THE PACKET

FALL

OCTOBER 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:

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

HOW EXCITING

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- 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 I hope you find this month filled with more treats than tricks as you finish up your 7 week 1 classes this semester. Welcome to the spooky edition of The Packet, as the leaves begin to change, and the nights become cooler we are once again reminded of the winter season soon approaching. Fall always feels like it goes away too soon so I will be sure to enjoy it as much as I can. October also has quite the history as it relates to cybersecurity. I remember the Mirai botnet attack against DynDNS which knocked out a lot of services for individuals on the east coast. The "alleged" author of the Mirai botnet posted on a forum that I frequented, and I never seen this user before. I found that to be so strange to be part of history in my own little way. The Marai botnet incident was simple and impressive at the time it was released. Being able to observe how a bot net is put together is interesting, as you are able to see the choices, they make to develop the malicious aspects of the final piece of malware. It should be noted that this is a rare event as many malware authors do not post their source code until much later if ever. That was quite a fun trick to release in the month of October. Our October edition of The packet also has a fun trick, a scary experience you can build against an unsuspecting victim making them believe they are installing a virus on there machine.

--- END MESSAGE ---

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

NEW MALWARE USES WINDOWS SUBSYSTEM FOR LINUX FOR STEALTHY ATTACKS

Security researchers have discovered malicious Linux binaries created for the Windows Subsystem for Linux, indicating that hackers are trying out new methods to compromise Windows machines. The finding underlines that threat actors are exploring new methods of attack and are focusing their attention on WSL to evade detection. The next step is to inject the malware into a running process using Windows API calls, a technique that is neither new nor sophisticated. From the small number of samples identified, only one came with a publicly routable IP address, hinting that threat actors are testing the use of WSL to install malware on Windows. "As the negligible detection rate on Virus Total suggests, most endpoint agents designed for Windows systems don't have signatures built to analyze ELF files, though they frequently detect non-WSL agents with similar functionality" - Black Lotus Labs. One of the variants, written completely in Python 3, does not use any Windows API and seems to be the first attempt at a loader for WSL. It uses standard Python libraries, which makes it compatible with both Windows and Linux. Black Lotus Labs assesses that the WSL malware loaders are the work of a threat actor testing the method from a VPN or proxy node.

CYBERATTACKS AGAINST THE AVIATION INDUSTRY LINKED TO NIGERIAN THREAT ACTOR

Researchers have unmasked a lengthy campaign against the aviation sector, beginning with the analysis of a Trojan by Microsoft. On May 11, Microsoft Security Intelligence published a Twitter thread outlining a campaign targeting the "Aerospace and travel sectors with spear-phishing emails that distribute an actively developed loader, which then delivers RevengeRAT or AsyncRAT.". Cisco Talos researchers Tiago Pereira and Vitor Ventura published a blog post on Thursday documenting the scheme, dubbed "Operation Layover," which has now been linked to an actor that has been active since at least 2013 - and has been targeting aviation for at least two years. In addition to Microsoft's investigation, the cybersecurity company has established connections between this threat actor to campaigns against other sectors, spanning over the past five years. Based on passive DNS telemetry, the team believes the threat actor is in Nigeria, due to 73% of IPs connected to hosts, domains, and the attacks at large originate from this country. The threat actor has also been linked to crypter purchases from online forums, email addresses, and phone numbers, although these findings have not been verified. The malware identified as CyberGate has since been replaced with AsyncRAT in recent campaigns, with over 50 samples detected that are communicating with a command-and-control server used by the threat actor.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

ROMANCE SCAMMERS MAKE $133M IN FIRST HALF OF 2021

Over $133m has already been lost this year to romance scams, with victims increasingly urged to invest in fraudulent cryptocurrency opportunities, according to the FBI. A new Public Service Announcement was published yesterday revealing that the FBI Internet Crime Complaint Center received over 1,800 complaints from January 1 to June 31 this year, resulting in soaring losses for victims. Victims are typically approached on dating and social media sites, where the scammer establishes a relationship with them designed to build confidence. In time, the scammer will share information on a new cryptocurrency investment or trading opportunity, which is claimed to generate significant profits, according to the FBI. The victim is then directed to a scam website where they hand over some money for the investment. "After the successful withdrawal, the scammer instructs the victim to invest larger amounts of money and often expresses the need to 'act fast.' When the victim is ready to withdraw funds again, the scammers create reasons why this cannot happen," the Public Service Announcement continued. "The victim is informed additional taxes or fees need paid, or the minimum account balance has not been met to allow a withdrawal. This entices the victim to provide additional funds. Sometimes, a 'customer service group' gets involved, which is also part of the scam. Victims are not able to withdraw any money, and the scammers most often stop communicating with the victim after they cease to send additional funds.“ Romance scams are a perennial money-maker for fraudsters. The addition of a cryptocurrency element taps into a growing parallel trend of scammers making money from eager investors looking to get rich quickly.

