THE PACKET

THE UNIVERSITY OF ARIZONA

SUMMER
JULY 2020

THE PACKET
JULY 2020

IN THIS ISSUE

LETTER FROM THE EDITOR
3
HACKS OF THE MONTH
4
CYBER NEWS UPDATES
5
BOOK REVIEW
6
FORENSICS IDENTIFICATION OF DEEP FAKES
7
JOB BOARD
9
INTERNSHIP BOARD
14
STUDENT INTERVIEW
15
CYBER OPERATIONS FALL SCHEDULE
18
HACKING POC
20
QUICK PROJECT
24
CYBER SECURITY HISTORY
26
CYBER SECURITY DEFENSIVE PROTOCOL
27

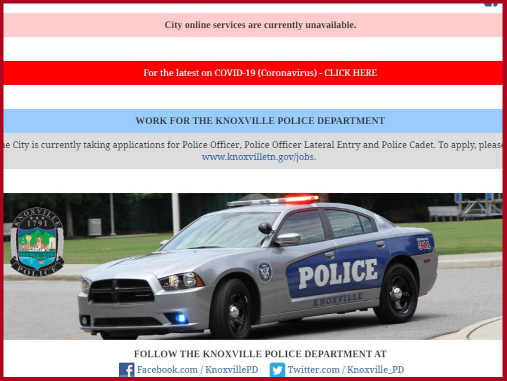
--- BEGIN MESSAGE ---

Welcome to the **JULY** issue of **"The PACKET"** produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde and I am here again with the July issue. We are all living in history that will be reviewed over the years as many case studies are developed from our current situation. In the INFOSEC community, we are witnessing how work from home policies are adjusting to this pandemic and how many enterprise networks are juggling access to network services and availability to remote employees. In office employees may not be a thing for a few more months and many organizations' original answer to work from home policies was to simply not allow the practice. Recent events have shown how shortsighted that decision was, and now many policies that have been put into place are a cookie cutter approach with no regard to the enterprise's infrastructure. This allows holes to open and malicious actors will exploit all that they can. I would like to predict that the INFOSEC community will see a large increase in data breaches and exploitation scams as businesses transition to this new reality and try to play catch up to other businesses with remote infrastructure that have learned these lessons months or even years ago. Students of the Cyber Operations program are in a unique position to not only learn about how to address these issues but also apply them in practice as students connect to University network services.

--- END MESSAGE ---

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

HACKS OF THE MONTH



City online services are currently unavailable.

For the latest on COVID-19 (Coronavirus) - CLICK HERE

WORK FOR THE KNOXVILLE POLICE DEPARTMENT

e City is currently taking applications for Police Officer, Police Officer Lateral Entry and Police Cadet. To apply, please www.knoxvilletn.gov/jobs.

FOLLOW THE KNOXVILLE POLICE DEPARTMENT AT

Facebook.com / KnoxvillePD Twitter.com / Knoxville_PD

A Knock-Knock on Knoxville Ransomware…

The city of Knoxville was hit with a ransomware that has knocked many services for the city offline. On Thursday June 11, many services to include the police and internal network services became unavailable. On Monday June 15, the services were still offline and unavailable. An initial assessment indicates that no financial or personal information was compromised, though. City IT believe the threat has been isolated.

Almost 2 weeks after being warned, the city of Florence Alabama gets some ransomware.

In Alabama's city of Florence the mayor was warned by a security official from Krebs on Security that the city could be hit by ransomware. Well just 12 days following that alert the city was hit with ransomware. The city has decided to pay the ransom of $291,000 or 30 bitcoin after negotiations were talked down from 378,000 or 39 bitcoin.

So many flavors of cyber attack and you choose salt ….. Err I mean ransomware.

A managed service provider named Conduent was recently infected with malware that pushed ransomware out to its victims. The attackers used a Maze ransomware variant. Attackers choose MSP's because they can provide the attacker with easy access to multiple targets. The actual attack took place May 29 and apparently only lasted for a few hours before the company took back control.

CYBER NEWS UPDATES

CAPITAL ONE RECENT COURT DECISION AND CORPORATE CYBERSECURITY

Capital One must provide outsiders with a third-party incident response report. The practice allows the organization to communicate with a law team to build an attorney client privilege which allows sensitive data to be protected. When you want a company to investigate a data breach this gives them some protections. A judge has said no more and is allowing the information to be discoverable in an upcoming class action suit.

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

THE 'NEW NORMAL' AS CYBER-SPIES NAVIGATE PANDEMIC

Intelligence analysts say some of the normally less active states have begun using cyber-espionage more aggressively and they have seen allies target each other for information for the first time. "It's a free-for-all out there - and with good reason - you don't want to be the intelligence agency that doesn't have a good answer for what's going on," says John Hultquist, director of threat analysis at Mandiant.

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

DARPA INVITES HACKERS TO BREAK HARDWARE TO MAKE IT MORE SECURE

The Defense Advanced Research Projects Agency is turning hardware over to hackers who can earn up to $25,000 for bugs they find. Hardware hacks often involve identifying vulnerabilities in how a computer chip handles information, like the flaw uncovered in Intel microprocessors in March that could have allowed attackers to run malicious code early in the boot process. “It’s not about patching the vulnerabilities, it’s about preventing the exploit,” Synack CTO

DISCOVER MORE
CYBV 474 ADVANCED ANALYTICS FOR SECURITY OPERATIONS
CYBV 435 CYBER THREAT INTELLIGENCE
CYBV 329 CYBER ETHICS
CYBV 301 FUNDAMENTALS OF CYBERSECURITY

BOOK REVIEW

Rector-134

The Art of Invisibility, by Kevin Mitnick

“If I have seen further than others, it is by standing upon the shoulders of giants,” is a phrase that has echoed in the sciences since Newton first said those words, and in the comparatively new field of cyber security, those words hold especially true. Kevin Mitnick had little guidance when he began hacking in 1979, but if you want somebody’s shoulders to stand on so you can see into the distance - his are a good choice.

