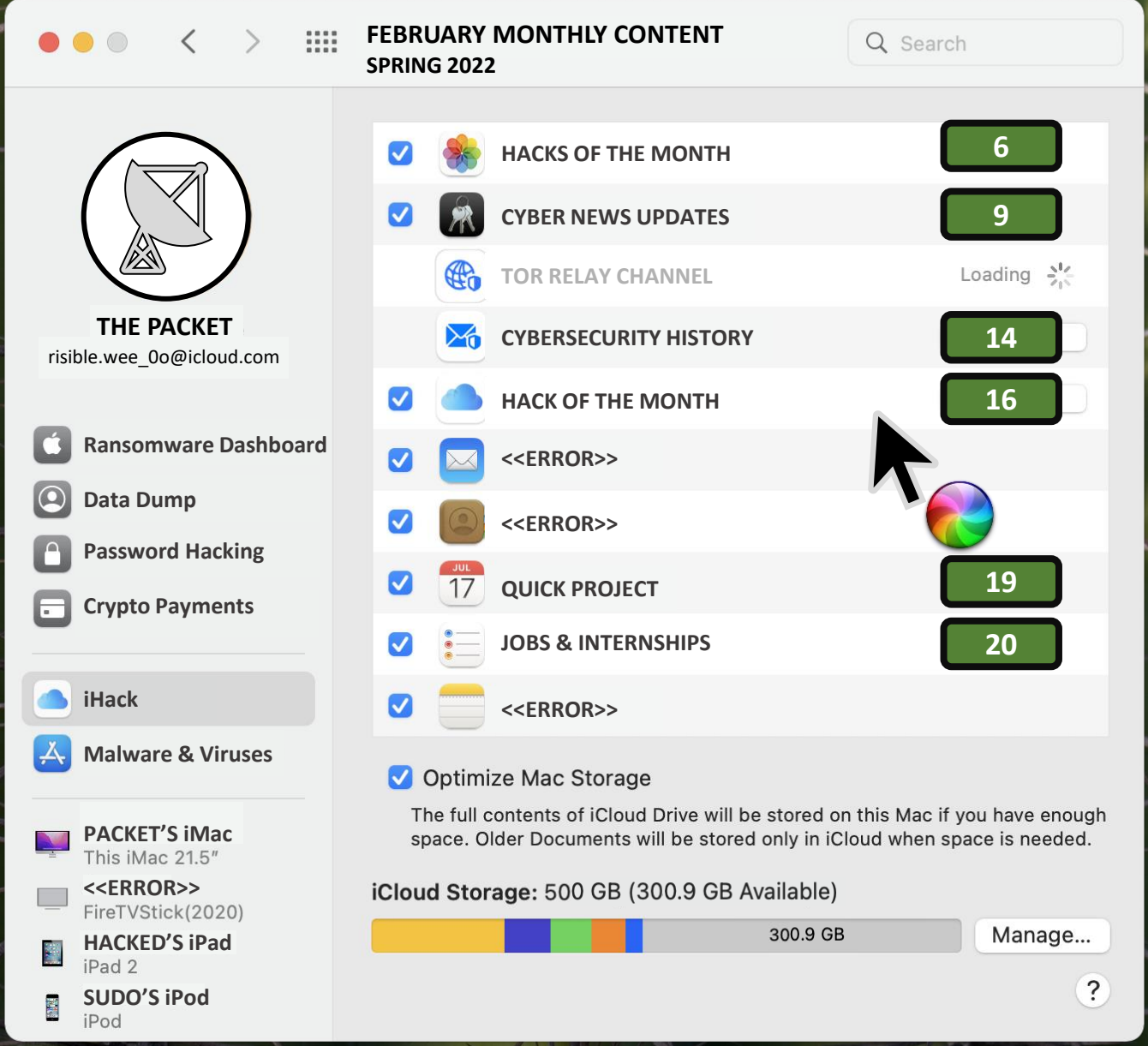
THE PACKET



THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY

>. HELLO_WORLD_☺

≥ ----- ESTABLISHING CONNECTION -----

≥ Welcome to the FEBRUARY 2022 issue of "THE PACKET," produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. This month we are focusing on OSX, and the past few weeks have been very damaging to Apple as they needed to release two huge security updates to fix some serious zero-day exploits. This month we are going to take apart an old Remote Access Trojan or RAT on the OSX system called eggshell. Eggshell needs to be deployed to a system to be effective so another vulnerability would either need to be known or a victim would need to be tricked into activating the executable. However, this framework is written in Python, and I am excited to start updating the code to work in modern OSX environments.

≥ The research club, Saguaro Pod is in the process of setting up its research lab and the Cyber Operations security club Cyber Saguaros are looking for new members. Also, a nice promotional poster is included on page 4.

≥ The University also now has an opening for a Cybersecurity Analyst student worker and the details of that position are included on page 22.

≥ As I close out this message, I just want to say I hope you really enjoy the month of February, I hope to see you at CACTUSCON, and I hope you join one of our cyber security clubs. If nothing else, we can chat on the unofficial DISCORD channel.

>. SAGUARO_POD_UPDATE

>. CARTER_LAYMAN

≥ **FINIS CORONAT OPUS:** LATIN FOR "THE END CROWNS THE WORK." SAGUARO POD HAS ENTERED MONTH FOUR OF ITS RESEARCH PROJECT AND IS NOW DEVELOPING THE FIRST POC FOR ITS "AUTOMATED IOT SCANNER." AS OF JANUARY 1ST, WE HAVE LAUNCHED THE RAPID DEVELOPMENT PHASE AND ARE WORKING WITH THE UNIVERSITY TO TEST IOT TECHNOLOGY AND DEVELOP SECURITY FOR SAID TECHNOLOGY ON A DEDICATED NETWORK.

