THE PACKET

APRIL 2023

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

IC CAE Speaker Series 2023.

AI Based Machine Learning/ Intelligence Analysis

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

SPEAKERS

CRAIG NAZARETH AND CHET HOSMER

Assistant Professors of Practice

College of Applied Science & Technology,
University of Arizona

WEDNESDAY

April 19, 2023
Starts at 4:00 PM AZ

Intelligence Community Centers for Academic Excellence

College of Applied Science & Technology
Cyber Convergence Center

CYBER & INFORMATION TECHNOLOGY CONTRACTOR EXPO

Explore career opportunities, join in on Informational sessions, and Interact with contractors working on the groundbreaking technology that powers Fort Huachuca's missions and beyond.

APRIL 6TH
10:00 AM - 4:00 PM

Cochise College Student Union
901 Colombo Ave, Sierra Vista, AZ 85635

agile DEFENSE®

SVAC
SIERRA VISTA AREA
CHAMBER OF COMMERCE

www.svachamber.com.com (520) 458 - 6940 @SierraVistaChamber

ATTACKER CLAIMS TO HAVE US MARSHAL WIRETAP AND MILITARY DATA

Threat actors claim they're selling 350GB of sensitive information, such as wiretap data and photos of military bases, stolen from the US Marshals Service. A malicious actor posted an 'advert' on a Russian-language cybercrime forum, announcing sale of what it said was a USMS data haul. The author claims the dataset includes drone videos of military bases, passports, and IDs, as well as information about convicts, witnesses, drug cartels, and other sensitive details. In February 2023, USMS announced it was hit by a major ransomware attack, compromising sensitive information on known fugitives, legal proceedings, and USMS employees. At the time, the policing body said no data on individuals in the witness protection program was exposed. The author did not provide any data samples as proof but claimed the information dates from 2021 to February this year. The threat actors claiming the theft have put a $150,000 price tag on the dataset, which supposedly includes files marked "Top Secret" and backdoor software for Apple devices.

NEW DARK POWER RANSOMWARE CLAIMS 10 VICTIMS IN ITS FIRST MONTH

A new ransomware operation called "Dark Power" has emerged, which targets organizations globally and demands relatively small ransoms of $10,000. The ransomware uses a compiled date of January 29, 2023, and is written in Nim, a niche cross-platform programming language that is not typically detected by defense tools. Upon execution, the ransomware encrypts files using AES and renames them with the ".dark_power" extension. Notably, it excludes system-critical files and folders to keep the infected computer operational, allowing the victim to view the ransom note and contact the attackers. Dark Power has targeted organizations in the USA, France, Israel, Turkey, the Czech Republic, Algeria, Egypt, and Peru, and is a double-extortion group that threatens to publish stolen data if the ransom is not paid.

NEW MACSTEALER MACOS MALWARE STEALS PASSWORDS FROM ICLOUD KEYCHAIN

A new malware-as-a-service (MaaS) called MacStealer is targeting macOS users, stealing their credentials stored in iCloud KeyChain and web browsers, as well as cryptocurrency wallets and sensitive files. The malware is being sold for $100 as premade builds on dark web hacking forums, and it can run on macOS Catalina and later versions. The developer claims that the malware is still in early beta development and can collect various sensitive data. The malware sends the stolen data to remote command and control servers to be collected later by the threat actor. Users are advised to remain vigilant and avoid downloading files from untrustworthy websites.

FBI CONFIRMS ACCESS TO BREACHED CYBERCRIME FORUM DATABASE

The FBI has officially announced the arrest of Conor Brian Fitzpatrick, the owner of the notorious Breached hacking forum, for his involvement in the theft and sale of sensitive personal information. The forum was notorious for hosting, leaking, and selling data obtained from breached companies, governments, and various organizations. Since the arrest, the remaining admin, Baphomet, had taken the site offline while transferring it to new infrastructure secured from potential compromise by law enforcement. However, Baphomet disclosed that he believes law enforcement has access to the site's servers, leading to the decision to shut down the site permanently. The FBI confirmed that they have access to the database of the Breached forum. Hacking forums are being seized by law enforcement, resulting in threat actors migrating to Telegram as new channels can easily be launched as existing ones are shut down. Telegram has become a hotbed of cybercrime activity, with threat actors amassing followers as they leak stolen data, sell stolen accounts, and discuss their latest attacks.

NEW GOBRUTEFORCER MALWARE TARGETS PHPMYADMIN, MYSQL, FTP, POSTGRES

A new botnet malware called GoBruteforcer has been discovered by researchers at Palo Alto Networks' Unit 42. The malware is written in Golang and scans for and infects web servers that run phpMyAdmin, MySQL, FTP, and Postgres services. GoBruteforcer uses brute force tactics to hack into devices with weak or default passwords, and for each targeted IP address, it scans for phpMyAdmin, MySQL, FTP, and Postgres services. After detecting an open port, the malware attempts to log in using hard-coded credentials. Once in, it deploys an IRC bot on compromised phpMyAdmin systems or a PHP web shell on servers running other targeted services. The botnet is capable of finding potential victims within a Classless Inter-Domain Routing (CIDR), which grants it a broad selection of targets to infiltrate networks. The malware is believed to be in active development with its operators expected to adapt their tactics to stay ahead of security defenses.

MEDUSA RANSOMWARE GANG PICKS UP STEAM AS IT TARGETS COMPANIES WORLDWIDE

The Medusa ransomware group, which launched in June 2021 with few victims, has recently increased its activity and started targeting corporate victims worldwide with million-dollar ransom demands. The group uses a Windows encryptor, and experts are not sure whether a Linux version is available. The ransomware terminates over 280 Windows services and processes for programs that could prevent file encryption and deletes Windows Shadow Volume Copies to prevent their use in file recovery. The group's double-extortion strategy involves leaking data for victims who refuse to pay a ransom and giving paid options to extend the countdown before data is released, delete it or download all of it. Unfortunately, there are no known weaknesses in the Medusa ransomware encryption that would enable victims to recover their files for free.