For Mitnick, everything was new. Also for Mitnick, everything he did held risk. His unique experiences of staying ahead of the law (and even playing jokes on the FBI as they tried to catch him) make him an expert in how to hack and how not to get caught. It also makes him an expert in how to not be hacked.

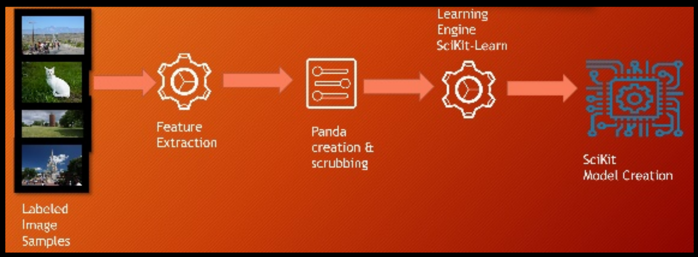
Those are the insights he shares in The Art of Invisibility. From proper password selection, encrypting your devices and keeping your refrigerator from spying on you, to stories about scamming the DMV into giving him a person’s phone number so he could scream at them for cutting him off on the highway - Mitnick covers it all. Whether you’re just getting started in the career field, or you’ve been around for a while, you’ll learn something new by reading this book.

FORENSIC IDENTIFICATION OF DEEP FAKES

Part 1/2

Chester Hosmer

The global impact resulting from the distribution of doctored digital photographs has reached epidemic proportions. These digitally altered photos are distributed via social media, news outlets, traditional web resources and are currently making there way into mainstream media. The impact these photos make can dramatically change the way people think, act, react, and believe- and can potentially cause harm. At the simplest level, they represent visual fraud.



The methods and techniques used for fake photo identification differ but rely on similar deep StegAnalylsis of digital images. The application and continued research, development, and application of machine learning technologies represent an important step in combatting the proliferation of deep fakes throughout social media.

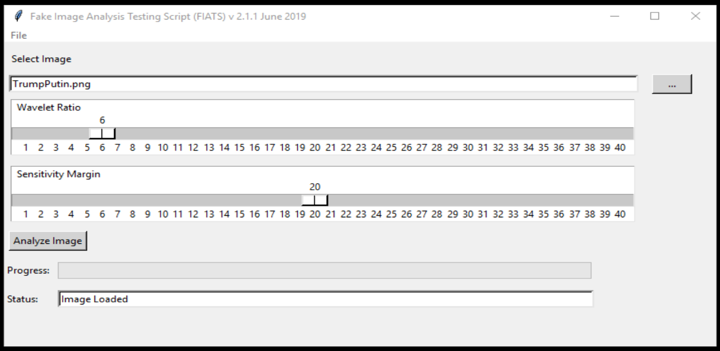
Steganography - the art of making slight changes to images, audio, video, and network protocols (typically referred to as the carrier) to conceal hidden content, or to covertly communicate information (typically referred to as the payload). Steganography differs from encryption where the goal of steganography is to hide the mere existence of hidden data or the message, while encryption is used to keep the content of the information private. Many steganography programs first encrypt the message content, then hide the data into the carrier, thus providing multiple layers of disguise.

FORENSIC IDENTIFICATION OF DEEP FAKES

Part 2/2

Chester Hosmer

To counter this threat, we must research and develop new tools, methodologies, and theories to accurately identify these fakes. The example shown here is an image depicting a proof-of-concept prototype written in Python. The algorithm detects anomalies in the image and highlights the impacted areas in yellow. The core technology is an outgrowth of over two decades of work surrounding the detection and analysis of steganography within images, multimedia content and network protocols.


Fake Image Analysis Testing Script (FIATS) v 2.1.1 June 2019

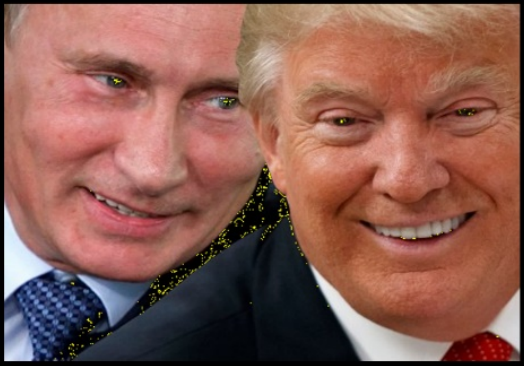
Select Image: TrumpPutin.png

Wavelet Ratio: 6

Sensitivity Margin: 20

Progress:

Status: Image Loaded



NOTES:

ARIZONA STUDENTS CAN STUDY, EXPERIMENT, AND PARTICIPATE IN THE ADVANCEMENT OF THESE TECHNIQUES IN THE FOLLOWING COURSES: CYBV-473 AND CYBV-474

JOB BOARD

Information System Security Professional

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 Analyst

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!