PHISHERS IMPERSONATE US DOT TO TARGET CONTRACTORS

A new phishing campaign has been uncovered targeting companies that may work with the US Department of Transportation. The campaign, discovered by security company INKY, found that phishers are impersonating the US Department of Transportation to harvest Microsoft Office 365 credentials, INKY's Roger Kay wrote in a blog post. Kay noted that the phishing emails peaked around August 16-18, right after the US Senate passed the $1 trillion infrastructure bill on August 10. Dozens of phishing emails sought to impersonate the DOT, with attackers contacting multiple companies in the engineering, energy architecture industries asking them to submit bids for federal contracts. "The basic pitch was, with a trillion dollars of government money flowing through the system, you, dear target, are being invited to bid for some of this bounty," Kay said. "By creating a new domain, exploiting current events, impersonating a known brand, and launching a credential harvesting operation, the phishers produced an attack just different enough from known strikes to evade standard detection methods.“ The phishers made their website look legitimate by copying the HTML and CSS from the real USDOT website.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

BOT ATTACKS GROW 41% IN FIRST HALF OF 2021

A new cybercrime report from LexisNexis Risk Solutions has found that bot attacks are up significantly in 2021, growing by 41% in the first half of the year. The biannual report found that the financial services industry and media businesses are facing the brunt of bot attacks while human-initiated attacks fell by 29%. According to the report, financial services companies saw 683 million bot attacks from January to June, while media companies dealt with 351 million, up 174% year over year. LexisNexis Risk Solutions researchers wrote that the United States still leads the way as the largest originator of automated bot attacks by volume, followed by the UK, Japan, Canada, Spain, Brazil, Ireland, India, Mexico and Germany. Bot attacks increased worldwide, with every region recording growth in bot volume in the first half of 2021. Financial services companies are increasingly attacked through payment transactions, which "Continue to be attacked at a higher rate than any other industry." Media companies also face a significant number of new account creation attacks, with criminals using media organizations to test stolen identity data. The report notes that there has also been an increase in attacks on cryptocurrency wallets. "Where fraud had been so heavily targeted on COVID-related stimulus packages and related scams, how will this approach evolve as support is wound up and economies start to rebuild? Will fraudsters start to capitalize on the fruits of their bot labors and use validated credentials in higher-volume human-initiated attacks?" the researchers wrote.

GOOGLE ADDRESSES A NEW CHROME ZERO-DAY FLAW ACTIVELY EXPLOITED IN THE WILD

Google Chrome 93.0.4577.82 for Windows, Mac, and Linux that addressed eleven security issues, including two zero-days actively exploited. Google released Chrome 93.0.4577.82 for Windows, Mac, and Linux that fixed eleven security issues, including two zero-days vulnerabilities actively exploited in the wild. This is the tenth zero-day vulnerability in Chrome fixed by Google that was exploited in attacks in the wild. Both zero-day vulnerabilities fixed in Chrome 93.0.4577.82 were disclosed to Google on September 8th, 2021. Google did not provide details about the attacks either information about the threat actors exploiting the vulnerabilities. The two zero-day flaws could be exploited to trigger a DoS condition and under specific circumstances they can allow attackers to escape the sandbox, perform remote code execution, and carry out other malicious activities. Google urges its users to update their Google Chrome installs to the latest version immediately.

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

HOW ATTACKERS INVEST IN CLOUD-FOCUSED CYBERCRIME

Attackers appear to be in lockstep with enterprise organizations in the march to the cloud - but with an entirely different set of objectives, research shows. The team's research shows attackers have sharply increased their focus on cloud targets as enterprises accelerated their adoption of SaaS, IaaS, and PaaS over the past year. One of the most troubling signs of increased attacker interest, researchers say, is a thriving black market for stolen credentials used to access enterprise accounts and resources on public cloud platforms. IBM X-Force discovered some 30,000 cloud credentials potentially available for sale on Dark Web forums. More than 70% of credentials advertised for sale offered Remote Desktop Protocol access to cloud resources. The factors influencing prices for cloud access credentials include the level of access a credential potentially offers - privileged access credentials were pricier than those offering less privileged access - and the amount of credit associated with an account. We saw sellers offering 7-to-14-day refunds if buyers weren't able to access the cloud environment using the purchased compromised accounts.“ DeBeck says the growing investment in cloud malware among attackers is particularly interesting. "This indicates to me that threat actors realize cloud is where things are going and they're investing accordingly, and that means that cloud security will continue to be critical."

GENERAL PROMISES US 'SURGE' AGAINST FOREIGN CYBERATTACKS

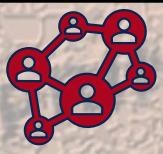
The general who leads U.S. efforts to thwart foreign-based cyberattacks, and punish those responsible, says he's mounting a "Surge" to fight incursions that have debilitated government agencies and companies responsible for critical infrastructure. In an interview Tuesday with The Associated Press, Gen. Paul Nakasone broadly described "An intense focus" by government specialists to better find and share information about cyberattacks and "Impose costs when necessary." Those costs include publicly linking adversarial countries to high-profile attacks and exposing the means by which those attacks were carried out, he said. Nakasone jointly leads the National Security Agency, the chief intelligence agency tracking foreign communications, and U.S. Cyber Command, the Pentagon's force for offensive attacks. President Joe Biden directly pressed Russian President Vladimir Putin in July to act against cyber attackers, telling reporters, "We expect them to act if we give them enough information to act on who that is.“ Nakasone also oversees efforts to track and stop foreign efforts to influence U.S. elections. Biden said in July that Russia had already begun efforts to spread misinformation regarding the 2022 midterm elections, calling them a "Pure violation of our sovereignty." Nakasone declined to detail allegations against Russia, saying intelligence agencies were "Generating insights which will move to sharing information in the not-too-distant future.“ U.S. agencies are not aware of any specific threats related to the California gubernatorial recall election that concludes Tuesday, Nakasone said.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

'NO INDICATION' RUSSIA HAS CRACKED DOWN ON RANSOMWARE GANGS

The FBI's No. 2 on Tuesday said the agency has seen no evidence that the Russian government has moved against ransomware gangs operating on its soil. "Based on what we've seen, I would say there is no indication that the Russian government has taken action to crack down on ransomware actors that are operating in the permissive environment that they've created there" since bilateral talks began with the Biden administration earlier this year, FBI deputy director Paul Abbate said during a panel discussion at a summit in National Harbor, Maryland hosted by the AFCEA International and the Intelligence and National Security Alliance. He added that the U.S. has asked for "Help and cooperation" with those cybercriminals it knows to be operating inside of Russia, including those who have indictments against them, but received nothing in return. Abbate's comments are the strongest yet by a senior administration official that the Kremlin is ignoring President Joe Biden's request to crack down on ransomware groups following his one-on-one meeting with Russian President Vladimir Putin. He publicly vowed that if they were struck by Russian-based cybercriminals, the U.S. would respond. White House officials in recent weeks have refrained from attributing a recent lull in ransomware attacks to actions by Putin's government. U.S. Cyber Command chief Army Gen. Paul Nakasone demurred when asked if the time had come for Washington to strike back at Moscow.