≥ **UPDATES:**

- ≥ SOME TECH TO BE ACQUIRED ARE, BUT ARE NOT LIMITED TO
  - ≥ CAMERAS
  - ≥ ROUTERS
  - ≥ IN-HOME CHILD SAFETY DEVICES
- ≥ THE CALL FOR VILLAGES IS OPEN AT DEFCON 30, AND WE WILL LIKELY SUBMIT TO IOT VILLAGE OR ANY OTHER THAT ALIGNS WITH OUR RESEARCH.
- ≥ WE ARE VERY OPTIMISTIC AND OPEN-MINDED ABOUT THE TRIALS AND TRIBULATIONS AHEAD OF THIS RESEARCH. WE HOPE NOT ONLY TO LEARN MORE ABOUT IOT SECURITY BUT TEACH EACH OTHER A THING OR TWO!
- ≥ OUR GROUP OBJECTIVES ARE BEING MET DAY BY DAY AS WE RESEARCH, DEVELOP, AND PUBLISH
- ≥ SEE YOU SOON.

SAGUARO_POD

OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

JOIN CYBER SAGUAROS TODAY

CYBER_SAGUAROS

DOD CYBER SCHOLARSHIP PROGRAM (DOD CYSP)

The Department of Defense (DoD) Cyber Scholarship Program (CySP) is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA).

The objectives of the program:

- Promote higher education in all disciplines of cybersecurity
- Enhance the Department's ability to recruit and retain cyber and IT specialists,
- Increase the number of military and civilian personnel in the DoD with this expertise, and ultimately
- Enhance the nation's cyber posture.

- The DoD is working with universities like the University of Arizona and other defined National Centers of Academic Excellence (CAE). Interested students need to apply directly with the University of Arizona at CYSP@EMAIL.ARIZONA.EDU

- Minimum cumulative GPA of 3.2 (undergraduate)
- Must be entering junior or senior year.
- Must be a U.S. Citizen.
- Must agree to work for the DoD as a civilian for one year for each year of scholarship received.

- **LINK TO APPLY**

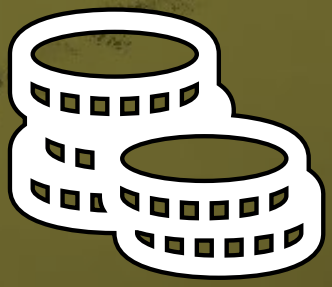
THE DEADLINE IS TUESDAY, FEBRUARY 1, 2022 AT 11:59 P.M. EASTERN TIME. YOU MUST HAVE YOUR APPLICATION AND ALL MATERIALS SUBMITTED BY THAT DATE AND TIME.

CAE IN CYBERSECURITY COMMUNITY

The NSA CAE-CO designation provides UA graduates access to the CAE Community and all of its resources.

>. HACKS_OF_THE_MONTH

CRYPTO.COM CONFIRMS 483 ACCOUNTS HACKED, $34 MILLION WITHDRAWN



Crypto.com has confirmed that a multi-million dollar cyberattack led to the compromise of around 400 of its customer accounts. In an interview with Bloomberg Live, Crypto.com's CEO Kris Marszalek acknowledged that approximately 400 customer accounts were compromised following a recent hack suffered by the platform. As explained below in the article, the exact number of customer accounts impacted is 483. A statement from Crypto.com seen by BleepingComputer today puts the total amount of unauthorized withdrawals across different cryptocurrencies at approximately US$34 million. Crypto.com had first detected the cyber incident via its risk monitoring systems on January 17th, 2022, when "a small number of users had unauthorized crypto withdrawals on their accounts." "No customers experienced a loss of funds. In most cases, we prevented the unauthorized withdrawal, and in all other cases, customers were fully reimbursed. The incident affected 483 Crypto.com users."

- **ARTICLE LINK**
- **TECHNICAL DETAILS**
- **TWITTER STORY**

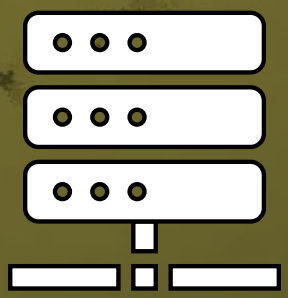
NEW MOONBOUNCE UEFI MALWARE USED BY APT41 IN TARGETED ATTACKS

Security analysts have discovered and linked MoonBounce, "The most advanced" UEFI firmware implant found in the wild so far, to the Chinese-speaking APT41 hacker group. The laced firmware component is CORE DXE, which is called during the early phase of the UEFI boot sequence. Kaspersky couldn't retrieve that payload for analysis or figure out how exactly the actors infected the UEFI firmware in the first place. Kaspersky found multiple malware samples and loaders in other machines in the same network, but those were non-UEFI implants. Kaspersky found plenty of evidence linking MoonBounce to APT41, ranging from the deployment of the ScrambleCross malware itself to unique certificates retrieved from its C2 servers, which match previous FBI reports on APT41 activity. While the U.S. Department of Justice identified and charged five APT41 members in September 2020, the existence of MoonBounce and the operation around it proves the threat actors weren't discouraged by the legal pressure. APT41 remains a sophisticated threat actor who can develop evasive tools that bypass even the most impenetrable corporate networks.