BLACKLOTUS BOOTKIT BYPASSES UEFI SECURE BOOT ON PATCHED WINDOWS 11

Security researchers from ESET have discovered a new UEFI bootkit called BlackLotus that can bypass the Secure Boot mechanism of fully-patched Windows 11 systems. BlackLotus is the first known public example of UEFI malware that can avoid Secure Boot, which allows it to disable key security features such as the BitLocker data protection feature, the Microsoft Defender Antivirus, and the Hypervisor-protected Code Integrity. Researchers noted that BlackLotus is designed to leverage the vulnerability from CVE-2022-21894 that was discovered last year. This allows the malware to achieve persistence on machines with UEFI Secure Boot enabled. While Microsoft addressed the vulnerability in June 2022, the UEFI DBX has yet to be updated with the untrusted keys and binary hashes used in booting systems with Secure Boot enabled. The cost of a license for BlackLotus was reported to be $5,000.

CHINESE HACKERS USE NEW CUSTOM BACKDOOR TO EVADE DETECTION

Mustang Panda, a Chinese advanced persistent threat group, has been spotted using a new custom backdoor named 'MQsTTang' in cyber attacks. The group is known for data theft attacks and previously deployed customized versions of the PlugX malware to target organizations worldwide. The latest campaign targets government and political organizations in Europe and Asia, focusing on Taiwan and Ukraine. MQsTTang is a "barebones" backdoor that allows the threat actor to execute commands remotely on a victim's machine and receive their output. The malware's use of the MQTT protocol for command-and-control server communications gives it resilience to takedown attempts, while it’s checking for debugging and monitoring tools on the host that makes it more challenging to detect.

Arizona Intelligence Community Center for Academic Excellence

Intelligence Community Scholar Application

We want to invite you to apply to become an IC CAE Scholar!

IC CAE Scholars are students with demonstrated academic, professional, and/or research strengths which are interested in a career in the Intelligence Community.

BENEFITS

- **Competitive advantage when applying for internships and jobs in the Intelligence Community.**
- **Increased networking and engagement opportunities with Intelligence Community agencies and professionals.**

REQUIREMENTS

- **Must be a U.S. Citizen**
- **Interested in a career with the U.S. Intelligence Community**
- **To receive the IC Scholar designation and documentation, you must have a 3.0 GPA to apply and maintain a 3.0 GPA or higher upon graduation.**
- **Current student at the University of Arizona who has completed at least 6 credit hours of study in IC CAE study areas listed below, check one or more: o University of Arizona Cyber Operations or Intelligence & Information Operations degree programs**
- **University of Arizona Intelligence Studies minor**
- **University of Arizona College of Applied Science and Technology CIIO Department certificate programs or other degree programs approved at the discretion of the Principal Investigator for the Arizona IC CAE Program.**

Must be an active participant annually in the IC Scholar program. This means that students are required to attend four professional development events per year, at a minimum. Events include Study Abroad, DNI and IC Internships, Annual Colloquium, University of Arizona Guest Speaker Events, or others as specified and/or approved by the Arizona IC CAE Program.

Students must submit a summary after the event following the requirements:

One page
Single Spaced
Times New Roman 12

Please let us know if you have any questions at cbuldrini@arizona.edu

Intelligence Community
Centers for
Academic
Excellence
Diversity. Knowledge. Excellence.

ROYAL, LOCKBIT, AND MEDUSA OH MY

Ransomware attacks have become an increasingly common and costly threat to businesses and organizations worldwide. Three ransomware groups have recently gained attention for their aggressive tactics and high-profile attacks are Royal, Lockbit, and Medusa ransomware groups. According to articles from SecurityWeek, ZDNet, BleepingComputer, and Security Boulevard, each ransomware group has distinct characteristics and strategies for targeting victims. This article will compare and contrast the Royal, Lockbit. Medusa ransomware groups, discussing their origins, methods of operation, and special attacks, provide insights into the evolving landscape of cybercrime and the importance of implementing robust cybersecurity measures.

NO KINGDOM IS SAFE - ROYAL RANSOMWARE

Royal ransomware employs a distinct technique of partial encryption that enables the attacker to select a particular proportion of data within a file for encryption. Using this method, the attacker can decrease the percentage of encryption for larger files, making it more difficult to detect. Along with encrypting files, the Royal ransomware perpetrators utilize double extortion tactics, threatening to expose the encrypted information publicly unless the victim pays the ransom.

Double extortion is a ransomware attack strategy that involves not only encrypting the victim's data but also threatening to expose or leak the data to the public if the ransom is not paid. In other words, the attackers not only demand payment for the decryption of the victim's data but also threaten to reveal sensitive information publicly, which can have severe consequences for the victim's reputation, finances, or security. This strategy puts additional pressure on the victim to pay the ransom to prevent the exposure of their data.

Double extortion has become increasingly prevalent in recent years, and many ransomware groups have adopted this strategy to increase their chances of receiving a ransom payment. Some attackers have even created websites or marketplaces to auction off the stolen data if the victim does not pay the ransom. Double extortion attacks have affected various organizations, including large corporations, hospitals, government agencies, and educational institutions.

After gaining entry into the network, the Royal ransomware operators establish communication with their command and control (C2) infrastructure and download various tools to consolidate their position within the victim's network. They often repurpose legitimate Windows software to strengthen their foothold further. Like many other ransomware operators, the Royal actors frequently utilize open-source projects to facilitate intrusion activities. For instance, they have recently been observed using Chisel, a tunneling tool that is transported over HTTP and secured via SSH, to communicate with their C2 infrastructure.