SSID STRIPPING: NEW METHOD FOR TRICKING USERS INTO CONNECTING TO ROGUE APS

A team of researchers has identified what appears to be a new method that malicious actors could use to trick users into connecting to their wireless access points. According to the researchers, SSID Stripping affects devices running Windows, macOS, Ubuntu, Android and iOS. They showed how an attacker could manipulate the name of a wireless network, specifically the SSID, so that it's displayed to the user with the name of a legitimate network. Attacks often involve the attacker setting up a rogue AP that has the same name as a connection typically used by the target. Operating system vendors have implemented protections designed to prevent users from unwittingly connecting to rogue APs by matching not only the name of a connection but also other attributes before automatically connecting to it. In an SSID Stripping attack, the user would see a connection whose name matches a connection they trust, but they would have to manually connect to it for the attack to work. On the other hand, this bypasses the security controls since the device processes the actual name of the SSID - the string that the attacker has entered, not what the victim sees on the screen - and does not prevent the victim from connecting to the rogue AP. The researchers described their findings as a vulnerability, but impacted vendors don't seem to view it as a serious security issue. AirEye has released a free tool that can be used by organizations to assess the susceptibility of corporate devices to SSID Stripping attacks.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

MYSTERIOUS WIPER PARALYZES IRANIAN TRAINS WITH EPIC TROLL

On July 9, 2021, an apparently politically motivated cyber attack targeted the Islamic Republic of Iran Railways, executed by a non-state sponsored actor dubbed "Indra." The attackers produced false displays of passenger trains' operational information, indicating cancelations or citing their status as "long delayed because of cyberattack." Further, the hackers sought to cause disruption and embarrassment to the Iranian government as the false displays instructed passengers to direct their complaints to the office of the Iranian Supreme Leader, Ali Khamenei, and provided a phone number. A second cyber attack occurred the next day on July 10, targeting and reportedly crippling the performance of websites of Iran's Ministry of Roads and Urbanization.

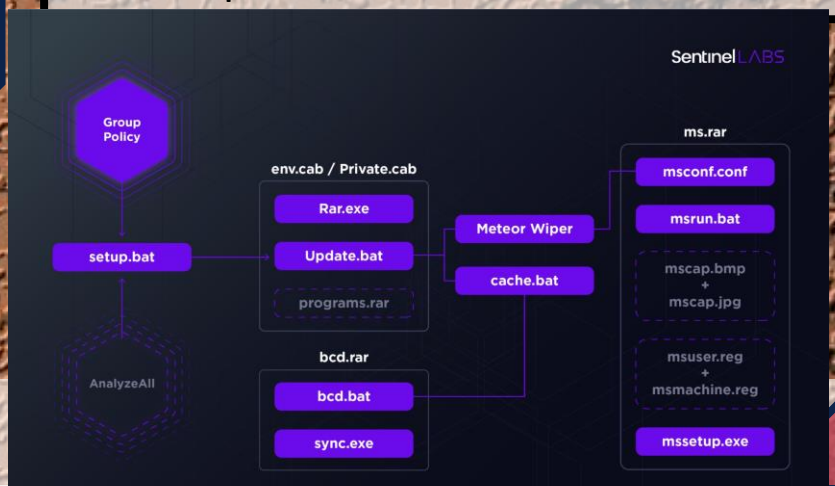
- Evidence indicating the success of this attack spread across social media with depiction of a computer monitor with an image stating, "We attacked the computer systems of the Railway Company and the Ministry of Roads and Urban Development."
- Further, images posted on social media depicted a monitor of one of the hacked computers – through which responsibility was claimed for the consecutive attacks.

The attacks, which research firm SentinelLabs tracked under the codename of MeteorExpress based on the artifacts found in the code, did cause cancelations and delays of trains across Iran. Another researcher based in Iran, Amnpardaz Software, published a short technical analysis of a piece of malware that is possibly related to these attacks, dubbed Trojan.Win32.BreakWin.

- Indra was first identified in 2017. According to its social media posts, this hacktivist group targets any organizations that have trading relations with the current Iranian regime.
- September 2017: Indra targeted the Al-Fadhl Exchange based on the asserted claim that the Iranian company supported terrorism using the funds of its customers.
- February 13, 2018: Indra disclosed flight and passenger information of the Syrian Cham Wings airline, which, according to the hacking group, had been used Iranian supporters of terrorism to travel in the region.

Several dark web social media services are reporting that there may be an alternative cyber threat actor responsible for the attacks on the Iranian Railway – a previously unknown ransomware group identifying as "MBC" or "MBC Ransomware.". Indra's official twitter account had not posted any claims of responsibility as of the date of this advisory. All accounts associated with Indra went silent after November 2020.

The type of malware used in the Iranian attacks is referred to as a "wiper" since its main goal is to delete files and data to cause business and operational disruptions. This malware is not commonly used as part of a criminal enterprise, but rather for more destructive and usually politically motivated operations.