- **ARTICLE LINK**
- **TECHNICAL BREAKDOWN**
- **MALWARE ANALYSIS**

>. HACKS_OF_THE_MONTH

CISCO BUG GIVES REMOTE ATTACKERS ROOT PRIVILEGES VIA DEBUG MODE



Cisco has fixed a critical security flaw discovered in the Cisco Redundancy Configuration Manager for Cisco StarOS Software during internal security testing. "A vulnerability in Cisco RCM for Cisco StarOS Software could allow an unauthenticated, remote attacker to perform remote code execution on the application with root-level privileges in the context of the configured container," Cisco said. "An attacker could exploit this vulnerability by connecting to the device and navigating to the service with debug mode enabled. A successful exploit could allow the attacker to execute arbitrary commands as the root user," Cisco added. Today, Cisco also fixed a medium severity information disclosure bug in the Cisco RCM for Cisco StarOS caused by a debug service incorrectly listening to and accepting incoming connections. Remote attackers could exploit this second bug by executing debug commands after connecting to the debug port. Last year, Cisco patched several other vulnerabilities that allow threat actors to execute code and commands remotely with root privileges. It addressed critical pre-authentication RCE flaw impacting SD-WAN vManage that could enable threat actors to get root privileges on the underlying OS in May. Another pre-auth bug in the same software, allowing attackers to gain RCE as root, was fixed in April.

- ARTICLE LINK
- TECHNICAL DETAILS
- PATCH DOWNLOAD

PERVASIVE APPLE SAFARI BUG EXPOSES WEB-BROWSING DATA

Typically, a web browser permits scripts on one web page to access data on a second web page only if both pages have the same origin/back-end server. Without this security protection in place, a snooper who manages to inject a malicious script into one website would be able to have free access to any data contained in other tabs the victim may have open in the browser, including access to online banking sessions, emails, healthcare portal data, and additional sensitive information. Put simply, malicious websites can learn a user's identity and link it to multiple separate accounts that use the same ID, researchers warned. Beyond Google sites, the firm found that at least 30 Alexa Top 1,000 most-visited websites could be likewise affected by identity leakage. "The results show that more than 30 websites interact with indexed databases directly on their homepage, without any additional user interaction or the need to authenticate," FingerprintJS researchers noted. The researchers have created a proof-of-concept demo that demonstrates how a malicious website can learn the Google account identity of any visitor. If a user visits "Multiple different websites within the same tab, all databases these websites interact with are leaked to all subsequently visited websites," warned the firm.

- ARTICLE LINK
- TECHNICAL BREAKDOWN
- PROOF OF CONCEPT

>. HACKS_OF_THE_MONTH

OiVaVoii – AN ACTIVE MALICIOUS HYBRID CLOUD THREATS CAMPAIGN

Proofpoint researchers observed a new malicious hybrid cloud campaign named OiVaVoii. This campaign uses hijacked Office 365 tenants and a sophisticated combination of cleverly-crafted lures, malicious OAuth apps, and targeted phishing threats. OAuth is a standard for token-based authentication and authorization, removing the need to enter account passwords. Three of these apps appear to be created by verified publishers, which indicates that the threat actors compromised the account of a legitimate Office tenant. While original publishers' accounts remain compromised, the campaign stays alive, which means new apps can be created and authorized. The threat actors then used the apps to send out authorization requests to high-ranking executives in the targeted organizations.

- **ARTICLE LINK**
- **TECHNICAL DETAILS**

LAZARUS HACKERS USE WINDOWS UPDATE TO DEPLOY MALWARE

North Korean-backed hacking group Lazarus has added the Windows Update client to its list of living-off-the-land binaries. It is now actively using it to execute malicious code on Windows systems. In the next stage, the LNK file is used to launch the WSUS / Windows Update client to execute a command that loads the attackers' malicious DLL. "This is an interesting technique used by Lazarus to run its malicious DLL using the Windows Update Client to bypass security detection mechanisms," Malwarebytes said. The researchers linked these attacks to Lazarus based on several pieces of evidence, including infrastructure overlaps, document metadata, and targeting similar to previous campaigns. As BleepingComputer reported in October 2020, this tactic was discovered by MDSec researcher David Middlehurst, who found that attackers could use the Windows Update client to execute malicious code on Windows 10 systems. In this case, threat actors do it by running malicious code from a previously dropped malicious DLL, loaded using the Windows Update client's Microsoft-signed binary. The Lazarus Group is a North Korean military hacking group active for more than a decade, since at least 2009. Last year, Google spotted Lazarus targeting security researchers in January due to complex social engineering attacks and a similar campaign during March.