The Royal ransomware operators frequently use RDP to move laterally across the network. They have also been known to leverage the Microsoft Sysinternals tool PsExec to facilitate lateral movement. Additionally, the FBI has observed the use of remote monitoring and management (RMM) software, such as AnyDesk, LogMeIn, and Atera, by the Royal actors to achieve persistence in the victim's network. In some cases, the actors have managed to move laterally to the domain controller. There is at least one confirmed instance in which the actors gained access to a legitimate admin account, which they used to log on to the domain controller remotely. Once there, the threat actors deactivated antivirus protocols by modifying Group Policy Objects.

TECHNIQUE	DESCRIPTION
Phishing	Royal actors use phishing emails to trick victims into unknowingly installing malware that delivers Royal ransomware. Third-party reporting shows that this is the most common vector for initial access, accounting for 66.7% of incidents.
Remote Desktop Protocol (RDP)	Royal actors compromise RDP to gain initial access to victim networks. This method accounts for 13.3% of incidents.
Public-facing applications	Royal actors exploit vulnerabilities in public-facing applications to gain initial access to victim networks. This method has been observed by the FBI.
Brokers	According to reports from third-party sources, Royal actors may use brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs. This is a less common method of initial access.

The Royal ransomware operators use legitimate cyber pen-testing tools like Cobalt Strike and malware tools like Ursnif/Gozi, to gather and exfiltrate data from the victim's network. They repurpose these tools for their data aggregation and exfiltration activities. According to third-party reports, the initial hop for the Royal actors during their exfiltration and other operations is often through a U.S. IP address.

The Royal ransomware operators undertake several actions before initiating the encryption process, including:

- Utilizing the Windows Restart Manager to determine whether the targeted files are currently in use or blocked by other applications.
- Using the Windows Volume Shadow Copy service (vssadmin.exe) to delete shadow copies, thus preventing system recovery.
- Creating numerous batch (.bat) files on impacted systems, usually transferred as an encrypted 7zip file. These batch files are designed to perform multiple tasks, including creating a new admin user, enforcing a group policy update, configuring relevant registry keys for auto-extraction, executing the ransomware, monitoring the encryption process, and deleting files upon completion. This includes Application, System, and Security event logs.

THE MCDONALDS OF RANSOMWARE - LOCKBIT RANSOMWARE

LockBit 3.0, also known as "LockBit Black," is a highly modular and evasive ransomware variant that shares similarities with Blackmatter and Blackcat ransomware.

LockBit 3.0 is configured during compilation with multiple options that dictate the ransomware's behavior. Once the ransomware is executed within a victim's environment, additional arguments can be supplied to modify its behavior further, such as specific operations in lateral movement and rebooting into Safe Mode (refer to LockBit Command Line parameters under Indicators of Compromise). If a LockBit affiliate does not have access to passwordless LockBit 3.0 ransomware, they must enter a password during the execution of the ransomware. The ransomware cannot be executed if the correct password is not provided. The password serves as a cryptographic key that decodes the LockBit 3.0 executable. By encrypting its code in this way, LockBit 3.0 can evade malware detection and analysis, as its code is unreadable and unexecutable in its encrypted form.

Signature-based detections may also fail to identify the LockBit 3.0 executable since its encrypted portion varies based on the cryptographic key used for encryption, generating a unique hash. Upon receiving the correct password, LockBit 3.0 will decrypt the main component, decompress its code, and execute the ransomware.

LockBit 3.0 will only infect systems that do not have language settings matching a predefined exclusion list, which can be set during compilation. The exclusion list includes languages like Romanian (Moldova), Arabic (Syria), and Tatar (Russia). If LockBit 3.0 detects a language from the exclusion list, it will stop execution without infecting the system.

LockBit 3.0 ransomware operates under a Ransomware-as-a-Service (RaaS) model and is the latest iteration of previous LockBit versions, including LockBit 2.0 and LockBit. Starting in January 2020, LockBit transitioned into an affiliate-based ransomware variant. Affiliates who deploy LockBit RaaS utilize various tactics, techniques, and procedures (TTPs) to attack a diverse range of businesses and critical infrastructure organizations. This can make it challenging to implement effective computer network defense and mitigation strategies against LockBit attacks.

The Ransomware-as-a-Service (RaaS) model is a type of cybercrime in which ransomware developers offer their software and related infrastructure to other cybercriminals, known as affiliates, for a fee or commission. This model allows the developers to create and distribute ransomware more efficiently while reducing their own operational risk. Affiliates, on the other hand, benefit from this model as they can obtain a ready-to-use ransomware kit that includes the ransomware software, delivery mechanisms, and payment collection infrastructure without developing the ransomware themselves.

In the affiliate-based ransomware model, developers recruit affiliates responsible for deploying the ransomware and infecting targets. The developers offer support to the affiliates, including guidance on how to use the ransomware kit and take a percentage of the ransom payment as their commission. This model allows ransomware operators to scale their operations and targets a broader range of victims without directly engaging in illegal activities themselves.

The affiliate-based ransomware model has become increasingly popular among ransomware operators, allowing them to generate revenue without the risk of being caught by law enforcement. The model also benefits affiliates, as they can earn significant profits with a minimal upfront investment, making it an attractive proposition for many cybercriminals. The downside is that the affiliate-based model can make it harder for law enforcement to track down the original ransomware operators, as affiliates operate independently and can be located anywhere in the world. Additionally, the model can lead to more attacks and more extensive damage to victim organizations as affiliates may use varying tactics and attack a wide range of targets.

