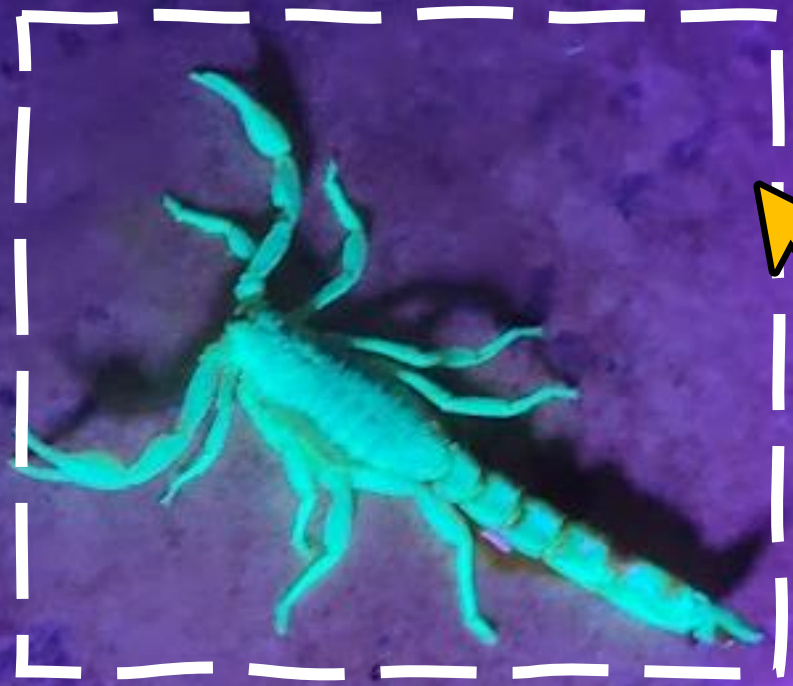
THE FRACKET



Cut

Copy

Paste

Remove from Internet

Post to Internet

INSTALL FEAR

OCTOBER MONTHLY CONTENT FALL 2022

X

NATIONAL SECURITY AGENCY

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

DIVERSITY IN THE INTELLIGENCE COMMUNITY

Thursday - October 13, 2022

8:00AM - 7:00PM (Arizona MST)

University of Arizona

Student Union Memorial Center - Grand Ballroom

Explore careers in the intelligence community

Learn about the future of national intelligence

Meet with national, state and industry intelligence leaders

Special Keynote Speaker

Avril D. Haines, Director of National Intelligence

Free admission for ALL UArizona Students, Faculty, Staff, and government/commercial attendees!

A portion of the proceeds for this event will be directed to student scholarships.

College of Applied Science & Technology

THE UNIVERSITY OF ARIZONA

Cyber Convergence Center

>. HELLO_WORLD_☺

> ----- ESTABLISHING CONNECTION -----
> > Welcome to the October 2022 issue of "THE PACKET", produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. I want to start off and urge everyone who can attend the Southern Arizona Intelligence Summit this month on the 13th to make it. I will be there and am excited to see everyone. There will be many people to interact with and networking is a great way to get your name out there. In this issue, we will look at how to read encrypted SSL communication with Wireshark allowing you to understand what is under all that encrypted traffic. We also have a new article from our own Professor Thomas Jewkes and a continuation of the publication from last edition, Professor Jordan A. VanHoy. In September, we have seen some interesting data breaches from a few companies, the largest being from UBER and Rockstar Games. UBER claims the attack came from the LAPSUS$ group but I have my doubts. We have also seen an increase of cyberattacks against various government services if they go against the Russian Federation. These attacks are not advanced attacks, but they are disrupting government services and mainly come in the form of distributed denial of service attacks (DDOS) and phishing campaigns. While more advanced cyberattacks require planning and tool development, it is likely we will see an increase in the next few months as the Ukraine and Russia conflict continues to be ongoing. Finally, for our spooky content we will bring back a classic fake malware website template that you can build and deploy. Learn HTML and how easy it is to build something convincing. Use it just for fun though and don't give anyone a heart attack. Good luck on this month's midterms and I look forward to putting together the November edition for next month, Anyone know a good recipe for turkey malware!

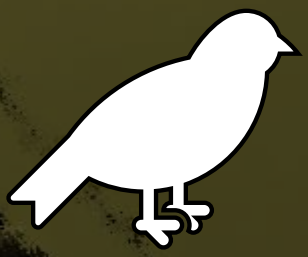
>. HACKS_OF_THE_MONTH

FINLAND'S PARLIAMENT HIT WITH CYBERATTACK

Finland's parliament website was temporarily offline on Tuesday following a cyberattack that coincided with President Biden's move to admit the Nordic country to NATO. The Finnish parliament said in a statement on Twitter that a denial-of-service attack hit the parliament's external websites at around 2:30 p.m. local time. The attack against the parliament occurred the same day Biden signed a measure backing Finland and Sweden's admittance into NATO. Biden's signature makes the U.S. the 23rd NATO country out of 30 member states to approve the two Nordic countries' admission to the alliance. Biden called the move a "Watershed moment" for the transatlantic alliance, adding that the decision to incorporate Finland and Sweden into NATO is "For the greater security stability of the world." "At a moment when Putin's Russia has shattered peace and security in Europe, when autocrats are challenging the very foundations of a rule-based order, the strength of a transatlantic alliance and America's commitment to NATO is more important than it's ever been," Biden said on Tuesday at an event attended by the ambassadors of Finland and Sweden. Finland, along with Sweden, applied for NATO membership in May, a move prompted by Russia's invasion of Ukraine in February. Following Sweden's decision to join NATO, the country's Prime Minister Magdalena Andersson expressed concerns of possible cyber retaliation from Russia. Experts have warned that Russia could potentially use its cyber arsenal against Finland and Sweden and say it's likely that the country chooses to launch small-scale and unsophisticated types of cyberattacks, including distributed denial-of-service attacks and website defacement, as a form of protest against the expansion.

- **ARTICLE LINK**
- **SWEDISH CONCERNED**

TWITTER HACKER STEALS 5 MILLION ACCOUNTS' PERSONAL INFORMATION



A Twitter breach has allowed hackers to find the names and email addresses associated with millions of accounts. This includes accounts of people who would rather keep their information pseudonymous, such as whistleblowers and celebrity accounts. "We want to let you know about a vulnerability that allowed someone to enter a phone number or email address into the log-in flow in an attempt to learn if that information was tied to an existing Twitter account, and if so, which specific account", Twitter said in a blog post confirming the attack. Twitter received a report at the start of this year about a vulnerability in its system, whereby if someone submitted an email address or phone number to Twitter's systems, Twitter's systems would tell the person what Twitter account the submitted email addresses or phone number was associated with, if any. The company said at the time that it had no evidence of a malicious individual using this exploit, but that changed in July 2022 when it was reported that information on over 5.4 million accounts were sold on a hacker forum for $30,000.

- **ARTICLE LINK**
- **TWITTER RESPONSE**

>. HACKS_OF_THE_MONTH

RUSSIAN SVR HACKERS USE GOOGLE DRIVE, DROPBOX TO EVADE DETECTION

State-backed hackers' that are a part of Russia's Federation Foreign Intelligence Service have started using Google Drive's legitimate cloud storage service to evade detection. "We have discovered that their two most recent campaigns leveraged Google Drive cloud storage services for the first time," Unit 42 analysts who spotted the new trend said. "The ubiquitous nature of Google Drive cloud storage services - combined with the trust that millions of customers worldwide have in them - make their inclusion in this APT's malware delivery process exceptionally concerning. "As Mandiant revealed in an April report tracking one of the group's phishing campaigns, this is not the first time APT29 hackers have abused legitimate web services for command-and-control and storage purposes. Just as in the campaigns observed by Unit 42, Mandiant also saw the cyberespionage group's phishing attacks against employees of various diplomatic organizations across the world, a focus consistent with current Russian geopolitical and strategic interests and previous APT29 targeting. APT29 is the Russian Foreign Intelligence Service hacking division that carried out the SolarWinds supply-chain attack, which led to the compromise of multiple U.S. federal agencies in 2020. Unit 42 has also recently observed the Brute Ratel adversarial attack simulation tool deployed in attacks suspected to be linked to the Russian SVR cyberspies.

- **ARTICLE LINK**
- **APT 29 TACTIC OVERVIEW**

LOCKBIT RANSOMWARE BUILDER LEAKED ONLINE BY "ANGRY DEVELOPER"

The LockBit ransomware operation has suffered a breach, with an allegedly disgruntled developer leaking the builder for the gang's newest encryptor. According to security researcher 3xp0rt, a newly registered Twitter user named 'Ali Qushji' states their team hacked LockBits servers and found a builder for the LockBit 3.0 ransomware encryptor. After security researcher 3xp0rt shared the tweet about the leaked LockBit 3.0 builder, VX-Underground shared that they were contacted on September 10th by a user named 'protonleaks,' who also shared a copy of the builder. VX-Underground says that LockBitSupp, the public representative of the LockBit operation, claims they were not hacked, but rather a disgruntled developer leaked the private ransomware builder. Regardless of how the private ransomware builder was leaked, this is not only a severe blow to the LockBit ransomware operation but also to the enterprise, which will see a rise in threat actors using it to launch their own attacks. The leaked LockBit 3.0 builder allows anyone to quickly build the executables required to launch their own operation, including an encryptor, decryptor, and specialized tools to launch the decryptor in certain ways. This builder is not the first time a ransomware builder or source code was leaked online, leading to increased attacks by other threat actors who launched their own operations.

- **ARTICLE LINK**
- **~~GITHUB CODE REPO~~**

>. HACKS_OF_THE_MONTH

RUSSIAN SANDWORM HACKERS POSE AS UKRAINIAN TELCOS TO DROP MALWARE

The Russian state-sponsored hacking group known as Sandworm has been observed masquerading as telecommunication providers to target Ukrainian entities with malware. Sandworm is a state-backed threat actor attributed by the US government as part of the Russian GRU foreign military intelligence service. Starting in August 2022, researchers at Recorded Future have observed a rise in Sandworm command and control infrastructure that uses dynamic DNS domains masquerading as Ukrainian telecommunication service providers. Recent campaigns aim to deploy commodity malware like Colibri Loader and the Warzone RAT onto critical Ukrainian systems. Another spoofed Ukrainian telecommunication services provider is Kyivstar, for which Sandworm uses the facades "Kyiv-star[.]ddns[.]net" and "Kievstar[.]online.“ The attack begins by luring victims to visit the domains, typically via emails sent from these domains, to make it appear like the sender is a Ukrainian telecommunication provider. Possibly, the Russian hackers want to make tracking and attribution harder for security analysts by using widely available malware and hoping that their tracks are "Lost in the noise."

- **ARTICLE LINK**

UBER LINKS BREACH TO LAPSUS$ GROUP, BLAMES CONTRACTOR FOR HACK

Uber believes the hacker behind last week's breach is affiliated with the Lapsus$ extortion group, known for breaching other high-profile tech companies such as Microsoft, Cisco, NVIDIA, Samsung, and Okta. The company added that the attacker used the stolen credentials of an Uber EXT contractor in an MFA fatigue attack where the contractor was flooded with two-factor authentication login requests until one of them was accepted. "From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack," Uber explained in an update to the original statement. We identified any employee accounts that were compromised or potentially compromised and either blocked their access to Uber systems or required a password reset. Throughout, we were able to keep all of our public-facing Uber, Uber Eats, and Uber Freight services operational and running smoothly. "First and foremost, we've not seen that the attacker accessed the production systems that power our apps; any user accounts; or the databases we use to store sensitive user information, like credit card numbers, user bank account info, or trip history. We also encrypt credit card information and personal health data, offering a further layer of protection," Uber said.

- **ARTICLE LINK**
- **UBER REPLY**

A CHICKEN TALE

>. THOMAS JEWKES

Imagine you are a chicken rancher. Your chicken are free-range, no antibiotics, and (most importantly) hypo-allergenic. So, people with egg allergies can use your eggs to make cookies and other goodies. If they ever inadvertently eat store bought eggs they would die. You can see the value in your eggs.

But who would even want to harm your business. You are small. You only serve a small geographic area. Imagine, you have a very elite clientele. Because your eggs are so unique, your clientele consists of some very influential and powerful people. If a criminal wanted to target a powerful person, they wouldn't have to do it directly. All they must do is gain access to your hen houses and plant store bought eggs. Then wait for you to deliver them to your clients. It doesn't even matter to the criminal if they hurt others as well. Those would merely be collateral damage to the criminal. As long as their target was affected, their mission is complete.

This is pretty much how supply side software attacks happen. A legitimate software vendor with lackadaisical security on their software repository (the henhouse) gets infiltrated by a threat actor. A legitimate file (your precious eggs) gets infected with malware (store bought eggs), then the threat actor simply waits for the vendor to ship out the infected file.

Does this happen? You bet it does. A while ago, a huge software vendor named SolarWinds had this happen to them. It affected about 18,000 of their high value customers.

A CHICKEN TALE

>. THOMAS JEWKES

So now we find we can't even trust the vendors to keep their software repositories (their hen houses) safe. But what can you do about it? Here's what you can do. Before you install any new software or any update, you can upload the software to virustotal.com and have the file scanned for you at no cost. It's not foolproof but will give you at least a small measure of assurance the file hasn't been tampered with.

There are two possible problems here.

- First, Virus Total is a public website, so don't upload any sensitive files.
- Second, Virus Total will only report a file as malicious if:
  - Virus Total has seen it before AND
  - The antivirus engines it uses to scan the file has verified the file is malicious.

What this means to you is, if the good eggs were just switched out for bad eggs this morning, Virus Total will not know it's bad. And you will install malicious software. So, with this technique, your mileage may vary.

TO THE CYBERCRINIMIALS WE DEFEND AGAINST

WE'RE THE HACKERS UP TO NO GOOD

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 enjoyed 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

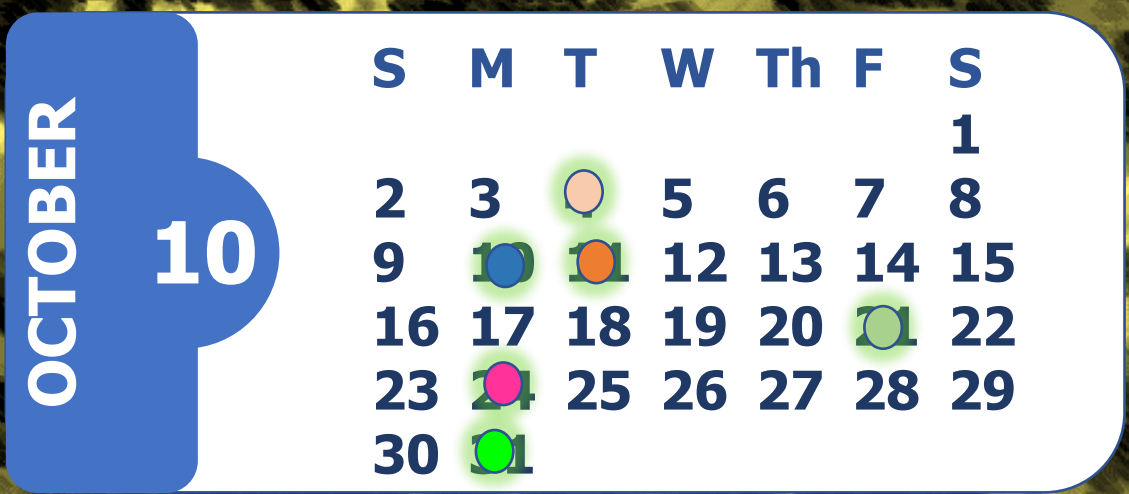
On June 1, 1990, Poulsen took over all the telephone lines for Los Angeles radio station KIIS-FM, guaranteeing that he would be the 102nd caller and win the prize of a Porsche 944 S2. When the Federal Bureau of Investigation started pursuing Poulsen, he went underground as a fugitive. In June 1994, Poulsen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



>. CYBER_SECURITY_HISTORY

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

OCTOBER 10

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

FAKE VIRUS INSTALL

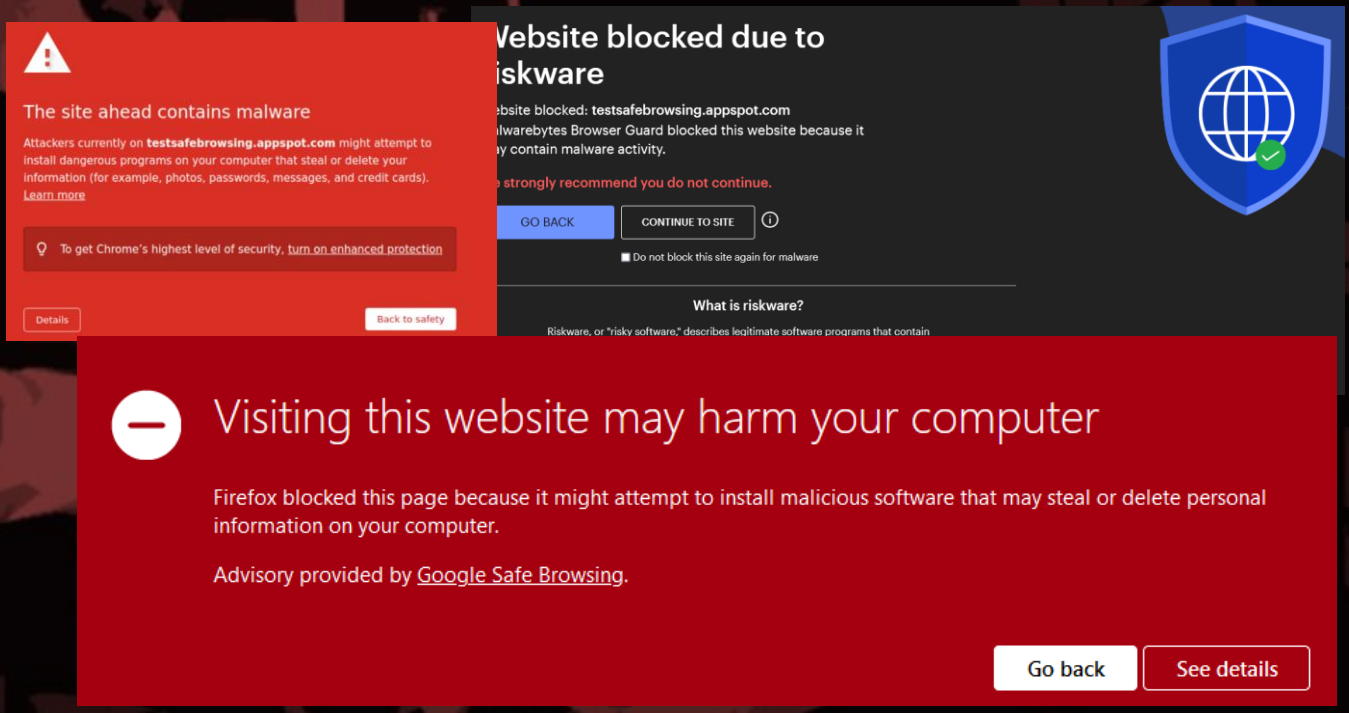
Halloween is upon us, and it is time for us to explore our spooky side. We are not talking about a scary movie or trick-or-treating, no, we are going to make an unsuspecting user believe they are installing a virus on there machine. Now you do not need any coding knowledge whatsoever for this project, 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.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. HACKING_POC IS INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS. IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

FAKE VIRUS INSTALL

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!

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.

FAKE VIRUS INSTALL

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.

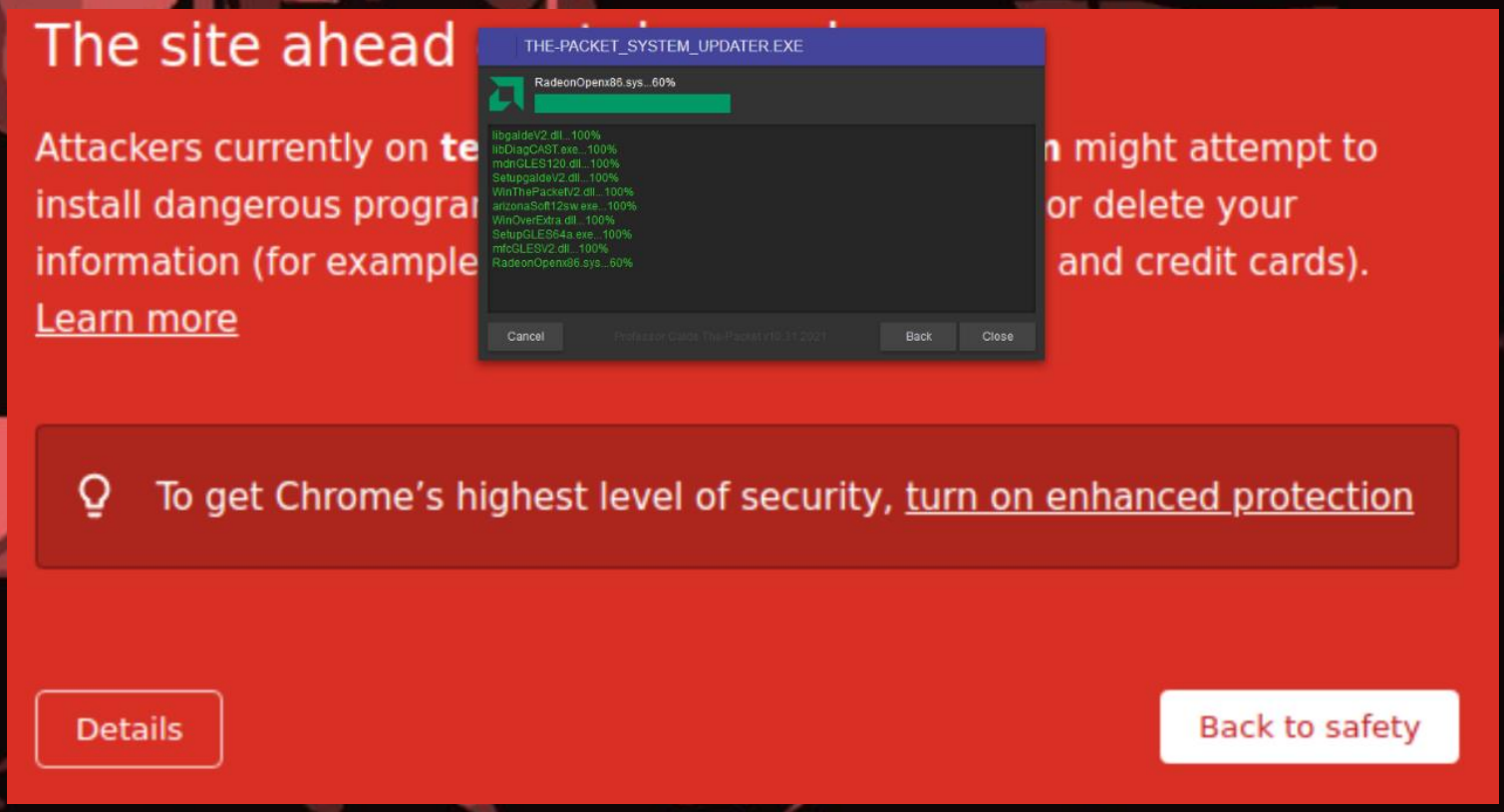
Next, we have the lower portion of the buttons that don't do anything like close, cancel and back, and then my personalization with my name to claim my stake into this visualization.
Next, we have an array we can manipulate to make our virus more unique and "dangerous" looking. Under the array labeled 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'
    word: ['ThePacket', 'Installer', 'GLES', 'Soft', 'Diag', 'Ov
    suffix: ['Installer.exe', 'Extra.dll', '64a.exe', 'V2.dll',
}
```

FAKE VIRUS INSTALL

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 zero day or 0-day malware.

```
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']
}
```



Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

www.linkedin.com/company/uarizona-wicys/

www.twitter.com/UWicys

www.facebook.com/UAZWicys

www.instagram.com/uarizonawicys/

THE UNIVERSITY OF ARIZONA

WiCyS
women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER

DECRYPT ENCRYPTED NETWORK TRAFFIC FOR ANALYSIS

If you have taken CYBV 326 for network analysis then you know Wireshark, and you are also aware of the challenges of capturing modern web traffic as well. HTTP messages are typically are not sent in plaintext. Instead, the TLS protocol is used to provide communications security against tampering and surveillance of communications based on HTTP protocol.

TLS is a complex protocol consisting of several sub-protocols, but for simplicity lets think of it as an encrypted and authenticated layer on top of the TCP connection, that also does some server (and optionally client) verification through public key cryptography.

If we try to sniff HTTPS traffic without any preparations, we will not be able to go far, as the TLS protocol is doing its job to prevent adversaries from reading contents of our communication by sniffing the network.

However, if we control one of the endpoints, for example your desktop system with a web browser, we can set the **SSLKEYLOGFILE** environment variable to the path of textile we can access.

Software that implements TLS will typically write keys and other TLS secrets to this file. This applies to curl, Chrome, Firefox and many desktop apps that use NSS/OpenSSL libraries.

We will then use a program like Wireshark and if it is configured correctly, we will be able to read this file and decrypt the intercepted TLS packets. This is what we call a client-side capture of session keys.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. HACKING_POC IS INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS. IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

DECRYPT ENCRYPTED NETWORK TRAFFIC FOR ANALYSIS

So, How exactly do we set the environment variable? This is dependent on your operating system and whether we want to cover all apps that are installed.
On Linux, we could edit /etc/environment or /etc/profile depending on your Linux distribution. You will then set the following variable in the configuration file

```
export SSLKEYLOGFILE=~/.sslkeyfile
```

You would then need to reboot to set this as a global variable.

On Windows, you can set SSLKEYLOGFILE environment variable by creating a folder you want to save the keys to and then in a PowerShell window in that directory run the following command.

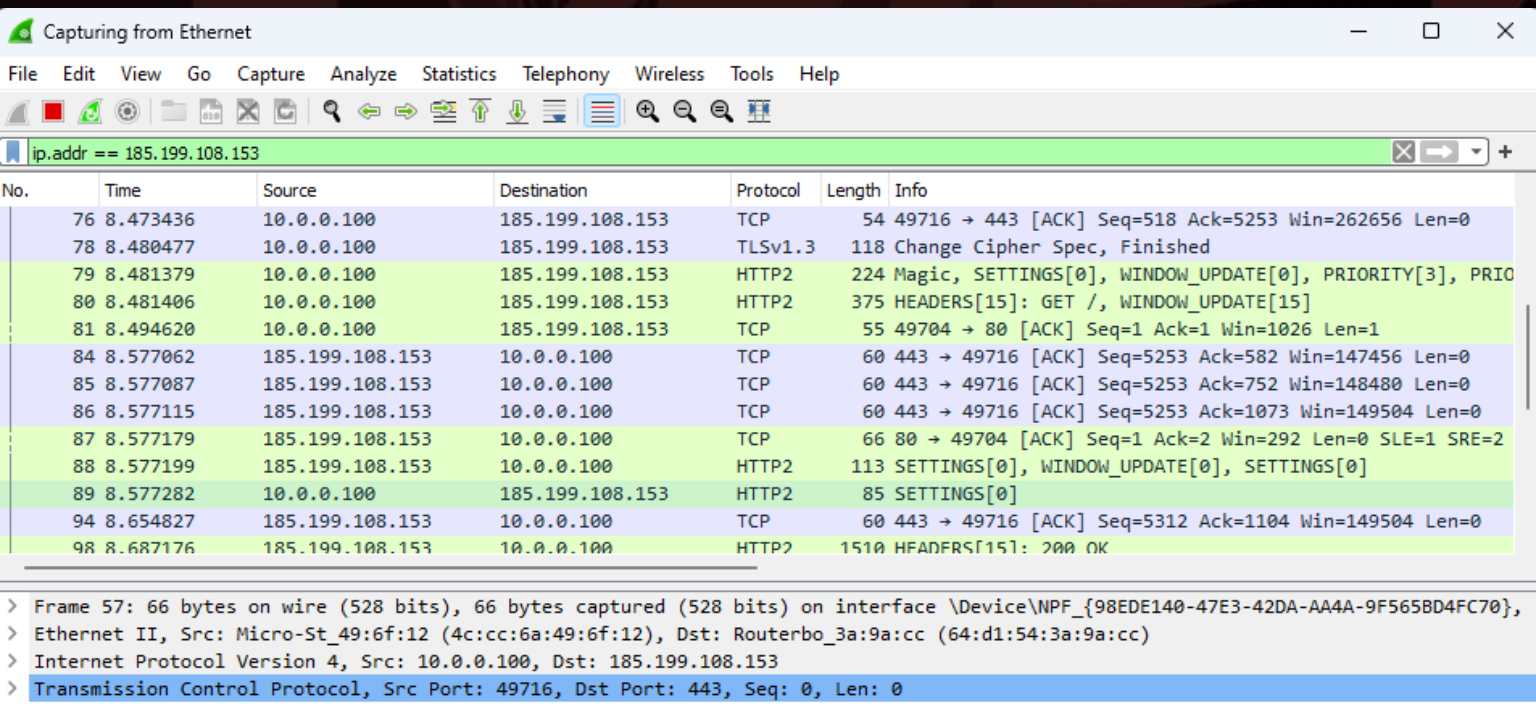
```
SetX SSLKEYLOGFILE "$(get-location)\ssl.log"
```

Once this is done, we need to restart the browser and/or other software that communicates over HTTPS. If everything is okay, the file should start to get populated.

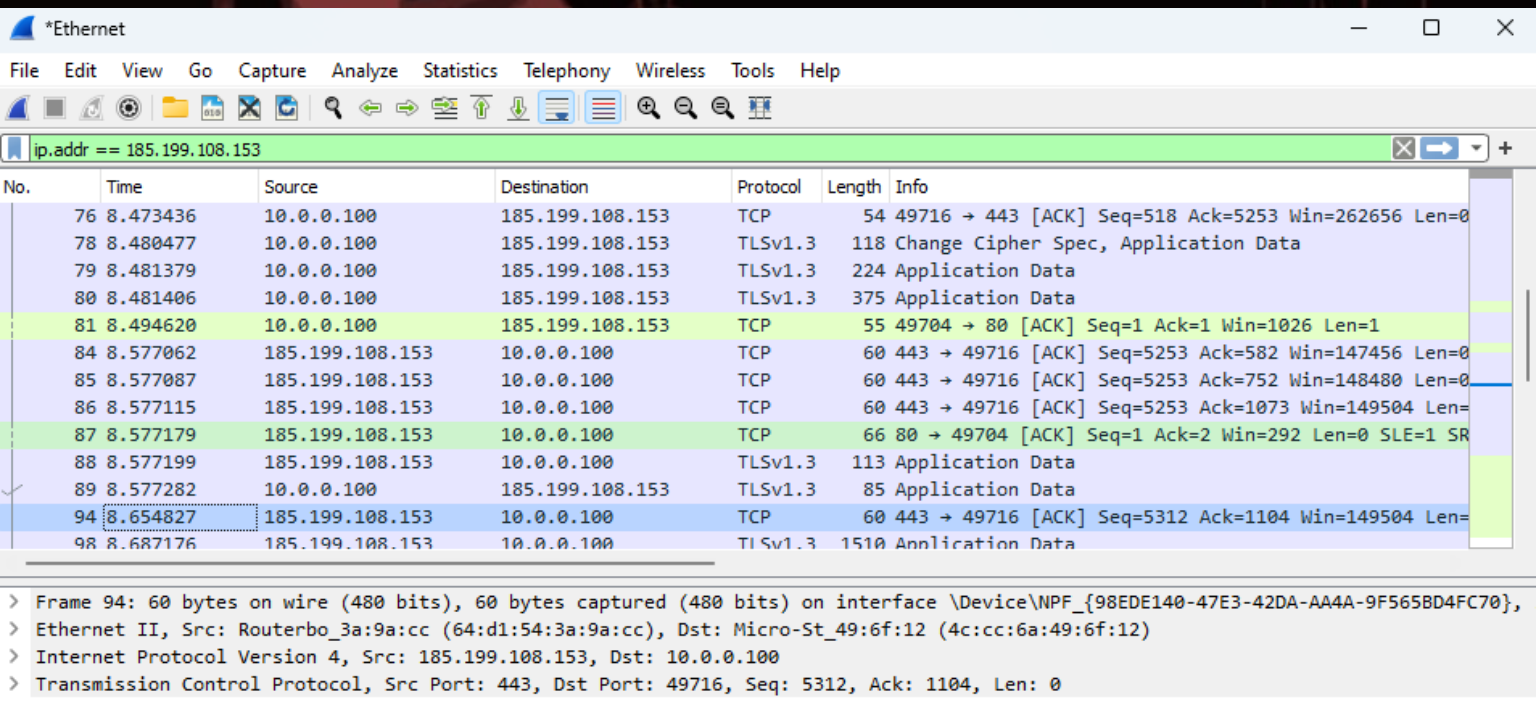
We are ready to configure Wireshark now, this is simple. All we must do is go to Edit -> Preferences -> Protocols -> TLS and put the value of SSLKEYLOGFILE into “(Pre-)Master Secret Log filename”.
You should also tick the checkboxes about reassembling TLS records and application data.

DECRYPT ENCRYPTED NETWORK TRAFFIC FOR ANALYSIS

TLS data decrypted



No TLS data decryption



>. JOBS/INTERNSHIPS

CYBERSECURITY INTERNSHIP
MALAGA, WA

Our team is looking for a Cyber Security Intern to join them in the upcoming weeks. This position is great for an aspiring cyber security professional looking to work on business-critical projects and gain relevant work experience.
You will learn how to:

- Support the identification of cyber security solution opportunities (e.g., by optimizing cyber security processes/procedures, organizations, and services)
- Assist in identifying operational requirements and proposing solutions to ongoing cyber security architecture/organization issues
- Assist in the preparation of individual cyber security project proposals and plans
- Monitor IT security systems and respond to incident reports as they arise (incident management)
- Evaluate log data, PCAP, and analyze malware
- Implement our cyber security solutions
- Update the internal team's engineering knowledge by presenting analysis results
- Provide other ad hoc technical support to other teams

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

CYBERSECURITY INTERNSHIP
LAS ANGELES, CA

All interns will be given the choice to work remotely or relocate to the internship location. The company will cover relocation services and will provide a living student to supplement housing, utility, and office supply costs.
Games Information Security Internship: Learn what it takes to protect our games. If you have experience or interest in security and cryptography, then this is the team for you.
Global Information Security Internship: The Global Information Security Intern reports into Global Information Security team and maintains strong relations with all Line of Business technology groups. This person will work closely with several key individuals and teams to analyze and assess vulnerabilities in the infrastructure (software, hardware, networks), security assessments, and security incident response.

- Gain experience working in the forefront of the gaming industry where the environment and work is dynamic.
- Collaborate with some of the best engineers in the industry.
- Apply analytical thinking to balance design and operational excellence to help our teams drive innovation.
- Expand your skills and learn new technology.
- Spend a summer focusing on a meaningful project that directly impacts game development while having an unparalleled experience.
- Participate in learning and development tech talks to understand how our employees come together to launch AAA games

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

FOREIGN AFFAIRS IT Fellowship

College of Applied Science & Technology

What is the FAIT Fellowship?

We are excited to host a 30-minute virtual info session with the Foreign Affairs Information Technology (FAIT) Fellowship, one of several high-profile U.S. Department of State diversity recruitment programs.

The two-year fellowship provides up to $87,000 in academic funding over the two years, summer internships, professional development, and mentorship – and culminates in a career in Foreign Service as an Information Management Specialist.

Who Will be Speaking?

The application for the 2023 cohort is open September 12, 2022, through February 3, 2023. Don't miss this chance to get a brief overview of the FAIT Fellowship and hear from:

- **Sara Robinson-Camarena**, University of Arizona alumna and FAIT Fellow (2020 cohort), U.S. Consulate Frankfurt
- **Antoinette Hurtado**, Diplomat in Residence Southwest, U.S. Department of State

About the Opportunity

The Foreign Affairs IT Fellowship, designed as a two-year cohort model, offers both undergraduate and graduate fellowships. The undergraduate fellowship is for your junior and senior years of an IT-related bachelor's degree program. The graduate fellowship is for a two-year IT-related master's degree program.

Fellows selected for the 2023 cohort will begin their two-year fellowship in fall 2023 and complete the fellowship in Summer 2025.

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 love the idea of a Foreign Service career using your tech skills to support U.S. diplomacy, traveling the world, and learning about different cultures, the FAIT Fellowship is your opportunity of a lifetime.

Register Now

OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

JOIN CYBER SAGUAROS TODAY

Cyber Saguaros

CYBER_SAGUAROS

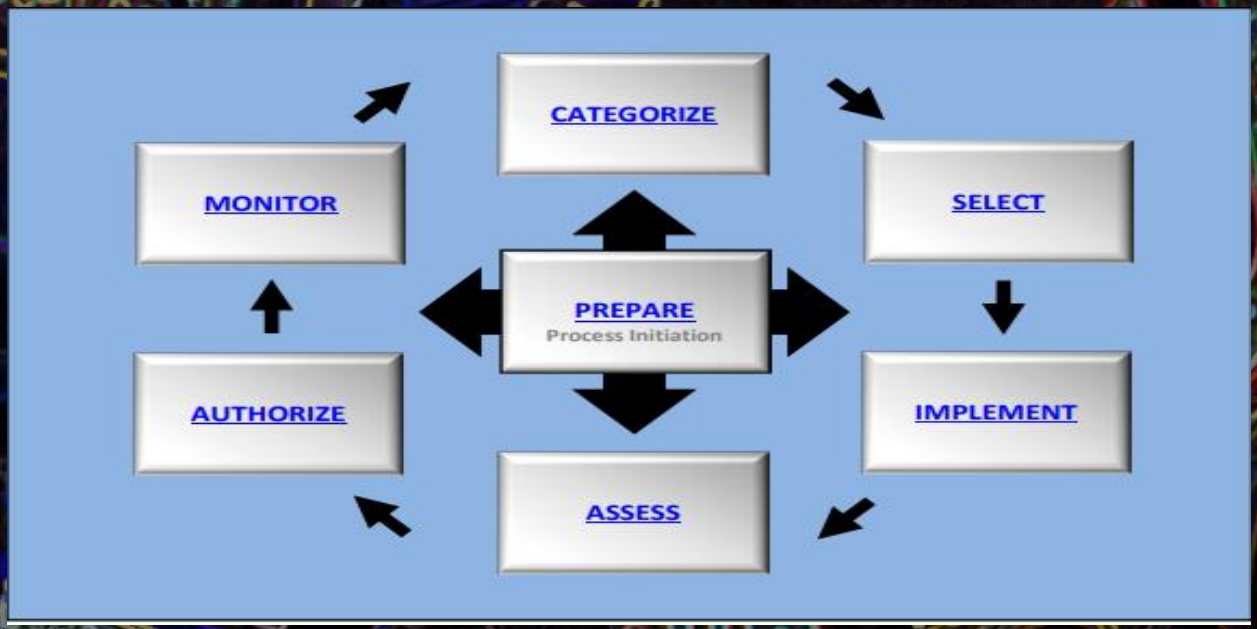
THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 2 OF 6

>. Jordan A. VanHoy

Actualized Harm by Failed Risk Management

This is part two of a six-part series of a paper written by Professor VanHoy



Prepare. In the first step of the NIST risk management framework the organization begins to prepare for the implementation of the program at the enterprise and system level. The NIST document details seven high level tasks that are achieved at this level to prepare the organization for the unveiling of the framework. In a broad sense, this entails developing priorities and understanding of the current landscape employed by the organization. This is an essential element to the risk management framework as the tasks completed at this level lay the groundwork for the structural integrity of the information security program. During the completion of this step, key roles are identified, a risk management strategy developed, risk assessment conducted, control baselines established, systems prioritized, and continuous monitoring strategy implemented. These are displayed as a list of tasks in a checklist like manner for ease of implementation to the business.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 2 OF 6

>. Jordan A. VanHoy

Task priority one has an expected outcome of delivering a documented list of risk management framework role assignments. This can be internal and external to the organization depending on the complexities at hand. Primary considerations include deconflicting assignments and building out separation of duties to prevent collusion of fraud. The NIST has developed SP 800-160r1 for assisting in the development of a risk management organizational chart. Upon completion of this step the risk management strategy becomes the focal point and provides one of the most important aspects that will be accomplished in the prepare stage by establishing the organization risk appetite. The risk appetite is the maximum allowable level of risk an organization has deemed appropriate in accordance with the business mission statement. Every organization may have a unique level of risk that leadership is willing to accept, and this may also vary from department to department within the organization. Further, because risk is a dynamic concept, there exist a level of variance in acceptable risk which is the slight deviation of higher risk than the current appetite provides for. The next step is to conduct a risk assessment by taking into consideration the totality of risk from information systems and enterprise architecture. This information may be used in the development of a gap analysis which provides the organization the opportunity to assess where the current posture is in relation to where the posture needs to be. This provides an accurate picture of the actual deficiencies and where the organization may need to provide resources in improving so that the end state is able to be achieved.

Upon examination of this information, it is time to conduct a current risk assessment. The risk assessment would be considered a point in time snapshot as risks to the organization are considered dynamic. However, this vital piece of information establishes an understanding of the potential threats the organization may face in the operation of normal business operations. If the organization is currently leveraging the NIST Cyber Security Framework, the results of the risk assessment may establish a profile within the framework. After task priority three has been completed, the organization may optionally pick up task priority four. This task requires the establishment, documentation,

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 2 OF 6

>. Jordan A. VanHoy

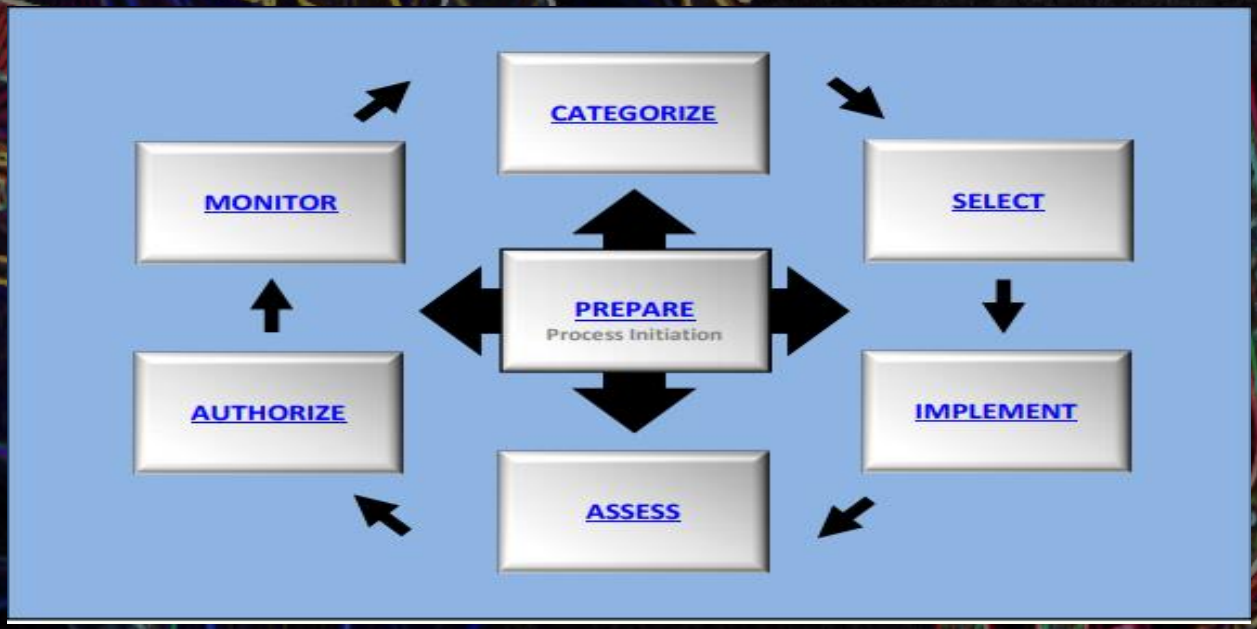
and publication of organizationally tailored control baselines and cybersecurity framework profiles. In layman terms, this is where the organization specifies the applicability of the NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations and documents any exceptions that may or may not exist. Upon completion of task priority four, the fifth task is to determine common control inheritance amongst the system, component, or process levels. The following step is vital to understanding the data flows of the organization as task priority six has the organization prioritize systems in the classification of low, moderate, or high impact depending on the sensitivity of information processes. Many organizations will have a combination of the three classifications, but the majority of systems will remain at the low impact categorization. This is an optional task when examining the prepare portion of the risk management framework but is a vital step to take in any organization vying for accurate measurement of system protection. The final step is to implement an organizational continuous monitoring strategy to ensure the longevity of risk mitigation. This is where automation must be leveraged to provide a heartbeat sensor type of monitoring for rapid response to anomaly detection. Additionally, am effective implementation of the continuous monitoring phase will reduce overall cost while maintaining high levels of security and privacy.

While the portions of the risk management framework focus on the organizational level, there are system level tasks assigned to the prepare stage as well. These are the technical implementations of the risk management framework and cover a wide range of tasks to include identifying the types of information processed, stored, and transmitted, identifying the enterprise architecture, and identifying assets owned by the organization. While these are clearly very important steps for the organization to take, this exceeds the scope of this paper in developing a continuous monitoring strategy.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 2 OF 6

>. Jordan A. VanHoy



Categorize. Just as many ventures in life require immense preparation, the risk management framework is no different. When transitioning from the prepare phase to the categorize phase, there are a total of 18 tasks in preparation and three in categorize. This phase of the framework is dedicated to understanding the adverse impact to business processes and assets, individuals, other organizations, and if applicable the nation Specifically, this phase examines loss as it pertains to the confidentiality, integrity, and availability of information as the information traverses the information lifecycle. The first major task to be accomplished by the organization is to determine comprehensive system descriptions by taking into consideration the characteristics of the system. The level of detail is left to the organization to determine but in most cases become more detailed the higher the classification of the system. The amount of information that may be included in this section is staggering as it has the potential to describe every aspect of the system. Examples of information included during this task are hardware, software, topology, system interdependencies, and individuals who are responsible for the oversight of the system.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 2 OF 6

>. Jordan A. VanHoy

The subsequent task dictates that the system be categorized and document the security categorization based upon the impact level of the information type and objective. When operating in the government sector, additional resources for determining this information can be derived from federal information processing standard (FIPS) 199 and 200. FIPS 199 is the Standards for Security Categorization of Federal Information and Information Systems while FIPS 200 is the Minimum-Security Requirements for Federal Information and Information Systems. These documents in tandem with the NIST SP 800-53 determine applicable controls, system categorization, and minimum threshold for protection.

The final task associated with the categorize phase is to review the security categorization results and approve the information. Ensuring proper classification of the system will determine the level of protection necessary for the information being processed and should be classified at the lowest level possible. By classifying the system at the lowest level possible, this greatly reduces the cost associated with implementing controls and subsequently auditing and monitoring. Classifications in the government are considered to be unclassified, confidential, secret, and top secret depending on the sensitivity of information being processed. In the private sector, classifications can be arbitrary but generally fall into a public, sensitive, private, and confidential model.

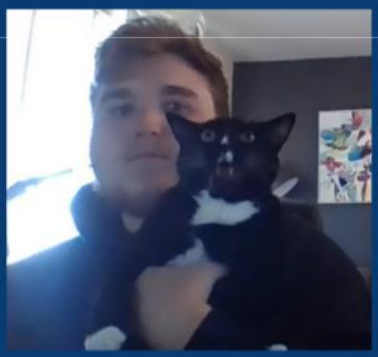
Information Security

Security Operations Center Student Program

The University of Arizona's SOC offers a student worker and internship program for Spring, Summer, and Fall semesters. Spring 2023 applications open up soon! To learn more: security@arizona.edu

Student Highlight

Niels Romine



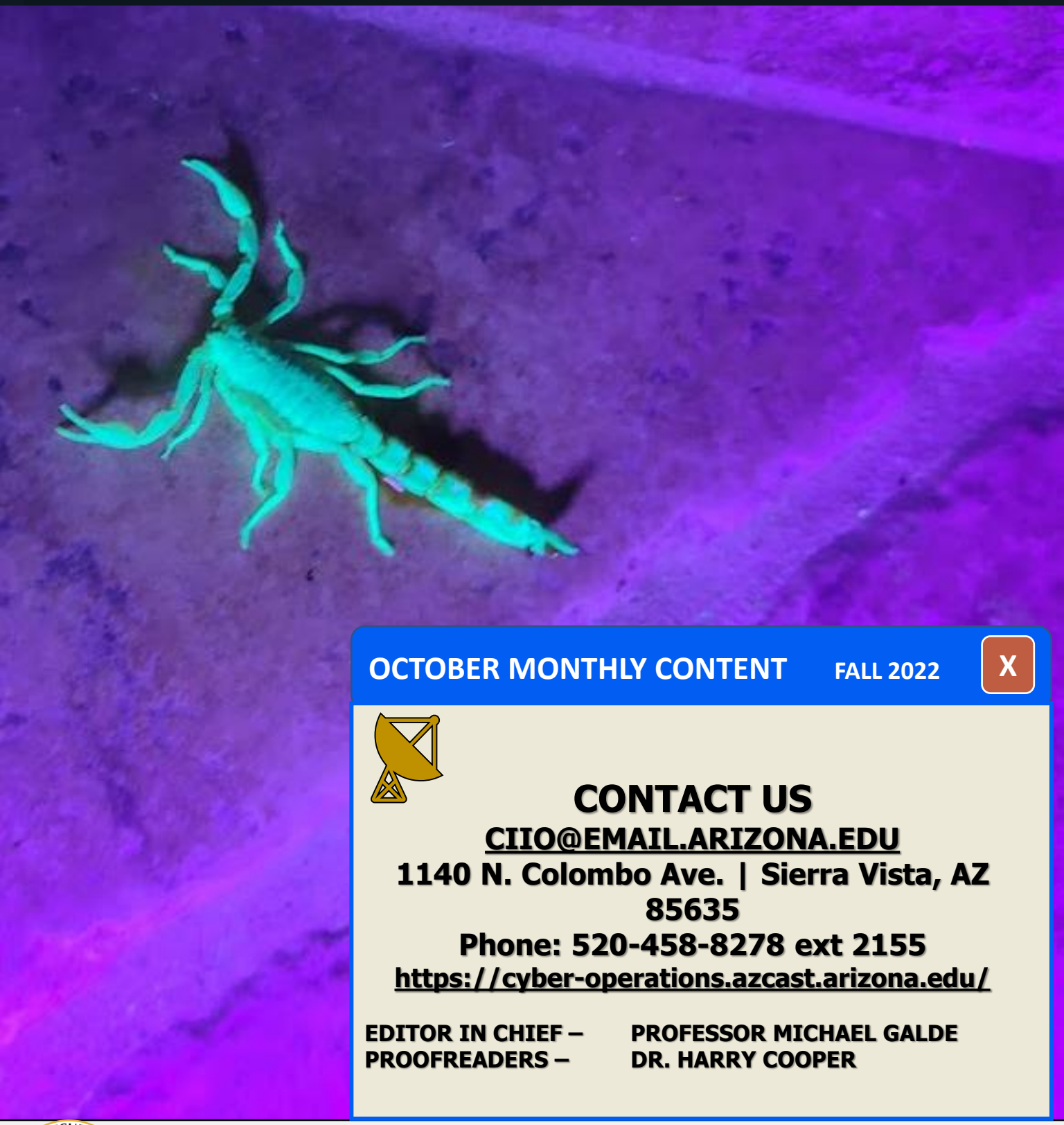
Q. Please tell us about your time so far working for the SOC.
A. Working for the SOC mixes real work experience without the pressure of feeling like you're an impostor. Everyone that I have encountered has been very patient, accommodating and most importantly kind to both myself and my coworker. Anyone that is looking to get started with cybersecurity regardless of experience should strongly consider a position at the SOC. This is the open door that will help you get started with your future career.

Q. How has CAST helped you achieve your goals in cyber?
A. Going into the university I didn't know anyone; I was an out of state transfer student and my last school didn't have this big of an emphasis on cyber. Through CAST I have met some people that I talk to daily and made some connections that will help me once I ultimately graduate.

Q. What field of cyber do you want to work in?
A. For the longest time I wanted to be in a 'red team' position or the cliché movie hacker role, where you take down the bad guy by clicking a key on your keyboard, but as time progressed, I found that I really enjoy the blockchain space. I am in awe at the new exploits/bugs that are being discovered on a weekly basis. I would be very interested in becoming a smart contract auditor.

Q. What is the best advice you can give to students wanting an internship in cybersecurity?
A. Take the time to learn your interests outside of a school/work setting. For example, if you want to learn how to script, then make something that intrigues you (make a bot that uses a specific API). Once you get involved in this kind of 'space', connections and friends will follow. The biggest part of my cybersecurity learning has been on my own or with very close friends.

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A SAFE AND FUN HALLOWEEN
>. HACK THE PLANET!!
>. ---END TRANSMISSION---



OCTOBER MONTHLY CONTENT **FALL 2022** X

CONTACT US

CIIO@EMAIL.ARIZONA.EDU
1140 N. Colombo Ave. | Sierra Vista, AZ 85635
Phone: 520-458-8278 ext 2155
https://cyber-operations.azcast.arizona.edu/

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

NATIONAL SECURITY AGENCY
THE UNIVERSITY OF ARIZONA
CAE IN CYBERSECURITY COMMUNITY