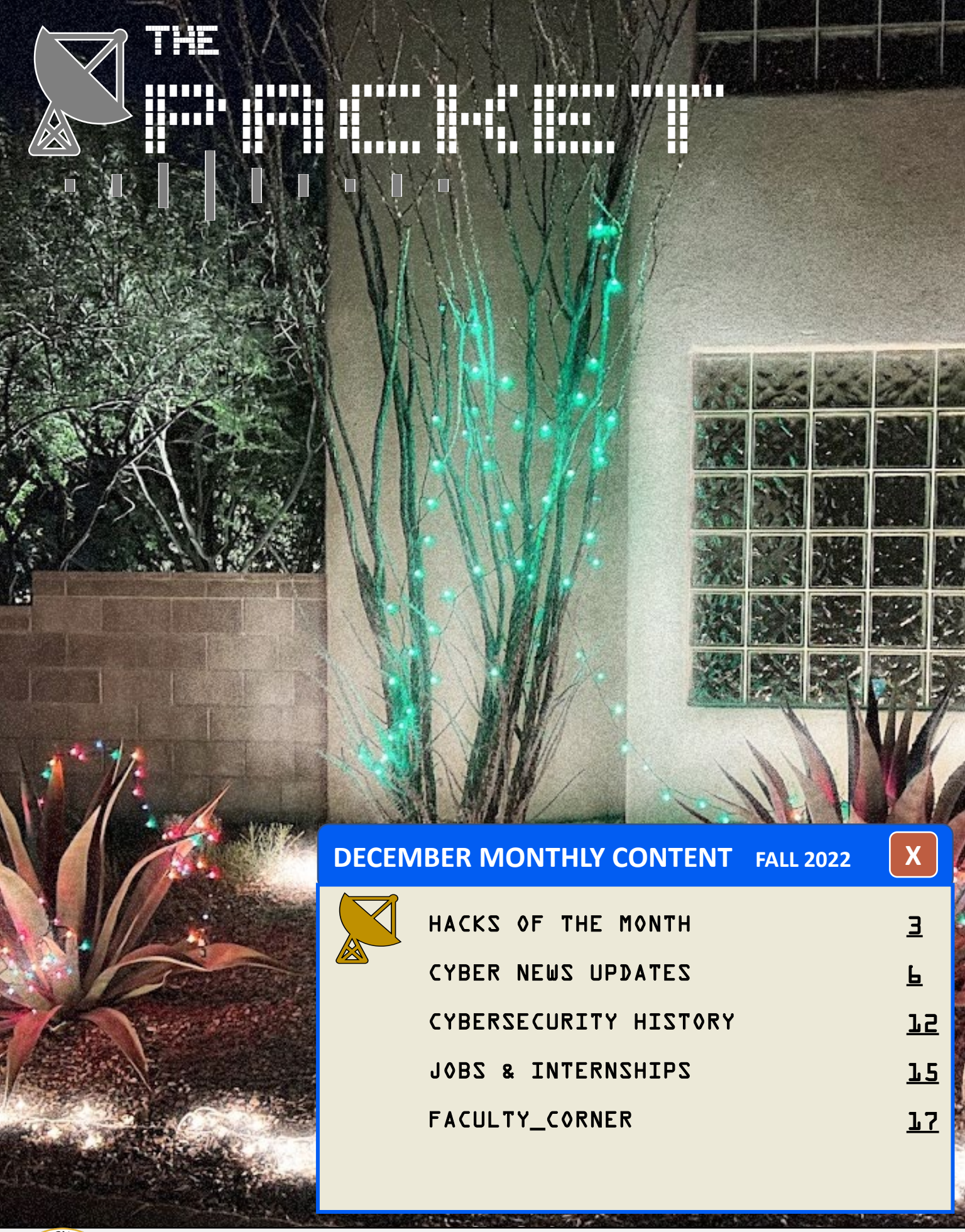
THE PACKET



DECEMBER MONTHLY CONTENT FALL 2022

X

NATIONAL SECURITY AGENCY

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

>. HELLO_WORLD_☺

≥ ----- ESTABLISHING CONNECTION -----

≥ ≥ Welcome to the December 2022 issue of "THE PACKET," produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. Good luck with finals. I know you are busy, but I sure am, as this semester is ending. This edition is late to the party, but as we are so close to finishing this semester and the year, we need to finish strong and bring the end to 2022. In a retrospective, this year has been interesting as we witnessed Russia and Ukraine begin a conflict that the international community is watching very closely. In addition, the cybersecurity community is watching the effects that may show what cyber war will look like with Russia. In addition, this year, the College of Applied Science and Technology hosted a very successful event, the Southern Arizona Intelligence Summit. Putting something like this on after the pandemic was quite challenging, but the staff and faculty made it a resounding success. So, as we close out this year, it is essential to reflect on the many lessons learned during this time and apply them to our mitigations in 2023. 2022 showed the cybersecurity community the dangers of relying on automated defenses and the importance of the "human in the loop" analysis cycle. Ransomware took a backseat this year but is still a key and active malicious player in our realm. The threat picture will only get more significant with so many geo-political events. So, in 2023, you can make it more boring. Many of us, including myself, need a little time to catch our breath. However, reviewing the trends in the last few years, this is an implausible approach, and we will likely see a significant breach at least once every two months. So, enjoy the rest of the year, because next year we will need you students even more in the cybersecurity space!

≥ HAPPY NEW YEAR!

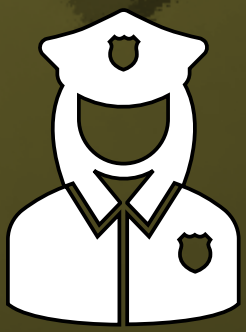
>. HACKS_OF_THE_MONTH

UKRAINE SAYS RUSSIAN HACKTIVISTS USE NEW SOMNIA RANSOMWARE

Russian hacktivists have infected multiple organizations in Ukraine with a new ransomware strain called 'Somnia,' encrypting their systems and causing operational problems. The Computer Emergency Response Team of Ukraine has confirmed the outbreak via an announcement on its portal, attributing the attacks to 'From Russia with Love', also known as 'Z-Team,' whom they track as UAC-0118. The group previously disclosed creating the Somnia ransomware on Telegram and even posted evidence of attacks against tank producers in Ukraine. Until today, Ukraine has not confirmed any successful encryption attacks by the hacking group.