- **ARTICLE LINK**
- **TECHNICAL BREAKDOWN**
- **MALWARE SAMPLE**

OUTLOOK RCE ZERO-DAY EXPLOITS NOW SELLING FOR $400,000

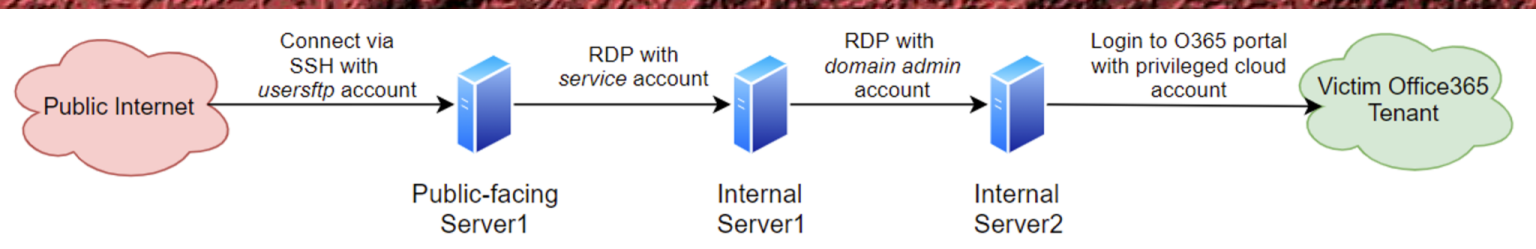
Exploit broker Zerodium is an American information security company founded in 2015. Its main business is developing and acquiring premium zero-day exploits from security researchers and reporting the research, along with protective measures and security recommendations, to its government clients as part of the ZERODIUM Zero-Day Research Feed. The company has more than 1,500 researchers and has paid more than $50,000,000 in bounties between 2015 and 2022. Well, Zerodium has recently announced a pay jump to $400,000 for zero-day vulnerabilities that allow remote code execution in Microsoft Outlook email clients. Zerodium's regular bounty for RCE vulnerability in Microsoft Outlook for windows is $250,000, expected to be "Accompanied by a fully functional and reliable exploit." "We are temporarily increasing our payout for Microsoft Outlook RCEs from $250,000 to $400,000. We are looking for zero-click exploits leading to remote code execution when receiving/downloading emails in Outlook, without requiring any user interaction such as reading the malicious email message or opening an attachment" - Zerodium. The same conditions apply for the exploit payouts for Mozilla Thunderbird, as in the case of Microsoft Outlook. While the company did not specify an end date for submitting zero-click Microsoft Outlook exploits, the period may be quite long. On March 31, 2021, Zerodium announced that it was temporarily tripling the bounty for WordPress RCE exploits, and the offer still stands today. At the moment, only WordPress, Mozilla Thunderbird, and Microsoft Outlook are listed as active on the page with temporarily increased bounties.

- **LIMITED TIME BUG BOUNTIES- Current list of temporary bug bounties**

APT29 HACKERS' STEALTHY MALWARE UNDETECTED FOR YEARS

Hackers associated with the Russian Federation Foreign Intelligence Service continued their incursions on networks of multiple organizations after the SolarWinds supply-chain compromise using two recently discovered sophisticated threats. Cybersecurity company CrowdStrike describes the latest tactics, techniques, and procedures observed in cyberattacks from APT29 state-sponsored hackers. CrowdStrike's report describes the steps that APT29 took to achieve persistence in a position that allowed them to read any email and SharePoint or OneDrive files of the compromised organization. During their incident response work on APT29 StellarParticle attacks, CrowdStrike's researchers used the User Access Logging database to identify earlier malicious account usage, which led to finding the GoldMax for Linux and TrailBlazer malware. **Tim Parisi, Director of Incident Response** at CrowdStrike, described that the covert activity of the two malware pieces delayed the discovery of the two malware pieces, as the researchers found them in mid-2021. After gaining access to a target organization's infrastructure and establishing persistence, APT29 hackers took every opportunity to collect intelligence that would allow them to further the attack. APT29 hackers are some of the most sophisticated threat actors in the cyber-espionage world, with top skills to infiltrate and stay undetected on a company's infrastructure for long periods.

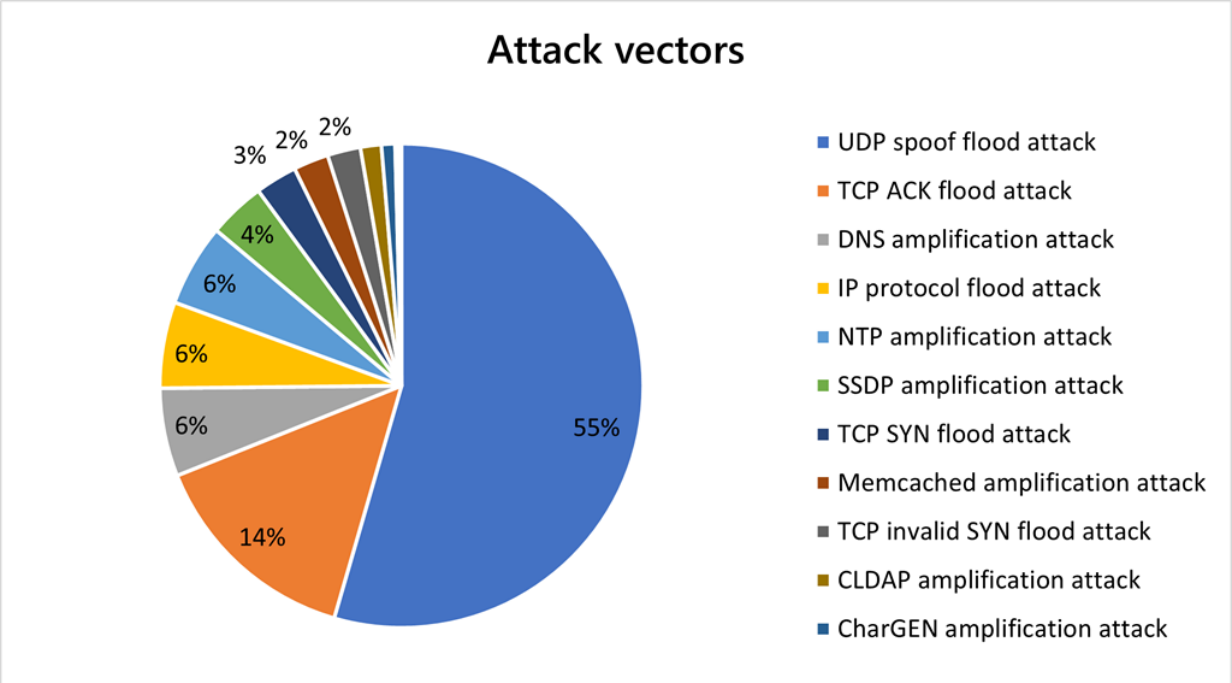
- **CROWDSTRIKE WRITE UP- Breakdown of the Stellar Particle Campaign**



