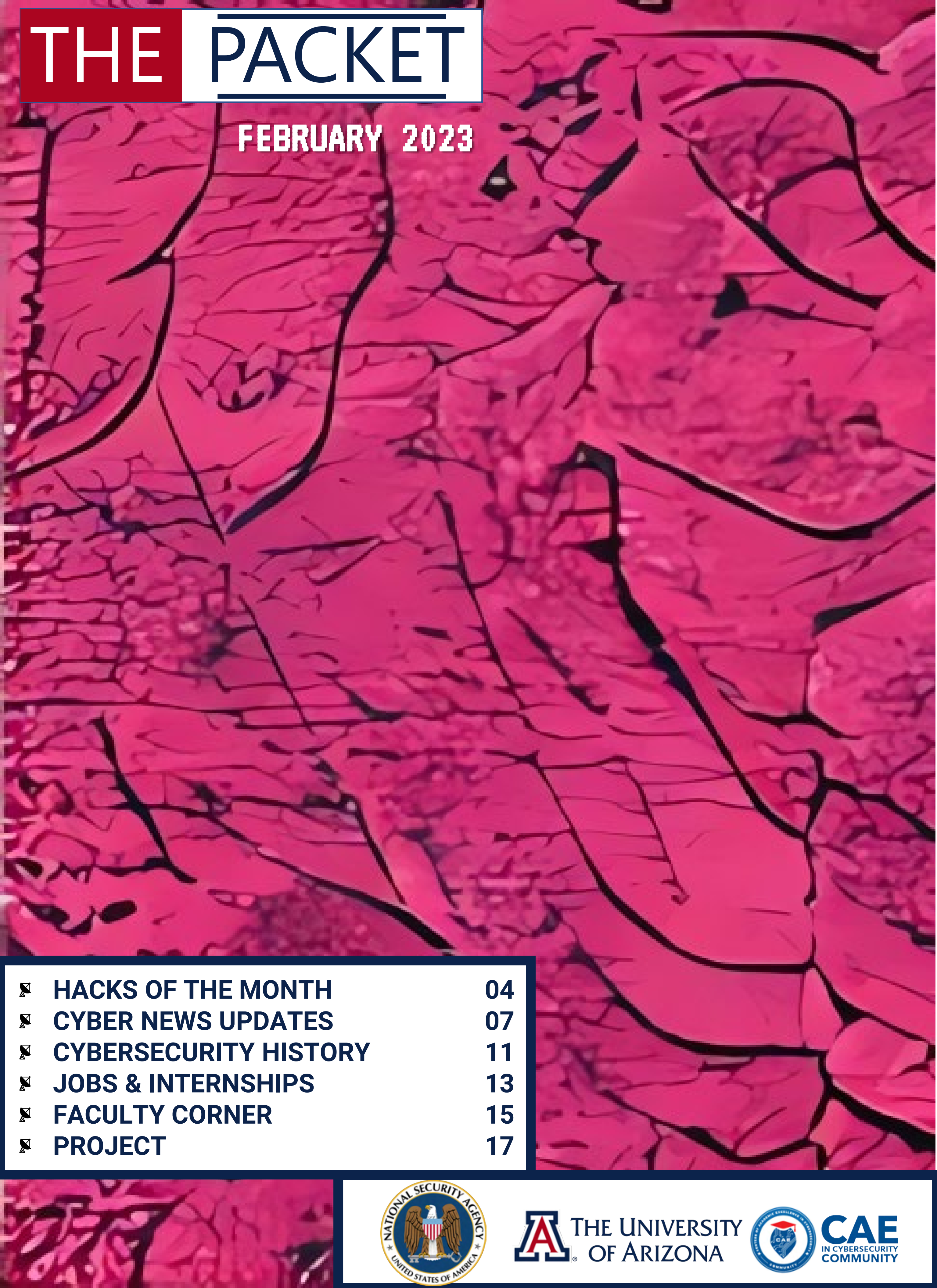
THE PACKET

FEBRUARY 2023



- HACKS OF THE MONTH 04
- CYBER NEWS UPDATES 07
- CYBERSECURITY HISTORY 11
- JOBS & INTERNSHIPS 13
- FACULTY CORNER 15
- PROJECT 17

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

IC CAE Speaker Series 2023.

The Digital Data & Social Media of Digital Gaming

Join us for our IC CAE Speaker Series in 2023! This is a series of virtual events that will highlight important themes in the Intelligence Community, providing students and faculty professional development.

Register Here

SPEAKER

AMBER SCHROADER

CEO and Founder of Paraben Corporation

MONDAY

February 27, 2023
Start at 4:00 PM AZ

Intelligence Community
Centers for
Academic
Excellence

College of Applied Science & Technology
Cyber Convergence Center

TALK ABSTRACT

THE DIGITAL DATA & SOCIAL MEDIAL OF DIGITAL GAMING

Over 1.2 billion people play online gaming, and it has become a hub of data for potential investigations. The average gaming session lasts hours and interaction in an entirely new virtual world can leave fingerprints of conversations, relationships, and data. Jump into this virtual reality of online gaming to see what new information can be gathered from this emerging social network. You will learn about the different popular gaming environments, social media tools used by gamers, and there associated artifacts.

SPEAKER BIO

AMBER SCHROADER

Over the past three decades, Ms. Schroader has been a driving force for innovation in digital forensics. Ms. Schroader has developed numerous software programs, courses, and guides in the areas of recovering data from smartphones, computer hard drives, cloud, email, and gaming systems. Ms. Schroader established protocols for the seizure and processing of digital evidence that has been used by numerous organizations throughout the world. Ms. Schroader has coined the concept of the “360-degree approach to digital forensics” and “Forensics of Everything-FoE” with her focus on unique problems in digital evidence and solutions.