The agency also notes that the latest samples of the Somnia ransomware strain used in these attacks rely on the AES algorithm, whereas Somnia initially used the symmetric 3DES. The file types targeted by Somnia ransomware are shown below, including documents, images, databases, archives, video files, and more, reflecting the destruction this strain aims to cause.
Somnia extension to the encrypted file's names when encrypting files. Somnia does not request the victims to pay a ransom in exchange for a working decryptor, as its operators are more interested in disrupting the target's operations than generating revenue.

- **ARTICLE LINK**
- **MALWARE ANALYSIS**

NEW AUSTRALIAN TASK FORCE TO "HACK THE HACKERS"



Following the latest Medibank data leaks, Australia's Cyber Security Minister Clare O'Neil said the government was considering a law that would make it illegal to pay ransoms, according to Australian ABC News. O'Neil noted that there were compelling reasons to make it illegal for companies to "Try to buy their way out of trouble" while praising Medibank's decision not to pay a $15 million ransom to prevent the release of user data. "The idea that we're going to trust these people to delete data that they have taken off and may have copied a million times is just frankly silly," she told Insiders on Sunday. She also announced the formation of a new Australian task force, which combines the expertise of the Australian Federal Police or ransomware gangs, "It is exposing their operations and turning them against each other. This would be well within reach of the attack team is alluding to here." The Medlab Pathology business suffered a data breach that affected about 223,000 accounts, marking corporate Australia's fourth major hack since September. The country's No.1 health insurer Medibank, No.2 telco Optus and retailer Woolworths Group's majority-owned online retailer MyDeal were also hit by breaches that compromised the data of millions of customers. There was no evidence of misuse of any of the information or any demand made of Medlab or ACL to date, the company said, adding that the compromised Medlab server had been decommissioned and ACL's broader systems were unaffected.