SIGN UP FOR CLASSES SOON

FALL SCHEDULE 2021

NOTES FROM YOUR ADVISORS

FALL 2021 ENROLLMENT IS CURRENTLY OPEN FOR 2nd 7 WEEK COURSES. 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

FALL SCHEDULE 2021

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 OCTOBER 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.

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
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

THE LINUX KERNEL WAS RELEASED BY LINUS TORVALDS

The Linux kernel was released by Linus Torvalds. "I can (well, almost) hear you asking yourselves "why?"... "This is a program for hackers by a hacker. I've enjouyed doing it, and somebody might enjoy looking at it and even modifying it for their own needs. It is still small enough to understand, use and modify, and I'm looking forward to any comments you might have.

OCTOBER 4, 1991

FIRST HACKER AIRED ON UNSOLVED MYSTERIES

On June 1, 1990, Poulsen took over all the telephone lines for Los Angeles radio station KIIS-FM, guaranteeing that he would be the 102nd caller and win the prize of a Porsche 944 S2. When the Federal Bureau of Investigation started pursuing Poulsen, he went underground as a fugitive. In June 1994, Poulsen pleaded guilty to seven counts of conspiracy, fraud, and wiretapping

OCTOBER 10, 1990

RELEASE OF SMURF - THE FIRST DDOS ATTACK TOOL

The `smurf' attack is quite simple. It has a list of broadcast addresses which it stores into an array, and sends a spoofed icmp echo request to each of those addresses in series and starts again. "When it was written I was not aware of the fact that a) the world would get its hands on it and b) it would have such a destructive effect on the computers being used to flood. My ignorance is my mistake. I extremely regret writing this, but as you well know, if things aren't `exploited' then they aren't fixed."

OCTOBER 11, 1997

RESPONSIBLE DISCLOSURE VS.INFORMATION ANARCHY

Scott Culp of Microsoft published his essay "It's Time to End Information Anarchy", criticizing public disclosure of exploit details. "If we can't eliminate all security vulnerabilities, then it becomes more critical that we handle them carefully and responsibly when they're found. Yet much of the security community handles them in a way that fairly guarantees their use, by following a practice that's best described as information anarchy. This is the practice of deliberately publishing explicit, step-by-step instructions for exploiting security vulnerabilities, without regard for how the information may be used". "This is not a call to stop discussing vulnerabilities. Instead, it is a call for security professionals to draw a line beyond which we recognize that we are simply putting other people at risk. By analogy, this isn't a call for people for give up freedom of speech; only that they stop yelling "fire" in a crowded movie house."

OCTOBER 15, 2001

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

CYBER SECURITY HISTORY

"HOW TO WRITE BUFFER OVERFLOWS" - PUBLISHED

Mudge published "How to Write Buffer Overflows", one of the first papers about buffer overflow exploitation. "This is really rough, and some of it is not needed. I wrote this as a reminder note to myself as I really didn't want to look at any more AT&T assembly again for a while and was afraid, I would forget what I had done." "If you are an old assembly guru then you might scoff at some of this... oh well, it works and that's a hack in itself."

OCTOBER 20, 1995

DDOS ATTACK ON DYN DNS

The Mirai botnet was used in multiple large-scale DDoS attacks against DNS provider Dyn, making high-profile sites such as CNN, Comcast, GitHub, Netflix, PayPal, Reddit, Shopify, Slack, Twilio, and Twitter unreachable to many. Mirai is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of a botnet in large-scale network attacks.

OCTOBER 21, 2016

RELEASE OF FRIENDGREET WORM, YOU AGREE TO SEND IT

The worm-like Friendgreet propagated by emailing all Outlook recipients. The twist was that the software presented a EULA stating it would do that. If users follow the link in the email, they are invited to install an application onto their computer. Two lengthy end-user license agreements (EULA) are displayed, the second of which states that by installing the application the user is giving permission to send a similar greeting card to all addresses found in the user's Outlook address book.

OCTOBER 24, 2002

U.S. CYBER COMMAND ATTAINED FULL OPERATIONAL CAPABILITY

The creation of USCYBERCOM marked the culmination of more than a decade's worth of institutional change. DoD defensive and offensive capabilities were now firmly linked, and, moreover, tied closely, with the nation's cryptologic system and premier information assurance entity, the NSA. That interlocking set of authorities, personnel, and organizations would also be better able to partner with both the geographic combatant commands and other U.S. Government agencies to defend the nation in cyberspace and ensure its freedom to maneuver in this new and challenging domain.

OCTOBER 31, 2010

>. SYS_ALERT

>. RECRUITMENT CHALLENGE

≥ **FINIS CORONAT OPUS:** LATIN FOR "THE END CROWNS THE WORK". THE NEW ORGANIZATION CALLED SAGUARO POD IS INTENDED TO GIVE UNDERGRADUATE STUDENTS BOTH REMOTE AND LOCAL THE OPPORTUNITY TO TAKE PART IN RESEARCH TOPICS RELATED TO CYBER-SECURITY. STUDENTS WOULD BE ENCOURAGED TO DEVELOP RESEARCH WHICH WILL BE PRESENTED AT VARIOUS CONFERENCES RELATED TO THE INFORMATION SECURITY FIELD.