IT Cybersecurity Specialist

In this position, the incumbent is responsible for performing work as an Information Technology Specialist . Typical work assignments include:

- Perform cyber defense incident triage, to include determining scope and potential impact, identifying the specific vulnerability, and making recommendations for remediation
- Perform event correlation using information gathered from a variety of sources within an enterprise to gain situational awareness;
- Determine tactics, techniques, and procedures (TTPs) for intrusion sets and recommend computing environment vulnerability corrections
- Perform system analysis to develop reports, briefings, and presentations on cybersecurity

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

Associate Proxy Administrator - Arizona

Works with customers analyzing, troubleshooting, and isolating network protocol issues and hardware/software problems using various network tools. Tools include, but not limited to, the build, configuration, full end-to-end traffic analysis, migration and deployment of Blue Coat Proxy. Provide recommendations to customers for rapid restoration of services. An understanding of the Transmission Control Protocol/Internet Protocol (TCP/IP) and the IP address scheme and understand Secure Socket Later (SSL) Protocol. Be able to provide written and oral communication within a team structure and operate as an individual under some supervision. Perform Log analysis, DNS entry coordination, ACL management and multi-system configuration control as required work within a team structure. Research and identify means for detection of malicious activity toward Army web resources.

Associate- Help Desk Technician - Illinois

As a Help Desk Technician, you provide phone and in-person technical support for end users in an enterprise level environment. This is a full-time position to support and maintain in-house computer systems, desktops, and peripherals. This includes installing, diagnosing, repairing, maintaining, and upgrading all hardware and equipment while ensuring optimal workstation performance. Troubleshoot problem areas in a timely and accurate fashion and provide end user training and assistance where required.

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

Network Administrator - Illinois

The ideal candidate will be responsible for administration and day-to-day operation of organization's local area network (LAN). The Network Administrator will provide integrated team support and maintenance of LAN hardware and software. The ideal candidate will have experience with protocol analysis, knowledge of common network protocols, satellite networks, and Cisco ASA and Palo Alto firewalls.

Information Security Engineer - Maryland

Responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within their Computing Environment (CE). Assesses architecture and current hardware limitations, defines and designs system specifications, input/output processes and working parameters for hardware/software compatibility. Provides recommendations on information assurance engineering standards, implementation dependencies, and changing information assurance related technologies.

Software Engineer - Maryland

Provides functional and empirical analysis related to the design, development, and implementation of software systems, including, but not limited to application software, utility software, development software, and diagnostic software. Participates in the development of test strategies, devices, and systems. Solving engineering problems (or managing the solution of engineering problems) in the functional area to which assigned.

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

Software Configuration Management Specialist - Maryland

Must be able to write Configuration Management (CM) Plans and audit software change procedures, software development, software testing, and software documentation to verify compliance with software CM plans and procedures. Must be capable of participating in design reviews, configuration audits, and evaluations of software products to ensure proper identification, control, and status accounting of the software baseline for each system. Working on code management, audits, baseline identification, and preparation and control of documentation for software projects.

Senior Network Administrator (SME) - Arizona

The selected candidate will assist with daily leadership and technical guidance for a team of network analysts while performing daily management network assets from various vendors to include firewalls, routers, switches, load balancers and VPNs on behalf of the United States Army. Writing documentation to include SOPs and TTPs. Utilizing a diverse suite of network monitoring technology, troubleshoot a dynamic and complex environment while assisting third parties to solve various network connectivity problems.

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.

INTERNSHIP BOARD

Cyber Exploitation Officer

As a Cyber Exploitation Officer intern for the CIA, you will work alongside career staff in the evaluation and exploitation of digital and all source intelligence information in a dynamic digital environment, using a variety of analytic and forensic tools to extract valuable information from digital data, as well as creating a range of products that will drive operations and further collection.

Cyber Exploitation Officer interns are generally required to work either a combination of one semester and one summer, or two 90 day summer internships.

Cyber Security Officer

As a Cyber Security Intern for the CIA, you will work side-by-side other Cyber Security professionals to protect Agency data and systems using sophisticated tools, instrumentation, and knowledge of CIA Information Technology and tradecraft to monitor, evaluate, and manage IT risk.

You will protect CIA data and IT systems by identifying current threats, mitigating vulnerabilities, and anticipating future cyber security challenges. You may additionally be required to analyze existing and future systems across the Agency, implement network defenses, develop threat models and security risk assessments, and conduct forensic analysis of security events and logs via sophisticated security and event management tools.

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.

STUDENT INTERVIEW

Part 1/3

I had the pleasure to meet with the recent University of Arizona recipient of the Department of State's Foreign Affairs Information Technology Fellowship.
Sara and I were able to talk about this amazing opportunity over the very popular COVID-19 zoom application.
So first off, the FAIT fellowship provides up to $37,500 annually in academic funding for two years of the student's IT-related degree program.

Students participate in two summer internships with stipend support
One in Washington, D.C., and one at a U.S. embassy or consulate
Professional development training.

After completing the two-year program and meeting Department requirements, the Fellows receive appointments as Foreign Service Information Management Specialists and begin exciting careers using their technology skills to support U.S. diplomacy abroad.

SO SARA, WHAT WAS YOUR MOTIVATION GROWING UP?

When I was little, I wanted to be a reporter or at least work in journalism like my dad! In fifth grade though, I attended my first Computer Challenge at Cochise College. The next year, I found a game where the goal was to "hack" into the alien spaceship. I really enjoyed that hacking aspect, so I took a deep dive into all things computer-related.