- **ARTICLE LINK**
- **ARTICLE ADDITION**

>. HACKS_OF_THE_MONTH

FBI: HIVE RANSOMWARE EXTORTED $100M FROM OVER 1,300 VICTIMS

The Federal Bureau of Investigation (FBI) said today that the notorious Hive ransomware gang has successfully extorted roughly $100 million from over a thousand companies since June 2021.To add insult to injury, the FBI says that the Hive gang will deploy additional ransomware payloads on the networks of victims who refuse to pay the ransom. "As of November 2022, Hive ransomware actors have victimized over 1,300 companies worldwide, receiving approximately US$100 million in ransom payments, according to FBI information," the FBI revealed. "Hive actors have been known to reinfect—with either Hive ransomware or another ransomware variant—the networks of victim organizations who have restored their network without making a ransom payment.“ The list of victims includes organizations from a wide range of industries and critical infrastructure sectors such as government facilities, communications, and information technology, with a focus on Healthcare and Public Health (HPH) entities. This was revealed in a joint advisory published today with the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS). Today's advisory was issued to share Hive indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) discovered by the FBI while investigating Hive ransomware attacks. The end goal is to help defenders detect malicious activity associated with Hive affiliates and reduce or eliminate the impact of such incidents. While submissions to the ID Ransomware platform don't include all Hive ransomware attacks, victims have submitted more than 850 samples since the start of the year, many of them pushed following a huge spike of activity between late March and mid-April.

- **ARTICLE LINK**
- **HIVE GROUP ANALYSIS**

PHISHING KIT IMPERSONATES WELL-KNOWN BRANDS TO TARGET US SHOPPERS

A sophisticated phishing kit has been targeting North Americans since mid-September, using lures focused on holidays like Labor Day and Halloween. The kit uses multiple evasion detection techniques and incorporates several mechanisms to keep non-victims away from its phishing pages. According to Akamai, whose security researchers discovered the campaign, one of the most interesting features of the kit is a token-based system that ensures each victim is redirected to a unique phishing page URL. The central theme of the phishing emails sent to prospective victims is a chance to win a prize from a reputable brand. The links in the email don't raise any alarms as they lead to the phishing site after a series of redirections, while URL shorteners conceal most URLs. Additionally, the attackers abuse legitimate cloud services like Google, AWS, and Azure, abusing their good reputation to bypass protection mechanisms. Everyone visiting the phishing site wins the promised prize after completing a short survey. In addition, a five-minute timer ensures those taking the survey are infused with a feeling of urgency. Some impersonated brands include sporting goods firm Dick's, high-end luggage maker Tumi, Delta Airlines, and the wholesale clubs, Sam's Club and Costco.

- **ARTICLE LINK**

>. HACKS_OF_THE_MONTH

ROMCOM THREAT ACTOR ABUSES KEEPASS AND SOLARWINDS

The threat actor known as RomCom is running a series of new attack campaigns that take advantage of the brand power of SolarWinds, KeePass, and PDF Technologies. The BlackBerry Threat Research and Intelligence Team uncovered the campaigns while analyzing network artifacts unearthed during our recent report on RomComRAT, which was targeting Ukrainian military institutions through spoofed versions of Advanced IP Scanner software. While Ukraine still appears to be the primary target of this campaign, we believe some English-speaking countries are being targeted as well, including the United Kingdom. This is based on the terms of service (TOS) of two of the malicious websites and the SSL certificates of a newly created command-and-control (C2). Given the geography of the targets and the current geopolitical situation, it's unlikely that the RomCom RAT threat actor is cybercrime-motivated. RomCom RAT, Cuba Ransomware, and Industrial Spy have an apparent connection. Industrial Spy is a relatively new ransomware group that emerged in April 2022. However, given the targets' geography and characteristics, combined with the current geopolitical situation, it's unclear if the real motivation of the RomCom threat actor is purely cybercriminal in nature.

