THE PACKET

MAY 2024

In This Issue:

Cybersecurity News Updates: 6

Student Highlight: Botnets and IoT: Has Mirai changed anything? 12

National Security Agency · United States of America

The University of Arizona

CAE in Cybersecurity Community

WE WANT YOU FOR THE SOC

Join UArizona's Security Operations Center today for a rewarding, for credit, cybersecurity Fall intern experience!

What Will You Do As A SOC Intern?

INVESTIGATION

Review vulnerability data, and record and track IT security incidents, including:

- Compromised Accounts
- Phishing
- Abuse reports

CORE OF THE INTERNSHIP

OPERATIONS

Get hands-on experience with security tools and practices within a professional environment:

- SIEM
- IPS
- Netflow

EXPERIENCE THE SOC WORKFLOW

HUNTING

Perform threat hunting to detect and eradicate threats using various paid and open source intelligence tools!

LEARN AND USE OSINT SKILLS

This internship is available to be taken **for credit** with advisor approval and provides opportunities to develop your skills as a professional in the industry.

Interested? Apply Now On Handshake:

https://arizona.joinhandshake.com/stu/jobs/8921717

MINIMUM Qualifications & PREFFERED Experience

- Located in **Tucson, Arizona**
- Access to **reliable internet connection** and **computing resources**
- **Internship** is available for **credit** — with **advisor approval**
- **15-25 hours** per week Mon-Fri || 9a -> 5pm
- **Must** be a **current UofA student** studying **Cyber Operations**, **Computer Science**, **or related degree**

- The **Incident Handling Process**
- **Networking** (TCP/IP, UDP, DNS, DHCP, HTTP, etc.)
- **Security technologies** and **concepts** (Firewalls, Network Intrusion Detection systems, SIEM, CIA Triad)
- **NIST Cybersecurity Framework**
- **Common data analysis** tools and techniques
- Understanding of **Information Security best practices** at a individual and/or organizational level

Questions or concerns?
Email: security@arizona.edu

A | Information Security

Welcome to the May edition of "The Packet"! As we approach the end of the academic year, we'd like to take a moment to recognize the hard work and dedication of our students, especially those who are preparing for their final exams and those who are about to embark on the next chapter of their lives as graduates.

To our students facing finals in early May, we encourage you to stay focused, maintain a positive attitude, and give your best effort. Remember that the knowledge and skills you've acquired throughout your cybersecurity education will serve you well, not only in your exams but also in your future careers.

Congratulations to our graduating students on this remarkable achievement! You have demonstrated resilience, adaptability, and a strong commitment to learning qualities that will undoubtedly make you exceptional defenders of our digital world. As you transition from the classroom to the professional arena, always keep in mind that the threat landscape is constantly evolving, and so must our defenses.

As future cybersecurity professionals, you are at the forefront of this ever-changing battle. Your education has provided a solid foundation, but your learning journey is far from over. Embrace the challenge of continuous learning, stay curious, and actively engage with the cybersecurity community to stay abreast of the latest developments, trends, and best practices.

In this issue of "The Packet," we have curated a selection of articles that showcase the diversity and complexity of the cybersecurity landscape. From cutting-edge research to real-world case studies, these stories will inspire you to think critically, explore new possibilities, and remain vigilant in the face of emerging threats.

So, as you prepare for your finals or step into the professional world, remember that you are part of a vibrant, dynamic community of cybersecurity enthusiasts, researchers, and practitioners. Together, we can make a difference in securing our digital future.

Best of luck to all our students, and once again, congratulations to our graduating class! Keep pushing forward, never stop learning, and always strive to be at the forefront of cybersecurity defense.

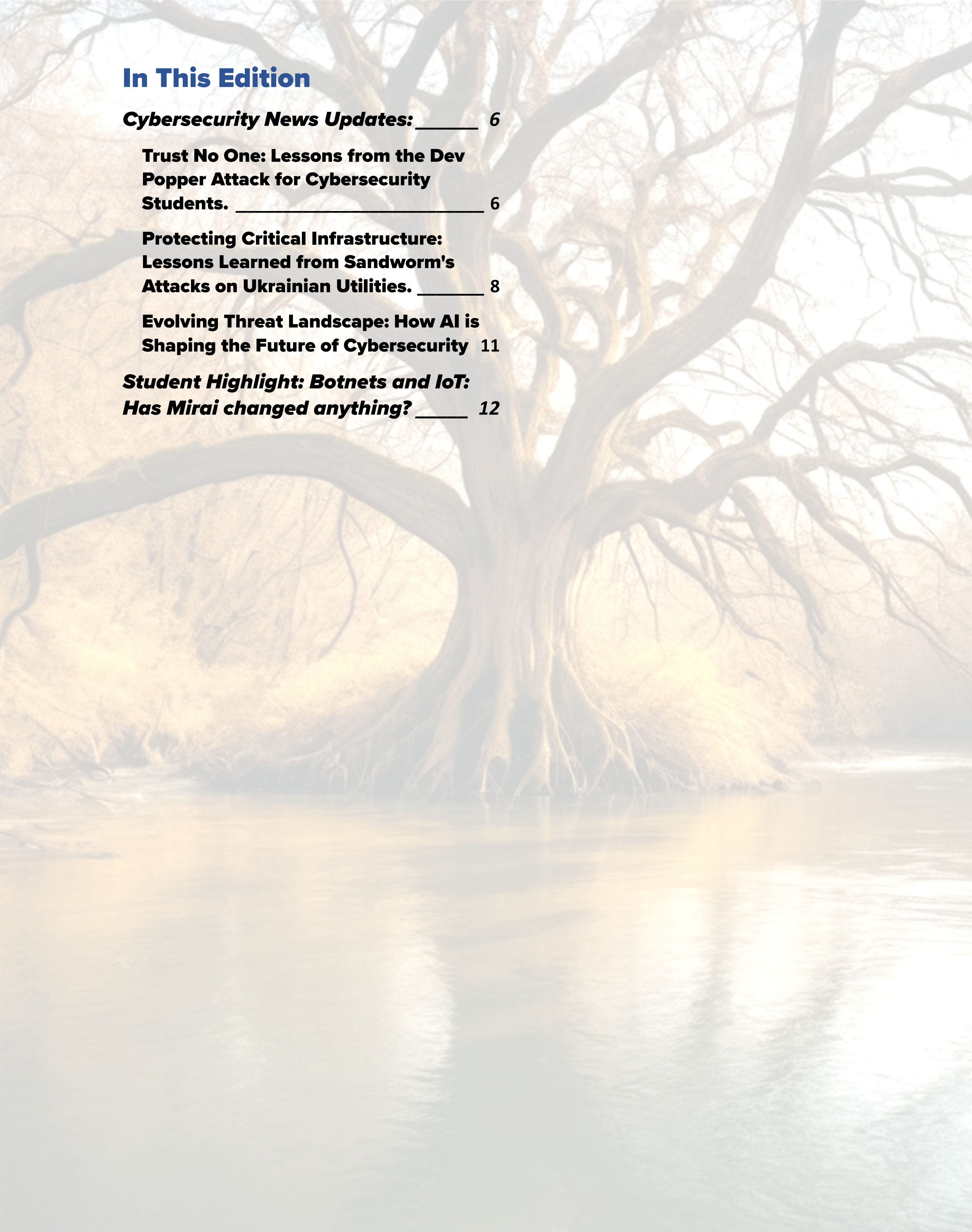
MAY 2024

Michael Galde

THE UNIVERSITY OF ARIZONA

Michael R Galde, MS
Assistant Professor of Practice
College of Applied Sci & Tech
THE UNIVERSITY OF ARIZONA

1140 N Colombo Dr. | Sierra Vista, AZ 85635
Office: 520-621-0634 | Cell: 520-621-0634
michaelgalde@email.arizona.edu



In This Edition

Cybersecurity News Updates: ______ *6*

Trust No One: Lessons from the Dev Popper Attack for Cybersecurity Students. ____________________________ 6

Protecting Critical Infrastructure: Lessons Learned from Sandworm's Attacks on Ukrainian Utilities. _______ 8

Evolving Threat Landscape: How AI is Shaping the Future of Cybersecurity 11

Student Highlight: Botnets and IoT: Has Mirai changed anything? _____ *12*

MAY 2024

THE UNIVERSITY OF ARIZONA
College of Applied Science & Technology

Master of Science
Cyber & Information Operations

01.

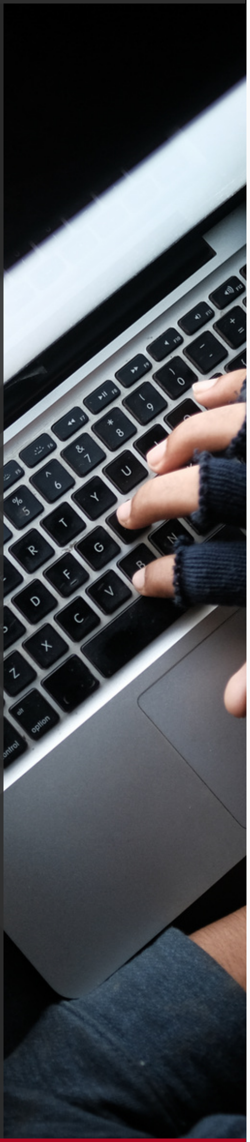
100% Online • Full and Part Time
The program provides an accessible and flexible graduate program to working professionals both in and out of technologically-oriented disciplines.

02.

Fall Only Admission
The MS in Cyber & Information Operations operates as a cohort model, allowing you to learn alongside your peers.

03.

Ample Career Opportunities
Students who graduate with the MS in Cyber and Information Operations degree will have tremendous opportunities in government, defense, and private industry.



Continue on with CAST!

3.5 million
unfilled cybersecurity jobs in 2021

$7 trillion
estimated cost of cybercrime damages in 2022

30 units
away from becoming a qualified cyber expert

Apply Now

Email your questions to CIIOGradProgs@arizona.edu

FUTURE FOCUSED, CAREER READY

azcast.arizona.edu

Cybersecurity News Updates:

As we approach the spring semester's end, all students must stay informed about the ever-evolving cybersecurity threat landscape. In this edition of "The Packet," we bring you the latest news and updates from the world of cybersecurity to help you stay vigilant and protect your digital assets.

Recent headlines have highlighted the increasing sophistication of cyber attacks targeting individuals, businesses, and government entities. From ransomware attacks crippling critical infrastructure to phishing scams seeking to steal sensitive information, the threats are diverse and persistent. By keeping abreast of these developments, you can better understand the risks and take proactive measures to safeguard your online presence.

Remember that cybersecurity is a shared responsibility as you focus on your upcoming final exams. While you dedicate yourself to your studies, make sure also to prioritize good cyber hygiene practices. This includes regularly updating your software and applications, using strong and unique passwords, enabling two-factor authentication whenever possible, and being cautious when clicking links or downloading attachments from unknown sources.

We extend our heartfelt congratulations to our graduating students on your remarkable achievement. As you embark on the next chapter of your lives, carry the knowledge and skills you have acquired during your time here. Remember that cybersecurity constantly evolves, and a lifelong learning commitment will serve you well in your future endeavors.

Good luck to all students on your final exams, and may your hard work and dedication be rewarded with success. Stay safe, stay informed, and keep up the good fight against cyber threats!

Trust No One: Lessons from the Dev Popper Attack for Cybersecurity Students.

As cybersecurity students at the University of Arizona, staying informed about the latest threats and attack vectors in the ever-evolving world of cybercrime is crucial. One recent campaign, dubbed "Dev Popper," has caught the attention of security researchers due to its targeted approach and potential links to North Korean threat actors. This article will delve into the details of the Dev Popper attack, its implications for aspiring cybersecurity professionals, and the lessons we can learn to protect ourselves and our future organizations.

Understanding the Dev Popper Campaign

The Dev Popper campaign is a sophisticated social engineering attack that targets software developers through fake job interviews. The attackers pose as potential employers and reach out to developers, offering them attractive job opportunities. During the interview, the candidates are asked to download and run code from a GitHub repository as part of a supposed coding task.

However, the provided code is a malicious NPM package containing an obfuscated JavaScript file. This file downloads and installs a Python-based remote access trojan (RAT) on the victim's system when executed. The RAT collects sensitive information, establishes persistent connections with command and control (C2) servers, and grants the attackers remote access to the compromised machine.

Implications for Cybersecurity Students

As future cybersecurity professionals, it is essential to recognize the potential impact of attacks like Dev Popper. Social engineering remains one of the most effective methods for attackers to gain initial access to a system or network. By exploiting the trust and ambition of job seekers, the Dev Popper campaign highlights the need for constant vigilance and skepticism, even in seemingly legitimate contexts.

Moreover, the use of obfuscated code and multi-stage infection chains demonstrates the increasing sophistication of threat actors. As students progress in their cybersecurity journey, developing a deep understanding of these techniques and the ability to analyze and detect malicious code is crucial.

Mitigation and Security Measures

To protect themselves from attacks like Dev Popper, cybersecurity students should adopt a multi-layered approach to security:

1. **Be cautious of unsolicited job offers**: Always verify the legitimacy of potential employers and job opportunities. Research the company and the individuals involved before engaging in any interview process.
2. **Avoid running code from untrusted sources**: Exercise extreme caution when asked to download and execute code from external repositories, especially during job interviews. If necessary, use isolated virtual machines or sandboxes to test suspicious code.
3. **Keep systems and software up to date**: Regularly update your operating system, applications, and security tools to ensure you have the latest security patches and features.
4. **Utilize endpoint protection and monitoring**: Implement robust endpoint protection solutions that can detect and block malicious activities, such as the execution of obfuscated scripts or the establishment of unauthorized connections.
5. **Foster a culture of security awareness**: Educate yourself and your peers about the latest threats and best practices in cybersecurity. Encourage open discussions and knowledge sharing within the university community.

The Dev Popper campaign is a stark reminder of the ever-present risks in the digital world, even for those pursuing a career in cybersecurity. As students at the University of Arizona, we are responsible for learning from these incidents, sharpening our skills, and developing a proactive approach to security.

By staying informed, practicing safe computing habits, and fostering a culture of security awareness, we can protect ourselves and contribute to the overall security posture of our organizations. Remember, in cybersecurity, trust no one and always verify.

Protecting Critical Infrastructure: Lessons Learned from Sandworm's Attacks on Ukrainian Utilities.

Protecting critical infrastructure has become a top priority for nations worldwide in recent years. The increasing reliance on technology and the interconnectedness of systems have made these vital assets more vulnerable to cyber threats. Among the most notorious threat actors targeting critical infrastructure is the Russian hacker group Sandworm, or APT44. This article will delve into the lessons learned from Sandworm's attacks on Ukrainian utilities, providing valuable insights for cybersecurity professionals and students alike.

Technical Breakdown

Sandworm's attacks on Ukrainian utilities have been characterized by sophistication and adaptability. The group has employed various tactics, including supply chain compromises, vulnerability exploitation, and custom malware.

In March 2024, Sandworm conducted operations to disrupt information and communication systems at energy, water, and heating suppliers in 10 regions of Ukraine. The attackers infiltrated the targeted networks by poisoning the supply chain, delivering compromised or vulnerable software, or leveraging the software provider's access to the organization's systems for maintenance and technical support.

Sandworm combined previously documented malware with new malicious tools, such as BIASBOAT and LOADGRIP for Linux, to gain access and move laterally within the compromised networks. Other tools in their arsenal included the Weevly webshell, Regeorg.Neo, Pitvotnacci, Chisel tunnelers, LibProcessHider, JuicyPotatoNG, and RottenPotatoNG. These tools were used for persistence, process hiding, and privilege escalation.

The group also utilized custom malware, such as QUEUESEED/IcyWell/Kapeka, a C++ backdoor for Windows that collects system information, executes commands, and communicates securely with command-and-control servers. BIASBOAT and LOADGRIP, two new Linux variants of QUEUESEED, were also discovered during the investigation.

Analysis

The success of Sandworm's attacks on Ukrainian utilities can be attributed to several factors. First, the group exploited weak points in the targets' cybersecurity posture, such as inadequate network segmentation and insufficient defenses at the software supplier level. This highlights the importance of implementing robust security measures within an organization and across its supply chain.

Second, Sandworm demonstrated adaptability by combining well-known malware with new, custom-built tools. This approach allows the group to evade detection and maintain persistence within the compromised networks. Cybersecurity professionals must stay informed about the latest threats and continuously update their defenses to keep pace with evolving attacker tactics.

Finally, the timing of the attacks, which coincided with Russian missile strikes on Ukrainian infrastructure, suggests a level of coordination between Sandworm and Russian military operations. This underscores the need for a holistic approach to critical infrastructure protection that considers cyber and physical threats.

The lessons learned from Sandworm's attacks on Ukrainian utilities are invaluable for cybersecurity professionals and students seeking to protect critical infrastructure. Key takeaways include the importance of robust cybersecurity measures within organizations and across supply chains, the need to stay informed about evolving threat actor tactics, and the recognition that cyber threats can be coordinated with physical attacks.

By studying the technical details of Sandworm's operations, such as their use of custom malware and exploitation of supply chain vulnerabilities, cybersecurity students can gain practical knowledge and insights that will help them defend against similar threats in the future. As the cyber threat landscape evolves, the next generation of cybersecurity professionals must learn from real-world incidents and adapt their strategies accordingly.

Protecting the Perimeter: What Cybersecurity Students Can Learn from the Palo Alto Networks Firewall Breach

In the ever-evolving landscape of cybersecurity, students and professionals must stay informed about the latest threats and vulnerabilities. The recent zero-day exploitation of Palo Alto Networks GlobalProtect firewall devices serves as a compelling case study, offering valuable insights into the tactics employed by state-sponsored threat actors and the importance of implementing a comprehensive security strategy. This article aims to provide an in-depth analysis of the incident, exploring its technical aspects, lessons learned, and defense-in-depth significance in mitigating such threats.

In-Depth Technical Analysis:

The zero-day vulnerability, identified as CVE-2024-3400, was actively exploited by a suspected state-sponsored threat actor, tracked as UTA0218, since March 26, 2024. The vulnerability allowed for unauthenticated remote code execution on affected Palo Alto Networks PAN-OS firewall software. Leveraging this flaw, the attackers installed a custom backdoor named "Upstyle" to pivot into the target's internal network and exfiltrate sensitive data.

The Upstyle backdoor was deployed through a Python script that created a path configuration file at '/usr/lib/python3.6/site-packages/system.pth'. This file contained code to execute every time Python started, enabling the backdoor to monitor web server access logs for attacker-specified patterns. The attackers would request non-existent web pages containing base64-encoded commands, which the backdoor would extract, decode, and execute. The command output was then appended to a legitimate CSS file, allowing the attackers to retrieve the results.

In addition to the backdoor, the threat actors deployed various payloads to establish reverse shells, exfiltrate PAN-OS configuration data, remove log files, and deploy the Golang tunneling tool GOST. They also pivoted to the internal network, stealing sensitive Windows files such as the Active Directory database, DPAPI keys, and browser data containing saved credentials and authentication cookies.

The Importance of Defense-in-Depth:

The Palo Alto Networks zero-day exploit highlights the insufficiency of relying solely on automated defenses or a single security product against determined and sophisticated attackers. A comprehensive defense-in-depth strategy is essential to mitigate the risk of such threats.

Defense-in-depth involves layering multiple security controls throughout an organization's network, systems, and applications. This approach ensures that if one layer of defense is breached, other measures are in place to detect, prevent, or mitigate the attack. In the case of the Palo Alto Networks incident, implementing network segmentation, multi-factor authentication, endpoint detection and response (EDR), and regular security monitoring could have helped detect and limit the breach's impact.

Furthermore, keeping all systems and devices updated with the latest security patches is crucial in preventing the exploitation of known vulnerabilities. Organizations should also conduct regular security assessments, penetration testing, and incident response drills to identify and address potential weaknesses in their security posture.

The Palo Alto Networks zero-day exploit is a stark reminder of the ever-present threat posed by state-sponsored actors and the importance of staying vigilant in the face of evolving cyber threats. By examining the technical aspects of the incident and understanding the tactics employed by the attackers, cybersecurity students, and professionals can gain valuable insights into the current threat landscape.

Moreover, this incident underscores the necessity of implementing a robust defense-in-depth strategy, combining multiple layers of security controls to mitigate the risk of successful attacks. By embracing a proactive and comprehensive approach to cybersecurity, organizations can better protect their assets, detect threats early, and minimize the impact of potential breaches.

As aspiring cybersecurity professionals, it is essential to continually learn from real-world incidents like the Palo Alto Networks zero-day exploit and stay informed about the latest threats, techniques, and best practices in the field. By doing so, we can contribute to building a more secure digital future and help organizations defend against even the most sophisticated adversaries.

Evolving Threat Landscape: How AI is Shaping the Future of Cybersecurity

As artificial intelligence (AI) continues to advance and become more accessible, its potential applications in various fields, including cybersecurity, are becoming increasingly evident. However, just as AI can be leveraged to enhance defensive capabilities, it can also be exploited by malicious actors to develop more sophisticated and evasive attacks. Recent events involving state-sponsored threat groups and their misuse of AI tools, such as ChatGPT, underscore the importance of understanding and preparing for this evolving threat landscape.

Detailed Threat Analysis:

In February 2024, OpenAI, in collaboration with Microsoft's Threat Intelligence team, took action against specific accounts associated with state-sponsored hacking groups from Iran, North Korea, China, and Russia. These advanced persistent threat (APT) groups were found to be misusing OpenAI's large language model (LLM) services, particularly ChatGPT, for various malicious purposes.

The threat actors, including Forest Blizzard (Russia), Emerald Sleet (North Korea), Crimson Sandstorm (Iran), Charcoal Typhoon (China), and Salmon Typhoon (China), utilized AI to enhance their strategic and operational capabilities. These capabilities ranged from conducting reconnaissance and generating spear-phishing content to optimizing cyber operations with scripting enhancements and developing evasion techniques.

While the observed cases did not involve the direct development of malware or custom exploitation tools using LLMs, the threat actors did leverage AI for lower-level tasks such as requesting evasion tips, scripting, disabling antivirus, and optimizing technical operations. This suggests that AI is currently being used to augment and streamline existing attack vectors, rather than creating entirely new ones.

Looking Forward:

As AI continues to advance and become more accessible, malicious actors will likely adapt and find new ways to exploit these technologies. In the near future, we can expect to see more sophisticated social engineering attacks, as AI can generate highly convincing and personalized phishing content. Additionally, AI may be used to automate the identification of vulnerabilities and develop custom malware that can evade detection by traditional security solutions.

Cybersecurity students and professionals must proactively develop and implement AI-driven defensive strategies to stay ahead of this evolving threat landscape. This includes leveraging AI for threat intelligence, anomaly detection, and automated incident response. Furthermore, it is crucial to foster collaboration between AI research organizations, such as OpenAI, and cybersecurity firms to ensure that AI technologies are developed and deployed responsibly, with built-in safeguards against misuse.

Mitigating the Threat:

To mitigate the risks associated with AI-enabled attacks, cybersecurity students should focus on the following areas:

1. Develop a deep understanding of AI technologies and their potential applications in offensive and defensive cybersecurity contexts.
2. Collaborate with AI research organizations and participate in the development of secure and responsible AI systems.
3. Implement and maintain robust security best practices, such as regular vulnerability assessments,

patch management, and employee security awareness training, to minimize the attack surface and reduce the impact of AI-enhanced attacks.

4. Stay informed about the latest developments in AI-driven threats and defensive strategies through continuous learning and engagement with the cybersecurity community.

The integration of AI into the cybersecurity landscape presents both opportunities and challenges. While AI can be leveraged to enhance defensive capabilities, malicious actors can also exploit it to develop more sophisticated and evasive attacks. As demonstrated by the recent actions of OpenAI and Microsoft against state-sponsored threat groups, proactive measures and collaboration between AI research organizations and cybersecurity firms are essential in combating the misuse of AI technologies.

For cybersecurity students, staying ahead of this evolving threat landscape requires a deep understanding of AI technologies, active participation in developing secure AI systems, and continuous learning and adaptation. By embracing these challenges and working together, the cybersecurity community can harness the power of AI to build a more secure and resilient digital future.

Student Highlight: Botnets and IoT: Has Mirai changed anything?

BY: ALEXANDER FRANCUZIK

The author of this paper is a dedicated student who has demonstrated a keen interest in cybersecurity, mainly focusing on the evolution and potential dangers of IoT botnets since the emergence of the Mirai botnet in 2016. The student's thorough analysis and well-researched content shed light on a critical issue that affects not only our devices but also the security of critical infrastructure.

In this paper, the student explores the history of the Mirai botnet, its current variations, and the potential for these botnets to be combined with ransomware attacks, posing a significant threat to IoT devices and the networks they connect to. The author also discusses the challenges in defending against these threats, such as the lack of standardized firmware updates and the need for user awareness.

By examining the current state of IoT security and the potential future risks, this student's work contributes to the ongoing discourse on cybersecurity. It highlights the importance of developing robust strategies to protect our increasingly connected world.

I am pleased to present this student's paper in its entirety. It offers valuable insights and serves as a testament to the high-quality research conducted by the students in Professor Duren's CYBV 626 course.

Botnets and IoT: Has Mirai changed anything

Internet of Things have become commonplace in our lives. From automating homes with appliances and lightbulbs to helping water and power utility companies run their operations more efficiently, it had a truly profound effect on society overall. However, hundreds of thousands of these devices were used to attack servers and wreak havoc on internet infrastructure. Additionally with the rise of ransomware, IoT has become a potential target too. But since the initial attacks 8 years ago, how have things changed and developed? Was there a change in the security of the devices while the IoT devices have grown more popular? What could be a potential future danger?

History of the Mirai Botnet

In August of 2016, the Mirai botnet malware was discovered on devices as it infected various Internet of Things devices, such as routers, DVRs and surveillance cameras (unixfreaxjp). While at the time not a seemingly large phenomenon, a larger cybersecurity focused blog called KrebsOnSecurity was attacked with the entire might of that newly found botnet (Krebs). With about 620 Gbps, this distributed denial-of-service attack was carried out by utilizing a DNS amplification attack, which asks the bot to send UDP packets to DNS resolvers, which contain instructions to deliver the information to the target (Cloudflare). At the time, this was the strongest attack by any botnet, and approximately half of the traffic came from devices within the Mirai botnet (Labs).

Within weeks of this attack, a user by the name of Anna-senpai on the Hackforums community forums, revealed that they are the creator of the bot and released the source code for the malware (Anna-senpai). While this allowed for incredible insight into the workings of the malware, it also allowed other attackers to make use of the code. Within a month of the KrebsOnSecurity attack, Lumen Technologies (formally known as Level3 Communications) reported the Mirai botnet participant count to be at around 493,000 (Labs).

After criminal investigation, it was found that the persons responsible for the initial botnet creation were Paras Jha and Dalton Norman, who were sentenced to six months of home incarceration and ordered to pay $8.6 million in restitution, just over two years after the attack on Krebs' website. (U.S. Attorney's Office, District of New Jersey). The original creators of the botnet were no longer active developing the malware, but as the source code was released, it brings the question if the Mirai botnet has stopped its operations.

Current day analysis of the Mirai-like botnets

In the 8 years since the Mirai botnet has shown its power, IoT has consistently grown: According to the most recent data, there are approximately 17.08 billion connected IoT devices worldwide, with the figure expected to double to 29.42 billion by 2030 (Duarte). However, with this flood of devices, are there still similar vulnerabilities that allow the Mirai botnet to expand?

Mirai works similarly to most DDoS-malware: It has both bots and an underlying infrastructure allowing for communication (Kambourakis et al.). The botnet consistently scans for any new victims that it can access via TELNET on either port 23 or 2323 by then utilizing 62 username & password combinations. Once a connection through the TELNET shell is established, the botnet then proceeds to report the new device to a report server through, which then synchronizes information with a C&C server. This server then can command an infection to a loader proxy, which logs into the new victim and executes a malicious binary. This binary instructs the newly created bot to listen to the C&C server, awaiting any attack instructions.

As the source code was fully distributed by the authors of Mirai, some threat actors used the code to create other species. One of the more recent ones is Okiru, which is a version aimed to infect devices running on ARC CPUs (Leyden). These RISC-based ARC embedded CPUs are used in a multitude of IoT devices, such as cars, phones, TVs, cameras, and other things. Especially as TVs and home surveillance cameras are usually connected either via WiFi or Ethernet, they make prime targets to allow for attacks to be carried out as they usually possess a stable connection. With about 1.5 billion products containing such processors each year being shipped, this became a substantially large target for attackers.

Another derivate version of the Mirai botnet is known as Satori. This particular botnet was detected around mid-June of 2018, targeting D-Link DSL-2750B routers, along with devices running uc-httpd 1.0.0 (Radware). However, instead of creating DDoS attacks against websites, Satori would instead attempt to access Ethereum cryptocurrency mining computers from its privileged spot within the network, attempting to change the destination cryptocurrency wallet addresses, in other to siphon off various miners (Ashford). The author of the malware, Nexus Zeta, continued to develop further Mirai variants such as Musata, which attempted to exploit other D-Link routers (Millman). However, he was indicted by authorities in 2018 (Poulsen).

In the same year, another mutation of the Mirai botnet was found: The OMG botnet (Durando). Unlike previous strains which focus on attacking another system, this one utilizes the Mirai source code to create a network of proxy servers. This in turn allows for threat actors to remain anonymous. This could become troublesome for owners of IoT devices turned proxy servers as any attempt to investigate and find the creators of malware would lead to innocent users.

Ransomware and IoT

Another cybersecurity topic has been popular during Mirai's initial heyday: Ransomware. This type of malware would attempt to gain access to a device and then proceed to quietly encrypt any potentially important user data during its initial run. Afterwards, it would prompt the user to pay, as the name suggests, a ransom to the threat actors to regain that encryption key or risk the files being lost forever. These kinds of extortion attacks have been more prominent as of late. However, in recent research papers, the idea comes up that IoT devices could very well be also locked behind a ransom wall (Zahra and Ahsan Chishti). Security researchers Andrew Tierney and Ken Kunro have demonstrated in 2016 that they could lock a thermostat and require a ransom to unlock its functionality. However, in 2016, a ransomware named flocker locked Smart TVs behind a $200 iTunes gift card ransom to allow the TV to be used.

Connecting the two dangers

While ransomware and Mirai-like botnets might not share a common platform beside them being malware, there is a concern that these systems could be combined to wreak havoc on IoT devices. The main difference in more recent versions of the Mirai botnet is that such are now available on more platforms to infect more devices. As such, each device within the larger botnet can act as an entry point for malicious software to be installed on devices within one's network. This could lead to the owner of the botnet allowing for installation of various malicious software, delivered as a payload through the botnet infected software. If coordinated properly, an attacker could cause ransom attacks on multiple things such as televisions, and even smart lights at the same time, causing the victim to have to resort to payment to restore their home (aside from unplugging everything).

While the idea of home electronics not being usable by their intended owners might not seem particularly problematic, this leads to a larger concern: Operational Technology. IoT has recently found popularity within various parts of critical infrastructure, such as power and water supply. The technology is used to help control various faucets of the system, allowing for authorized employees to make changes from anywhere, or even automation in some cases. However, as these things use similar technologies to other devices, they too are at risk to becoming part of a botnet, or rather a target of one. In fact, in a recent advisory, the US government through CISA warned critical infrastructure organizations about China state-sponsored threat actors being potentially in position on various devices, ready to attack (Fox-Sowell). While it is currently unknown whether these infections utilized botnets, such could be utilized for that.

A thought on how to defend against the dangers of IoT botnets and ransomware

Certainly, there's many things that we can do to protect against the dangers, just like with most computer systems. Ensuring the IoT devices are up-to-date with the latest firmware, flagging any suspicious traffic being sent across the network, and ensuring that each device is connected in a multi-layer security protocol to limit its access to other devices are items as commonplace on any list to help secure one's machine. However, there's only so much one can do in that area.

For one, ensuring the latest firmware being installed is a great starting point, but it requires the software to be installed. However, as manufacturers prioritize bringing new devices to market over maintaining older devices, such get a slower treatment, if any at all. Additionally, such security updates rarely add new features to the device, thus sometimes users tend to be not interested in updating unless new features are made available. Beyond that, it does appear that in recent years, bad update experiences have caused users to be more wary of updating their devices as well (Ahuja et al.). In recent studies it was found that users will delay any major upgrades for 80 days on average, with some responses ranging from "updates are useless" to things where there are concerns about system issues (Vitale et al.). It's reasons like this why operating systems like Microsoft Windows are now forcing users to update their software at some juncture, so much so that there are articles dedicated to "taming" the update feature ("How to Tame Windows Update.").

That said, there is currently no major accepted standard for updating IoT devices. Each manufacturer tends to try to set up their own architecture and pathway to firmware upgrades. While the IETF is currently working on a standard that would help standardize the process of installing updates, including ideas on ensuring that firmware is encrypted and only downloaded from secure sources within IoT, this does have a rather chilling effect (Moran et al.). A recent large-scale analysis of installed IoT firmware versions shows that the current average age of installed firmware versions is at 19.2 months as of April 2020 (Ebbers). While some devices like WiFi access points show a lower than average firmware age (11.0 months), smart home devices show a rather terrifying 77.0 months of firmware age on average. This is even more of a significant discovery as the analysis utilized Shodan, a IoT search engine to find devices displaying their firmware version publicly on the login screen. While the information is giving attackers information that shouldn't be published, this also confirms that these devices are in some way connected directly to the internet, either through a public IP address or port forwarding of some sort. While convenient for many users as they may wish to access their devices from afar, this creates a loophole through which devices could be attacked and turned into botnet participants. While the IETF proposed Software Updates for Internet of Things proposal could actively help with this, I believe the issue here also lies within ensuring that users of these IoT devices are also made aware of both the firmware upgrade functionality and the necessity to upgrade devices on a regular basis.

Another issue lies within flagging suspicious traffic. While corporate networks certainly do monitor their traffic to ensure cyber security insurance compliance, many home users do not. For the most part, many IoT devices ask the user to just connect to the WiFi their mobile phone utilizes, even making it as simple as asking for permission to use the same SSID and password credentials, all in the effort to make the setup process easier and more seamless. However, by using the same SSID, all the traffic from one's home, be it an IoT devices or a laptop creates a way for the IoT to directly connect to the laptop, especially if any malware is installed. One way to solve this particular issue is by creating SSIDs for Internet of Things devices to connect on. Not only would this segregate the network traffic from both sources to ensure no cross connectivity occurs, but it would also help with the performance of IoT devices (Kasif et al.). IoT devices have different needs than other WiFi devices like laptops and phones as they do not require as much bandwidth, but also require a consistent connection. Additionally, the IoT network could be set up in a way that would filter down any DDoS attacks, so that even in the event of a network device being part of an Mirai-type botnet, it could be limited by the network protections.

Future outlooks

Unfortunately, these Mirai-type botnets will continue to exist for a while. Without the code changing much in recent years, these botnets continue to ravage through the network and be utilized to bring down services. The reality is that owners of IoT devices need to be proactive about firmware updates and ensuring that their devices are up and running. Possibly, if an open ecosystem could be created to manage all the devices from one central app or website, it could alert and inform about required upgrades. This, however, would require multiple manufacturers to work together and settle on a standard that is workable for all. Additionally, IETF's SUIT proposal would need to be published and put into action by manufacturers as well to ensure that our devices remain secure. However, with all that said, there's already many IoT devices in the wild as is. Until those devices are eventually cycled out and upgraded to newer, standard-complying devices, we are likely to see these botnets continue to grow as systems continue to be insecure.

Another thought that could help this to be slowed down is for manufacturers to use a common operating system, similar to phones running the Android operating system. The benefits of approach are easy to see: One entity would manage the IoT operating system, and be the central point of contact if any security issues were found. Then it could publish updates to manufacturers who would then push it out to their own firmware. While great in theory, this approach still would have a couple flaws. First, who would the entity be and how would they be able to afford building and maintaining an OS for other companies to use? Additionally, just because the main OS would receive updates would not mean that IoT devices would automatically be updated as well: The Android Open Source Project, led by Google, does have annual major upgrades available, but it takes a while for manufacturers to process and push out those updates to the users as they need to implement their own modifications (Mahmoudi and Nadi). This is if such happens at all, with some manufacturers committing to a short period of updates before letting the devices go stale.

Literature Review

Throughout this paper, multiple sources of information were used to build the thoughts on this. This ranges from various papers and sources about the Mirai botnet and its related species, including a brief review of the source code to various IoT ransomware research papers investigating and creating various proofs of concept, demonstrating the feasibility of such. Additionally, more recent analysis papers were utilized to help understand the age and distribution of firmware updates.

Conclusion

Overall, in the eight years since the first Mirai botnet attacks, there were some changes. The IETF is actively developing a standard to help with regular firmware updates. But unfortunately there's a lot more Internet of Things devices on the web, with some having firmware that was never updated as in some cases, the users aren't even aware of firmware updates. That said, it's will likely take a while for things to be improving. We certainly do have the right ideas and are working on these things, but it will depend heavily on manufacturers wanting to consistently implement updates as opposed to pushing out new products with new features, quickly forgetting the devices released and the security holes left behind.

In theory, a global ecosystem of IoT devices could help with this, allowing for centralized control for the users. This could even be expanded to industrial and operational technologies, allowing for more insight and more connectivity. Unfortunately, this would require profit-driven companies to, once again, ensure that their devices are supported for a while to come. I fear Mirai is only the beginning to an issue quickly growing larger and out of control.

References

Ahuja, Sanju, et al. "Why Doesn't Microsoft Let Me Sleep? How Automaticity of Windows Updates Impacts User Autonomy." arXiv.Org, Jan. 2024. ProQuest, https://www.proquest.com/docview/2914966214?parentSessionId=3bL8zhJOnLKsWvoAEDMWZtkyH9%2FTePeTi4KschjRSDE%3D&pq-origsite=primo&sourcetype=Working%20Papers.

Anna-senpai. "[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC Sou...." HackForums, 29 July 2019, https://archive.is/I9uHb.

Ashford, Warwick. "Next-Gen Mirai Botnet Targets Cryptocurrency Mining Operations | Computer Weekly." ComputerWeekly.Com, 18 Jan. 2018, https://www.computerweekly.com/news/450433414/Next-gen-Mirai-botnet-targets-cryptocurrency-mining-operations.

Cloudflare. DNS Amplification DDoS Attack. https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/. Accessed 24 Mar. 2024.

Duarte, Fabio. "Number of IoT Devices (2024)." Exploding Topics, 22 Feb. 2023, https://explodingtopics.com/blog/number-of-iot-devices.

Durando, Jasper Manuel, Rommel Joven, Dario. "OMG: Mirai-Based Bot Turns IoT Devices into Proxy Servers." Fortinet Blog, 21 Feb. 2018, https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.

Ebbers, Frank. "A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild." IEEE Transactions on Software Engineering, vol. 49, no. 2, Feb. 2023, pp. 816–30. IEEE Xplore, https://doi.org/10.1109/TSE.2022.3163969.

Fox-Sowell, Sophia. "'We Know They're on the Network,' CISA Official Says of Nation-State Actors Infiltrating U.S. Critical Infrastructure." StateScoop, 19 Mar. 2024, https://statescoop.com/nation-state-actors-us-critical-infrastructure-cisa-2024/.

"How to Tame Windows Update." APC, no. 508, July 2022, pp. 86–90.

Kambourakis, Georgios, et al. "The Mirai Botnet and the IoT Zombie Armies." MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 267–72. IEEE Xplore, https://doi.org/10.1109/MILCOM.2017.8170867.

Kasif, Ahmet, et al. "Securing Internet of Things Networks with Gateways and Multi-SSID Technology." 2021 International Balkan Conference on Communications and Networking (BalkanCom), 2021, pp. 45–50. IEEE Xplore, https://doi.org/10.1109/BalkanCom53780.2021.9593270.

Krebs, Brian. "KrebsOnSecurity Hit With Record DDoS." Krebs on Security, 21 Sept. 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

Labs, Black Lotus. How the Grinch Stole IoT - Lumen. 19 Oct. 2016, https://blog.lumen.com/how-the-grinch-stole-iot/, https://blog.lumen.com/how-the-grinch-stole-iot/.

Leyden, John. "New Mirai Botnet Species 'Okiru' Hunts for ARC-Based Kit." The Register, 16 Jan. 2018, https://www.theregister.com/2018/01/16/arc_iot_botnet_malware/.

Mahmoudi, Mehran, and Sarah Nadi. "The Android Update Problem: An Empirical Study." 2018 IEEE/ACM 15th International Conference on Mining Software Repositories (MSR), 2018, pp. 220–30. IEEE Xplore, https://ieeexplore.ieee.org/document/8595205.

Millman, Rene. "Satori Creator Linked with New Mirai Variant Masuta." SC Magazine, 26 Jan. 2018, https://web.archive.org/web/20180207005039/https://www.scmagazineuk.com/satori-creator-linked-with-new-mirai-variant-masuta/article/739714/.

Moran, Brendan, et al. A Firmware Update Architecture for Internet of Things. Request for Comments, RFC 9019, Internet Engineering Task Force, Apr. 2021. IETF, https://doi.org/10.17487/RFC9019.

Poulsen, Kevin. "Newbie Hacker Fingered for Monster Botnet." The Daily Beast, 30 Aug. 2018.

www.thedailybeast.com, https://www.thedailybeast.com/newbie-hacker-fingered-for-monster-botnet.

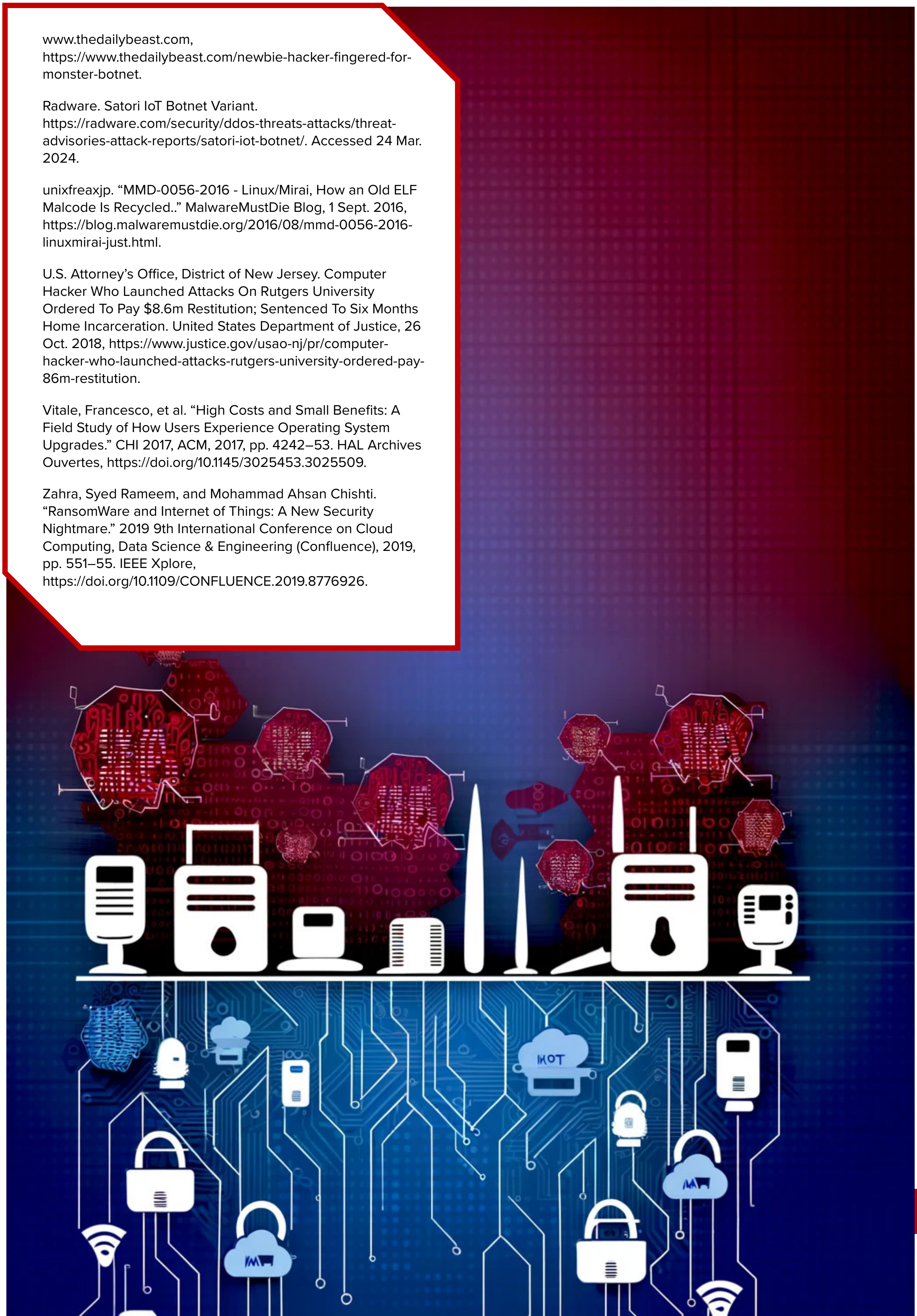
Radware. Satori IoT Botnet Variant. https://radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/. Accessed 24 Mar. 2024.

unixfreaxjp. “MMD-0056-2016 - Linux/Mirai, How an Old ELF Malcode Is Recycled..” MalwareMustDie Blog, 1 Sept. 2016, https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html.

U.S. Attorney’s Office, District of New Jersey. Computer Hacker Who Launched Attacks On Rutgers University Ordered To Pay $8.6m Restitution; Sentenced To Six Months Home Incarceration. United States Department of Justice, 26 Oct. 2018, https://www.justice.gov/usao-nj/pr/computer-hacker-who-launched-attacks-rutgers-university-ordered-pay-86m-restitution.

Vitale, Francesco, et al. “High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades.” CHI 2017, ACM, 2017, pp. 4242–53. HAL Archives Ouvertes, https://doi.org/10.1145/3025453.3025509.

Zahra, Syed Rameem, and Mohammad Ahsan Chishti. “RansomWare and Internet of Things: A New Security Nightmare.” 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, pp. 551–55. IEEE Xplore, https://doi.org/10.1109/CONFLUENCE.2019.8776926.



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