≥ **REQUIREMENTS:**

- ≥ MUST BE STUDENT OF UNIVERSITY OF ARIZONA
- ≥ STUDENT MUST MAINTAIN GOOD ACADEMIC STANDING
- ≥ STUDENT MUST PUBLISH RESEARCH / ARTICLES
- ≥ STUDENT MUST ATTEND 2 MEETINGS A MONTH OVER ZOOM

≥ **OCTOBER 31ST APPLICATION DEADLINE**

- ≥ CURRENT MEMBERS CAN INVITE ANOTHER BY VOUCHING FOR THE INDIVIDUAL

FINIS CORONAT OPUS

SAGUARO_POD

SYS_ALERT.<

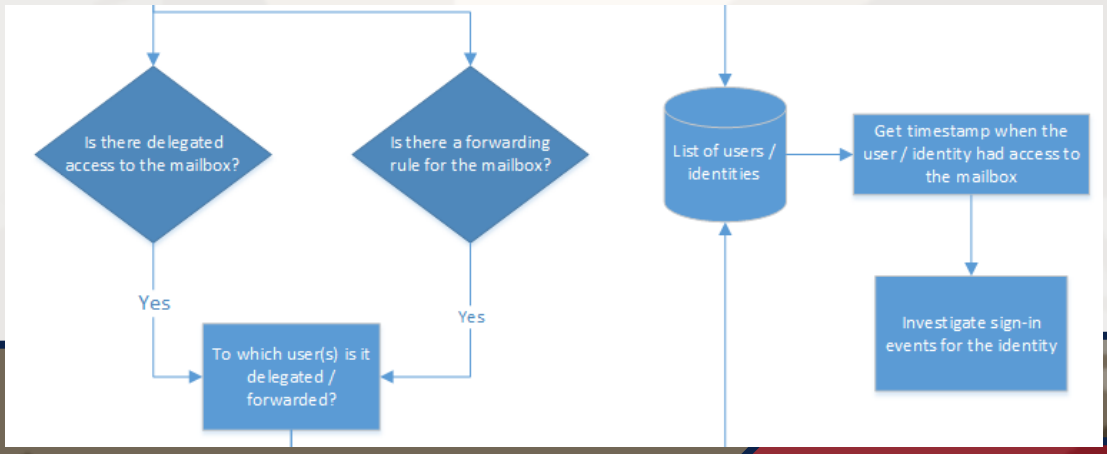
SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

In the information security world, you would be expected to weigh in on a variety of issues. From the development of policy, secure coding techniques, IT infrastructure management and my personal favorite, other duties as assigned. Sometimes you need to have a ready built guide of how t0 handle various situations, and I would like to introduce you to the world of Incident Response Playbooks. What do you do when you don't know what to do? Well, you consult an expert in the field and what better expert then the experienced individuals over at Microsoft. In this article we will look at the Microsoft incident response playbook for a Phishing investigation.

Microsoft breaks its playbooks up:

- **PREREQUISITES: Covers the specific requirements you need to complete before starting the investigation**
- **WORKFLOW: Shows the logical flow that you should follow to perform this investigation.**
- **CHECKLIST: Contains a list of tasks for each of the steps in the flow chart. This checklist can be helpful in highly regulated environments to verify what you have done or simply as a quality check for yourself.**
- **INVESTIGATION STEPS: Includes a detailed step-by-step guidance for this specific investigation**

For many of these steps, the focus is more on Microsoft products and what advantages an active directory environment allows. These already developed checklists and flow charts; however, these can be adopted to work with any environment and used as a starting framework.



HACKING POC

1/3

LET'S FAKE A VIRUS INSTALL

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

Halloween is upon us, and it is time for us to explore our spooky side. We are not talking about a scary movie or trick-or-treating, no, we are going to make an unsuspecting user believe they are installing a virus on there machine. Now you do not need any coding knowledge whatsoever for this project, and you could even use my GitHub Repo as a template and change a few parts to make it your own unique twist. So first, lets talk a little about what we are doing here today, we are going to play around with the concept of SCAREWARE. We are going to modify our version to be a little less malicious and more "fun", but Wikipedia defines scareware as "A form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software. Scareware is part of a class of malicious software that includes rogue security software, ransomware and other scam software that tricks users into believing their computer is infected with a virus, then suggests that they download and pay for fake antivirus software to remove it". Now we will not create anything to cause a form of extortion, but we will make use of the next defining sentence "The "scareware" label can also apply to any application or virus which pranks users with intent to cause anxiety or panic". And this is what we plan to do, just enough to cause some light anxiety or panic in the pursuit of having fun.
Our plan at this point is simple, we need to develop something that looks like it is doing something "wrong" without it really doing anything. So, the programs logic does not need to do anything real. We also don't want to create a program and must worry about dependencies, so we are going to keep it simple, lets make a webpage and make it look real!

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!!

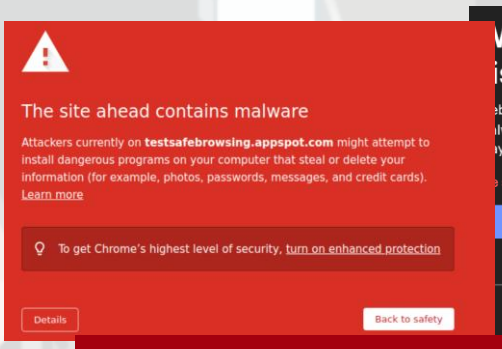
2/3

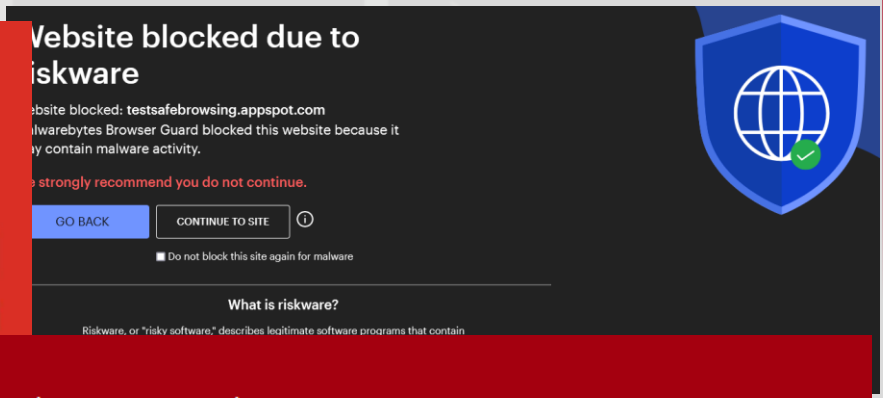
LET'S FAKE A VIRUS INSTALL

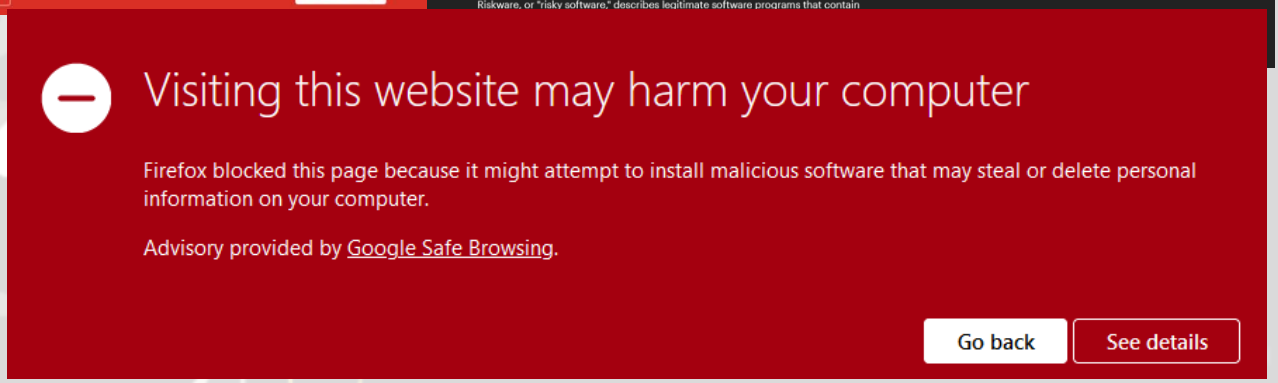
IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

The first thing we are going to do is select a background image, at this point we need this part to look 'real enough' for our trick to work. We just need something eye catching to alert our victim. Google has a malware test site that is used to test the internal Chrome malware defenses. Basically, Google has flagged a legitimate site to test its software as needed. The background image will just mimic this content and I will turn it into an image. If you have other browser guards like Malwarebytes or others, they also use these same testing platforms and look somewhat similar.







Depending on your browser, your warning may be different, but most browsers will have some type of built-in protection and as far as I could tell they all use the same test site.

3/3

LET'S FAKE A VIRUS INSTALL

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

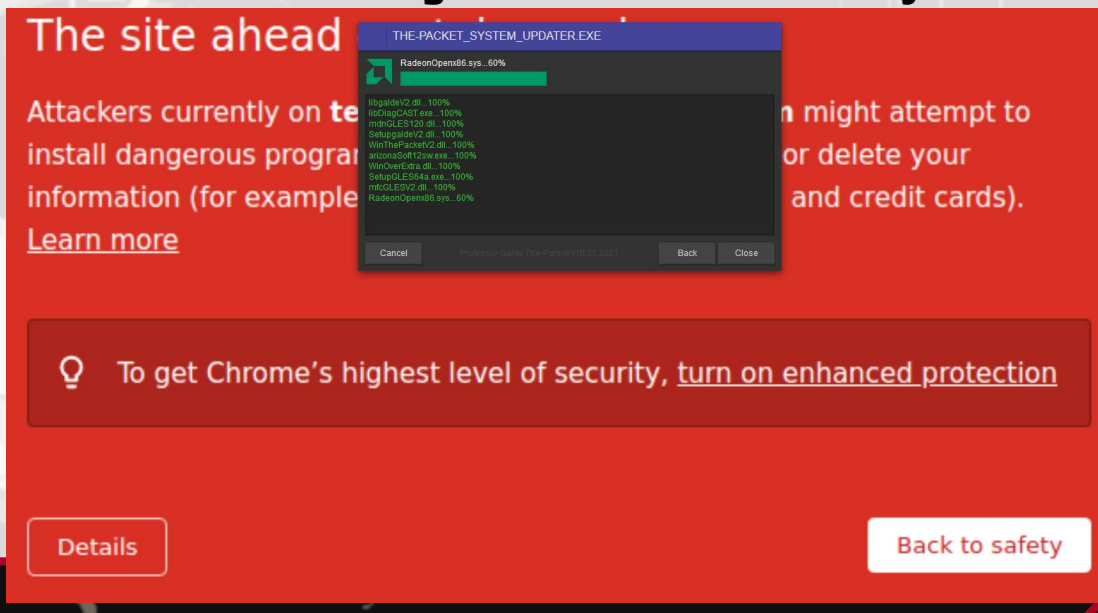
HACKING POC

Next, we are going to copy the index.html page and make a few edits after the <head> tag. First under the tag, , this is going to be our fake viruses program name. I have named mine: THE-PACKET_SYSTEM_UPDATER.EXE
next we have a few fake malware sounding names that will be loaded, feel free to add more or leave these be.

Next, we have the lower portion of the buttons that don't do anything like close, cancel and back, and then my personalization with my name to claim my stake into this visualization.
Next, we have an array we can manipulate to make our virus more unique and "dangerous" looking. Under the array labeled nameData feel free to change or add data to this array. When it runs, it will pretend to install these items and randomly mix the names together.

```
var nameData = {
   prefix: ['Win', 'Qt', 'Radeon', 'AMD', 'Setup', 'lib', 'mfc', 'ms', 'mdn', 'arizona'],
   word: ['ThePacket', 'Installer', 'GLES', 'Soft', 'Diag', 'Over', 'vcr', 'Open', 'Light', 'galde'],
   suffix: ['Installer.exe', 'Extra.dll', '64a.exe', 'V2.dll', '12sw.exe', 'x86.sys', '120.dll', 'CAST.exe']
}
```

In the Suffix section, make sure to include something like a .exe or .dll at the end to make it look more real. Now all we need to do is get our victim to click on our link and they will freak out that their system appears to be downloading the next version of 0-day malware.



>. 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.

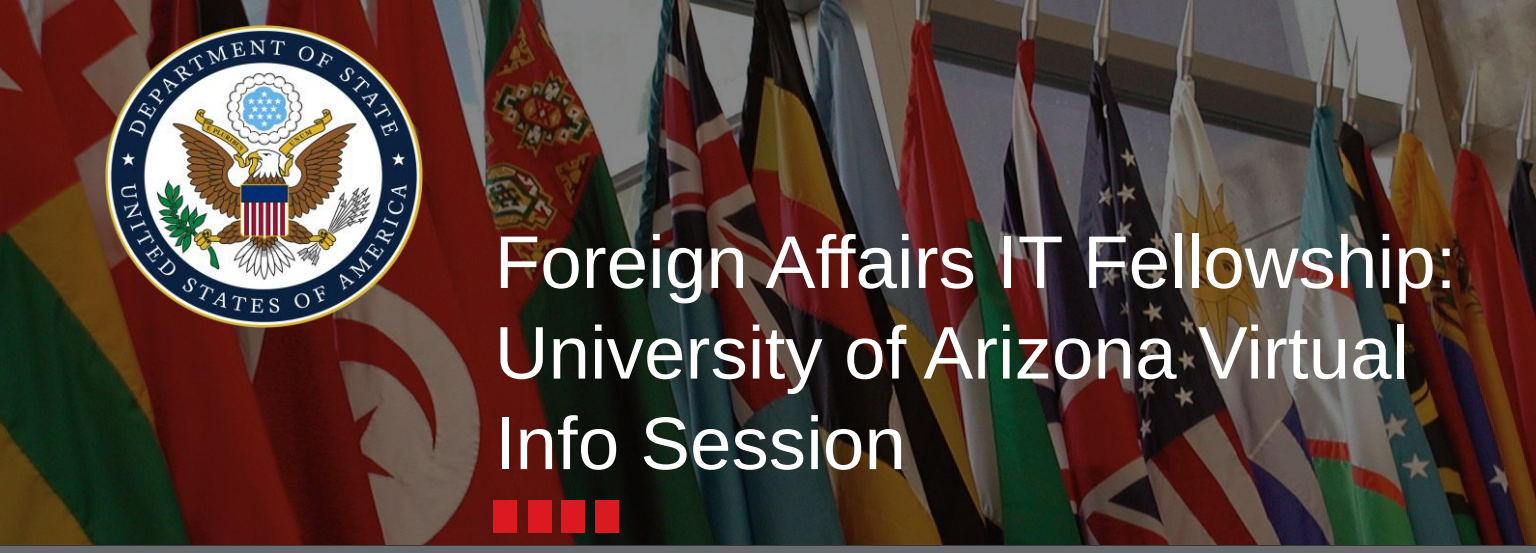
≥ THE CYBER-PHYSICAL SYSTEMS GROUP AT MIT LINCOLN LABORATORY CONDUCTS RESEARCH TO UNDERSTAND THE CYBERSECURITY IMPLICATIONS OF THESE PHYSICAL INTERFACES AND USE THE RESULTS OF OUR RESEARCH TO DEVELOP PROTOTYPES THAT SERVE AS PATHFINDERS FOR FUTURE TECHNOLOGICAL SOLUTIONS.

≥ 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



Foreign Affairs IT Fellowship: University of Arizona Virtual Info Session

We are excited to host a virtual info session with the Foreign Affairs Information Technology (FAIT) Fellowship program to present a unique opportunity for qualified students to get academic funding, internships, and a career in Foreign Service.

Foreign Affairs IT Fellowship: University of Arizona

Tuesday, October 5th, 2021 – 4 pm (MST)

REGISTER TODAY

The FAIT Fellowship, a two-year program funded by the U.S. Department of State, is a path to a career in the Foreign Service for students in IT-related degree programs The Fellowship provides up to $75,000 in academic funding total for your junior and senior years of college, or a two-year master's degree program. Plus, FAIT Fellows will have two summer internships (with stipends) and receive professional development and mentorship. Upon successful completion of the program and the State Department requirements, FAIT Fellows receive an appointment in the Foreign Service as a full-time Information Management Specialist.

With the goal of attracting top technology talent and increasing diversity in the Foreign Service, the program values varied backgrounds, including ethnic, racial, gender, and geographic diversity. Women, members of minority groups underrepresented in the Foreign Service, and those with financial need, are encouraged to apply.

If you would like to travel the world and use technology skills to support U.S. diplomacy, the FAIT Fellowship is an opportunity of a lifetime. Register now!

FOREIGN AFFAIRS IT Fellowship

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

NETWORK COMPUTING RESOURCES MANAGER

The Computing Resources Manager/Network Manager will play a unique role in enabling NSA to effectively execute its mission, supplying customers with advanced computing resources, and global networking. The Computing Resources Manager/Network Manager assists in the planning, designing, managing the configuration, identifying network faults, restoring service after faults occur, and the performance and security of operational networks.

Salary Range: $73,076 - $91,057 (Entry/Developmental)

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

CYBER SECURITY SUMMER INTERN 2022

Verizon's Corporate Information Security team protects Verizon's global operations, assets, stakeholders, and intellectual property from cyber security threats by proactively leveraging threat intelligence, advanced security processes, and technologies to reduce the number of incidents that affect Verizon and maintaining constant vigilance, monitoring, and response to rapidly minimize the impact of incidents that do occur.

- Current enrollment in a Bachelor's/Master's degree program in: Information Systems, Information Security, Computer Science, Cyber Security, Data Analytics, Business IT, or related majors with an expected completion date between December 2022 and June 2023.
- Authorization to work in the U.S. without restrictions or need for future sponsorship.
- Willingness to work remotely.

CYBERSECURITY OPERATIONS ANALYST INTERN

ANDURIL

As a cybersecurity operations analyst intern, you will be sitting on the front lines of defending Anduril against determined cyber adversaries. This is a remote position. You'll investigate alerts across a wide spectrum of systems, including corporate, cloud, command and control environments, product telemetry, and everything in between. Your efforts will keep our company, people, and products safe from attackers' intent on stealing intellectual property and sabotaging our operations.

- Triage and investigate potential computer security incidents.
- Analyzes security logs from a variety of sources to include corporate, cloud, and operational networks.
- Proactively hunt for threats across Anduril's environment.
- Research emerging attacker tradecraft and engineers robust monitoring and detection logic to mitigate.

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 OCTOBER 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.

HIGHLIGHT OF CURRENT AND FORMER STUDENTS, WHERE THEY ARE AND WHERE THEY ARE GOING

STUDENT INTERVIEW

1/3

INTERVIEW OF AGNEL DSILVA

I am honored to introduce Agnel Dsilva who was a student who recently graduated from the Cyber Operations program. Agnel works for the City of Danville in the state of Illinois. I was able to schedule a quick email exchange to pick their brain on a few topics of related to where they came from, how they discovered cyber and how they liked the program. So first, I know not everyone wants to do Cybersecurity when they are born so its always interesting to see how this evolves.

So Agnel, first off, what did you want to be when you grew up as a child and what made you want to be in cybersecurity?

I wanted to be a Chemical Engineer when I grew up. This changed when I enrolled myself in some computer programming classes during my high school days. I was curious about how computers really worked. I continued my quest and ended up getting a degree in computer science. I started working as a computer technician since I loved fixing computers. Over the years, I continued my education and acquired several IT certifications in Networking and Security. I worked for the Hewlett Packard company in India as a Network Engineer implementing Novell Netware (Network OS). I started looking into Cybersecurity in 2018. One of our department's networks was a victim of a EMOTET Malware. Fortunately, we were able to contain the malware and the incident did not result in a breach or data loss. I had very little experience on how to handle a situation like this. It took us a couple of months to fully recover from this attack. I started doing some research on Cybersecurity training. I came across UofA's Cyber Operations program and was impressed with the curriculum. I am glad that I picked UofA for my Cybersecurity education. The hands-on experience at UofA helped me improve my cybersecurity skills.

2/3 INTERVIEW OF AGNEL DSILVA

That is so interesting to see why you started from and where you have ended up so far, If you could talk to your self-10-ish years ago, what would you say?

If I had to go back 5-10-ish years ago, I would tell myself I am never getting old "mentally". Age is just a number. If you believe in yourself, there is no limit on what you can achieve. That is always a good reminder, don't quit and keep moving forward to your dreams.

So, during your time in the cyber operations program, what topic in cybersecurity was your favorite and what were you not so excited for?

For me most topics in Cybersecurity are important. My favorite topic is Social Engineering. I put myself in the shoes of social engineers and find ways to bypass our security controls. This helps in improving our cybersecurity posture.

You are working for the city of Danville, Illinois, any advice for others that would also like to work in city government?

Working for City government is both a fulfilling and rewarding job. There are so many challenges that come your way, but at the end it makes you proud of your accomplishments. The best part of working for local government is that we serve the people in our community. When I am out and about in the community, people recognize me, and they appreciate what we do.

Do you have any funny stories from your work experience related to your infosec career so far?

One thing that makes me laugh is a pen test engagement that I was involved during our monthly tests. I dropped off several USB drives in the strategic areas in various city buildings. These USB drives contained files that had non-malicious Macros. If a user plugged in one of these USB drives into their workstations and opened any of these documents, it would trigger a macro that would relay their user id, IP address and computer name to my alerting system. The funny thing was that our maintenance staff would pick these up and bring them back to the IT department.

3/3

INTERVIEW OF AGNEL DSILVA

I had to finally tell the maintenance staff that we are working on an experiment and not to touch these USB drives next time. To my surprise, no one fell for this trick. All the USB drives were accounted for. One of the employees told me " Nice try, I passed, and you failed". I am proud of these users. This shows that our Security Awareness program is effective. That is absolutely something to be proud of, it is hard to find an office working so well together and securely. It is funny that the maintenance department caught on to them first. It shows that every department has a role to play in cyber security.

Well as a final parting call, any last piece of advice you would like to pass on to any students reading this now?

My advice for current students- never quit. You are in one of the best Cybersecurity programs in the nation. These courses may be challenging. Always ask questions and communicate with your professors. Do not wait till the last minute to complete assignments. The more your practice the better you get at things. One of my favorite quotes:

"Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do"- Pele.

That is excellent and I also want to stress that you should not wait to the last moment to do assignments, it never works out in the end. Agnel, it has been a pleasure and thank you!

```
>.  ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE AN AWESOME HALLOWEEN
>. 31 OCTOBER 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/

THE UNIVERSITY OF ARIZONA