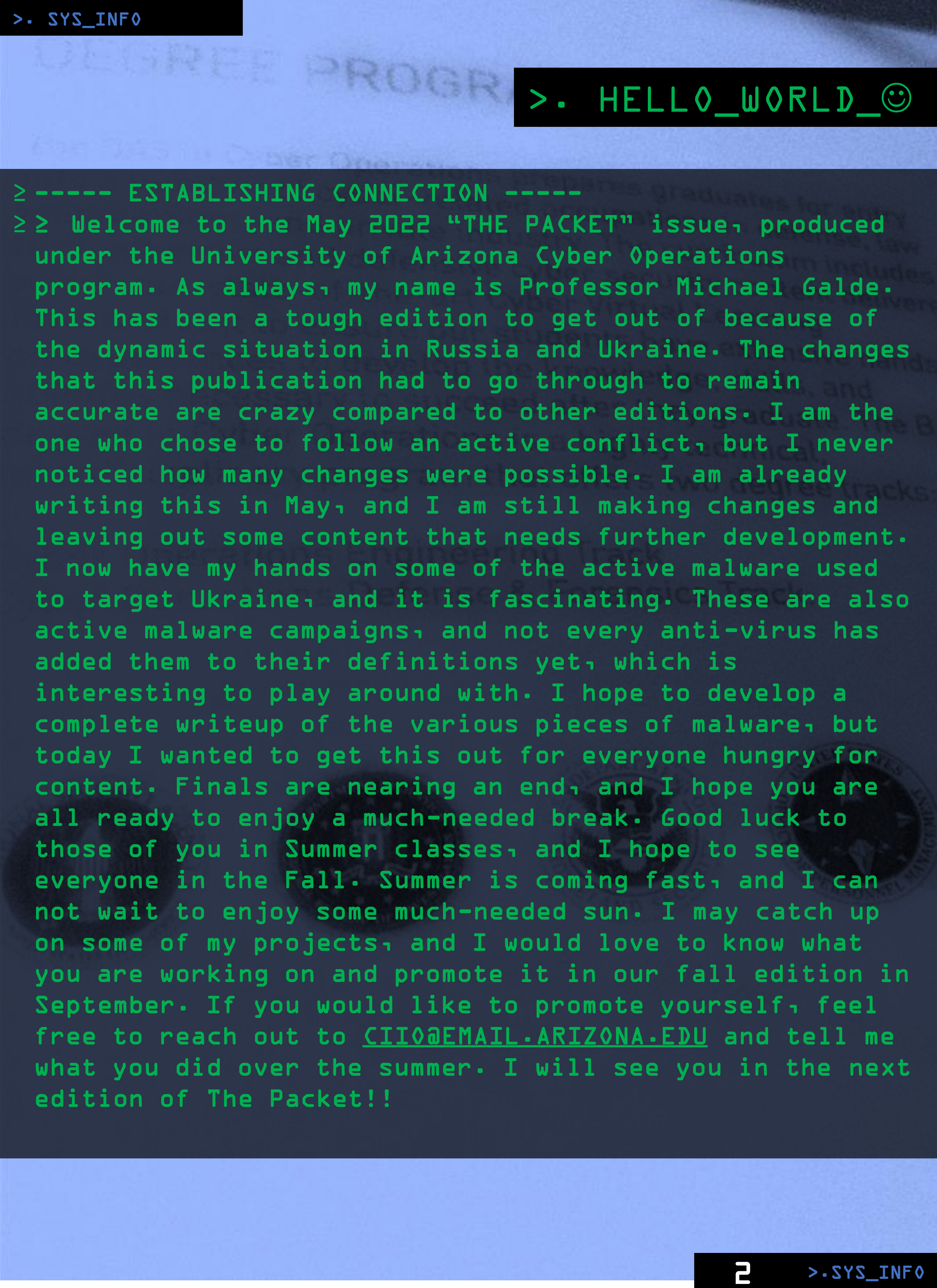
THE PACKET

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY



>. HELLO_WORLD_☺

≥----- ESTABLISHING CONNECTION -----

≥≥ Welcome to the May 2022 “THE PACKET” issue, produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. This has been a tough edition to get out of because of the dynamic situation in Russia and Ukraine. The changes that this publication had to go through to remain accurate are crazy compared to other editions. I am the one who chose to follow an active conflict, but I never noticed how many changes were possible. I am already writing this in May, and I am still making changes and leaving out some content that needs further development. I now have my hands on some of the active malware used to target Ukraine, and it is fascinating. These are also active malware campaigns, and not every anti-virus has added them to their definitions yet, which is interesting to play around with. I hope to develop a complete writeup of the various pieces of malware, but today I wanted to get this out for everyone hungry for content. Finals are nearing an end, and I hope you are all ready to enjoy a much-needed break. Good luck to those of you in Summer classes, and I hope to see everyone in the Fall. Summer is coming fast, and I can not wait to enjoy some much-needed sun. I may catch up on some of my projects, and I would love to know what you are working on and promote it in our fall edition in September. If you would like to promote yourself, feel free to reach out to CIIO@EMAIL.ARIZONA.EDU and tell me what you did over the summer. I will see you in the next edition of The Packet!!

OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

JOIN CYBER SAGUAROS TODAY

Cyber Saguaros

CYBER_SAGUAROS

Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

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

www.twitter.com/UWicys

f www.facebook.com/UAZWicys

www.instagram.com/uarizonawicys/

THE UNIVERSITY OF ARIZONA

WiCyS
women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER

THIS GANG IS GETTING A LOT QUICKER AT ENCRYPTING NETWORKS

- ARTICLE LINK
- TECHNICAL DETAILS
- FIN12 GROUP PROFILE

A highly successful and aggressive ransomware gang is getting faster at encrypting networks as they look to extort ransom payments from as many victims as possible. Researchers at Mandiant examined ransomware attacks by a cyber-criminal group they refer to as FIN12 - responsible for one in five attacks investigated by the cybersecurity company - and found that there's been a significant decrease in the amount of time between initially breaking into networks and their encryption with ransomware, most commonly Ryuk ransomware. According to data published in Mandiant's M-Trends 2022 report, the average dwell time of FIN12 campaigns - the amount of time between criminal hackers gaining initial access to the network and triggering the ransomware attack - has dropped from five to less than two days. One of the reasons the life cycle of these attacks has been so heavily reduced is because FIN12 campaigns don't focus on finding sensitive data and stealing it before triggering a ransomware attack. Searching