TECHNIQUE	DESCRIPTION
Remonte Desktop Protocol (RDP)	Affiliates exploit vulnerabilities in RDP configurations to gain access to victim networks.
Drive-by compromise	Affiliates use malware-laced websites to exploit vulnerabilities in victims' web browsers and deliver the ransomware.
Phishing campaigns	Affiliates use social engineering tactics to trick victims into clicking on malicious links or opening infected attachments.
Abuse of valid accounts	Affiliates leverage stolen or compromised credentials to gain unauthorized access to victim networks.
Public-facing applications	Affiliates exploit known vulnerabilities in public-facing applications to gain initial access to victim networks.

LockBit 3.0 affiliates utilize several tools and services to exfiltrate sensitive company data files before encryption. One of these tools is Stealbit, a custom exfiltration tool previously used with LockBit 2.0. They also use rclone, an open-source command line cloud storage manager, and publicly available file-sharing services such as MEGA. While these services are typically used for legitimate purposes, threat actors can leverage them for system compromise, network exploration, or data exfiltration.

In addition to these tools, LockBit 3.0 affiliates often employ other publicly available file-sharing services to exfiltrate data.

MALWARE IN THE SHADOWS - MEDUSA RANSOMWARE

Medusa Ransomware is a human-operated ransomware that emerged in June 2021 and has gained notoriety after several high-profile attacks on corporate victims, including the Minneapolis Public School district, where the group demanded a $1 million ransom for the decryption key. Medusa Ransomware is distinct from other malware, ransomware, and threat actors that share the same name, such as MedusaLocker or Medusa Botnet.

Upon infection, Medusa Ransomware shuts down over 280 Windows services and processes, including those for mail servers, backup servers, database servers, and security software that may prevent files from being encrypted. It also deletes Windows Shadow Volume Copies to prevent their use in file recovery. Medusa then encrypts files with the AES-256 + RSA-2048 encryption using the BCrypt library, appends the .MEDUSA extension to encrypted file names and creates a ransom note in each folder named "!!!READ_ME_MEDUSA!!!.txt" containing information about what happened to the victim's files. Unlike the older MedusaLocker Ransomware, Medusa uses different file extensions for encrypted files and ransom notes. Medusa Ransomware employs a double-extortion attack, claiming to exfiltrate data from compromised organizations. This attack is a way for the threat actor to encrypt compromised systems and sell or release the exfiltrated data publicly on their leak site, "Medusa Blog," if a ransom is not paid.

Medusa Ransomware is a relatively new variant, with additional information about its campaign, targets, and capabilities being discovered. While it is new to this space, the group is picking up some big targets in its wake as it moves from one cooperate entity to another.

CLOSING THOUGHTS

The year 2023 is emerging as a concerning period for companies dealing with ransomware threats. While Royal, Lockbit, and Medusa are among the prominent ransomware groups operating currently, several other threats pose a significant risk to companies. These groups have adjusted their financial models in response to the growing trend of not paying ransomware demands, indicating a shift in their tactics. In a ransomware attack, organizations may not have to pay to retrieve their encrypted files. However, there is still a possibility that someone might pay to access their internal data, or the attackers may expose the fact that the organization has been compromised. Therefore, companies must stay vigilant and invest in robust cybersecurity measures to protect their valuable assets from evolving ransomware threats.

Cyber Security Intern
DEPT OF HOMELAND SECURITY

The Arizona Department of Homeland Security - Cyber Command is recruiting for several Cyber Security Interns. This would be a prime opportunity for those interested in pursuing a career in Cybersecurity to gain invaluable hands-on experience within a large public sector environment. The Cyber Security Interns will apply critical thinking skills in a cyber environment, learn how to look for threats and risks and apply mitigation techniques. They will learn how to effectively evaluate supply chain compliance against industry risk management best practices for cyber security. Work within a team to apply a NIST-based policy and standards framework across diverse State Agencies.

Address: 1700 W. Washington, Suite 210, Phoenix, AZ 85007

Salary: $16.50
Grade: 01
Closing Date: Open until filled
U.S. Citizenship Required

Candidates must be enrolled in an accredited 4-year College or University with a focus on Computer Information Science, Computer Information Security, or related. They must successfully pass a Department of Public Safety fingerprint background check.

If you have any questions, please feel free to contact Ariel Gonzalez at agonzalez@az.gov for assistance

ARIZONA

SUCH A SIMPLE VIRUS, THE VIENNA VIRUS

The Vienna virus was straightforward and became a template for more complex and innovative viruses like Ghostballs, Chameleon, and (possibly) Zerobug as the source code was published in many places. Damage done by this virus was probably minimal regardless of how widespread it became. Vienna was the first virus to be neutralized by an antivirus program written by German hacker Bernd Fix, and this event also marks the first documented antivirus software ever written.

APRIL 01, 1988

HEARTBLEED VULNERABILITY PUBLICLY DISCLOSED

Heartbleed was a security bug in the OpenSSL cryptography library, which was a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed could be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It resulted from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. The Canada Revenue Agency reported a theft of Social Insurance Numbers belonging to 900 taxpayers and said that they were accessed through an exploit of the bug during a 6-hour period on 8 April 2014. The UK parenting site Mumsnet had several user accounts hijacked, and its CEO was impersonated. The site later published an explanation of the incident saying it was due to Heartbleed and the technical staff patched it promptly. Anti-malware researchers also exploited Heartbleed to their own advantage in order to access secret forums used by cybercriminals. The problem can be fixed by ignoring Heartbeat Request messages that ask for more data than their payload need.