Ms. Schroader has been a huge industry influence in pushing for a big-picture consideration of digital evidence. An accomplished design architect, curriculum developer, and instructor; Ms. Schroader has written and taught numerous classes for this specialized field as well as founded multiple certifications. Ms. Schroader continues to support her through book contributions and other industry speaking engagements.

US NIST UNVEILS WINNING ENCRYPTION ALGORITHM FOR IoT DATA PROTECTION

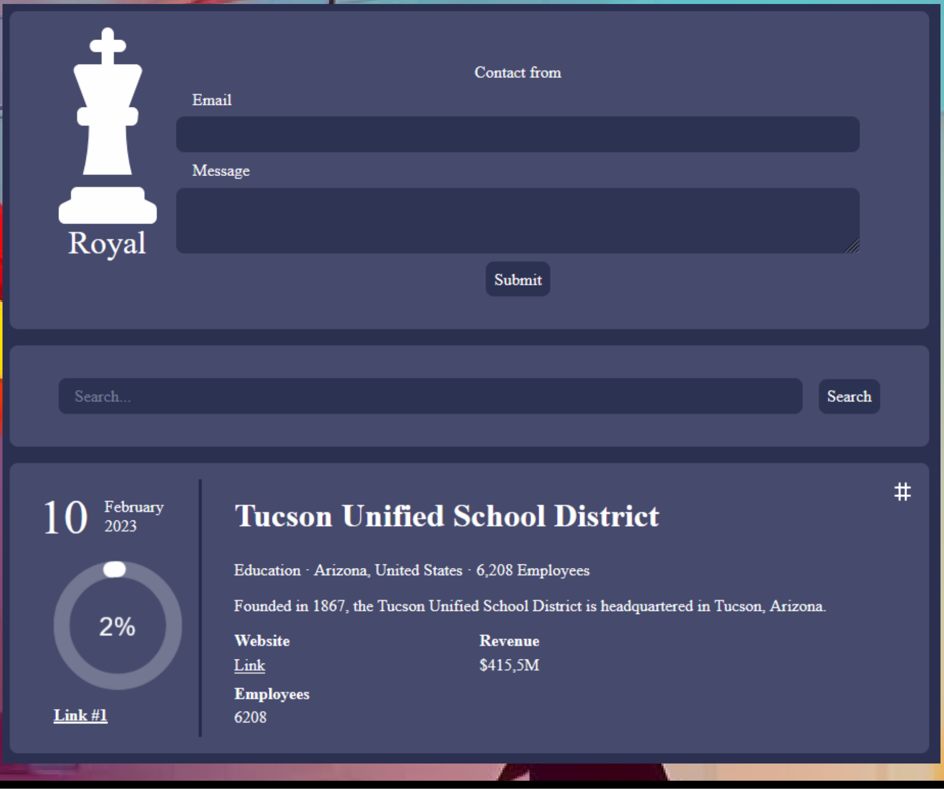
ASCON (AEAD for Secure Confidentiality and Non-repudiation) is a family of authenticated encryption algorithms designed to provide secure confidentiality and authenticity to data. It is a type of encryption algorithm that combines encryption and authentication into a single operation, offering both privacy and integrity to the data being transmitted or stored. The main features of ASCON include support for very high performance on a wide range of platforms, low latency, and low power consumption. It is also designed to be highly secure against attacks such as ciphertext tampering, known plaintext attacks, and dictionary attacks. Additionally, it offers full non-repudiation through the use of unique message keys. ASCON is suitable for use in a wide range of applications, including embedded systems, Internet of Things (IoT) devices, cloud computing, and secure communication systems. The algorithm has been standardized by the European Telecommunications Standards Institute (ETSI) and is considered to be a secure and efficient solution for many encryption and authentication needs. The National Institute of Standards and Technology (NIST) announced that ASCON is the winning bid for the "lightweight cryptography" program to find the best algorithm to protect small IoT (Internet of Things) devices with limited hardware resources. Small IoT devices are becoming increasingly popular and omnipresent, used in wearable tech, "smart home" applications, etc. However, they are still used to store and handle sensitive personal information, such as health data, financial details, and more. Despite ASCON's lightweight nature, NIST says the scheme is powerful enough to offer some resistance to attacks from powerful quantum computers at its standard 128-bit nonce. However, this is not the goal or purpose of this standard, and lightweight cryptography algorithms should only be used for protecting ephemeral secrets.

RUSSIAN HACKERS USING NEW GRAPHIRON INFORMATION STEALER IN UKRAINE

Graphiron is a malicious software, or malware, that has been used in cyber attacks. It is a type of Remote Access Trojan (RAT) that allows the attacker to gain unauthorized access to a victim's computer and control it remotely. Graphiron is known for its ability to hide on a compromised system, evade detection by security software, and steal sensitive information such as login credentials, financial information, and other confidential data. The malware can also be used to install additional malware on the infected computer, potentially compromising the entire network. The Russian hacking group known as 'Nodaria' (UAC-0056) is using a new information-stealing malware called 'Graphiron' to steal data from Ukrainian organizations. When launched, 'Graphiron will check for various security software and malware analysis tools, and if none are detected, download the information-stealing component. Some of the processes the downloader checks for include BurpSuite, Charles, Fiddler, rpcapd, smsniff, Wireshark, x96dbg, ollydbg, and idag. Nodaria is the same threat actor that deployed a fake ransomware named 'WhisperGate' on Ukrainian networks in January 2022, performing destructive data-wiping attacks.