STUDENT INTERVIEW

Part 2/3

So you got started young in cyber security!

By the time I was in high school, I had joined Cyber Patriots and enjoyed how the local organizer Dan Guilmette taught the trainings. Then a scholarship came up that would pay for the Associates of Applied Science in Cybersecurity at Cochise College. Dan would always talk about how he was teaching us the same way he taught the students in that program. I figured if I was already learning it and was enjoying it, I might as well get the degree! So, in short, it's basically thanks to Dan and video games that I got into cyber security.

What is your dream job and if you could have it all where do you see your self in 10 years?

My current dream job is to be a cybersecurity analyst, then work my way into an architect position, and eventually into a Chief Technology Officer role. In 10 years from now, I'm hoping I'll be that architect!

What topic in cybersecurity is your favorite vs. what could you do without?

Right now, my favorite topics or subjects are social engineering and everything that comes with pen testing! It's just very interesting to me and it seems fun sometimes. I was also really into Linux at one point, so Linux is always going to be a favorite of mine. I'm also interested in ways to secure our voting infrastructure. One of my professors from Cochise College wrote his master's thesis on how voting machines are vulnerable in cyber security so I want to ask if I can read it. The thing I could do without though is subnetting. It's just never clicked for me, so I've always had trouble with it. Thankfully, I haven't had to do it, but I have a feeling I'll probably encounter it during my academic career here.

STUDENT INTERVIEW

Part 3/3

At the end of this 2-year program you will receive an appointment as an Information Management Specialist abroad, Where do you hope to be posted?

I hope I get posted to a country in the EU. I mentioned France and Italy earlier and I think being in the EU would be cool because I'd be able to take a train to Germany or Ireland and be able to travel. I'm not super aware of the projects the Foreign Service has currently but honestly, anything is going to be very exciting. Not many people get this kind of opportunity.

Do you have any advice for any other students who wish to apply to the FAIT fellowship, maybe what they should be doing now?

Apply with an email that doesn't have a lot of spam! I made that mistake but on the plus side, I've finally unsubscribed to things I signed up for when I was 14. Also, ask for a letter of recommendation from someone who knows how well you work and study. I think that because my recommender knew how well I was able to work and do school at the same time, it gave me a better chance. Finally get multiple people to proofread your essays for it. I had about 5 or 6 tutors look at mine before I felt it was good enough.

And finally on main campus what restaurants would you recommend?

Yardhouse, Zinburger, Alibaba Mediterranean, Oregano's, Café à la C'Art and then the Tucson Mall has Kebab King and a really good Raspados place called Eat Fresh Mexican Food Raspados

Thank you, so much and good luck, in the program!

CYBER OPERATIONS FALL SCHEDULE

ADVISING UPDATE

A FRIENDLY REMINDER

THE ENROLLMENT FOR FALL CLASSES IS CURRENTLY OPEN AND CLASSES ARE STARTING TO FILL. IF YOU HAVE NOT ALREADY ENROLLED NOW IS THE TIME TO DO SO. IF YOU NEED ASSISTANCE CHOOSING YOUR COURSES, PLEASE SCHEDULE AN APPOINTMENT WITH YOUR ACADEMIC ADVISOR. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE:
HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

NOTE, TUITION AND FEES ARE NOT DUE AT THE TIME OF ENROLLMENT. THE DEADLINE TO PAY FOR ALL UNITS REGISTERED AS OF 8/19/20 WITHOUT LATE FEES IS 8/24/20. STUDENTS USING MILITARY BENEFITS HAVE CODES ADDED TO THEIR RECORD THAT KEEPS LATE FEES FROM BEING ADDED WHILE WAITING FOR BENEFITS TO PROCESS.

CYBER OPERATIONS FALL SCHEDULE

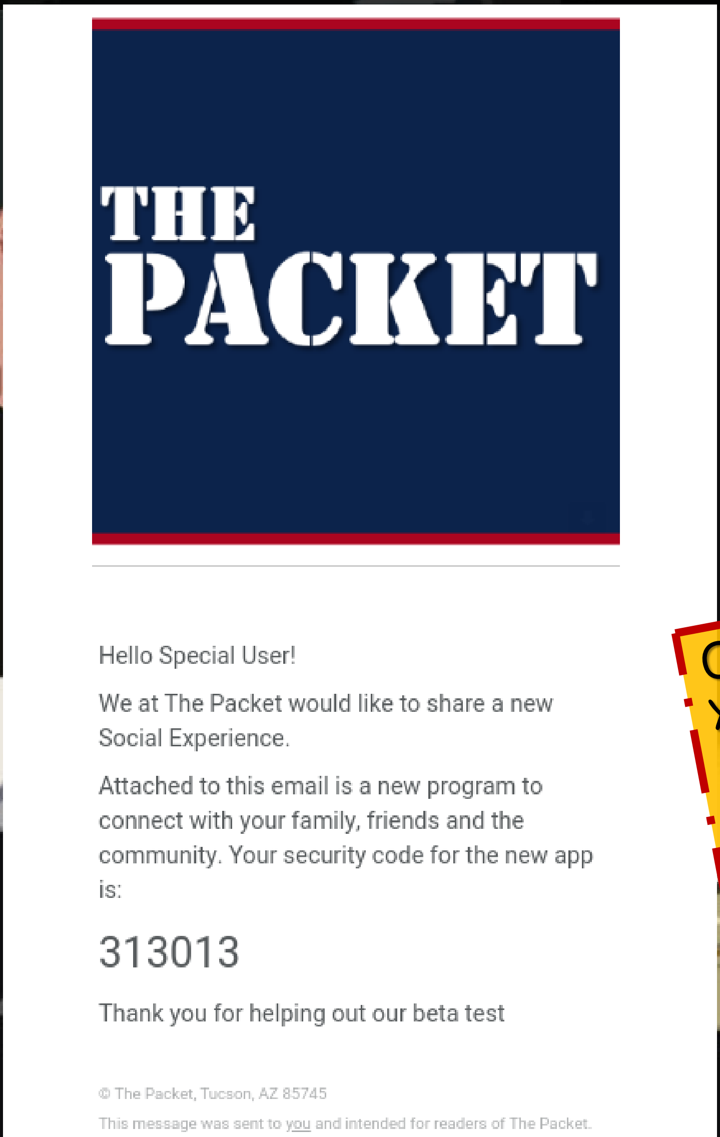
FILLING UP FAST

CAT #	COURSE
CYBV 301	FUNDAMENTALS OF CYBERSECURITY
CYBV 326	INTRODUCTORY METHODS OF NETWORK ANALYSIS
CYBV 329	CYBER ETHICS
CYBV 354	PRINCIPLES OF OPEN SOURCE INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 385	INTRODUCTION TO CYBER OPERATIONS
CYBV 388	CYBER INVESTIGATIONS AND FORENSICS
CYBV 400	ACTIVE CYBER DEFENSE
CYBV 435	CYBER THREAT INTELLIGENCE
CYBV 436	COUNTER CYBER THREAT INTELLIGENCE (7 WEEK CLASS 2 ONLY)
CYBV 440	DIGITAL ESPIONAGE (7 WEEK CLASS 1 ONLY)
CYBV 441	CYBER WAR, TERROR AND CRIME (7 WEEK CLASS 2 ONLY)
CYBV 454	MALWARE THREATS & ANALYSIS
CYBV 471	ASSEMBLY LANGUAGE PROGRAMMING FOR SECURITY PROFESSIONALS
CYBV 473	VIOLENT PYTHON
CYBV 480	CYBER WARFARE
CYBV 496	INTRODUCTION TO SECURITY SCRIPTING (7 WEEK CLASS 1 ONLY)
CYBV 498	CAPSTONE IN CYBER OPERATIONS

LET'S DISTRIBUTE MALWARE FOR FUN!!

Now that we have created some malware and have packed it into a program our users will trust we now need to get it to our victims. So to do that we are going to do a little Phishing!

On the left is what we will send to our victims and we will include our malware as an attachment.



THE PACKET

Hello Special User!

We at The Packet would like to share a new Social Experience.

Attached to this email is a new program to connect with your family, friends and the community. Your security code for the new app is:

313013

Thank you for helping out our beta test

© The Packet, Tucson, AZ 85745

This message was sent to you and intended for readers of The Packet.

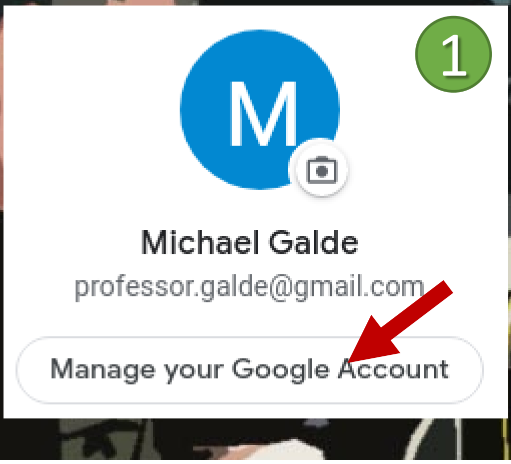
CAUTION — This article shows you how to create a piece of software some may misuse and/or misunderstand. This malware series is intended for academic purposes only and is intended to provide education to cyber security professionals… Plus you will likely be caught if you don't make major changes. You assume any risk of using the information in this article.

HACKING POC

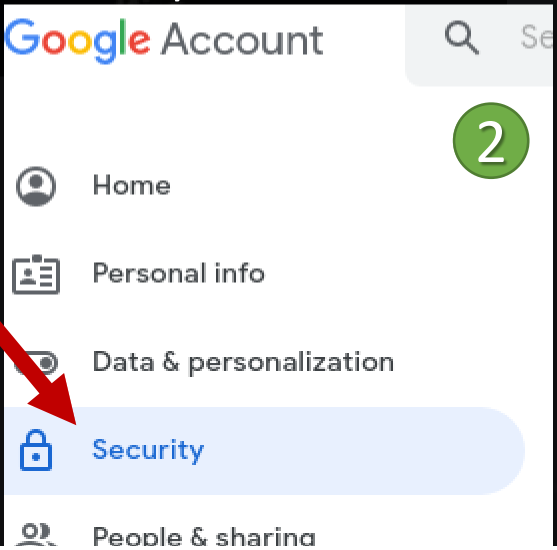
Part 2/4

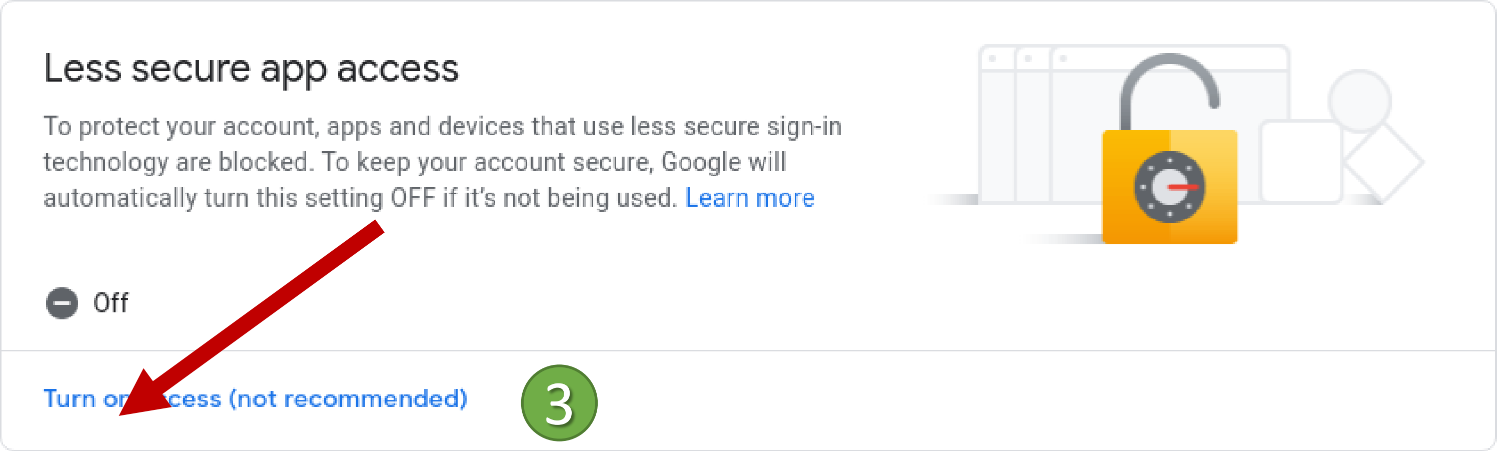
SETTING UP GMAIL

So we have some ready-made code that will do this project for you, but an email address will have to be provided. We are going to use a Gmail because that is what I personally like to use for these projects, but any email service would be possible. So the first thing we need to do is manage our account. In the upper right corner click on your name and go to manage your google account.



Go and click on security and find the section for less secure apps





Less secure app access

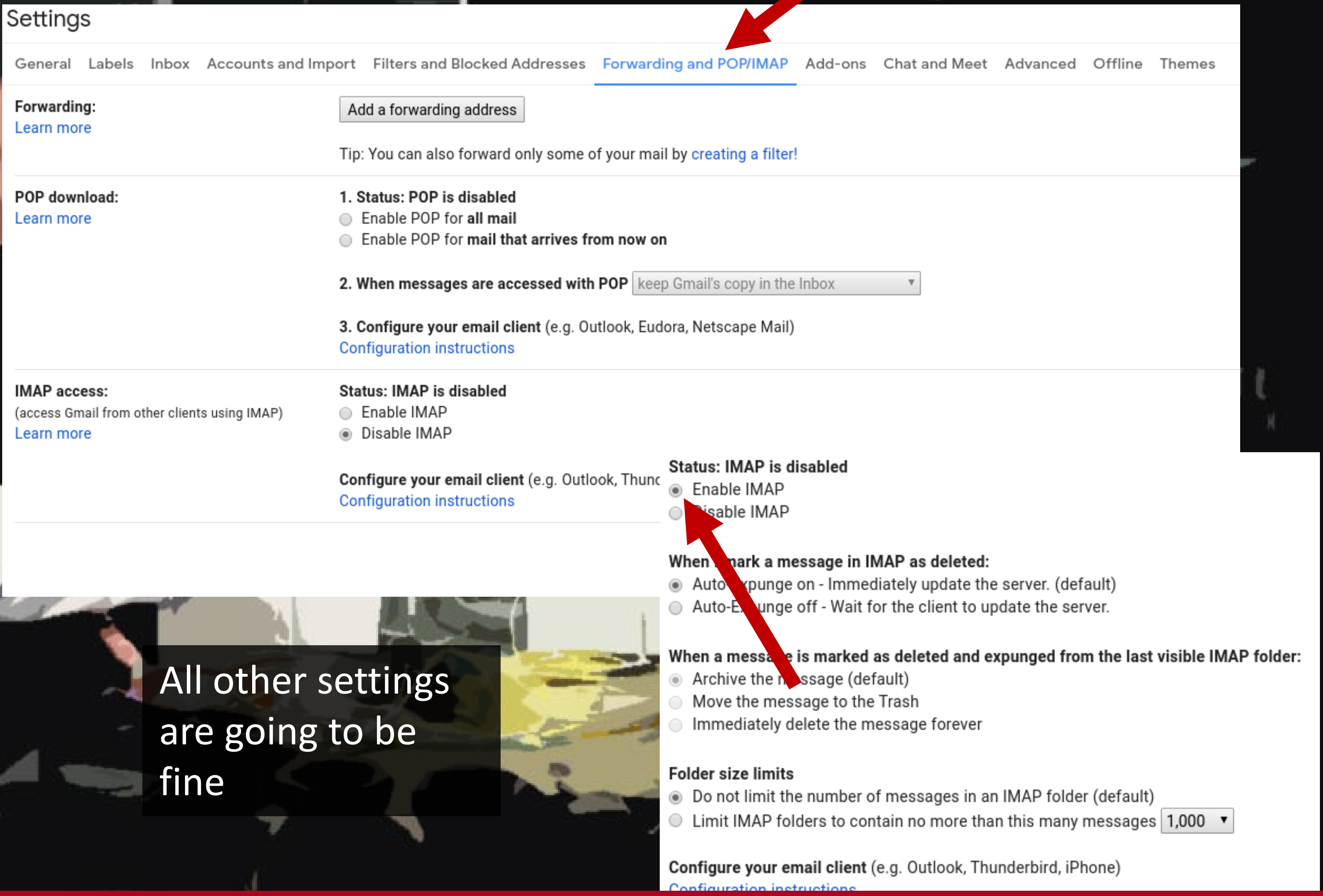
To protect your account, apps and devices that use less secure sign-in technology are blocked. To keep your account secure, Google will automatically turn this setting OFF if it's not being used. Learn more

HACKING POC

Part 3/4

SETTING UP GMAIL

Just so that we are clear, this should never be enabled for an account you care about. But if our goal is to send out phishing emails with malware then we can take this risk. Now go back into your Gmail and go to your settings and click on Forwarding and POP/IMAP and enable IMAP



Forwarding:
Learn more

Tip: You can also forward only some of your mail by creating a filter!

POP download:
Learn more

1. Status: POP is disabled
○ Enable POP for **all mail**
○ Enable POP for **mail that arrives from now on**

2. When messages are accessed with POP keep Gmail's copy in the Inbox ▾

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
Configuration instructions

IMAP access:
(access Gmail from other clients using IMAP)
Learn more

Status: IMAP is disabled
○ Enable IMAP
● Disable IMAP

Configure your email client (e.g. Outlook, Thunc
Configuration instructions

Status: IMAP is disabled
● Enable IMAP
○ Disable IMAP

When I mark a message in IMAP as deleted:
● Auto-Expunge on - Immediately update the server. (default)
○ Auto-Expunge off - Wait for the client to update the server.

When a message is marked as deleted and expunged from the last visible IMAP folder:
● Archive the message (default)
○ Move the message to the Trash
○ Immediately delete the message forever

Folder size limits
● Do not limit the number of messages in an IMAP folder (default)
○ Limit IMAP folders to contain no more than this many messages 1,000 ▾

Configure your email client (e.g. Outlook, Thunderbird, iPhone)
Configuration instructions

All other settings are going to be fine

HACKING POC

Part 4/4

SET UP ENVIRONMENT

Now let's clone our program located at https://github.com/The-packet-Board/Phish_Sender and we want to make sure we have:

- pyphish.py
- phish.txt
- notmalware.zip

If you don’t have it already make sure you install python-magic with the command:

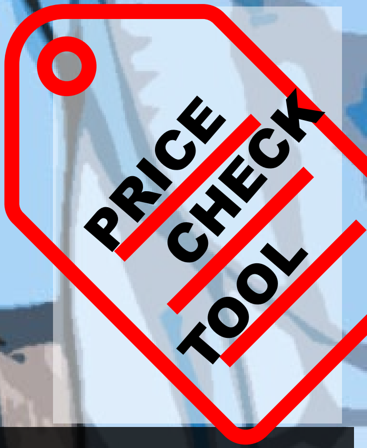
```
Pip install python-magic
```

Now everything is complete at this step we can edit the phish.txt which will be the HTML markup for our email content. I have included a quick template to use which includes The Packet logo in this example. And the commanded needed to send this out is as follows:

```
python pyphish.py --server smtp.gmail.com --port 587 --username youremail@gmail.com --password passwordwithno!@#$% --html phish.txt --subject 'BETA TEST' --sender youremail@gmail.com --sendto victim@gmail.com --start-tls --attachment notmalware.zip
```

So with this script the password must not include any special characters because it is not sanitizing the input. The rest I think is pretty easy to understand.

QUICK PROJECT



USE A BOT TO MONITOR PRICES

So I am a huge fan of everyone at HAK5 and the last time I was at DEFCON I almost got to say hello to Darren Kitchen and Shannon Morse, but I chickened out at the last moment. So if anything I looked like a creepy DEFCON stalker but that is in the past and today we move forward as the company HAK5 has the Elite Field kit with 16% off and that is exciting but $749.00 is a little much on a professors salary so I need to wait for a even larger discount.

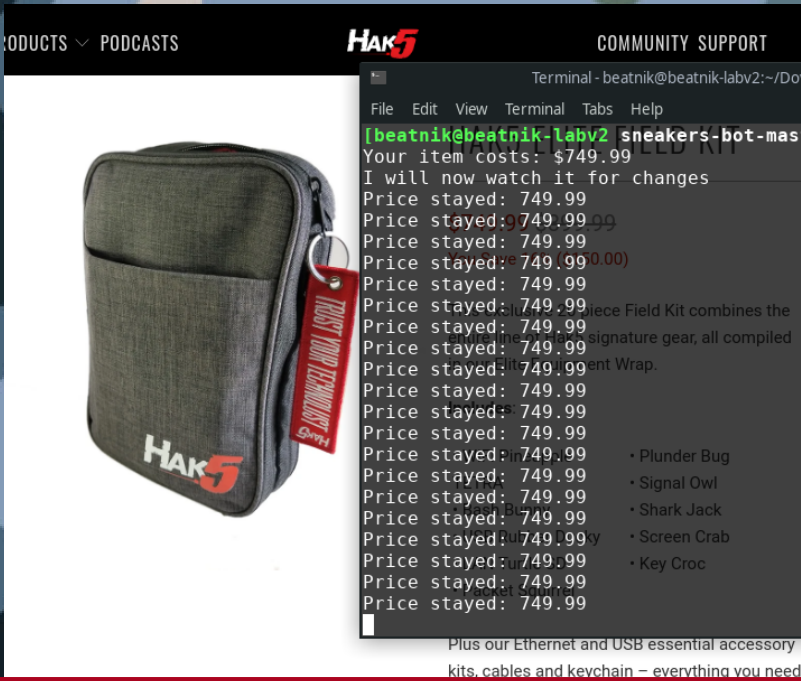
I can not refresh the site every day so I would like to set up some type of automation. Well me and my good friend selenium may just be the answer I am looking for. So first I need to get the appropriate chromedriver for my operating system. I am using Linux, so I just install the version that matches my instillation. Mac and Windows can download there version here. Next download main.py at our GitHub located here.

After that it is just pointing the program to the location of your chromedriver and letting it run. Once it detects a price change it will place an Alert in the command line. I have it set to check every 3 seconds, but you may wish to change this for your needs.

PRICE CHECK TOOL

EDIT THE BOT FOR YOUR USE

So if you wish to edit the bot to work for you only a few changes would need to be made. You would need to change the URL for what you want to monitor and then also change what the bot is looking for as well. I am searching for the price using find_element_by_class_name and you can use the selenium guide to help you find what your looking for here.


ODUCTS
PODCASTS
HAK5
COMMUNITY SUPPORT
Terminal - beatnik@beatnik-labv2:~/Do
File Edit View Terminal Tabs Help
• Plunder Bug
• Signal Owl
• Shark Jack
• Screen Crab
• Key Croc
Plus our Ethernet and USB essential accessory
kits, cables and keychain – everything you need

```
[beatnik@beatnik-labv2 sneakers-bot-mas
Your item costs: $749.99
I will now watch it for changes
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
Price stayed: 749.99
```

CYBER SECURITY HISTORY

FIRST BLACKHAT JULY 9, 1997

Blackhat or otherwise known as the Black Hat Briefings is a computer security conference that provides security consulting, training, and briefings to hackers, corporations, and government agencies around the world like DEFCON but with more of a cooperate angle. Blackhat was also funded by Jeff Moss who also founded DEFCON. Black Hat was acquired by CMP Media, a subsidiary of U.K.-based United Business Media (UBM) in 2005. I have never been to Blackhat but would love to go sometime in the future. Usually Blackhat is scheduled before DEFCON and many people who attend DEFCON also attend Blackhat. This is also known as the Hacker Summer camp which is one, I hope to attend once conferences are safe to attend one again. The conference is composed of three major sections: the Black Hat Briefings, Black Hat Trainings, and Black Hat Arsenal. The briefings cover various topics including reverse engineering, identity and privacy, and hacking. Training is provided by vendors and is a way to attend the conference and get some trainings as well with multiple peers who can offer insights and advice. The Arsenal is dedicated to giving researchers and the open source community a place to showcase their latest security tools. In the past, companies have attempted to ban researchers from disclosing vital information about their products, but this relationship has improved over the last few years.

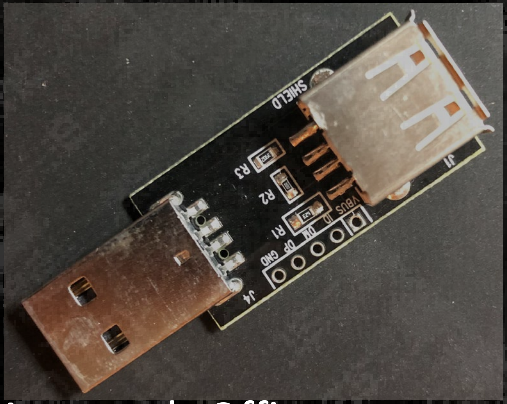
SIRCAM WORM JULY 17, 2001

So the worm W32.Sircam.Worm or otherwise known as SIRCAM became known to the world back in 2001 and targeted users running Windows 95, 98 and Me or Millennium edition. SIRCAM would choose random word documents and Excel files, infect them and send them to email contacts stored in the internal address book. Because of random files being chosen many personal and private files were sent to individuals who were known by the user. SIRCAM can also spread by open network shares on computers or shares with no password protection. For a year SIRCAM was on the top ten lists for viruses to watch out for. One interesting note however was due to a bug in the worm, the message was rarely sent in any form other than "I send you this file in order to have your advice." even thou it had 8 possible openers.

CYBER SECURITY DEFENSIVE PROTOCOL

PRACTICE SAFE SECURITY

We see what you do… You walk around town with your devices, and you'll plug them in just anywhere.



Into USB ports of the library computers…

Into the USB ports in the airport terminal…

Into a "friend's" laptop…

Well, in November 2019, Los Angeles' District Attorney's Office published an advisory to travelers about the potential dangers of public USB ports. These ports could be used for an attack that has been called juice-jacking.

'Juice Jacking' is a type of cyber attack where a USB port - typically masquerading as a charging port - doubles as a data connection, involving either the installation of malware or surreptitiously copying sensitive data from your device (this goes beyond simple keylogging).

In order to prevent this, you can use a USB Juice Jacking protector as a 'middleman' connection between your cable and the port you're connecting to. USB protectors do not physically possess data pins, allowing only the power pins to transfer electricity and completely restricting the transfer of data in either direction. The only downside? Many USB protectors do not have a charge setting resistor, so charge rates may be slightly slower. A worthwhile payoff when operating in an insecure environment.

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