MICROSOFT MITIGATED A RECORD 3.47 TBPS DDOS ATTACK

Last October, Microsoft reported on a 2.4 terabit per second (Tbps) DDoS attack in Azure that Microsoft successfully mitigated. Since then, Microsoft has mitigated three larger attacks. In November, Microsoft mitigated a DDoS attack with a throughput of 3.47 Tbps and a packet rate of 340 million packets per second (pps), targeting an Azure customer in Asia. Microsoft believes this to be the largest attack ever reported in history. This was a distributed attack originating from approximately 10,000 sources and from multiple countries across the globe, including the United States, China, South Korea, Russia, Thailand, India, Vietnam, Iran, Indonesia, and Taiwan. Attack vectors were UDP reflection on port 80 using Simple Service Discovery Protocol (SSDP), Connection-less Lightweight Directory Access Protocol (CLDAP), Domain Name System (DNS), and Network Time Protocol (NTP) comprising one single peak, and the overall attack lasted approximately 15 minutes. UDP attacks rose to the top vector in the second half of 2021, comprising 55 percent of all attacks, a 16 percent increase from the first half of 2021. Meanwhile, TCP attacks decreased from 54 percent to just 19 percent. UDP spoof floods was the most common attack type (55 percent), followed by TCP ACK floods (14 percent) and DNS amplification (6 percent).

- **DDOS Attack writeup - Microsoft Attack Trend writeup**



APPLE FIXES NEW ZERO-DAY EXPLOITED TO HACK MACOS

Apple has released security updates to fix two zero-day vulnerabilities, with one publicly disclosed and the other exploited in the wild by attackers to hack into iPhones and Macs. The first zero-day patched, **CVE-2022-22587** is a memory corruption bug in the IOMobileFrameBuffer. Successful exploitation of this bug leads to arbitrary code execution with kernel privileges on compromised devices. The bug was found by an anonymous researcher, **Meysam Firouzi** of MBition - Mercedes-Benz Innovation Lab, and **Siddharth Aeri** . Firouzi and Aeri said that they both found the bug independently and were unaware that threat actors exploited it in the wild. The second zero-day is a Safari WebKit bug in iOS and iPadOS that allowed websites to track your browsing activity and users' identities in real-time. The bug was first disclosed to Apple by **Martin Bajanik** of FingerprintJS on November 28th, 2021, and publicly disclosed on January 14th, 2022. After the researcher disclosed the bug, it was assigned the CVE-2022-22594 and fixed in today's iOS 15.3 and iPadOS 15.3 security update. These bugs are the first zero-day vulnerabilities fixed by Apple in 2022. However, Apple fixed what felt like a never-ending stream of zero-day bugs in 2021 that were used in attacks against iOS and macOS devices. These bugs included numerous zero-day vulnerabilities used to install the Pegasus spyware on the iPhones of journalists, activists, and politicians.

Apple security updates

Name and information link	Available for	Release date
Safari 15.3	macOS Big Sur and macOS Catalina	26 Jan 2022
Security Update 2022-001 Catalina	macOS Catalina	26 Jan 2022
macOS Big Sur 11.6.3	macOS Big Sur	26 Jan 2022
macOS Monterey 12.2	macOS Monterey	26 Jan 2022
tvOS 15.3	Apple TV 4K and Apple TV HD	26 Jan 2022
iOS 15.3 and iPad OS 15.3	iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)	26 Jan 2022

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	BOOK
CYBV 303	WINDOWS SECURITY ESSENTIALS	BOOK
CYBV 310	INTRO SECURITY PROGRAMMING I	BOOK
CYBV 311	INTRO SECURITY PROGRAMMING II	BOOK
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 351	SIGNALS INTELLIGENCE AND ELECTRONIC WARFARE	PENDING BOOK SELECTION
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	PENDING BOOK SELECTION
CYBV 382	NETWORK FORENSICS	PENDING BOOK SELECTION
CYBV 384	HOST AND FILE SYSTEM FORENSICS (WINDOWS)	PENDING BOOK SELECTION
CYBV 385	INTRODUCTION TO CYBER OPERATIONS	BOOK
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	BOOK 1, BOOK 2
CYBV 400	ACTIVE CYBER DEFENSE	BOOK 1, BOOK 2
CYBV 435	CYBER THREAT INTELLIGENCE	BOOK 1, BOOK 2
CYBV 436	COUNTER CYBER THREAT INTEL	BOOK 1, BOOK 2
CYBV 437	DECEPTION & COUNTER-DECEPTION	BOOK
CYBV 440	DIGITAL ESPIONAGE	PENDING BOOK SELECTION
CYBV 441	CYBER WAR, TERROR & CRIME	PENDING BOOK SELECTION
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	BOOK
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	BOOK
CYBV 473	VIOLENT PYTHON	BOOK 1, BOOK 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	BOOK 1, BOOK 2
CYBV 475	CYBER DECEPTION DETECTION	PENDING BOOK SELECTION
CYBV 479	WIRELESS NETWORKING AND SECURITY	BOOK 1, BOOK 2
CYBV 480	CYBER WARFARE	BOOK 1, BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION
CYBV 498	SENIOR CAPSTONE IN CYBER OPERATIONS	BOOK

>. CYBER_SECURITY_HISTORY

TWO MAC TROJANS RELEASED BY SAME PERSON

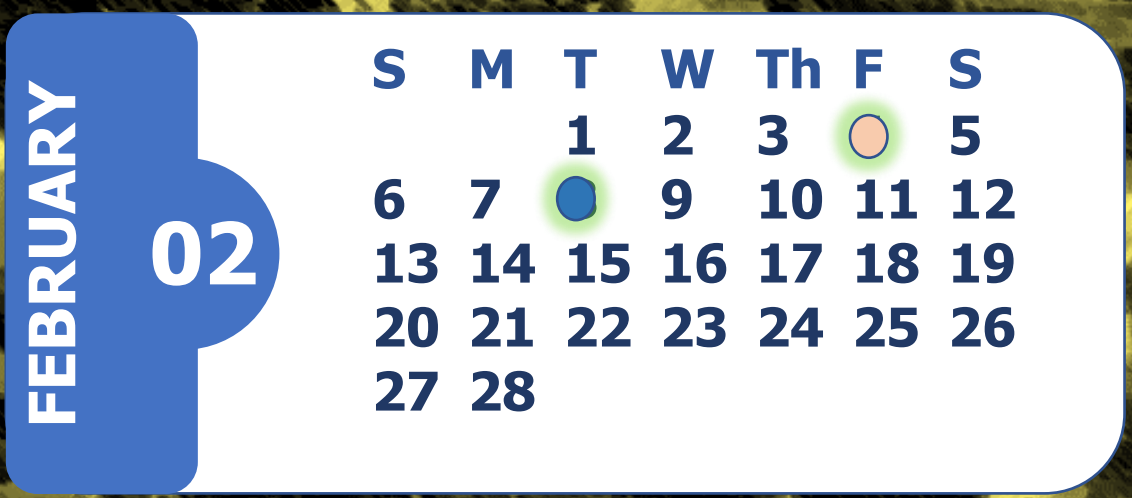
Two new Trojan horses have been reported recently which affect the Apple Macintosh. The first is embedded in the program 'Mosaic', the second in a Stuffit! archive containing 'FontFinder'. The first strain when launched will destroy the directories of all unlocked drives, renaming each destroyed drive as 'Gotcha!'. Unmounted hard drives are also attacked. Damage appears to be restricted to the destruction of directory information including file type and creator. Commercial data recovery utilities can normally restore the file structure. The second strain displays a list of font styles and point sizes in the system file. On, or after, 10th February 1990 it will trigger destroying the directory structure in a similar manner to strain 1. All indications are that these Trojans (first reported at the University of Alberta, Canada) are closely related in their destructive code and are assumed to have been released by the same person.

February 04 1990

THE STORY OF MAFIA BOY, THE KID WHO TOOK DOWN THE EARLY INTERNET

A high school student named Michael Calce, who went by the online handle Mafiaboy, brought down the websites of Amazon, CNN, Dell, E*Trade, eBay, and Yahoo!. At the time, Yahoo! was the biggest search engine in the world. "The New York Stock Exchange, they were freaking out, because they were all investing in these e-commerce companies," he remembers. "And then it's like, 'OK — a 15-year-old kid can shut us down at any point? Is our money really safe?' "

FEBRUARY 8 2000



≥ February 4-5, 2022

≥Mesa Convention Center, AZ

≥Hybrid Talks and Local Workshops

≥ CactusCon is back at the Mesa Convention Center in lovely Mesa, AZ, on February 4-5, 2022! There is ample parking at the venue, with potential overflow lots north of MLK Jr. Avenue. If you book at the extremely nearby Delta Hotel Marriott, your parking will be just as close as convention center parking.

≥ CactusCon is the most prominent annual hacker and security conference in Arizona. Our last event attracted just shy of 1,500 attendees from throughout the country. However, in the previous nine (9) years, our event has established itself as a top-tier security conference and has quickly become a must-attend learning and networking event.

≥ CactusCon is constantly evolving, striving to meet the changing needs and expectations of the InfoSec community. We attract sought-after industry leaders, offer cutting-edge workshops, and provide ample opportunities for mingling and networking with people who share a passion for information security.

≥ JOIN THE DISCORD https://www.cactuscon.com/cc10

ABUSING AN OSX MACHINE WITH A PYTHON BACKDOOR

I wish to introduce you to the developer of a fantastic tool and a useful OSX back door. Their name is Lucas Jackson, and they have been maintaining a GitHub project named Eggshell. Now Eggshell is considered a RAT or a Remote Administration Tool for iOS, OSX, and Linux. This backdoor allows you to do a few exciting things. First, you can do some expected remote administration tools you would expect to include, explore the filesystem, get the process ID of running executables, elevate user privileges and suspend or restart a machine. Eggshell additionally allows you to adjust the device's brightness, get the clipboard's content of the clipboard or download a file. Eggshell also hooks into many internal system programs as well. It allows you to send messages with iMessage, open and record the microphone of the system, open and record an image or video with a built-in camera, take a screenshot and send the user a dialog box to enter the password of the device. On an iOS mobile device, you also get the ability to dial a phone number, retrieve the passcode of the device, simulate button presses like the home button, enable location services, retrieve a device's current location, and much more. There are also some Linux functions available that allow you to download files and upload files. Either way having this piece of software on your device is not something you want, as you would lose a lot of control.

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!!

ABUSING AN OSX MACHINE WITH A PYTHON BACKDOOR

EggShell is a post exploitation surveillance tool written in Python. It gives you a command line session with extra functionality between you and a target machine. EggShell gives you the power and convenience of uploading/downloading files, tab completion, taking pictures, location tracking, shell command execution, persistence, escalating privileges, password retrieval, and much more. This version of Eggshell requires python 2.7. The Application gives you four options when you open the application, start a server or listener, start a “multihandler” to prepare for multiple connections, create a payload for a victim to run or to exit the program itself. You can also deploy this on an iOS jailbroken device using Cydia and a mobile terminal application. On a normal macOS or Linux environment you will run the following commands to execute eggshell on the server environment.

```
git clone https://github.com/neoneggplant/eggshell
cd eggshell
python eggshell.py
```

As a server is established and you are now waiting for your victim to communicate back to you, you can create a payload in a few different ways. Eggshell payloads are executed on the victim machine. The payload first sends over instructions for getting and sending back device details to our server and then chooses the appropriate executable to establish a secure remote-control session.