CYBERSECURITY INCIDENT SHUTS DOWN TUSD INTERNET, NETWORK SERVICES

A “cybersecurity incident” on Tucson Unified School District’s technology network shut down the district’s internet and network services. “We are actively working to correct the issue and have notified all the appropriate authorities,” said TUSD Superintendent Gabriel Trujillo in a written statement. All TUSD schools will continue their regular school schedules, he said. The district notified parents of the incident via a voice message sent late Monday morning. TUSD spokeswoman Leslie Lenhart declined to answer questions about whether the incident was a ransomware attack and whether any student or employee information was breached. She also did not respond to questions about the kind of information stored in the district’s network service. “We will share an update when more information is available,” Trujillo said, noting that the incident is still being assessed. The developers behind the Royal Ransomware claim to have taken credit for the infection and have placed TUSD on its victim list. It has listed 5 Gigs worth of information which is available for download.



10 February 2023

2%

Link #1

Tucson Unified School District

Education · Arizona, United States · 6,208 Employees

Founded in 1867, the Tucson Unified School District is headquartered in Tucson, Arizona.

Website Link	**Revenue** $415,5M
Employees 6208	

THE BENNIFITS OF AI FROM THE WORDS OF AN AI

Artificial intelligence (AI) is transforming the way organizations operate and secure their information systems. In recent years, the increasing reliance on technology has brought about new challenges for the cybersecurity industry. As cyber threats continue to evolve and become more sophisticated, traditional security measures are becoming insufficient. This is where AI can play a critical role in strengthening cybersecurity. In this article, we will explore how AI can benefit cybersecurity in various ways.

1. Threat detection and response: AI algorithms can analyze vast amounts of data from various sources in real-time to identify and respond to potential security threats. This is far more efficient than manual methods, as AI algorithms can process data at a much faster rate and detect anomalies that may go unnoticed by humans. For example, AI can be used to identify unusual network traffic patterns, detect zero-day attacks, or flag suspicious email attachments. By using AI to automate the detection and response process, organizations can reduce the time it takes to detect and respond to a cyber attack, which in turn can reduce the damage caused.

2. Fraud detection: Fraudulent activities such as phishing scams and account takeover attempts are common in the digital age. AI algorithms can be trained to recognize patterns in data that are indicative of fraud and automatically flag suspicious transactions for review. By analyzing large amounts of data and identifying trends, AI can help organizations detect fraudulent activities much more quickly and accurately than manual methods.

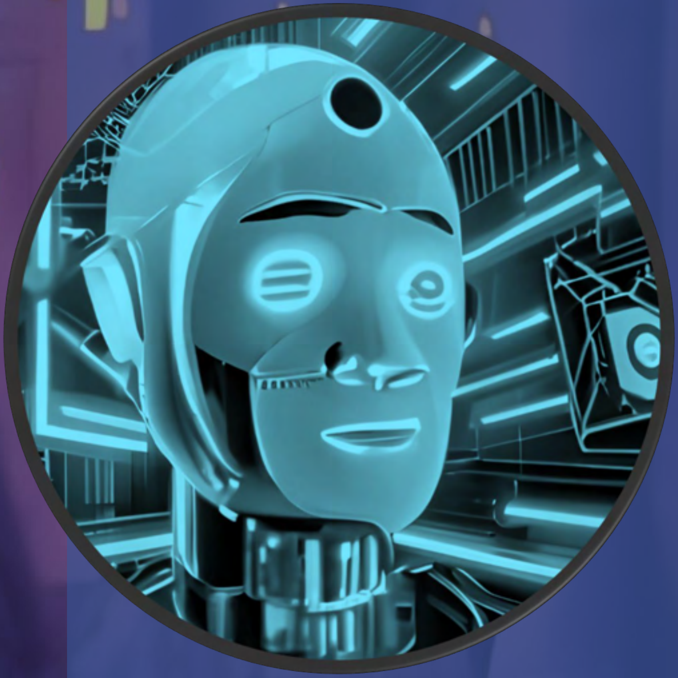
3. Network security: AI can be used to monitor and protect the organization's network from external and internal threats. For example, AI algorithms can be used to detect and prevent malicious activity, such as unauthorized access or data theft, by analyzing network logs and identifying patterns that may indicate an attack. Additionally, AI can be used to detect rogue devices on the network, which can pose a significant security risk.