APRIL 01, 2014

CHERNOBYL VIRUS DESTROYS BIOS AS A STUDENT CHALLENGE

CIH, also known as Chernobyl or Spacefiller, is a Microsoft Windows 9x computer virus which first emerged in 1998. Its payload was highly destructive to vulnerable systems, overwriting critical information on infected system drives, and in some cases destroying the system BIOS. The malware filled the first 1024 KB of the host's boot drive with zeros and then attacked certain types of BIOS. This payload served to render the host computer inoperable, and for most ordinary users the virus essentially destroyed the PC. The payload tries to write to the Flash BIOS. Those machines that can be successfully written to by the virus have critical boot-time code replaced with junk. This routine only worked on some machines. The virus made another comeback in 2001 when a variant of the LoveLetter Worm in a VBS file that contained a dropper routine for the CIH virus which was circulated around the internet, under the guise of a picture of Jennifer Lopez. On December 31, 1999, Yamaha released a software update for their CD-R400 drives that was infected with the virus and in July 1998, a demo version of the first-person shooter game SiN was infected by one of its mirror sites.

APRIL 26, 1992

Spring 2023: Cybersecurity Operations Intern (Undergraduate)

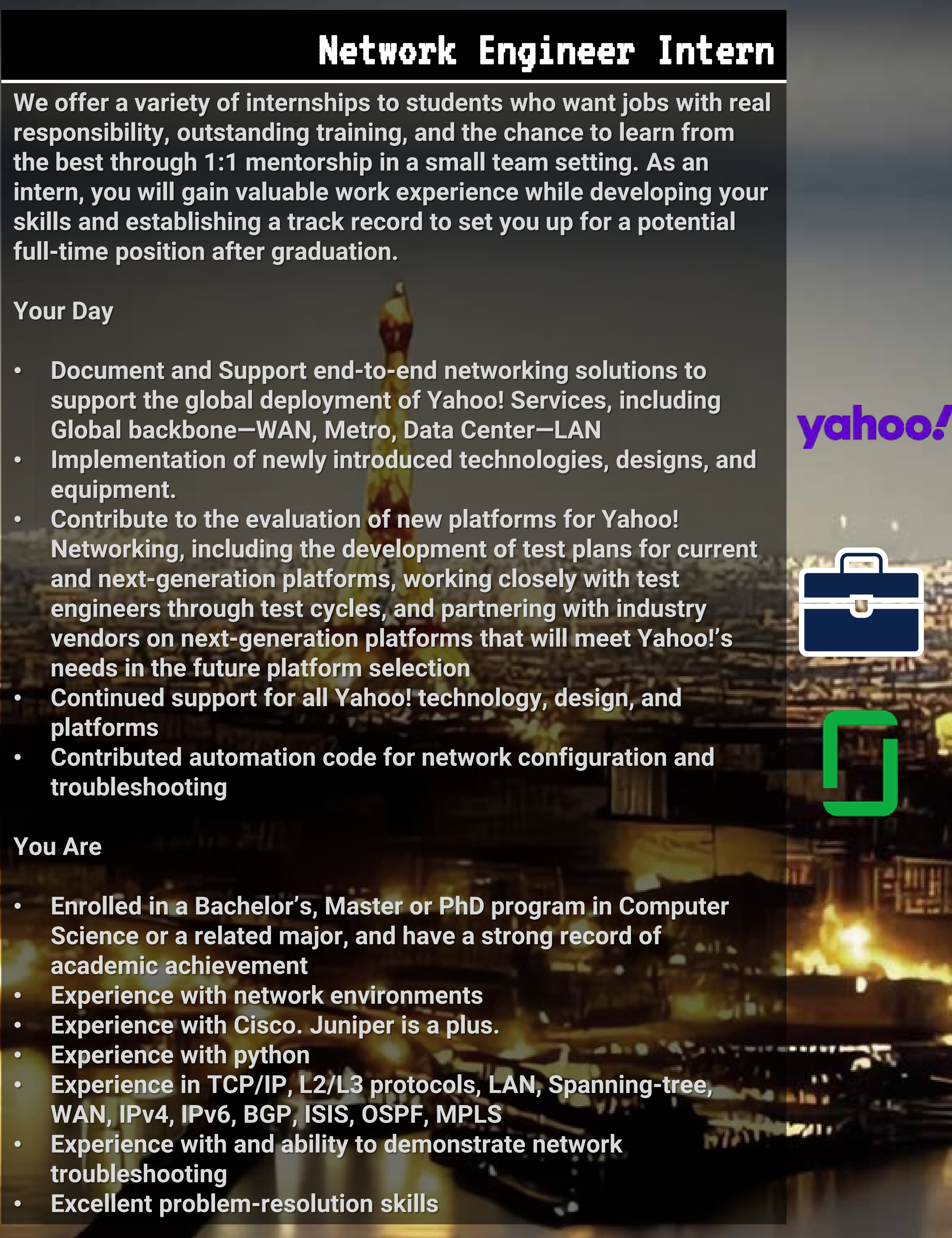
As a full-time (40hrs, M-F) intern, you will have the opportunity to work remotely or hybrid in our Bedford, MA office. In this exciting, fast-growing industry, you will work with some of the most talented and influential people in the robotics field, utilizing cutting-edge technologies.

Responsibilities:

- Identify and solve potential and actual security problems to safeguard information system assets.
- Define access privileges, control structures, and resources to protect the system.
- Recognize problems by identifying abnormalities and reporting violations.
- Conduct periodic audits to determine security violations and inefficiencies.
- Implement and maintain security controls to upgrade the system.
- Communicate system status by preparing performance reports and keeping users informed.
- Follow organization standards to maintain quality service.