TYPE	TECHNIQUE
bash	Create a single like bash script that needs to be ran on victims' system. This will require physical access or some type of existing exploit.
USB injection	Create a script that will run on a Teensy USB that will be physically pluged into the victim and automatically run the script.

ABUSING AN OSX MACHINE WITH A PYTHON BACKDOOR

Our friend Lucas Jackson has created an amazing framework but since iOS 13 this backdoor is no longer supported and because maintaining a backdoor script without a legitimate funding model this project has turned into a dying repo. A community fork has been published to add some additional features and is recently updated. However, projects like this need more people to become involved to keep it alive and a remote administration tool for pen testing is an absolute need in the iOS macOS environment as the area lacks tools for security research and pen testing. For the updated community edition, you can run this using the following commands.

```
git clone https://github.com/rpwnage/eggshell-community-fork eggshell && cd eggshell && python3 eggshell.py
```

And with that you can see the expanded capabilities on modern hardware and also the lack of additional features like screen captures.

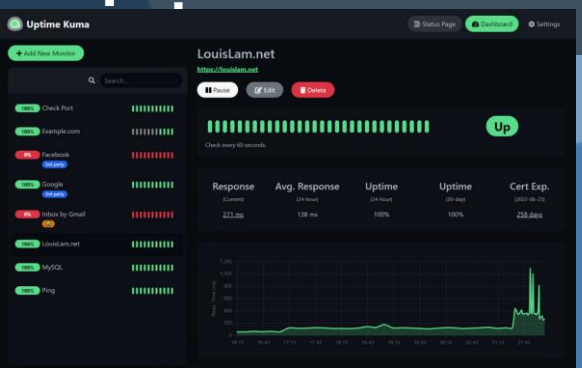
>. QUICK_PROJECT

BUILD AN UPTIME MONITOR USING DOCKER

Today, we will look at a "fancy" self-hosted monitoring tool that will simply record the uptime of various services. You can use this to check the status of services like web pages, pings of devices, DNS records, and Steam game servers. This is a great way to check if your internet service is up or down, if an external web service like Facebook is down or if an internal computer is off and not responding. This is just a simple way to observe the health and status of the network. The tool we will be installing and using will be Uptime Kuma which is available for Docker, or you can install it directly. For this example, docker would be able to offer a better experience, so for this project, we will assume that Docker is already installed.

- **docker volume create uptime-kuma**
- **docker run -d --restart=always -p 3001:3001 -v uptime-kuma:/app/data --name uptime-kuma louislam/uptime-kuma:1**

So now we can monitor what is working and what is not working. This can also send notifications when a service is down to alert you and start some form of the recovery process. Now you can finetune your dashboard to provide you details on every website that is an interest to you. You can also discuss this project on Reddit as well and look for new features and what the community thinks of this dashboard



>. JOBS/INTERNSHIPS

Digital Forensics & Incident Response Engineer

REMOTE

CRITICALSTART

As a Digital Forensics and Incident Response engineer, you will be a member of a team of forensic and Incident Response professionals representing Critical Start professional services. Your experience and skills will be utilized to respond to customer Security Incidents and Breaches, as well as participate in IR training, Tabletop exercises, and IR Readiness assessments.

- Represent Critical Start IR during Incident engagements
- Conduct IR investigations using Network Forensic, host Forensic, and/or Incident Handling expertise
- Contribute to client deliverables during engagements
- Assist in development and delivery of training, and IR assessments

- Competitive salary with bonus opportunity
- Employee Healthcare 100% paid for employees/50% for dependents
- Unlimited PTO Plan
- Dental & Vision Plan
- Employee Stock Options
- Employer Paid Life Insurance and Long-Term Disability coverage
- Employer Paid Short-Term Disability coverage
- Universal Life with Long-Term Care
- Additional Voluntary Life Insurance coverage
- 401(k) Plan with Matching Program
- Employee Assistance Program available 24/7/365
- Teladoc Mental Health Benefits
- Voluntary Pet Insurance
- **A NEW TESLA…HEY, JUST KIDDING! EXTRA POINTS FOR READING ALL THE WAY TO THE END.**

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

>. JOBS/INTERNSHIPS

Cyber Security Engineer - New Graduate

REMOTE

Demonstrate your skills that you learned in and out of school with the within ManTech. ManTech is seeking a motivated, mission-oriented Cyber Security Engineer Associate to join our mission. At ManTech, you will work on innovative projects that offer great technical challenges.

- A passion for cyber security engineering
- Knowledge of CSOC
- Knowledge of IT service delivery
- Knowledge of NIST Cyber Security Framework
- Security+ or IAT II Certification

- Individuals must be a U.S. Citizen and either hold an active US Security Clearance or must be eligible to obtain a US Security Clearance.
- Applicants with the appropriate skills but without a security clearance are still encouraged to apply.

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

Cyber Security Internship

REMOTE

Demonstrate the skills that you learned in and out of school within ManTech. ManTech is seeking a motivated, mission oriented Cyber Security Engineer Intern to join our Internship Program to be exposed to exciting hands-on technical work to grow your skills and obtain a better understanding of the Cyber Security Field. At ManTech, you will work on innovative projects that offer great technical challenges. Interns work on guided projects over the summer that can directly flow back to real contracts. At the end of the summer, all of our interns brief the success of their projects across ManTech.