for and stealing data has become a common tactic for many ransomware groups, who, in addition to encrypting the data, threaten to publish it if a ransom isn't paid. FIN12 tends to focus attacks against North American victims - but Mandiant warns that the ransomware group could potentially target a broader range of victims worldwide. "The United States government and law enforcement community have significantly excited the pressure on ransomware operators. This has increased the risks of ransomware groups targeting American organizations and makes EMEA a more tempting target," said Jamie Collier, senior threat intelligence advisor at Mandiant.

HACKERS EARN $400K FOR ZERO-DAY ICS EXPLOITS DEMOED AT PWN2OWN

- ARTICLE LINK
- TWITTER ALERT
- YOUTUBE ANALYSIS

Pwn2Own Miami 2022 has ended with competitors earning $400,000 for 26 zero-day exploits targeting ICS and SCADA products that were demoed during the contest between April 19 and 21. "Thanks again to all of the competitors who participated. Today, we couldn't have a contest without them," Trend Micro's Zero Day Initiative said. After the security vulnerabilities exploited during Pwn2Own are reported, vendors are given 120 days to release patches until ZDI publicly discloses them. During day one, they earned $20,000 after executing code on the Inductive Automation Ignition SCADA control server solution using a missing authentication weakness. The same day they exploited an uncontrolled search path vulnerability to gain remote code execution in AVEVA Edge HMI/SCADA software and were awarded $20,000. Finally, on day two of Pwn2Own Miami 2022, the team bypassed the trusted application check on the OPC Foundation OPC UA.NET Standard and added $40,000 to their awards stash. During the first edition of the ICS-themed Pwn2Own Miami, held back in January 2020, ZDI awarded $280,000 for 24 unique zero-day vulnerabilities in ICS and SCADA products.

RESEARCHER RELEASES POC FOR RECENT JAVA CRYPTOGRAPHIC VULNERABILITY

A proof-of-concept code demonstrating a newly disclosed digital signature bypass vulnerability in Java has been shared online. The high-severity flaw in question, CVE-2022-21449, impacts the following version of Java SE and Oracle GraalVM Enterprise Edition - . The issue resides in Java's implementation of the Elliptic Curve Digital Signature Algorithm, a cryptographic mechanism to digitally sign messages and data for verifying the authenticity and the integrity of the contents. In a nutshell, the cryptographic blunder - dubbed Psychic Signatures in Java - makes it possible to present a totally blank signature, which would still be perceived as valid by the vulnerable implementation. Successful exploitation of the flaw could permit an attacker to forge signatures and bypass authentication measures put in place. "If you are using ECDSA signatures for any of these security mechanisms, then an attacker can trivially and completely bypass them if your server is running any Java 15, 16, 17, or 18 version." In light of the release of the PoC, organizations that use Java 15, Java 16, Java 17, or Java 18 in their environments are recommended to prioritize the patches to mitigate active exploitation.

- ARTICLE LINK
- CVE-2022-21449
- OPENJDK ADVISORY

HACKERS SNEAK 'MORE_EGGS' MALWARE INTO RESUMES SENT TO CORPORATE HIRING MANAGERS

A new set of phishing attacks delivering the more eggs malware has been observed striking corporate hiring managers with bogus resumes as an infection vector, a year after potential candidates looking for work on LinkedIn were lured with weaponized job offers. "This year the more eggs operation has flipped the social engineering script, targeting hiring managers with fake resumes instead of targeting jobseekers with fake job offers," eSentire's research and reporting lead, Keegan Keplinger, said in a statement. Targeted entities include a U.S.-based aerospace company, an accounting business located in the U.K., a law firm, and a staffing agency, both based out of Canada. "More eggs achieves execution by passing malicious code to legitimate windows processes and letting those windows processes do the work for them," Keplinger said. The goal is to leverage the resumes as a decoy to launch the malware and sidestep detection. It's worth pointing out that more eggs, once deployed, could be used as a jumping off point for further attacks such as information theft and ransomware. "The threat actors behind more eggs use a scalable, spear-phishing approach that weaponizes expected communications, such as resumes, that match a hiring manager's expectations or job offers, targeting hopeful candidates that match their current or past job titles," Keplinger said.

- ARTICLE LINK
- VENOM SPIDER
- CODE ANALYSIS

RUSSIAN HACKERS TRIED ATTACKING UKRAINE'S POWER GRID WITH INDUSTROYER2 MALWARE

The Computer Emergency Response Team of Ukraine (CERT-UA) in early April disclosed that it thwarted a cyberattack by Sandworm, a hacking group affiliated with Russia's military intelligence, to sabotage the operations of an unnamed energy provider in the country. In short, the Ukrainian power grid was under attack, but the cybersecurity resources stopped this attack from taking place. Ukraine has had its critical infrastructure attacked before which including a successful attempt in 2015 and 2016. This new 2021 attempt however failed but the follow-on analysis is fascinating. Let me introduce you to Indestroyer2.

Industroyer2 was deployed as a single Windows executable named 108_100.exe and executed using a scheduled task on 2022-04-08 at 16:10:00 UTC. It was compiled on 2022-03-23, according to the PE timestamp, suggesting that attackers had planned their attack for more than two weeks.

Industroyer2 only implements the IEC-104 communication protocol to communicate with industrial equipment. To compare this to the American power grid, we use the DNP3 protocol which is different in any way but also similar. This includes protection relays, used in electrical substations. This is a slight change from the 2016 Industroyer variant which is a fully-modular platform with payloads for multiple ICS protocols.

Industroyer2 appears to be highly configurable. It contains a detailed configuration hardcoded in its body, driving the malware actions. This is different from Industroyer, which stores configuration in a separate .INI file. So, this appears that the attackers need to recompile Industroyer2 for each new victim or environment.

However, given that the Industroyer malware family has only been deployed twice, with a five-year gap between each version, this is probably not a limitation for Sandworm operators.

This is more than just this piece of malware this is also an updated version of CaddyWiper which we talked about just last month.

In coordination with the deployment of Industroyer2 in the ICS network, the attackers deployed a new version of the CaddyWiper destructive malware. This was intended to slow down the recovery process and prevent operators from regaining control of the ICS consoles. It was also deployed on the machine where Industroyer2 was executed, likely to cover their tracks and prevent an analysis like this from taking place.

RUSSIAN HACKERS TRIED ATTACKING UKRAINE'S POWER GRID WITH INDUSTROYER2 MALWARE

The first version of CaddyWiper was discovered by researchers in Ukraine on 2022-03-14 when it was deployed in the network of a bank. It was deployed via a Microsoft Group Policy Object (GPO), indicating the attackers had prior control of the target's network beforehand. The wiper erases user data and partitions information from attached drives, making the system inoperable and unrecoverable. In the new network deployment, attackers deployed a new version of CaddyWiper that uses a new loader, named ARGUEPATCH by CERT-UA.

ARGUEPATCH is a patched version of a legitimate component of Hex-Rays IDA Pro software, specifically the remote IDA debugger server. IDA Pro is not intended to be used in an ICS environment, as its main purpose is for software reverse-engineering including malware analysis. This was a poor decision by the authors as this would stand out compared to other software that would provide additional stealth. ARGUEPATCH was expected to be executed as a scheduled task once on 2022-04-08 14:58 UTC on one machine and at 16:20 UTC on the machine where Industroyer2 was deployed.
Alongside CaddyWiper, a PowerShell script was found both in the energy provider network and in the bank that was compromised earlier. This script enumerates Group Policies Objects (GPO) using the Active Directory Service Interface (ADSI). For more information about this process look at THIS.

Additional destructive malware for systems running Linux and Solaris was also found on the network. There are two main components to this attack: a worm and a wiper. The latter was found in two variants, one for each of the targeted operating systems.

Ukraine is once again at the center of cyberattacks targeting its critical infrastructure. This new Industroyer campaign follows multiple waves of wipers that have been targeting various sectors in Ukraine.

ILOVEYOU – THE FIRST WORM I REMEMBER

The ILOVEYOU computer worm infected over ten million Windows computers. The virus sent a user an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.txt.vbs". The file extension was most often hidden by default on Windows leading unwitting users to think it was a normal text file. Opening the attachment activated the worm which overwrote random types of files and sent a copy of itself to all addresses in the Windows Address Book used by Microsoft Outlook. This made it spread much faster than any other previous email

MAY 5, 2000

RELEASE OF WANACRY – THE FIRST BIG PUSH OF RANSOMWARE

WannaCry was a ransomware crypto worm that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments. It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself. The attack began on Friday, May 12, 2017, with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed at the time. Malware researcher Marcus Hutchins discovered the kill switch domain hardcoded in the malware. Marcus then registered the hidden domain name and created a DNS sinkhole. This ended up stopping the attack from spreading as a worm because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do. Marcus Hutchins is also known at the twitter user MalwareTech and was celebrated for his efforts in stopping this attack. However, Marcus was arrested by the FBI due to his involvement in developing the rootkit Kronos.

MAY 17, 2017

MAY

05

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

PHISH USING AN EXCEL DOCUMENT

During a red team engagement, you noticed that the Microsoft application Excel was actively used as a password manager. Trying to protect an organization's internal infrastructure is a challenge. If it wasn't for password managers that cater to corporate environments, Excel might have been a solution a decade ago, but now that is like playing with fire. Exposing your organization's passwords like this is inexcusable. Extracting the password from a password-protected Excel document is not easy, but it is also not overly complicated. This article will go over what the engagement team did to crack the password for the Excel document and then "gain the keys to the castle." So, first, for a little bit of background, a user can create an Excel document and provide a password to protect the document by selecting

- **File**
- **Info**
- **Protect Workbook**

Encrypt with Password in the menu options. This is available for the user to ensure that only the correct users can access or change values in the Excel workbook. This provides a level of protection suited for this purpose; however, trying to use this method to protect passwords is not advised as the password protections can be easily removed in older versions of Excel by editing the XML data within the Excel document. A newer version of Excel encrypts the whole workbook, making decryption more difficult. The engagement team did not want to spend resources decrypting the document, and they wanted the employees to give them the password using a phishing technique.

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

PHISH USING AN EXCEL DOCUMENT

First the engagement team used the build in Excel VBA editor to create a message box to mimic the real please enter your password screen. This is then edited to look like the password screen offered to the user when a password is requested. Now that a dialog box has been created to mimic the password dialog box, we can add logic to collect the entered password, encrypt the password and then transmit the encrypted message to something that the engagement team controls. So first, we want to take the password and encode it into something we can read later, like base64 encoding. This will allow our program to take the text and then encode it into something that looks encrypted. Base64 encoding is a simple method to achieve this as the math is easy to implement and will provide us with something that would not be easily identified. Next, you want to exfiltrate this data to some server or system that you control using the Excel XML HTTP system. So, when the password is collected, it will be sent to us for later analysis and to use later against the legitimate password-protected file. In this example, the engagement team has a compromised machine waiting at 192.168.100.128 on the local network. This is where the phished password will be sent. Finally, the engagement team wants to avoid suspicion about their activities. It uses this phishing document to open the legitimate file if the password was entered correctly with the following code. This will open the legitimate file using the provided password to avoid any suspicion from the legitimate employee. If the wrong password is supplied, an error can be displayed by adding additional code when our new phishing program catches an error. This engagement team was able to exfiltrate a password to a password database without brute force or by installing a keylogger. The team just waited for the users to tell them what the password was so that they could access all of the lovely intel inside.

LET’S DUMP AND EXPLOIT MEMORY USING AVAST

Being able to explore memory allows you to see items that you may not be allowed to see normally. Using the Avast Home Security product suite, the researcher behind Arch Cloud found an exciting way to do just that if your victim was using Avast as their Anti-Virus. Avast comes with a program called avdump.exe, and this allows you to “dump” the memory contents of a selected program from its PID while it is running. Using PowerShell, you can execute this with the command in the Avast directory by typing

```
.\AvDump.exe --id (Program PID) --exception_ptr 0 –thread_id 0 –dump_level 0 –dump_file
```

(Directory of where you want the memory to go). Now that we have the memory dump, we can try and find valuable data. Using PowerShell again, we can run strings.exe against the memory dump and see if anything stands out. The researcher used a notepad as an example and wrote the message “Hello World” inside it. Now, this document is not saved but is running in system memory. So by running AvDump.exe against the PID of notepad.exe, we captured what was being held in memory. By running strings.exe against this memory capture, we can extract data to see what was inside. Now, this can be applied to different running programs, and if a “victim” is running this software, you would have a technique available to you that allows you to see what system memory is holding. This could be anything from system credentials depending on how they are stored and processed, or messages not intended for saving on the local machine. Either way, dumping memory allows you to bypass many mitigations if you have this level of access to a device you would not usually have access to.

>. JOBS/INTERNSHIPS

INFORMATION SECURITY INTERN

PHOENIX, AZ

CAE

- APPLY HERE
- WEBSITE
- GLASS DOOR

Opportunity for current college students with an educational background in cyber engineering (vulnerability / software development). Seeking undergraduate and graduate college students for a unique role on several projects combining vulnerability research and software development.
Desired Requirements:

- Previous information security, network security, computer science, or information technology experience (in the classroom or internship)
- Knowledge of server operating systems, including Microsoft Windows servers and Linux
- Knowledge of desktop operating systems, including Microsoft platforms, macOS, & Linux variants
- An understanding of networking fundamentals such as a firewall/network segmentation, firewall ACLs, security groups, and network topology
- Hands-on hardware

INTERN, CYBERSECURITY RISK MANAGEMENT

PHOENIX, AZ

CIRCLE K

- APPLY HERE
- WEBSITE
- GLASS DOOR

Assist the security team with building and rolling out our new global TPCRM (Third-Party Cybersecurity Risk Management) program. The Intern will help with testing the Service Now VRM module configurations and building out the inventory and reporting capabilities.

RESPONSIBILITIES/ACCOUNTABILITIES:

- Review Azure Security console policies and events
- Fine-tune label policies filtering out false positives
- Create initial metrics and reporting
- Create mitigation procedure based on CK RASCI
- Assist in general security activities

KNOWLEDGE, SKILLS AND OTHER QUALIFICATIONS REQUIRED:

- Microsoft Office (Excel, Word, Outlook, Project, Visio)
- Microsoft SharePoint
- Project Management basics
- Cybersecurity awareness is a preference but is not mandatory

STUDENT INTERN, IT COMPLIANCE

TUCSON, AZ

We are looking for an energetic candidate with a strong foundation. We provide on-the-job training. This role will work with the IT Compliance team to perform day-to-day compliance reviews, access reviews, as well as process and documentation updates. Intern will assist with the maintenance of new or updated compliance programs and requirements.

Position-Related Responsibilities

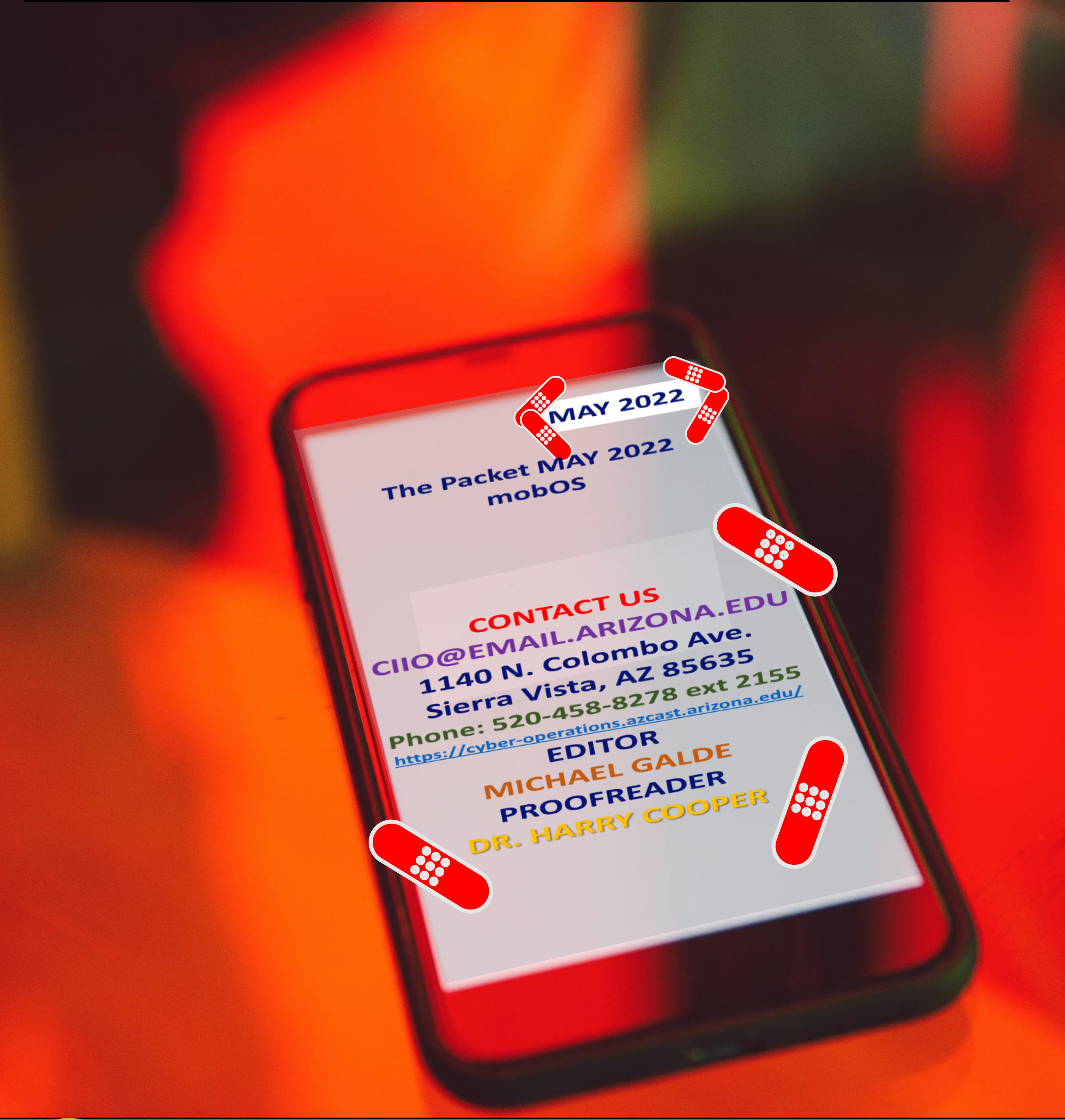
- Participate in projects that the IT Compliance Department is coordinating.
- Assist in preparing for, tracking, and responding to audit data requests from internal or external auditors.
- Assist in the oversight processes for access controls, change control, and patching.
- Execute compliance-related test cases in various software applications and document results.
- Assist in the completion of various Information Technology ("IT") compliance programs evidence.
- Maintain key lists that are required for compliance, such as key system inventory lists and other related documents.
- Perform other duties as assigned.

Knowledge, Skills & Abilities

- Must be pursuing a degree in Information Technology, Computer Science, Mathematics, or related discipline with a graduation date no earlier than May 2023.
- Must be able to work a minimum of 15 – 20 hours per week during regular business hours; and 20 – 40 hours a week during the summer and school breaks.
- Must demonstrate effective verbal and written communication skills.
- Must be able to work independently as well as in a team environment.

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

```
>.  ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A FUN AND SAFE SUMMER BREAK
>.  WE WILL BE BACK IN SEPTEMBER!!
>. ---END TRANSMISSION---
```



MAY 2022

The Packet MAY 2022
mobOS

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

EDITOR
MICHAEL GALDE
PROOFREADER
DR. HARRY COOPER