- **ARTICLE LINK**
- **ROMCOM THREAT**
- **MALWARE ANALYSIS**

OPERA1ER HACKERS STEAL OVER $11 MILLION FROM BANKS AND TELCOS

A threat group that researchers call OPERA1ER has stolen at least $11 million from banks and telecommunication service providers in Africa using off-the-shelf hacking tools. Between 2018 and 2022, the hackers launched more than 35 successful attacks, about a third of them carried out in 2020. Analysts at Group-IB, working with the CERT-CC department at Orange, have been tracking OPERA1ER since 2019 and noticed that the group changed its techniques, tactics, and procedures (TTPs) last year. Concerned about losing the threat actor's tracks, the cybersecurity company waited for the group to resurface to publish an updated report. This year, Group-IB observed that the hackers were active once again. The hacker group is formed of French-speaking members believed to operate from Africa. Apart from targeting companies in Africa, the gang also hit organizations in Argentina, Paraguay, and Bangladesh. OPERA1ER relies on open-source tools, commodity malware, and frameworks like Metasploit and Cobalt Strike to compromise company servers. They obtain initial access through spear-phishing emails leveraging popular topics like invoices or postal delivery notifications. The emails have attachments that deliver the first-stage malware, among them Netwire, bitrat, venomRAT, AgentTesla, Remcos, Neutrino, BlackNET, and Venom RAT. Group-IB also says that the hackers distributed password sniffers and dumpers.

- **TECHNICAL REPORT**
- **ARTICLE LINK**

RISE OF THE CYBER LAMB CHOPS

>. THOMAS JEWKES

In the 1950s, a ventriloquist, named Shari Lewis, put a sock on her hand and became famous. Lewis created the persona of a 6-year-old sheep, named "Lamb Chop," that spoke the punch-line to her jokes. A sockpuppet helped her rise to fame with a very popular 1990's children's program. Fame and fortune from a sock!

Social media today has thousands of sockpuppets. No, Lamb Chop hasn't taken over. A sockpuppet is a phony online identity using "real" accounts for the purpose of deception. Originally, this term referred to people who responded to their own blog posts, or authors who applauded their own books, while criticizing their competition. Nowadays, sockpuppets are used for a wide range of objectives. They are used to shower praise on a person or organization or to antagonize them; they are used to manipulate public opinion, to circumvent restrictions and suspensions, or get others banned from web sites. For instance, Utah Senator Mitt Romney acknowledged operating a secret Twitter account, "Pierre Delecto," in order to defend himself against criticism -- his sockpuppet.

The impact of sockpuppets would be marginal, except for the fact that nation-states create armies of sockpuppet bots to divide people and dispense misinformation. A single operative may monitor hundreds of sockpuppets, and an organization may use hundreds or thousands of operatives. The bot may simply "re-tweet," "like," or "re-post" a divisive headline or comment.

RISE OF THE CYBER LAMB CHOPS

>. THOMAS JEWKES

While a human Twitter user may post a few times a day, a bot may tweet hundreds of times per day, all day, on a specific topic. One study by USC analyzed election-related tweets sent in September and October 2016 and found that 1 in 5 were sent by an automated sockpuppet. Some social media platforms have developed software to identify and block bots, so puppeteers have developed something called Cyborgs. These Cyborg accounts mix human subtleties with the 24/7 work ethic of a bot. These are much harder to identify.

Awareness of threats is a step in the right direction. Michelle Menninger, a student in the University of Arizona's Cyber Operations program recently made this comment to me,

"Technology opens up an entire world to my kids that could easily destroy their innocence. Being in the Cyber program gives me the opportunity to speak openly with them about the dangers of technology and allows me to be in control of it, instead of letting technology control us."

Nation-state actors use technology to attack the U.S. and spread misinformation in order to destabilize our republic. An article on Wired calls the Russian campaign of disinformation "Active Measures" (https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/). Their objective is to get Americans to argue about an issue – any issue, as long as it's divisive.
These sockpuppets may appear as someone trusted in your community to draw you into the fray and make you think there is an actual human behind an idea or a movement. They spread lies or half-lies, innuendos, and fake news. They are looking to degrade civil discussion of a given topic and inflame opposing views.

RISE OF THE CYBER LAMB CHOPS

>. THOMAS JEWKES

For these actors, a divided America is much less of a threat than a united one.

We are all susceptible to these propaganda campaigns on social media. With all the re-posting and re-tweeting, sometimes it is hard to find the origin of a comment. However, awareness that a sockpuppet army, whose intent is to manipulate public opinion, is out there may provide some protection from taking the bait.

So, the next time you are on social media responding to a post that got your blood boiling, keep in mind that you may be arguing with "Lamb Chop."

BACK TO THE BASICS

>. THOMAS JEWKES

In the Disney classic, "The Sound of Music," the troublesome but optimistic nun turned nanny, Maria, is teaching the Von Trapp children how to sing since they did not know how. She starts into song saying "Let's start at the very beginning, a very good place to start, when you read begin with A-B-C, when you sing begin with do-re-mi." Here at the Cyber Tripwire, we change that second part a bit to apply to cybersecurity. "When you cyber, begin with C-I-A." OK, so maybe it won't be sung by teenagers around the world, and I'll have to postpone my song writing career.

With cybersecurity, getting back to the basics is as easy as C-I-A … Confidentiality, Integrity, and Availability. These are the high-level basics.

CONFIDENTIALITY means that only the people who are supposed to access the data have access.

INTEGRITY means that there are no unauthorized changes to data at all during transmission, in use, or while stored.

AVAILABILITY means that the computer resources are ready and can be accessed by legitimate users.

Together they are referred to as the "C-I-A Triad." For most organizations a chink in the armor of any of the three could cause havoc. Let's look at each one closer.

BACK TO THE BASICS

>. THOMAS JEWKES

The importance of confidentiality differs depending on your industry. If you have a secret recipe like Colonel Sanders, it is critical. If your organization handles any personal information, the protection of that confidential information is required by law. Here are some examples of failure to maintain confidentiality. An unauthorized person access data.

An unauthorized process gains access to data. Consider a hacker that uses malware to copy your data. An unauthorized person accesses an approximate data value, a range. For instance, if someone found out that an employee's salary is within a certain range.

Loss of confidentiality could even be an unauthorized person finding out that a piece of data exists. If you are sending personal information over unencrypted email, the confidentiality of the data is highly at risk.

Integrity does not necessarily require hacker intervention to be lost. It is possible to lose integrity through careless use by an authorized user. For instance, a user that accidently saves unapproved modification to a file without realizing it. Information system errors could also affect the integrity of data. For data to have integrity, it needs to be precise, accurate, meaningful and useful. Modification made must use acceptable ways and only by authorized people or processes. When a hacker captures unencrypted data, changes it, and sends it to the original recipient, the integrity of that data is lost.

BACK TO THE BASICS

>. THOMAS JEWKES

Availability allows authorized users to access and use network resources, like a printer or a website. Available resources must complete the service request in a reasonable time. When I was in college, I remember that the telephone networks lost availability every Mother's Day. The telephones circuits could not handle the flood of calls.

Similar things happen today on the internet when there is an Amazon Day or occasionally during Cyber Monday. When hackers use malware to overload a particular service or website, it is called a Denial Of Service (DOS) attack.

A DOS attack is intended to remove the availability of its victim's resources. As many of you know from experience, you don't need a hacker to lose availability. It could be lost with a malfunctioning resource, or an upgrade gone bad.

So, there it is, the basics of cybersecurity, the C-I-A Triad. Now, we can all go back and singing the rest of the Von Trapp family songs – "So long, farewell, auf wiedersehen, good night."

TROY HUNT LAUNCHES HAVE I BEEN PWNED? (HIBP)

HAVE I BEEN PWNED, is by far one of the most influential advances in cyber security because it made user education easy and straight forward. All you do is go to the HAVE I BEEN PWNED website, enter your email and then it will inform a user if a breach has been detected. User education is one of the hardest to push and this site made it easy and pushed cybersecurity forward.

DECEMBER 4, 2013

THE BIRTH OF RANSOMEWARE

Joseph Lewis Popp allegedly mailed floppy disks to the UK which were labeled "AIDS Information Introductory Diskette" but contained the AIDS trojan which demanded $189 to "renew the license" by sending payment to a post office box in Panama.

DECEMBER 11, 1989

TRAKE DOWN VS. GHOST IN THE WIRES

Kevin Mitnick allegedly performed a remote attack against Tsutomu Shimomura's personal computer, gaining access by using source address spoofing and TCP sequence prediction. But there's no proof he did it and it's generally accepted he lacked the required technical skills. Tsutomu Shimomura is a Japanese-born American physicist and computer security expert. He is known for helping the FBI track and arrest hacker Kevin Mitnick. Takedown, his 1996 book on the subject with journalist John Markoff, was later adapted for the screen in Take Down in 2000. So, in December 1994, when someone broke into Tsutomu Shimomura's elaborate computer system in his San Diego home using a never-before-seen, sophisticated hacking method and then stole some fancy cellular phone tools, Shimomura took it as a personal challenge. The trail apparently led to Mitnick and his later arrest.

DECEMBER 25, 1994

DECEMBER 11

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

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

STUDENT WORKER OPPORTUNITIES

THE CYBER CONVERGENCE CENTER WELCOMES ALL STUDENTS TO APPLY FOR STUDENT WORKER OPPORTUNITIES IN CYBERSECURITY!

INTERESTED? SUBMIT COVER LETTER AND RESUME TO MICHAEL GALDE

Play a critical role in the continuous monitoring and response to significant incidents affecting the Facilities Management critical infrastructure network, including monitoring a ticket queue, alarms, incidents, and trouble tickets. Develop, document, and execute threat hunting operations to detect known adversary TTPs. Document and communicate hunt methodologies and findings. Provide metrics to measure the impact of hunting operations; track and report metrics. Review and document security-related change requests and advise management on approval decisions. Provide investigations, responses, and root cause analysis on incidents affecting the network. Make necessary notifications on identified incidents and critical situations in a calm, problem-solving manner. Assignments are often self-initiated. All other duties assigned.

Minimum Qualifications

- Passed CYBV 301 or CYBV 385
- Passed CYBV 326
- Current University of Arizona Student, enrolled in a minimum of 6 units
- This position requires an FBI Background Check
- Demonstrate experience with Windows desktop environment
- Demonstrate experience with Wireshark
- Experience participating in Capture the Flag events
- Located within reasonable commuting distance to Main Campus as this position is in-person

Preferred Qualifications

- Passed CYBV 400
- Previous work experience in a Security Operations Center environment
- Experience with Linux command line
- Experience with PowerShell

Required Knowledge, Skills, and Abilities

- Attention to detail
- Well-developed organization skills
- Self-starter

LOCATION / HOURS

UNIVERSITY OF ARIZONA
MAIN CAMPUS

9 AM TO 4 PM
20 HOURS A WEEK
$15.00 AN HOUR

CONTACT

michaelgalde@arizona.edu

520-621-0634

THE UNIVERSITY OF ARIZONA
College of Applied Science & Technology

College of Applied Science & Technology
Cyber Convergence Center

>. JOBS/INTERNSHIPS

SECURITY OPERATIONS CENTER ANALYST

TUCSON, AZ

As a Cyber Security Operations (SOC) Analyst you will join the Enterprise Cyber Security (ECS) Operations (Ops) team in providing ongoing support in the areas of incident response and investigation, vulnerability management, full-spectrum digital analysis and applied research in emerging areas of cyber security.

- The ideal candidate must be willing to work in a 24 x 7 x 365 Security Operations Center environment.
- Enterprise IT operational experience - Strong understanding of operating systems, infrastructures, protocols and applications
- Working knowledge of cyber threat actor tactics, techniques, and procedures (TTPs), including the ability to troubleshoot cybersecurity issues, configurations and incidents across a wide range of devices, and infrastructure environments
- Review alerts, alarms, dashboards, and reports to determine relevancy and urgency of cybersecurity threats, vulnerabilities, and incidents.
- Ability to work shift schedule.

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

ADVANCED CYBER THREATS INTERN

REMOTE USA

Job Description:

We are the information security team at Yahoo; known as "The Paranoids". You are a highly motivated current student interested in threat intelligence and investigations who will use Yahoo internal and external tools to protect our consumer and corporate platforms from government-backed actors. During your time here we will give you the opportunity to learn and be an investigator, at internet scale, enable you to protect our users, and empower you to learn from other team members while following the investigation through to the end and disseminating intelligence to appropriate stakeholders.

- Monitor geopolitical events which may have an impact on Yahoo and/or industry partners
- Perform proactive research and identification of Advanced Persistent Threat (APT) groups attempting to target users
- Assess security incidents and assist Yahoo business units to remediate issues
- Work with a variety of cybersecurity tools to investigate, conduct tactical and strategic analysis, draft risk assessments, and disseminate your findings to stakeholders.

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

OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

JOIN CYBER SAGUAROS TODAY

Cyber Saguaros

CYBER_SAGUAROS

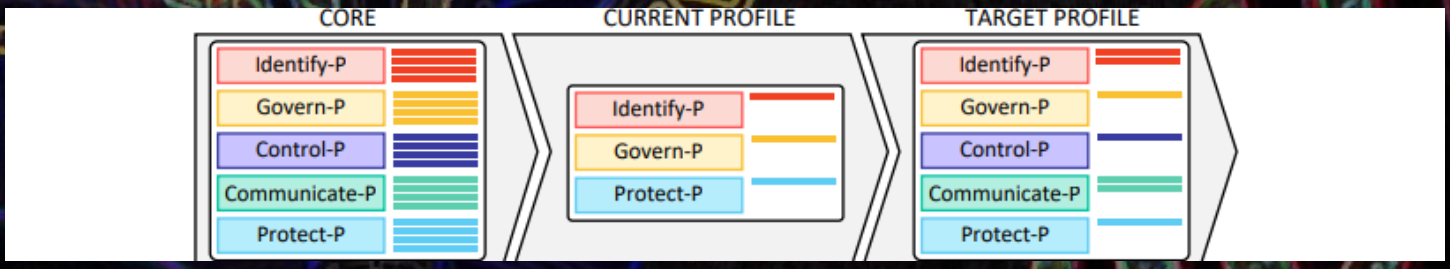
THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 4 OF 6

>. Jordan A. VanHoy

Actualized Harm by Failed Risk Management

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



Cybersecurity Framework

The NIST Cyber Security Framework (CSF) is an alternative approach to the NIST Risk Management Framework. The NIST CSF was introduced in early 2014 and was intended to provide a common language between government and private sector. This was specifically created for the critical infrastructure and commercial organization, but recently adopted by the federal government under executive order 13800. While these documents have traditionally been executed separately, the latest risk management framework revision creates clear mappings to the CSF in order to provide the ultimately flexibility of using the two frameworks in tandem. This was especially useful at the onset of executive order 13800 which required federal organizations to leverage both frameworks. Therefore, this paper would be remiss if the cybersecurity framework was not covered as both documents are now intertwined to provide protection to information, assets, and people. The core elements of the CSF attempt to organize cybersecurity activities at the highest level which are indicated in figure two. The ability to organize at this high level offers immense benefits which include the ability to express priorities, enable risk management decisions, and show the impact of investments in cybersecurity. The functions are further broken down into categories driven by programmatic needs and specific outcomes. These categories may further be broken down into subcategories that specify specific outcomes associated with the desired outcomes of the mapped category. This may be as granular as indicating that encryption is being used on data at rest and in motion.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 4 OF 6

>. Jordan A. VanHoy

Finally, the furthest delineation of the core elements are informative references. Informative references are a set of standards, guidelines, and best practices that are common amongst the sector that maps to a positive outcome desired for the subcategory the reference belongs to.

Identify. This is the first core function as defined by NIST in the CSF. The information developed in this stage will set the foundation for those following by developing an understanding of how to manage cybersecurity risk to assets, people, systems, data, and capabilities. Many factors contribute to the identify stage such as understanding the business function and inherent risks associated with the type of business.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 4 OF 6

>. Jordan A. VanHoy

Protect. The subsequent stage following identify is to develop and implement appropriate safeguards at the system and organizational level. This may also serve as a platform for containing a cybersecurity incident in the event it has already occurred so that the incident does not sprawl further than necessary. Alternative means to protection includes education, awareness, and training, identity management, access control, and maintenance.

Detect. The detect phase is geared towards successful identification of a cybersecurity event within the organization. This may occur through technical means such as logging, intrusion detection, intrusion prevention, or through manual continuous monitoring. The goal of this phase is to detect anomalies within the network as quickly as possible so that the anomaly may be remediated if necessary. It may be necessary to manually assess the alerts from technical equipment as many intrusion notification devices are known for their ability to generate false positive notifications.

Respond. While developing the respond function, the organization needs to have the physical, administrative, and technical means to mitigate and stop the spread of a cybersecurity incident. Well-rehearsed policies allow for efficient response in the wake of a chaotic and confusing situation. These techniques can be taken manually or through automated actions. Notes should be completed immediately after the response to conduct an after-action report to discuss the efficiency of the response and subsequent use of tool employment. This provides a basis of continuous improvement for further cybersecurity incidents.

Recover. During the recover phase the organization attempts to maintain resiliency and return to normal operations. If any assets or systems have been taken offline during the incident, it is vital to repair and put back into production as quickly as possible. Strong communication is key, with input from the business continuity plan, disaster recovery plan, continuity of operations plan, and tabletop exercises.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 4 OF 6

>. Jordan A. VanHoy

Cybersecurity Framework Tiers.
The NIST CSF offers a grading factor for implementation of the CSF in the organization. The framework tiers are specifically mentioned to not be a measure of maturity, but rather define the level of capability the organization has for cybersecurity risk management practices. This is derived off of a number of factors, and while organizations are generally encouraged to progress towards tier four, a cost-benefit analysis is the primary driving factor. The tiers range in numerical order of one to four with one being the least capable and four the most capable. Beginning with the tier one which is defined as partial, the organization has ad hoc security management provisions. There is a limited amount of awareness amongst employees in the organization nor does the company understand their role in the greater ecosystem in the information security conflict. Further, the organization fails to leverage external agencies such as the Information Sharing and Analysis Centers (ISACs). Tier two is defined as being risk informed and while risk management practices are approved by management, they may not be organizationally distributed policies. This level introduces the ability to prioritize protection needs based on business requirements, threats to the organization, and organizational objectives.

Tier three is the next logical progression and indicates the entity has repeatable habits. Policies are generally formalized and widely distributed across the enterprise and make risk informed decisions. Management fully understands the severity and impact on all lines of business when cybersecurity is not handled correctly and strives to maintain awareness of the roles and responsibilities within the greater community. This is to say that the organization may have dependencies on other organizations and understand the impact of their decisions in relation to their partners. Finally, the most capable organizations maintain a level of adaptive risk management processes, have an integrated risk management program, and leverage external parties such as ISACs while maintaining situational awareness of support dependencies.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 4 OF 6

>. Jordan A. VanHoy

Cybersecurity Framework Profiles.

A profile as defined by the CSF is the conglomerate and alignment of the functions, categories, subcategories, and if applicable informative references. Profiles represent a resemblance to the gap analysis by determining the current organizational framework profile composition and developing a profile in which the organization wishes to obtain. This is based on business functions and feasibility of implementation but defines a road forward for continuous improvement.

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A GREAT END TO THE SEMESTER
>. GOOD LUCK ON FINALS
>. HACK THE PLANET!!
>. ---END TRANSMISSION---

DECEMBER 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