- Individuals must be a U.S. citizen and either hold an active US Security Clearance or must be eligible to obtain a US Security Clearance.
- Applicants with the appropriate skills but without a security clearance are still encouraged to apply.

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

>. JOBS/INTERNSHIPS

IT Analyst, Incident Response

REMOTE

ZIMMER BIOMET

As the Incident Response Analyst, you will proactively assist and manage local security programs and processes to reduce the severity of potential and actual Information Security incidents. The Incident Response Analyst plays a key role in protecting the organization.

- Monitor, detect, and report any threats directed against the company's networks and systems
- Develop playbooks and processes for incident management and response
- Plan for business continuity and disaster recovery in event of incident
- Perform tests, exercises, and drills of all response plans
- Perform problem management, root cause analysis, and postmortem reviews following the occurrence of an incident
- Conduct forensic investigations and work with law enforcement and other regulatory bodies during and following an incident

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

Cybersecurity Analyst

SUMMER 2022

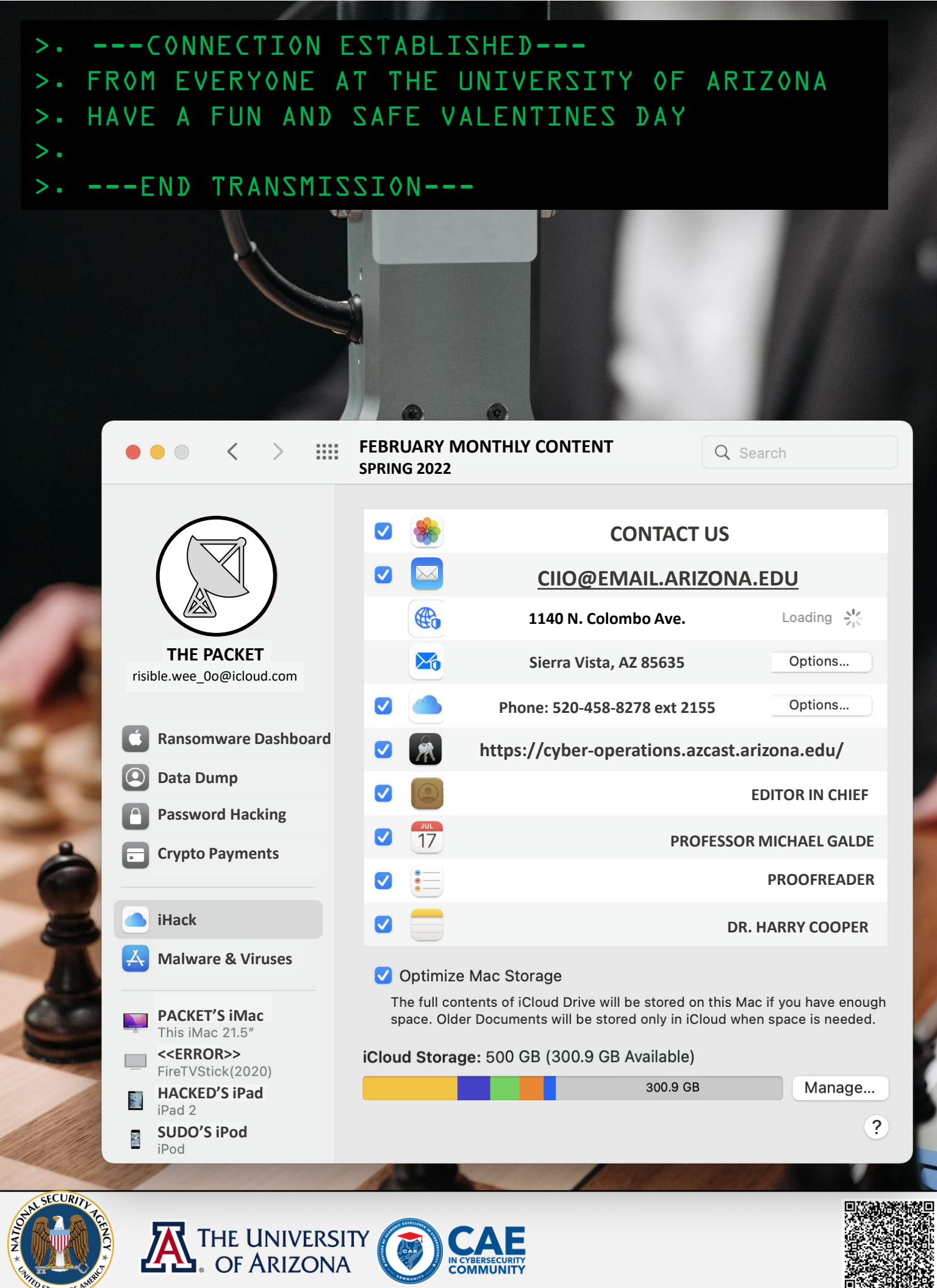
THE UNIVERSITY OF ARIZONA Information Security

The Office of Information Security is looking to add a student worker who desires to gain hands on experience within the University of Arizona's Security Operations Center. The cybersecurity analysts will work under the direction of the Security Operations (SOC) team. These positions will involve documentation, analysis, investigation, incident response, network security monitoring, and administrative duties as assigned. Additionally, the analysts will perform threat hunting by utilizing various data sources which are fed into a SIEM. There is one student position (15-20 hours/week). The schedule will be set during the working hours of 8:00 AM to 5:00 PM, Monday-Friday. Students must be enrolled in the Cyber Operations Program within the College of Applied Science and Technology.

Please Submit:

- Cover Letter
- Resume
- One letter of recommendation

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



THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY