV 437	DECEPTION & COUNTER-DECEPTION	Book
CYBV 440	DIGITAL ESPIONAGE	Book 1, Book 2
CYBV 441	CYBER WAR, TERROR AND CRIME	Book 1, Book 2
CYBV 450	INFORMATION WARFARE	Book 1
CYBV 454	MALWARE THREATS & ANALYSIS	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 480	CYBER WARFARE	Book 1, Book 2
CYBV 481	SOC ENG ATTACK & DEFENSE	Book 1, Book 2
CYBV 496	SPCL TOPICS IN CYBER SECURITY	Book
CYBV 498	CAPSTONE IN CYBER OPERATIONS	

JOB BOARD

Information System Security Designer (Entry/Developmental)

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!

Cyber Mitigations Engineer/System Vulnerability Analyst

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's critical Infrastructure? If so, NSA is the place for you!

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

Computer Network Defense Analyst

Computer Network Analysts are hired into positions directly supporting a technical mission office (either on the offensive or defensive side) or one of a few different development programs like the Intrusion Analyst Skill Development Program (IASDP) and the Cybersecurity Operations Development Program (CSODP) (formerly named the Information Assurance and Cyber Development Program (IACDP)). These development programs are 3 years in length and combine formal training and diverse work assignments that may cross both offensive and defensive missions.

Cyber Network Professional

This position is well-suited for individuals who enjoy visiting network security websites, attending conferences such as Black Hat / DEFCON, setting up and maintaining their own network or competing in Capture the Flag events. NSA is in search of top-notch cyber professionals with technical expertise and driving desire at the forefront of their field. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satellite communications networks) that are deployed across NSA worldwide. Help protect national security interests as part of the world's most advanced team of cyber professionals!

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

HACKING POC

Part 1/3

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 go get a job that pays you to do it - legally!!

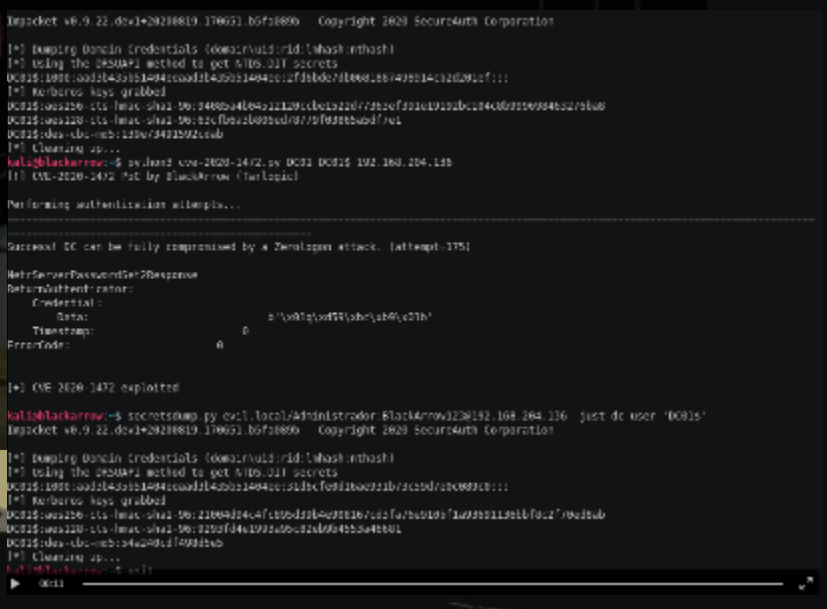
Let's explore the POC for CVE-2020-1472

Today we will review a Proof of Concept (PoC) exploit/tool for abusing the vulnerabilities associated with CVE-2020-1472 (Zero logon) which when unpatched will allow a user to initiate a full system takeover of a Windows domain controller. Running this exploit the password will be set to an empty one.

EXPLOIT STEP 1: SPOOFING THE CLIENT CREDENTIAL

The POC starts by exchanging challenges to login, once the client tries to authenticate itself by doing an authentication call with the server. During this transaction it has a call that takes place labeled ClientCredential, The protocol allows the client to set this challenge request and there's nothing stopping us from setting this challenge to 8 zeroes. This means that for 1 in 256 session keys, the correct ClientCredential will also consist of 8 zeroes!

With this method, we can log in as any computer in the domain. This includes backup domain controllers, and even the targeted domain controller itself!



Let's explore the POC for CVE-2020-1472

EXPLOIT STEP 2: DISABLING SIGNING AND SEALING

Step 1 allowed the user to bypass the authentication call, we however still have no idea what the session key is. Windows Server however allows digital signing and sealing to be optional and can be disabled by simply not setting a flag in the authentication call.

EXPLOIT STEP 3: SPOOFING A CALL

Even when encryption is disabled, every request to authenticate must contain an authenticator value. The malicious user can authenticate our user by simply providing an all-zero authenticator and an all-zero timestamp.

EXPLOIT STEP 4: CHANGING A COMPUTER'S AD PASSWORD

So now that we can authenticate as any computer, what shall we do? Well the malicious user can request to change the local password on the active directory side, and it turns out setting an empty password is not forbidden. This means we can set an empty password for any computer on the domain. Now we can login to the user with the password now being empty. When changing a computer password in this way it is only changed in the AD. The targeted system itself will still locally store its original password. That computer will then not be able to authenticate to the domain anymore, and it can only be re-synchronized through manual action. So at this point we already have a pretty dangerous denial-of-service exploit that allows us to lock out any device from the domain. Also, whenever a computer account has special privileges within a domain, these can now be abused.

HACKING

POC

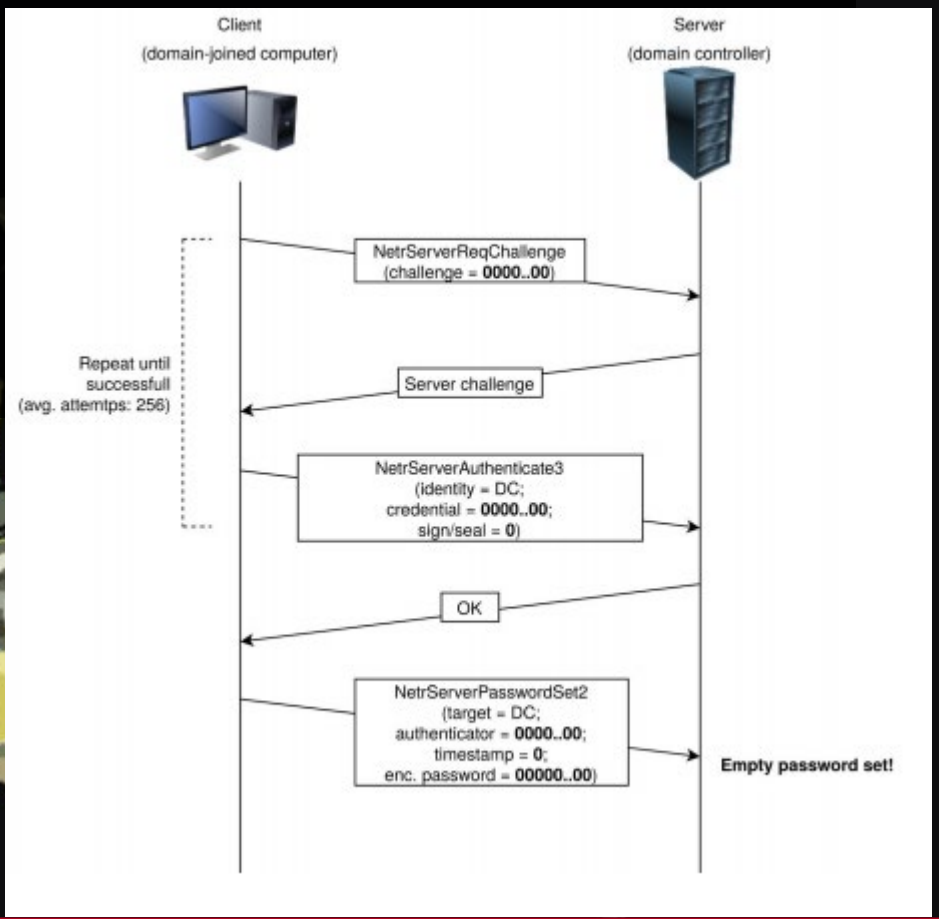
Part 3/3

Let's explore the POC for CVE-2020-1472

EXPLOIT STEP 5: FROM PASSWORD CHANGE TO DOMAIN ADMIN

One of the computers of which we can change the password is that of the domain controller itself. Doing so creates an interesting situation, where the DC password stored in AD is different from the password stored in its local registry. Running Impacket's 'secretsdump' script will successfully extract all user hashes from the domain through the Domain Replication Service (DRS) protocol. The malicious user can then use a "pass-the-hash" attack and update the local DC password and become the domain admin!

Read the white paper at Secura which was used to create this guide and make a lab to try this out!



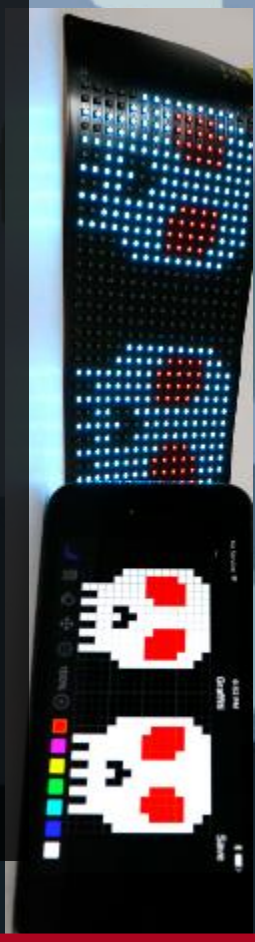
QUICK PROJECT

HOMEMADE LED MASK

LET'S MAKE A MASK FOR HALLOWEEN

So it looks like everyone has a mask currently and depending where you are located Halloween may be canceled but that does not mean you can't have a little fun. Today we are going to build a mask and shoving some LED's inside to show off some scarry images or just to be a little unique. Thanks to Lumen Couture for the idea!

1. So the first thing we need is addressable LED's, there are many options and for this project we are going to use something that has a built-in application that utilizes Bluetooth. We can pick up the Large LED matrix from Wearable Tech. This retails for $40.00 and can be found here.
2. Now it is time to head down to your local fabric store or Walmart and pick up for cotton fabric to make your mask. You want two layers, a thicker layer to make it useful as a mask and a thin layer to allow the LED's to shine through. You can use a pattern which can be located here.
3. Now we sew it all together and insert our LED lights into the mask with the battery pack and install the app on your phone here. This will last about 4 to 8 hours and its just enough time for your Trick or Treat adventures thou you may be in a party of one. Send your pictures in of your mask to show off in the November Issue!!



CYBER SECURITY HISTORY

ANONYMOUS HACKER GROUP LAUNCHED — OCTOBER 1, 2003

Anonymous originated in 2003 on the imageboard 4chan and you might have seen them in the iconic Guy Fawkes masks from the film V for Vendetta. Multiple members have been arrested for involvement in Anonymous cyberattacks in countries including the United States, United Kingdom, Australia, the Netherlands, Spain, India, and Turkey. Supporters have called the group "freedom fighters" while critics have described them as "a cyber lynch-mob" or "cyber terrorists". In 2012, Time called Anonymous one of the "100 most influential people" in the world. Journalists have commented that Anonymous' secrecy, fabrications, and media awareness pose an unusual challenge for reporting on the group's actions and motivations which is the point as Anonymous has no leadership, no action can be attributed to the membership as a whole.

NATIONAL CYBER SECURITY AWARENESS MONTH — OCTOBER 1, 2004

In 2004, the Department of Homeland Security and the National Cyber Security Alliance launched National Cyber Security Awareness Month as a broad effort to help Americans stay safe and secure online. CISA and the National Cyber Security Alliance (NCSA) announced 2020's theme as "Do Your Part. #BeCyberSmart."

COMPUTER FRAUD AND ABUSE ACT ENACTED — OCTOBER 16, 1986

The Computer Fraud and Abuse Act, also known as the CFAA, is the federal anti-hacking statute that prohibits unauthorized access to computers and networks. This law gives the federal government the power to charge individuals with a crime if they "knowingly" access a system they should not. Now the law is broad and has been adapting over the years but is known for being the law to bring charges after the Morris worm or the charging of TJX hacker Albert Gonzalez. The law however has also been abused and used to go after individuals who may have created fake accounts on social media, opening email in a protected environment and other challenges. The law is evolving as it adjusts to our ever-changing world but is one of the cornerstones to federal law of cyber criminals.

FOREIGN AFFAIRS IT Fellowship

FAIT FELLOWSHIP BENEFITS

- **Undergraduate candidates:** Up to $37,500 annually for tuition, room and board, books, mandatory fees and some travel expenses for junior year and senior year of undergraduate studies related to an IT field.
- **Graduate candidates:** Up to $37,500 annually for tuition, room and board, books, mandatory fees and some travel expenses for a two-year master's degree in an IT related field.
- **Two summer internships,** one at a domestic office of the Department of State in Washington, D.C. and one overseas at a U.S. embassy or consulate. The program provides stipends, transportation and housing for these internships.
- **Orientation** to the Foreign Affairs IT Fellowship program, the Foreign Service career path and to the Department of State.
- **Mentoring** from a Foreign Service IMS throughout the duration of the fellowship.
- **Employment in the Department of State Foreign Service** for those who successfully complete the program and the Foreign Service IMS entry requirements.

OBLIGATIONS OF AN FAIT FELLOW

- Attend the orientation in Washington, D.C., which takes place in June after selection.
- Fulfill the summer internship obligations during your first year and second year as a Fellow.
- Be prepared to enter the Foreign Service within two years of becoming a Fellow.
- Obtain and maintain medical, security and suitability clearances to remain in the program.
- Complete a minimum of five years of service as a Foreign Service Information Management Specialist (IMS). Candidates who do not complete the program and do not meet Foreign Service entry requirements may be subject to a repayment obligation to the Department of State.

YOU ARE INVITED

Foreign affairs information technology (fait) fellowship program, on Wednesday, October 21, 2020 at 5:00 pm (Arizona).

- Register for the virtual info session here.
- If you aren't able to attend at this time, but are still interested, please register so that you can get access to the recording. An email will go to all registrants after the webinar that provides a link to the recording of the webinar.

Eligibility Requirements

- Applicants must be a U.S. citizen.
- Undergraduate applicants must be enrolled in a degree program relevant to Information Technology at a U.S.-based accredited institution, and entering the junior year in the fall of the cohort year.
- Graduate applicants must be seeking admission to a master's degree program relevant to Information Technology at a U.S.-based accredited institution beginning in the fall of the cohort year.
- Applicants must have a minimum cumulative GPA of 3.2 or higher on a 4.0 scale at the time of application, and maintain this GPA throughout participation in the program.

As a member of our team, you will help safeguard communications and promote transparent, interconnected diplomacy throughout more than 270 U.S. embassies, consulates and missions.

You will have the unique opportunity to engage in diplomacy and make a positive impact worldwide – all while developing yourself personally and professionally.

Every day, you will experience the challenge and excitement of a career at the forefront of international affairs.

CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

Today's internet, with its terabytes upon terabytes of publicly available information (PAI) and other stored records of user and government data, offers more exploitable vulnerabilities than ever before. The instantaneous spread of information, and worse, disinformation or misinformation, occurs at faster upload and download speeds every year. The velocity by which information travels and is consumed only exacerbates the situation, as people conduct more of their daily transactions (social, political, economic) through the internet. Information operations and information warfare is not new, but today's internet enables criminals and other nefarious actors to have an unprecedented level of access into homes and governments despite security protocols. Digital platforms and manipulation tools available to anyone at minimal cost via the internet will increasingly challenge national security and every individual's ability to discern fact from fiction.

CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

Criminal and terrorist organizations (including individual opportunists) have realized the extremely low barrier to entry to using the internet to pursue their goals, and so have state actors with significant capabilities in the information space. ISIS' recruitment and propaganda videos in the mid-2010s are a testament to the effectiveness of the digital platforms. Opportunists continue to hack their way into our lives by deploying malware or scouring "breached data" to exploit unassuming users. These are all significant threats with definite near-term and potential long-term effects on individuals and on western democracies. The greatest strategic threat in the information space against individuals and western democracies one could argue however, is from countries that can not only wield state power through overt and transparent state-craft, but can also conduct covert and clandestine operations using state-funded organizations and proxies to further enhance intelligence collection and wage war within the cyberspace domain and information environment.

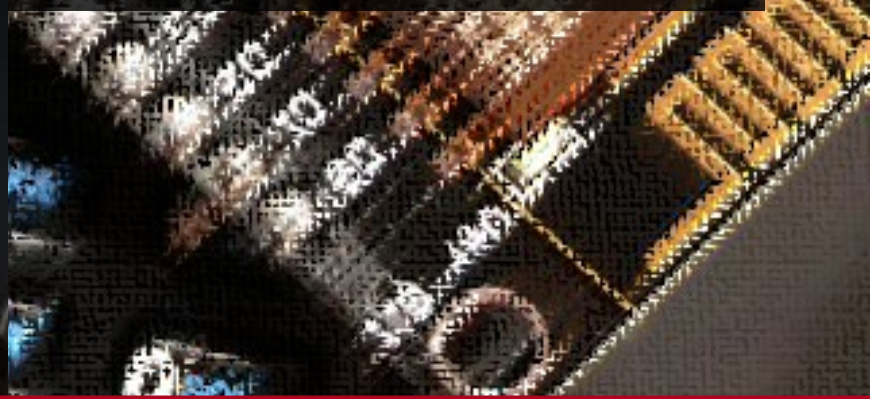
INFO — Intelligence practitioners from across government and law enforcement should scrutinize all available information and intelligence to assess how potential adversaries will exploit the information space and cyberspace domain to pursue their goals or objectives. The upcoming American presidential elections, and the relatively open digital avenues into the American voter's mind, create valuable targets of opportunity.

CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

Countries like Russia and China, two proclaimed near-peer competitors of the United States (Dunford, 2018), continue to pose a threat to U.S. national security, but Russia has demonstrated its intent and capability as a potential peer threat to the U.S. in the information environment. Russia has employed overt, clandestine and covert cyber warfare and information operations against Estonia, Georgia, Ukraine, Crimea, and the United States and other U.S. partners and allies in recent history. Russia has been mobilizing internet and information savvy coders and designers to craft artful campaigns of cyber and information warfare and are increasingly nimble at doing so in support of strategic end states. The 2016 U.S. Presidential election influence campaigns and cyber attacks attributed to Russian actors are demonstrative of this. Of course, Russia has had a long history of using active measures within and through the information space to create effects across domains of war (air, land, sea, space, cyberspace) to achieve its end states (Rid, Active Measures).

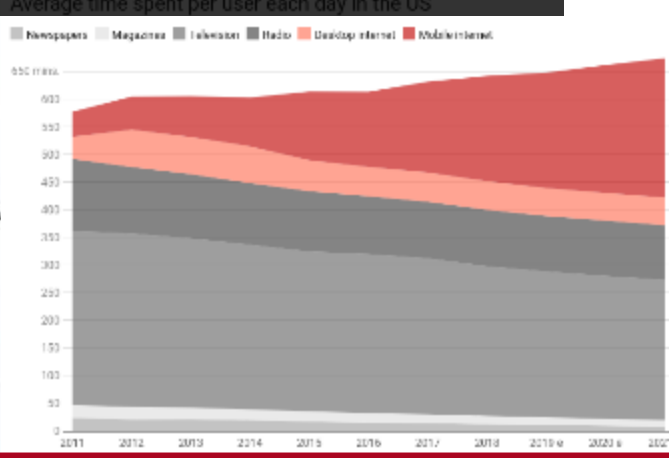


CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

The capability and intent of near-peer competitors has grown by leaps and bounds mostly due to our reliance on digital media combined with marked innovations in data and information manipulation technology. Reliance is driven by our need to stay connected, stay current on the news cycle, and stay on top of the myriad automations that rule some of our lives. Whether it is Facebook, Twitter, Whatsapp, Youtube, TikTok, or some new application exploding on the digital scene, the internet has our rapt attention. Vox published an article in early 2020 that claimed "...American adults spent about 3 hours and 30 minutes a day using the mobile internet in 2019, an increase of about 20 minutes from a year earlier" (Molla, Vox). Contrast that to today, in the COVID-19 environment, where the average user has likely doubled that usage due to the stay-at-home orders and fear of the virus. This creates increasingly more reliance on the internet and more opportunities for criminals and near-peer competitors to conduct targets of opportunity.

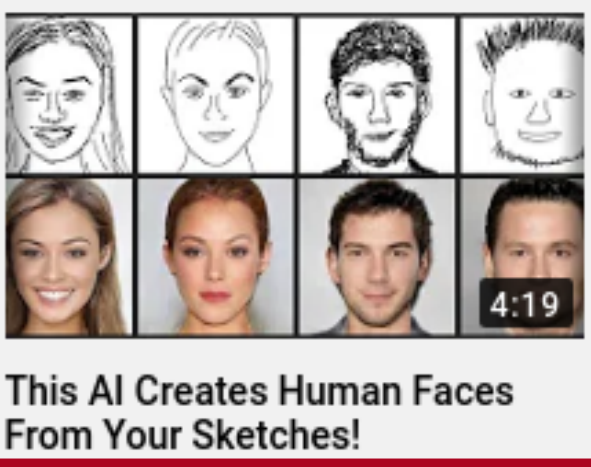


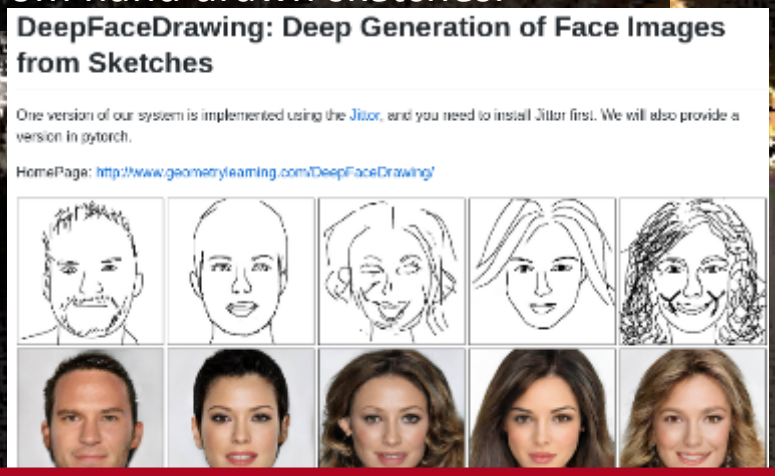
CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

Recent innovations have begun to shake the world of artificial intelligence and computing, creating an enticing avenue for nefarious actors to achieve their goals. Tim Hwang, author of Manuever and Manipulation, argues that "…the weakening ability for civil society and the public to analyze truth and falsity is creating a threat to the health and sustainability of democratic institutions" (Hwang, xi). We should expect adversaries to use some of these tools to manipulate facts and undermine the credibility of people and organizations you trust in the future. For example, face-swapping technology was good for a laugh, but now deep-fake technology and machine learning algorithms have exploded in ways few could have predicted. There are numerous videos circulating the web demonstrating these dangerous innovations. Dr. Károly Zsolnai-Fehér, who runs a Youtube channel called "Two-Minute Papers," highlights how learning algorithms are used to create digital animations of life-like looking people from hand drawn sketches.



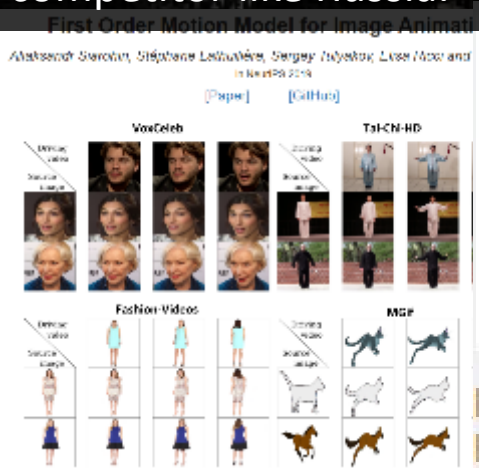


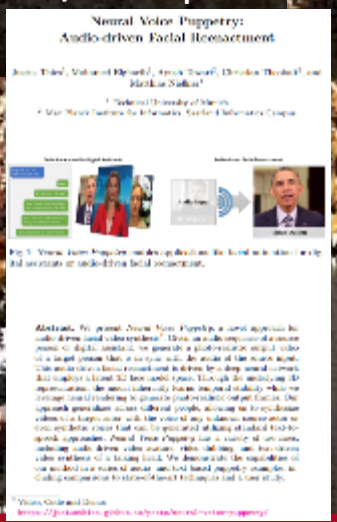
CYBER SECURITY DEFENSIVE PROTOCOL

NAZARETH, CRAIG

INFORMATION THAT SHOULD SHOCK ALL OF US

Other learning algorithms in deepfake (and lower cost/lower fidelity cheap fake audio and video) technology can clone movements and project animations in real time from a live human "puppet master" onto other real people using just a digital photograph of that real person. Dr. Zsolnai-Fehér shared the article "*Neural Voice Puppetry*" to demonstrate the advances in this field. The deep-fake technology is getting better at reducing digital anomalies, or artifacts in the digital images, so detecting the changes will continue to challenge even the best forensics professionals. Artificial intelligence algorithms can also create completely fabricated conversations from scratch, interacting with real computer users who assume they are interacting with real people. The technology has officially left the "fun and games" station and has arrived at the "extremely dangerous to national security" station, especially when added to the digital arsenal of a peer/near peer competitor like Russia.





STUDENT JOB BOARD

THE UNIVERSITY OF ARIZONA

Academic Assistant

The Disability Resource Center is hiring an Academic Assistant To assist a blind student with verbal descriptions of visual materials in the UArizona's Cybersecurity program. Ideally, the assistant chosen will have successfully taken CYBV 326 and 388 successfully prior to this semester. We may hire between 2-3 people to cover all the classes. (This position will be remote as long as necessary.)

The assistant will not be enrolled in this class, but must be available to log-in to the lectures at their meeting times:
CYBV 326: W, 4pm-7pm

The assistant will also work out a schedule with the student to be available an additional 3-4 hours per week based on mutually convenient times.

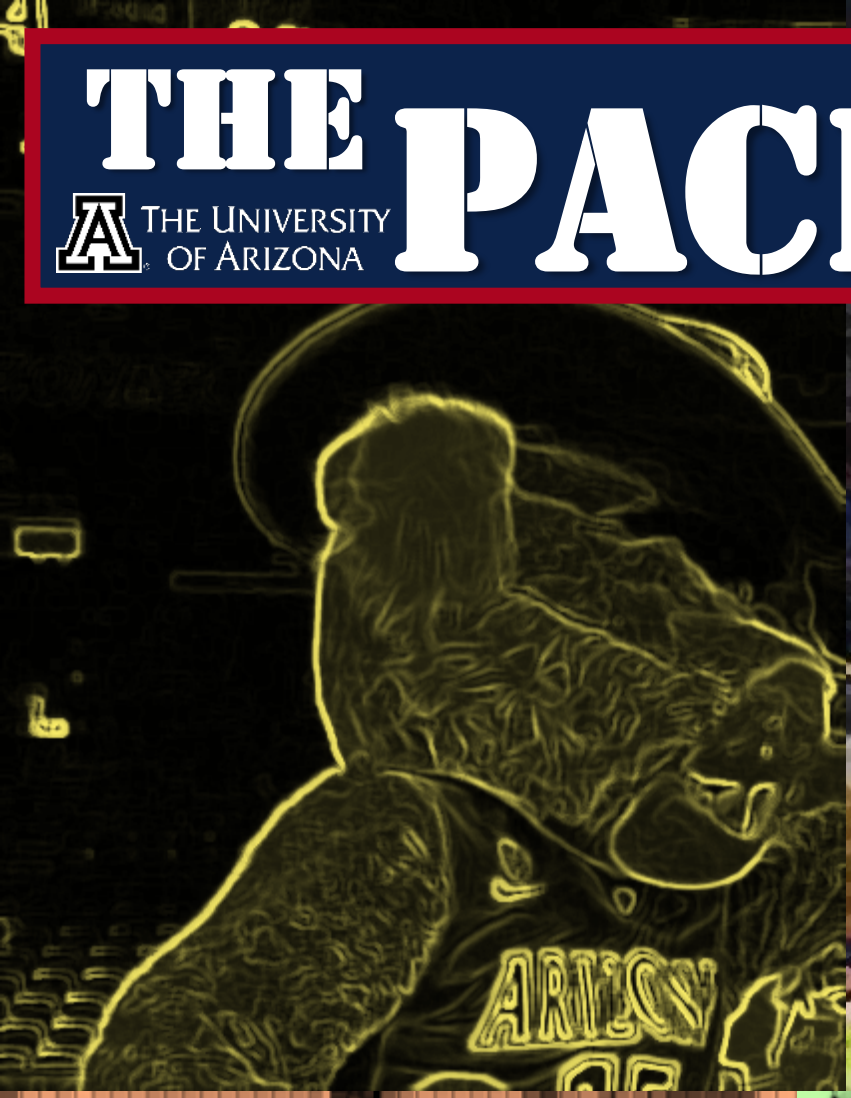
Pay is $15 an hour for 7 to 10 hours per week.

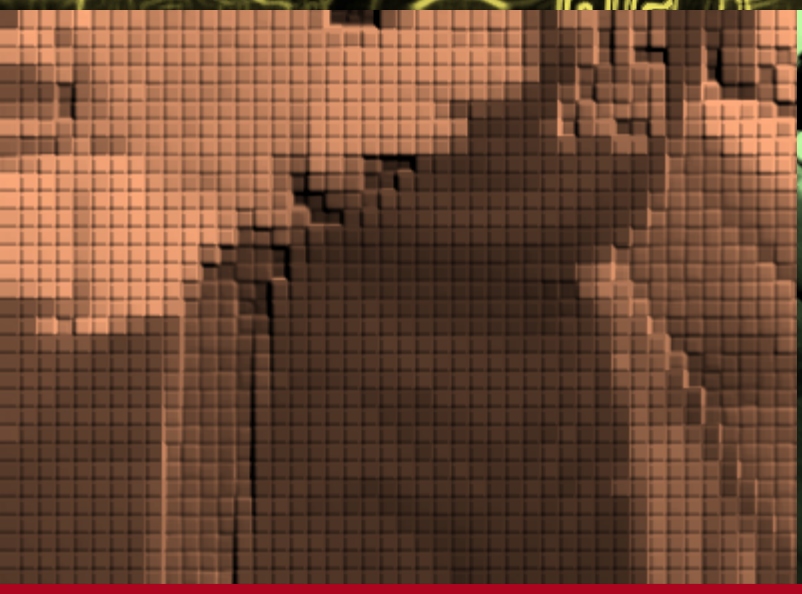
Please contact Carsen Kipley with any questions.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

THE PACKET

THE UNIVERSITY OF ARIZONA





CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

http://cyber-operations.azcast.arizona.edu/

THE UNIVERSITY OF ARIZONA