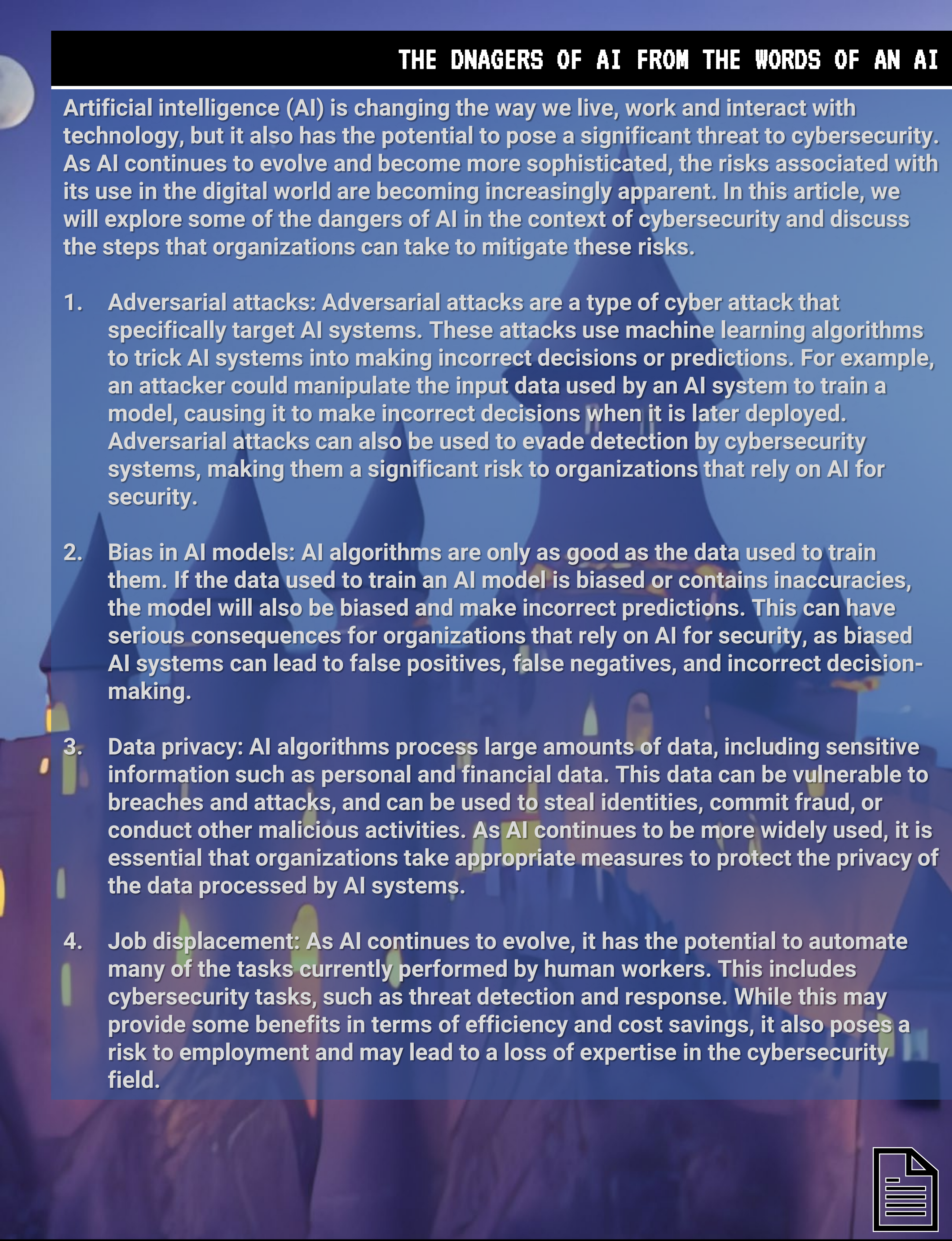
4. Vulnerability management: Vulnerabilities in software and systems are a common target for cyber criminals. AI algorithms can be used to automate the process of identifying and prioritizing vulnerabilities, so that organizations can take the necessary actions to address them in a timely manner. This can help organizations stay ahead of potential security threats and reduce the risk of data breaches.

5. Predictive analysis: AI algorithms can analyze historical data and identify patterns and trends that can be used to predict future security threats. This can help organizations proactively identify and mitigate potential risks before they become a problem. Predictive analysis can also be used to identify high-risk employees who may be more likely to engage in malicious activity, allowing organizations to take proactive measures to mitigate the risk.

6. Human augmentation: While AI algorithms can automate many of the routine tasks associated with cybersecurity, they are not a replacement for human expertise. Rather, AI can be used to augment human capabilities, allowing cybersecurity professionals to focus on more complex tasks. For example, AI algorithms can automate the process of categorizing and prioritizing security alerts, allowing security professionals to focus on more critical tasks.

In conclusion, AI has the potential to greatly benefit the cybersecurity industry. By automating routine tasks, detecting threats in real-time, and providing organizations with the ability to analyze vast amounts of data, AI can help organizations stay ahead of potential security threats and reduce the risk of data breaches. However, it’s important to note that AI is not a silver bullet solution to all security problems, and organizations must be cautious when implementing AI-based solutions. To effectively use AI in cybersecurity, organizations must carefully consider their specific needs and the potential risks and benefits of different AI-based solutions.





THE DNAGERS OF AI FROM THE WORDS OF AN AI

Artificial intelligence (AI) is changing the way we live, work and interact with technology, but it also has the potential to pose a significant threat to cybersecurity. As AI continues to evolve and become more sophisticated, the risks associated with its use in the digital world are becoming increasingly apparent. In this article, we will explore some of the dangers of AI in the context of cybersecurity and discuss the steps that organizations can take to mitigate these risks.

1. Adversarial attacks: Adversarial attacks are a type of cyber attack that specifically target AI systems. These attacks use machine learning algorithms to trick AI systems into making incorrect decisions or predictions. For example, an attacker could manipulate the input data used by an AI system to train a model, causing it to make incorrect decisions when it is later deployed. Adversarial attacks can also be used to evade detection by cybersecurity systems, making them a significant risk to organizations that rely on AI for security.

2. Bias in AI models: AI algorithms are only as good as the data used to train them. If the data used to train an AI model is biased or contains inaccuracies, the model will also be biased and make incorrect predictions. This can have serious consequences for organizations that rely on AI for security, as biased AI systems can lead to false positives, false negatives, and incorrect decision-making.

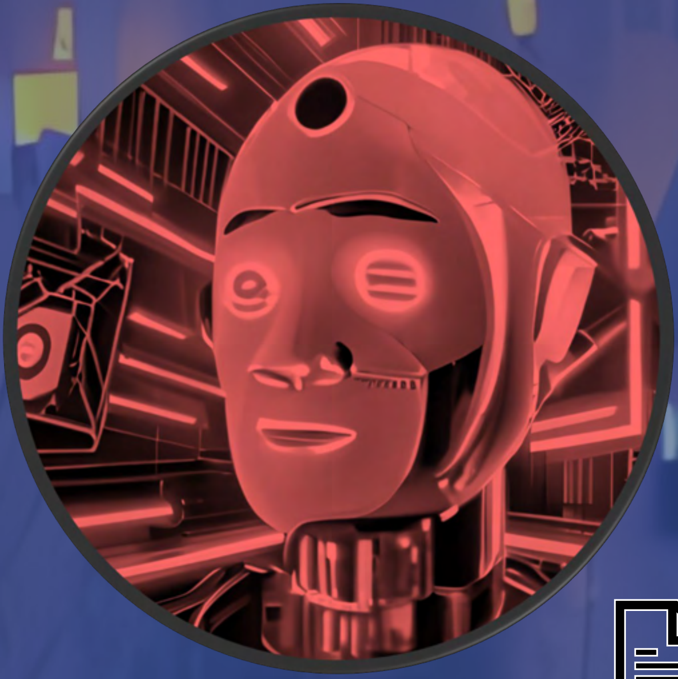
3. Data privacy: AI algorithms process large amounts of data, including sensitive information such as personal and financial data. This data can be vulnerable to breaches and attacks, and can be used to steal identities, commit fraud, or conduct other malicious activities. As AI continues to be more widely used, it is essential that organizations take appropriate measures to protect the privacy of the data processed by AI systems.

4. Job displacement: As AI continues to evolve, it has the potential to automate many of the tasks currently performed by human workers. This includes cybersecurity tasks, such as threat detection and response. While this may provide some benefits in terms of efficiency and cost savings, it also poses a risk to employment and may lead to a loss of expertise in the cybersecurity field.

5. AI-powered cyber attacks: AI algorithms can be used by attackers to automate their attacks and make them more sophisticated and effective. For example, AI algorithms can be used to conduct large-scale phishing campaigns, automate the process of identifying vulnerabilities in systems, or even develop new malware and exploits. The use of AI by attackers can make it more difficult for organizations to detect and respond to cyber attacks, increasing the risk of data breaches and other security incidents.

6. Cybersecurity talent shortage: The increasing use of AI in cybersecurity is creating a shortage of skilled cybersecurity professionals who have the necessary expertise to implement and manage AI-based security systems. This shortage of talent can make it difficult for organizations to effectively leverage the benefits of AI and may increase the risk of security incidents.

In conclusion, AI has the potential to greatly benefit cybersecurity, but it also poses significant risks that organizations must be aware of. To mitigate these risks, organizations must carefully consider the potential consequences of AI and take appropriate measures to protect their systems and data. This includes investing in cybersecurity talent, implementing robust data privacy and security measures, and regularly reviewing and updating their AI-based security systems. By taking these steps, organizations can maximize the benefits of AI while minimizing the risks associated with its use.



FIRST SHMOOCON

ShmooCon is an American hacker convention organized by The Shmoo Group. There are typically 40 different talks and presentations on a variety of subjects related to computer security and cyberculture. Multiple events are held at the convention related to cryptography and computer security such as Shmooganography, Hack Fortress, a locksport village hosted by TOOOL DC, and Ghost in the Shellcode. ShmooCon will not be held in 2021, but in the past tickets for this event sold out very quickly, for the 2020 event they sold out in 17 seconds after being offered for sale.

FEBRUARY 04, 2005

THE FIRST DOCUMENTED DOS-STYLE ATTACK ("MAFIABOY")

Michael Calce is a security expert and former computer hacker from Île Bizard, Quebec, who launched a series of highly publicized denial-of-service attacks in February 2000 against large commercial websites, including Yahoo!, Fifa.com, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. He also launched a series of failed simultaneous attacks against nine of the thirteen root name servers. On February 7, 2000, Calce targeted Yahoo! with a project he named Rivolta, meaning "rebellion" in Italian. Rivolta was a denial-of-service attack in which servers became overloaded with different types of communications to the point where they become unresponsive to commands. At the time, Yahoo! was a multibillion-dollar web company and the top search engine. Mafiaboy's Rivolta managed to shut down Yahoo! for almost an hour. Calce's goal was, according to him, to establish dominance for himself and TNT, his cybergroup, in the cyberworld. Calce was also responsible for bringing down eBay, CNN, and Amazon via DDoS. Calce attempted but was unsuccessful in bringing down Dell during this DDoS attack.

FEBRUARY 07, 2000

SSL RELEASED BY NETSCAPE

SSL 2.0 was released by Netscape, the SSL 1.0 version was never released to the public because of its serious security flaws. SSL 2.0 also contained security flaws and was quickly replaced by SSL 3.0 in 1996. Then, in 1999, the first version of TLS (1.0) was released as an upgrade to SSL 3.0. Since then, there have been three more TLS releases, with the most recent release being TLS 1.3 in August 2018. SSL, short for Secure Socket Layers, is a cryptographic protocol that encrypt data and authenticates a connection when moving data on the Internet. TLS is actually just a more recent version of SSL. It fixes some security vulnerabilities in the earlier SSL protocols SSL is no longer used but you may come across website certificates being referred to as SSL certificates. The reason why most people still refer to them as SSL certificates is basically a branding issue. There's no such thing as just an SSL certificate or just a TLS certificate, and you don't need to worry about replacing your SSL certificate with a TLS certificate. All the "SSL Certificates" that you see advertised are really SSL/TLS Certificates which includes the free certificate via Let's Encrypt.

FEBRUARY 09, 1995

Security Research Intern

Remote

The position will be Remote. During the 12-week internship, you'll be a full-time member of the Security Research team and paired with a mentor on your team. You will have the guidance, environment, and responsibility to execute small projects directly impacting our organization. You will work on real projects, features, and updates that will affect our customers worldwide!

QUALIFICATIONS:

- Pursuing a degree in Computer Science or a related field, with demonstrated cyber security talent and a passion for becoming a security expert.
- Must be currently enrolled in a full-time degree program and returning to the program after completing the internship.
  - Comfortable writing code in at least one programming language
  - Familiarity with relational databases (MySQL, Postgres, SQLServer, Oracle) and ease of working with UNIX or any Linux Platform
  - Knowledge of typical attacker TTPs
  - Understanding of threat intelligence and IOCs is a plus
- Understanding of Common Vulnerabilities and Exposures (CVE)
- Curious mind and eager to learn a variety of tools and technologies

PREFERRED QUALIFICATIONS:

- Experience with Python and SQL
- Working knowledge/experience with AWS, GCP, or Azure
- Working knowledge/experience with Containers
- Sharp analytical abilities and proven design skills
- Experience in data analysis

Information Security Intern

Remote

The Information Security team is looking for someone with a strong work ethic, a fantastic attitude, and comfortable tackling any challenge. We provide significant flexibility and autonomy to team members, have high expectations, and expect everyone to contribute meaningfully to our broader collective goals.

- Promptly respond to all security incidents and provide thorough post-event analysis.
- Participate in security tool tuning and improvement to minimize false positives and maximize detection and prevention of threats.
- Participate in growing and maturing SOC processes.
- Provide support for IT audits as needed.

QUALIFICATIONS:

- At a minimum, you should be a rising junior, senior, OR masters-level student in a degree/certificate-seeking accredited program
- Strong troubleshooting skills
- Ability to multi-task across multiple technologies and work both independently and in a team environment
- Ability to interact with a broad cross-section of personnel to explain complex security topics in technical and non-technical settings.
- Strong project management skills, including planning and execution
- Strong written and verbal communication skills, including presenting information
- Strong quantitative, analytical and problem-solving skills
- Strong interpersonal, leadership, and communication skills
- Ability to work in a dynamic, collaborative environment

wex™

DEFENDING THE CASTLE OF GONDOR BY: Professor Thomas Jewkes

The brutal battle of the Pelennor Fields in The Lord of the Rings epic, is instructive for cyber defense. Gandalf, the White Wizard, was charged with defending Minas Tirith, and the majestic Castle of Gondor. The castle was constructed with a series of concentric castle walls for protection. During the attack of Dark Lord Sauron's minions, Gandalf tried to hold ground. Eventually, the first wall was breached, so Gandalf ordered his army back behind the next wall. The situation was bleak, but moving behind the next interior wall bought them time as they waited for Aragorn to come with reinforcements.

Cybersecurity for your organization is a lot like defending the Castle of Gondor. You need to slow down the attackers before they get to your critical assets. Protection in layers in the cyber world, much like that concentric castle, is called "defense in depth." An article from Force Point (https://www.forcepoint.com/cyber-edu/defense-depth) defines it well. "Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information." With cyber DiD, like with the Castle of Gondor, if one set of defenses fails, there is another mechanism in place to impede the attack. Sometimes the cyber DiD is called the castle defense due to the parallels between cyber warfare and physical warfare.

The goal of DiD is to slow down the attacker and get them to make "noise," so they can be detected, and the user can get reinforcements. Unlike Gondor, where the siege was quite obvious, cyber-attacks can go undetected for weeks and even months. This is where your cyber-layered defenses can help to slow the attacks down and make some noise.

DEFENDING THE CASTLE OF GONDOR BY: Professor Thomas Jewkes

A control is an action, a device, a procedure, or a technique that removes or reduces a vulnerability. Controls, when used in depth, can make severe vulnerabilities hard for attackers to take advantage of, or exploit.

In the cyber world, there is no single control that can successfully protect against every single type of attack. For your network, the expensive firewall is not going to stop everything, nor will the next-generation anti-virus. You need to have a layered cyber strategy that includes preventive, detective, and deceptive controls to protect your network.

A layered defense would start with the basics of firewalls and anti-virus/anti-malware, but it might also include an intrusion prevention system, end-point detection, centralized monitoring, encryption, web application firewalls, and access control lists, to name a few. Besides these technical controls, you can also add procedural and policy controls – a set of rules to follow, and the proper way of doing things. In addition, you can work on human security by adding cybersecurity training to your layered defense. Human security is critical, as all the leading-edge technology is helpless if the end user provides the hacker the keys to the kingdom.

Aragorn brought the Army of the Dead to save Minas Tirith from Sauron's army. When it came to their defense-in-depth strategy, the sum of the protective layers was much greater than what was offered by each individual component. Just like the Castle of Gondor, your cyber defense needs overlapping and redundant defenses. If the attackers make enough noise, you may have time to get reinforcements in place.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THE PACKET PROJECTS ARE 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!!

First, a word from our friendly AI which will describe the benefits of a honeypot. A honeypot is a security technique used in cybersecurity to detect, prevent, and analyze cyberattacks. It is a decoy system or network that is designed to mimic a vulnerable target, such as a website or a database, in order to attract and trap attackers. The use of honeypots offers several benefits for cybersecurity, including:

1. Early detection of attacks: By attracting attackers to a decoy target, a honeypot allows organizations to detect and analyze attacks at an early stage. This enables organizations to respond quickly and effectively to threats, reducing the impact of attacks on the real systems and data.

2. Analysis of attack techniques: Honeypots provide valuable information about attack techniques and trends. By observing how attackers interact with the decoy system, organizations can gain insight into the methods and tools used by attackers, enabling them to improve their defenses against similar attacks in the future.

3. Identification of new threats: Honeypots can help identify new and unknown threats, as attackers may use different techniques or tools to compromise the decoy system. This information can then be used to develop new countermeasures and improve the overall security of the organization.

4. Reduction of false positives: Honeypots can help reduce false positives generated by security systems, as they provide a clear and distinct target for attackers, reducing the likelihood of false alarms.

5. Improved security awareness: By using honeypots, organizations can improve their overall security awareness and preparedness. By understanding the techniques and tools used by attackers, organizations can better anticipate and defend against future attacks.

6. Cost-effective security solution: Compared to other security solutions, such as intrusion detection systems or firewalls, honeypots are relatively low cost and easy to implement. This makes them an attractive option for organizations of all sizes, especially for those with limited budgets and resources.

In conclusion, honeypots offer several benefits for cybersecurity, including early detection of attacks, analysis of attack techniques, identification of new threats, reduction of false positives, improved security awareness, and cost-effectiveness. By implementing honeypots as part of a comprehensive security strategy, organizations can better protect their systems and data against cyberattacks.

Now, Protecting your network infrastructure is a challenge and after taking CYBV 326 you should be much more aware of how a connection between a client and a server takes place. One of the challenges to protecting your infrastructure is figuring out when a system has been compromised.

You may have been infected by that is trying to avoid detection and while it is running on your network you are at this point unaware that there is any problem. Deploying a honeypot into your network may be one of the early points to alert you to an infrastructure breach. This however will only work if the service we plan to mimic is seen by an attacker and is then attempted to be exploited. So, we want to attract an attacker and will need to mimic a service that is popular enough that the attacker will attempt to connect. For this project we will attempt to mimic a SSH server waiting for a connection on our internal network. To do this for our project we will use a quick and dirty python script to open a connection listener which will wait for a connection to be established and then once an attacker connects to the connection will close the program and then send us an email alerting us to the breach. The goal is to never receive this email but if we do ever receive this email, we will know something, or someone is snooping around on out network, and we need to identify them and then flush them out. So, to create this python project one of the dependencies we will need is yagmail. To do this we will need to install yagmail using the python package manager PIP with the command

```
PIP INSTALL YAGMAIL
```

After this is installed, we will open a python interpreter and type

```
import yagmail
Yagmail.register (‘yourgmailaddress@gmail.com’,
‘yourgmailpassword’)
```

Now I would recommend that you set up an application specific password for this connection so that you are quickly able to revoke it if needed. After this is done you will then have added your credentials into your systems keyring and yagmail can call it the next time that it sends you an email alert.

Next, we will create a new python project and name it something like ssh.py and we can start to code. First, we will list everything we plan to import into our project:

```
import sys
import argparse
import yagmail
import datetime
import time
from socket import socket, AF_INET, SOCK_STREAM
```

Now I want to set up a global variable for our IP address. We will do this with the following:

```
address = “ip address“
welcome  = b”Secret Server Login: “
```

We will simply change the IP address to our system’s IP address for us to pass that into the later functions. Welcome will be our welcome message when a connection is opened.

Now I want to set up a function to run to send us an alert when the program detects a connection, we will do this with the following calls:

```
def send_email(src_address):
            ts = time.time()
            st = datetime.datetime.fromtimestamp(ts).strftime('%Y-%m-
%d %H:%M:%S')
            contents = ("Port 22 SSH was accessed by: " + (src_address) +
" at: " + (st))
            print (contents)
             yagmail.SMTP('Your yagmail account').send('your email',
'HONEYPOT ALERT! - SSH', contents)
             pass
```

So, we are naming our function send_email but we will define this in a later function. Next, I am asking the system for the current time so that I can provide an accurate date and time stamp. I then format this into a format that I like so that I can quickly reference it.

Next, I define contents which is the technical information which will let me know the who and when in an email alert sent to me. This will let me know that port 22 was accessed by a defined IP address that connected to me and then the date and time stamp that this took place. I then print this so that I can see that this took place and pass everything into yagmail to send me my alert email.

The next function will set up the connection watcher and we will do this using the following :

```
def ssh(address,port=22):
        try:
                ski=socket(AF_INET,SOCK_STREAM)
                ski.bind((address, port))
                ski.listen()
                conn,addr = ski.accept()
                print('ALERT! you have been visited by ' + addr[0])
                send_email(addr[0])
                conn.sendall(welcome)
                while True:
                data=conn.recv(1024)
                ski.close(2)
                sys.exit()
        except:
                ski.close()
                sys.exit()
```

So, in this function we are naming this ssh and are opening the port of 22 to mimic a ssh server. The program then just simply waits for a connection. Once a connection has been established it sends the client our welcome message mimicking a login request. This then sends the client IP address to the send_email function to alert us of the intrusion and closes the connection. The logic in this function is quite simple and you could set up a more flushed out interface for the client to interact with, but this will make the intruder think that the server crashed or went down. Either way you would now be aware that someone is on your network.

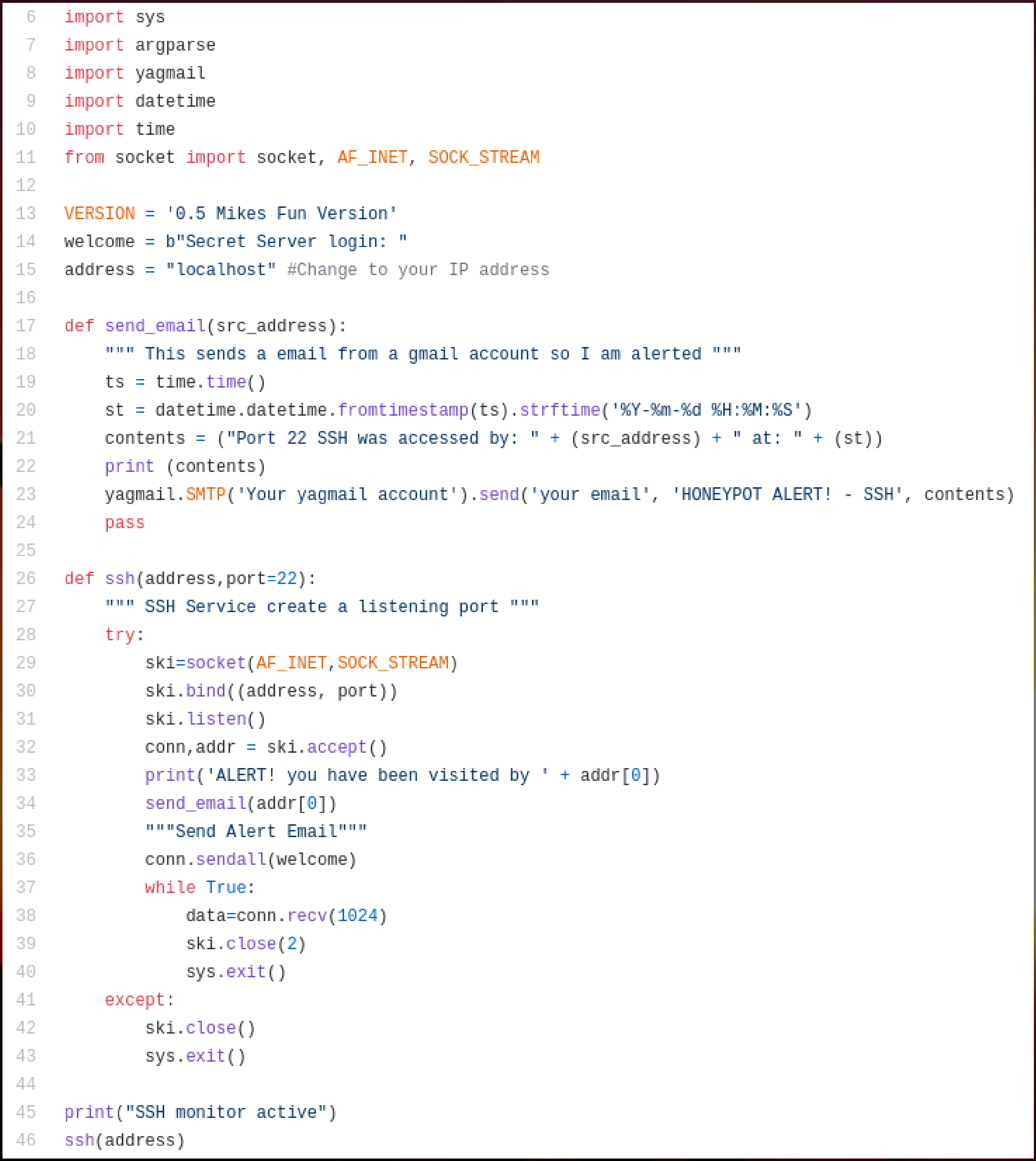
A full copy of my SSH honeypot is available at

https://github.com/mgalde/Mikes_Bee_Knees/blob/master/ssh.py

and you can change and edit any item to make it work for you in your detection attempts. This is a quick and dirty honeypot to at least give you a quick view of a network infiltration. Developing additional logic to make the user think that this is a legit ssh server can make your honeypot less likely to be detected as fake and if you do develop additional logic, I would love to see your work. Please feel free to send them to me and or a pull request.

Providing greater network visibility is one of the most effective ways of identifying a compromised network as most organizations don't have these types of detection mechanisms. This honeypot is less likely to also send you false positives as you will not have a legitimate need to run a ssh server on this machine.

Happy hunting and remember a honeypot are not the only way to identify threats present on your network and if this is activated, it is likely that a compromise has already taken place.



```python
import sys
import argparse
import yagmail
import datetime
import time
from socket import socket, AF_INET, SOCK_STREAM

VERSION = '0.5 Mikes Fun Version'
welcome = b"Secret Server login: "
address = "localhost" #Change to your IP address

def send_email(src_address):
    """ This sends a email from a gmail account so I am alerted """
    ts = time.time()
    st = datetime.datetime.fromtimestamp(ts).strftime('%Y-%m-%d %H:%M:%S')
    contents = ("Port 22 SSH was accessed by: " + (src_address) + " at: " + (st))
    print (contents)
    yagmail.SMTP('Your yagmail account').send('your email', 'HONEYPOT ALERT! - SSH', contents)
    pass

def ssh(address,port=22):
    """ SSH Service create a listening port """
    try:
        ski=socket(AF_INET,SOCK_STREAM)
        ski.bind((address, port))
        ski.listen()
        conn,addr = ski.accept()
        print('ALERT! you have been visited by ' + addr[0])
        send_email(addr[0])
        """Send Alert Email"""
        conn.sendall(welcome)
        while True:
            data=conn.recv(1024)
            ski.close(2)
            sys.exit()
    except:
        ski.close()
        sys.exit()

print("SSH monitor active")
ssh(address)
```

- Welcome to the FEBRUARY 2023 issue of THE PACKET! The Packet publication is from the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and if you have yet to notice, this came out late. Again! Happy Valentine's day anyhow, and yes, I am already starting the March issue and hope to get it out on time. A short month, however, is not helping.
- TUSD, the Tucson Unified School District, experienced a cybersecurity incident earlier this month, and I have been trying to find out more about this incident. There has been no direct admission that the school district was hit with a ransomware attack, but there were rumors. Finally, the group behind the Royal Ransomware claimed they were responsible for the cybersecurity incident and made a little under 5 GIGS of data available for download. Networking services are back up and running today, and it seems as if the school district did not pay the ransom, which is the correct decision overall.
- So, more than ever, we need you, the cyber operations students, to help fill these many cybersecurity gaps. Infecting a school district is not an attack on critical infrastructure or a business organization, but these incidents disrupt daily lives. Organizations like elementary schools to high schools rely on technology, and even these organizations need additional help.

- 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/

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA
THE UNIVERSITY OF ARIZONA
CAE IN CYBERSECURITY COMMUNITY