Qualifications:

- Currently pursuing a Bachelor's degree in Cybersecurity, IT, Computer Science or a related field.
- Demonstrated decision-making skills and experience working in a collaborative team environment.
- Intuitiveness with an ability to identify and solve complex problems related to rapidly changing technology.
- Basic knowledge of cybersecurity principles, tools, and devices, such as WireShark, ELK, and Splunk.
- Effective communication skills to articulate technical challenges and solutions.
- Basic understanding of Microsoft Office suite, including Word, PowerPoint, Excel, and Teams.



Network Engineer Intern

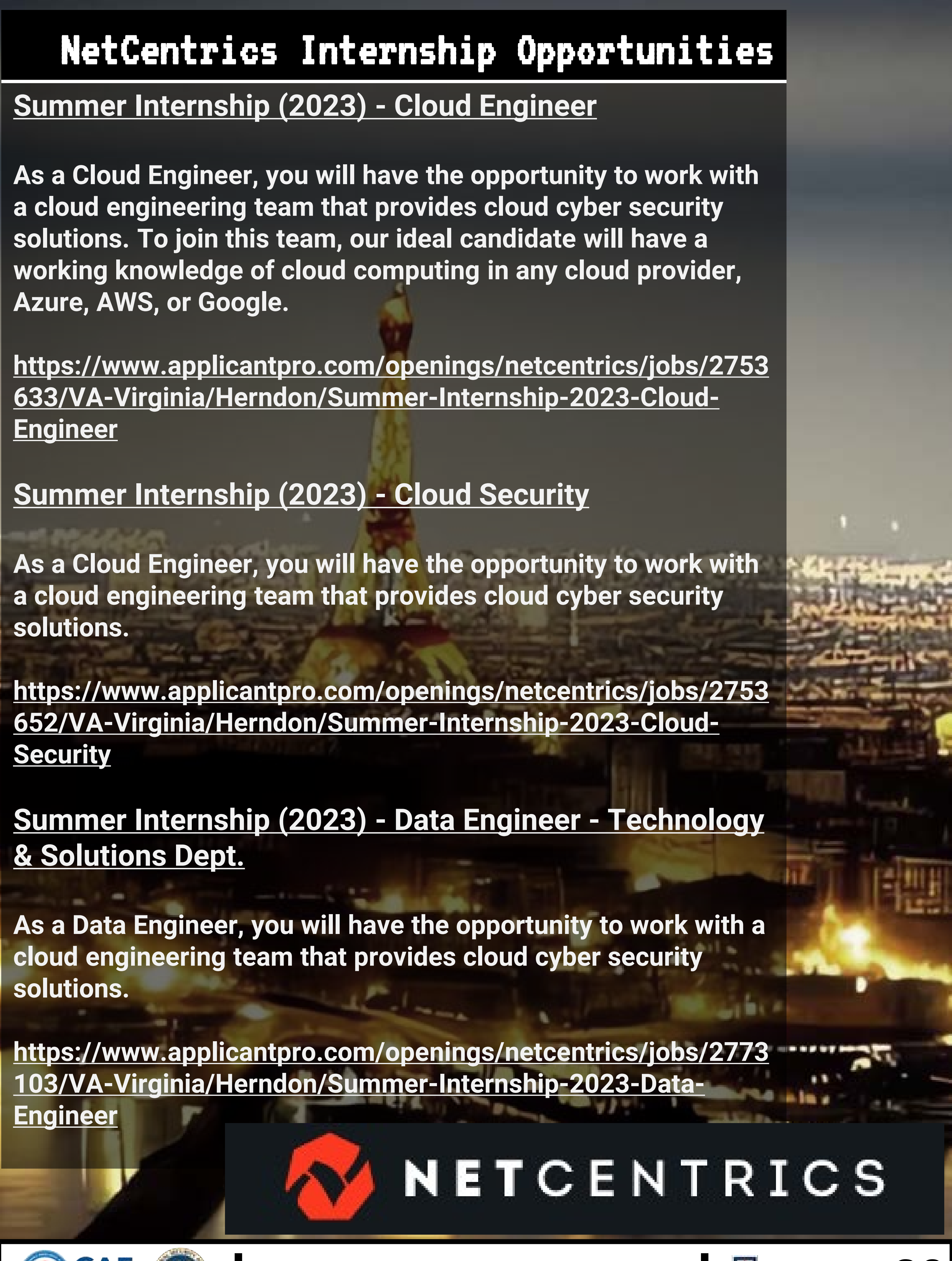
We offer a variety of internships to students who want jobs with real responsibility, outstanding training, and the chance to learn from the best through 1:1 mentorship in a small team setting. As an intern, you will gain valuable work experience while developing your skills and establishing a track record to set you up for a potential full-time position after graduation.

Your Day

- Document and Support end-to-end networking solutions to support the global deployment of Yahoo! Services, including Global backbone—WAN, Metro, Data Center—LAN
- Implementation of newly introduced technologies, designs, and equipment.
- Contribute to the evaluation of new platforms for Yahoo! Networking, including the development of test plans for current and next-generation platforms, working closely with test engineers through test cycles, and partnering with industry vendors on next-generation platforms that will meet Yahoo!'s needs in the future platform selection
- Continued support for all Yahoo! technology, design, and platforms
- Contributed automation code for network configuration and troubleshooting

You Are

- Enrolled in a Bachelor's, Master or PhD program in Computer Science or a related major, and have a strong record of academic achievement
- Experience with network environments
- Experience with Cisco. Juniper is a plus.
- Experience with python
- Experience in TCP/IP, L2/L3 protocols, LAN, Spanning-tree, WAN, IPv4, IPv6, BGP, ISIS, OSPF, MPLS
- Experience with and ability to demonstrate network troubleshooting
- Excellent problem-resolution skills



NetCentrics Internship Opportunities

Summer Internship (2023) - Cloud Engineer

As a Cloud Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions. To join this team, our ideal candidate will have a working knowledge of cloud computing in any cloud provider, Azure, AWS, or Google.

https://www.applicantpro.com/openings/netcentrics/jobs/2753633/VA-Virginia/Herndon/Summer-Internship-2023-Cloud-Engineer

Summer Internship (2023) - Cloud Security

As a Cloud Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions.

https://www.applicantpro.com/openings/netcentrics/jobs/2753652/VA-Virginia/Herndon/Summer-Internship-2023-Cloud-Security

Summer Internship (2023) - Data Engineer - Technology & Solutions Dept.

As a Data Engineer, you will have the opportunity to work with a cloud engineering team that provides cloud cyber security solutions.

https://www.applicantpro.com/openings/netcentrics/jobs/2773103/VA-Virginia/Herndon/Summer-Internship-2023-Data-Engineer

DISH Network Outage - The hack behind the scene

In February 2023, Dish Network suffered a cyberattack resulting in a network outage and the theft of personal information from its internal servers. While the company's pay-tv and wireless and data networks remain operational, satellite TV and Sling TV subscriptions have decreased. The company reported Q4 revenue of $4.04bn, down about 1%. The ransomware gang behind the attack has not yet been named, but sources have suggested that it is the Black Basta gang.

Dish Network is still working to restore customer services fully. Some data was extracted from its systems, but it remains unclear whether it was personal or commercial. Dish has hired "cybersecurity experts and outside advisors" and informed law enforcement of the incident.

The suspected group is the Black Basta ransomware group, a relatively new threat that emerged in February 2022. Once activated, the ransomware deletes all Volume Shadow Copies and changes the Desktop Wallpaper to a new JPG image.

Unlike other ransomware families, Black Basta does not skip files based on their extensions. However, it avoids encrypting critical folders that would make the system inoperable. The ransomware uses the ChaCha20 algorithm to encrypt files, with the key and nonce being encrypted using the hard-coded RSA public key. The encryption of files varies, with the malware encrypting files partially or entirely based on their size. The encrypted files are given a new .basta extension by the ransomware.

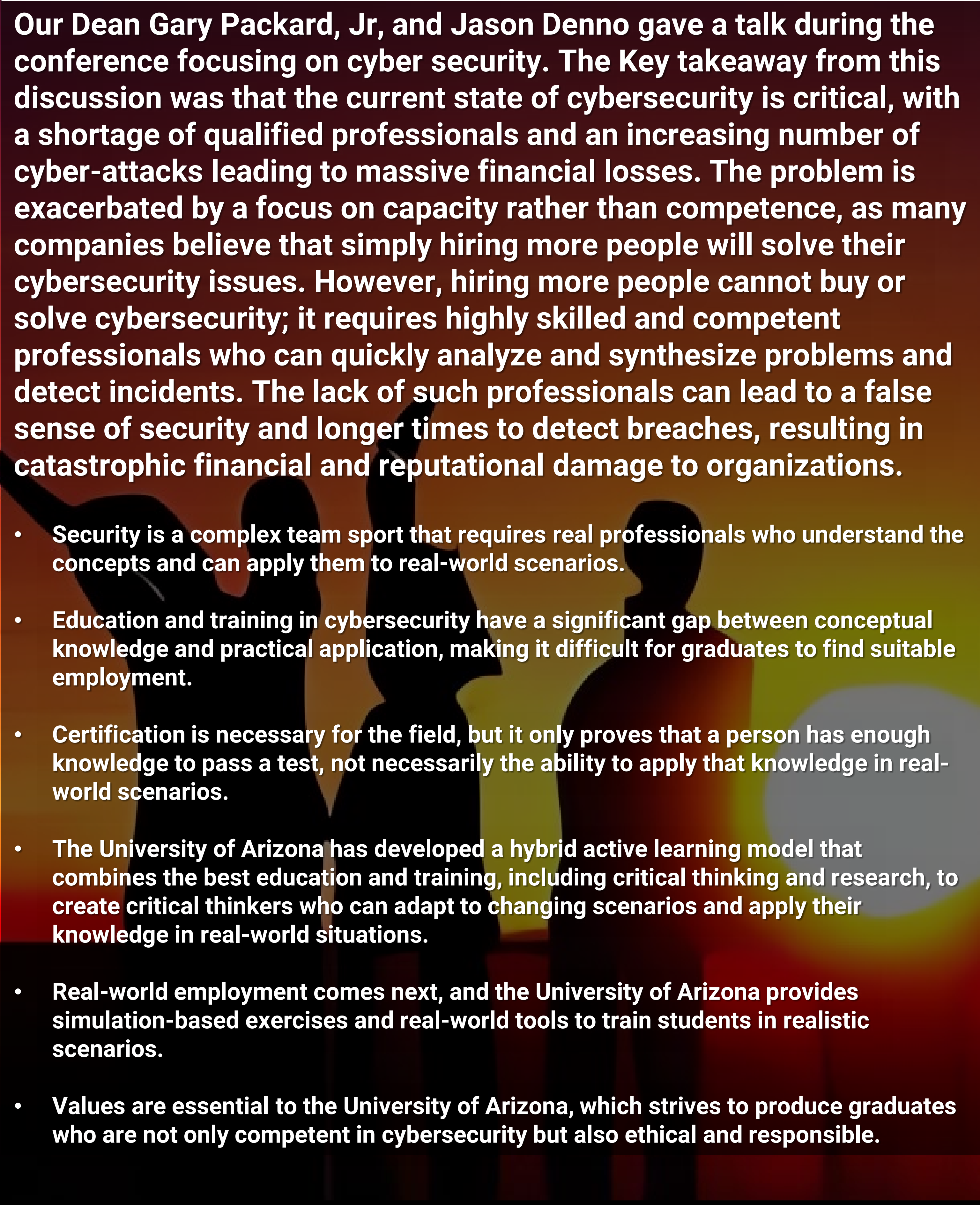
Many U.S. companies are being targeted by an "aggressive" Qakbot malware campaign leading to Black Basta ransomware infections on compromised networks. The campaign uses QakBot malware to gain initial entry and moves laterally within an organization's network. Black Basta uses the double extortion method of stealing sensitive data from targeted companies and then extorting cryptocurrency payments by threatening to release the stolen information. This is not the first time the ransomware crew has been observed using Qakbot, as Trend Micro disclosed similar attacks.

According to cybersecurity researchers, in a previous attack, a spear-phishing email containing a malicious disk image file starts the attack chain, which triggers Qbot, a banking Trojan that retrieves the Cobalt Strike payload. After credential harvesting and lateral movement activities, the Black Basta ransomware is launched on several servers. The threat actors gained domain administrator privileges in less than two hours. They initiated the ransomware deployment in less than 12 hours, affecting over ten customers in the past two weeks. In some instances, the attackers locked the victims out of their networks by disabling the DNS service to complicate recovery efforts.

Black Basta is a ransomware group that is motivated primarily by financial gain, which is typical for most cybercriminals in the field. The group has demanded ransom fees that can reach millions of dollars and has shown a preference for targeting English-speaking countries, particularly those in the "Five Eyes" alliance, indicating a potential political agenda. According to cybersecurity researchers, Black Basta is linked to the Russian-speaking RaaS threat group FIN7, which has been successful in its sophisticated and aggressive ransomware operations since 2013. Evidence of the connection includes the use of similar attack techniques, such as Cobalt Strike, and the use of the same backdoor by both groups. Black Basta also shares similarities with other ransomware groups, including BlackMatter and Agenda. The splintering of loosely connected Russian-speaking ransomware groups has made it challenging for officials to identify and crack down on these groups due to the blurred lines between criminal ransomware and state-backed hacking efforts.

South by Southwest (SXSW) is an annual conglomerate of film, interactive media, and music festivals and conferences in Austin, Texas, United States. It started in 1987 and has grown in size and scope every year since. The conference lasts for ten days, with the interactive track lasting for five days, music for seven days, and film for nine days. The Austin Convention Center in Downtown Austin serves as the "hub" of the festival, and most events associated with the festival take place at venues in and around Downtown Austin.

The University of Arizona's Wonder House returned to the South by Southwest Conference between March 11-14, providing attendees with four days of immersive experiences, music, and speakers. The Wonder House debuted at SXSW last year, featuring researcher talks on topics such as edible insects, creating stress-free environments, and gathering dust from the early solar system. The event also featured 360-degree virtual reality short films and multimedia art installations. I attended because we had cybersecurity talks this year, and Professor Michael Duren and I showcased the Cyberapolis VLE to attendees.



Our Dean Gary Packard, Jr, and Jason Denno gave a talk during the conference focusing on cyber security. The Key takeaway from this discussion was that the current state of cybersecurity is critical, with a shortage of qualified professionals and an increasing number of cyber-attacks leading to massive financial losses. The problem is exacerbated by a focus on capacity rather than competence, as many companies believe that simply hiring more people will solve their cybersecurity issues. However, hiring more people cannot buy or solve cybersecurity; it requires highly skilled and competent professionals who can quickly analyze and synthesize problems and detect incidents. The lack of such professionals can lead to a false sense of security and longer times to detect breaches, resulting in catastrophic financial and reputational damage to organizations.

- Security is a complex team sport that requires real professionals who understand the concepts and can apply them to real-world scenarios.

- Education and training in cybersecurity have a significant gap between conceptual knowledge and practical application, making it difficult for graduates to find suitable employment.

- Certification is necessary for the field, but it only proves that a person has enough knowledge to pass a test, not necessarily the ability to apply that knowledge in real-world scenarios.

- The University of Arizona has developed a hybrid active learning model that combines the best education and training, including critical thinking and research, to create critical thinkers who can adapt to changing scenarios and apply their knowledge in real-world situations.

- Real-world employment comes next, and the University of Arizona provides simulation-based exercises and real-world tools to train students in realistic scenarios.

- Values are essential to the University of Arizona, which strives to produce graduates who are not only competent in cybersecurity but also ethical and responsible.

THE PACKET

- Welcome to the APRIL 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 with summer fast approaching, we bring you the latest cybersecurity threats and trends.
- This month's edition covers a range of cyber threats, including a new strain of Mac malware called MacStealer that steals passwords from iCloud Keychain and the FBI confirming access to a breached cybercrime forum database. We also look at the Chinese hackers using a new custom backdoor to evade detection and a new malware called Gobruteforcer that targets PHPMyAdmin, MySQL, FTP, and Postgres.
- I am also proud of my article, "Royal, Lockbit, and Medusa, Oh My," which is a deep dive into the Royal, Lockbit, and Medusa malware groups. We also break down the Dish Network hack, providing a technical analysis of the Black Basta ransomware group behind the attack.
- Finally, I would like to share my experience at the South by Southwest event, where the Cyber Operations team attended and heard talks on cybersecurity from our dean Gary Packard, Jr., and Jason Denno. It was an eye-opening experience, and we are excited to share our learnings with you.
- As cyber operations students, it is essential to stay up-to-date on the latest cybersecurity threats and trends. These incidents remind us of our crucial role in protecting organizations and individuals from cyber attacks. Stay vigilant, stay informed, and stay safe.

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

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY