THE PACKET

THE UNIVERSITY OF ARIZONA

APRIL 2020

MESSAGE FROM DEAN DENNO REGARDING COVID-19

Dear CAST Student,

You should have received a notification from University of Arizona President Robbins, informing you that Spring Break has been extended until March 18, and that students are being asked not to return to campus. All University of Arizona classes are being transitioned to fully online learning modalities in response to the quickly evolving COVID19 situation. Because most CAST students have experience with fully online courses, we believe our college—and our faculty—are in many ways more prepared, but we will be doing all we can to assist both students and faculty in this transition.

In order to give all of our faculty and departments time to prepare for the transition to fully online modality, classes will not resume until March 18, 2020. All instruction will officially resume beginning March 18th. Please let me be very specific: NO class activity, whether in a continuing 15 week class or a 7wk2 class is to take place prior to **March 18th.** Your instructors will be revising their course syllabi to accommodate the change in schedule. Your instructors will be communicating directly with you about curriculum adjustments, including changes in assignments, assessments, due dates, etc. Thank you for your patience and understanding for our faculty during this quickly evolving situation.

We are here to support you and will do our best to answer questions or address concerns as the COVID-19 situation progresses. Please be aware, however, that CAST Advising offices will not be open. Your advisor will be available by phone, Zoom, and email for advising appointments until further notice. Please call **520-626-2422** if you have questions.

We also want to ensure that you are prepared with the necessary technology and internet access for continuing your classes entirely online. If you are in a situation where you do not have the means to participate in fully online courses, please reach out immediately to Dannielle Hallahan through email at daniellehallahan@arizona.edu, so that we can help devise a workable solution for you quickly.

Linda Denno, PhD
Interim Dean
ldenno@email.arizona.edu

IN THIS ISSUE

--- BEGIN MESSAGE ---

Welcome to the **APRIL** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. My name is PROFESSOR GALDE and I have taken over "**The PACKET**" to give everyone who is interested, news related to the cybersecurity and the INFOSEC community. I hope you find this useful and if you have any questions please feel free to reach out and contact the Cyber Operations program.

There is an increasing **demand** for cyber security professionals and the University of Arizona is one of the few schools designated by the NSA as a Center of Academic Excellence in Cyber-Operations (**CAE-CO**) and we need people like you in the field protecting the United States and its interests from a growing field of cyber terrorists and other advisories who want nothing more then to see the United States fail. If you are interested in a career I urge you to reach out to a academic professor and see if the cyber operations program is right for you in one of the following:

- **Cyber Engineering Track**
- **Defense & Forensics Track**
- **Cyber Law & Policy Track**

The country needs **you** and the global cybersecurity / INFOSEC community needs talented individuals. Let us help you get there!

--- END MESSAGE ---

CYBER CLASSIFIED BY: PROFESSOR GALDE
REASON: CYBER OPERATION PROGRAM
DECYBER ON: DECEMBER 2060

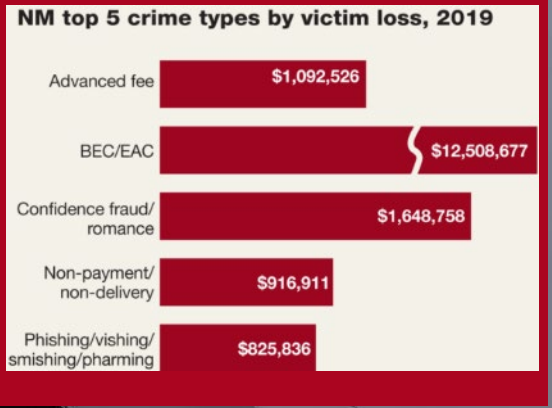
HACKS OF THE MONTH

What will they think of next?

Two Malware campaigns were observed using legitimate Gigabyte kernel drivers as part of its delivery process to bypass the Windows OS driver signature enforcement to install malware by disabling antivirus

Where did the government go?

They Ransomware ….. Get it. Well the City of Racine Wisconsin suffered a ransomware attack that the city says they will not pay. Which is great news for the INFOSEC community, not so much for the IT staff that need to rebuild everything … or my awesome joke



It adds up … to a lot

The State of New Mexico conducted a study with the FBI and concluded that the state of New Mexico lost $18 Million to cyber crime in 2019. These crimes ranged from extortion, defrauding businesses, internet purchases and romance scams

CYBER NEWS UPDATES

CRITICAL CITRIX RCE FLAW STILL THREATENS 1,000S OF CORPORATE LANS

Remote Code Execution (RCE) and myriad other types of attacks could take aim at the 19 percent of vulnerable companies that haven't yet patched CVE-2019-19781

FACEBOOK SAYS IT DISMANTLES RUSSIAN INTELLIGENCE OPERATION TARGETING UKRAINE

"The operation tried to poison the well of information by using false personas to plant pro-Kremlin and anti-Western narratives online and in local news outlets"

US CHARGES HUAWEI WITH CONSPIRACY TO STEAL TRADE SECRETS, RACKETEERING

Huawei allegedly launched a policy instituting a bonus program to reward employees who obtained confidential information from competitors. The policy made clear that employees who provided valuable information were to be financially rewarded.


THE INAUGURAL
SOUTHERN ARIZONA INTELLIGENCE SUMMIT
THE FUTURE OF INTELLIGENCE
Friday, October 23, 2020
7:30 AM – 7:00 PM
University of Arizona
Health Sciences Innovation Building
Explore careers in the intelligence community
Learn about the future of national intelligence
Meet with national, state and industry intelligence leaders
Learn more and register online at
>> https://intelligence-studies.azcast.arizona.edu/content/summit
University of Arizona and Community College students are FREE

JOB BOARD

Network /Capabilities Manager

NSA is in search of top-notch cyber professionals with technical expertise and driving desire at the forefront of their field. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satelli...

Information System Security Professional

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's ...

Cyber Mitigations Engineer/System Vulnerability Analyst

Are you a cyber professional with the drive and expertise to be on the forefront of the cyber fight; tackling NSA's complex mission to defend against cyber threats of today and tomorrow? NSA, the nation's leading cyber agency, has exciting and challenging positions in Cyber Security Engineering and Cyber and TEMPEST vulnerability analysis/mitigation. Are you ready to help secure our Nation's ...

JOB BOARD

Capabilities Watch Officer/Network Manager (Texas location)

NSA is in search of top-notch cyber professionals. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satelli...

Cyber Network Professional (Offensive/Defensive Operations)

NSA is in search of top-notch cyber professionals. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satelli...

Computer Network Analyst

NSA is in search of top-notch cyber professionals. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satelli...

JOB BOARD

Cybersecurity Principal Specialist - Awareness #402

This is advanced professional work assessing effectiveness and efficiency of instruction according to usefulness of the instructional technology used and student learning, knowledge transfer, and satisfaction outcomes. The incumbent will coordinate with internal and external subject matter experts to ensure existing qualification ...

Cybersecurity Senior Specialist #5360

This is professional work coordinating, implementing and maintaining technologies and processes to protect the confidentiality, integrity, and availability of Senate information systems. Work includes translating functional requirements into technical solutions, building, installing, configuring, and testing dedicated cyber defense hardware and checking system hardware availability, functionality, integrity, and efficiency.

Cybersecurity Senior Specialist - Host #44 - Washington, DC or Manassas, Virginia

This is professional work coordinating, translating functional requirements into technical solutions, building, installing, configuring, and testing dedicated cyber defense hardware. Work includes checking system hardware availability, functionality, integrity, and efficiency, employing secure configuration management processes and managing accounts, network rights, and access to systems and ...

5TH ANNUAL CYBER SOUTHWEST SYMPOSIUM

LEARN | COLLABORATE | NETWORK

Registration is Open!

www.ndiasw.org

Friday, August 28, 2020 8 am - 5 pm
Univeristy of Arizona - Eller College of Management
McClelland Hall 2nd Floor - Berger Auditorium

NDIA Southwest

AFCEA

ACTRA

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 301	Fundamentals of Cybersecurity (7 Week class)	Paul Wagner
CYBV 326	Introductory Methods of Network Analysis Section 101 - 106	Jordan Vanhoy
CYBV 326	Introductory Methods of Network Analysis Section 107 - 110	Michael Galde
CYBV 329	Cyber Ethics (7 Week Class)	Heidi Calhoun-Lopez
CYBV 354	Principles of Open Source Intelligence (7 Week Class)	John Mccary
CYBV 385	Introduction to Cyber Operations (7 Week Class)	Michael Galde
CYBV 388	Cyber Investigations and Forensics Section 101 - 104	Troy Ward
CYBV 388	Cyber Investigations and Forensics Section 105 - 106	Steven Wood
CYBV 393	Internship in Cyber Operations	Jason Denno

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 399 CYBV 499	Independent Study	Jason Denno
CYBV 400	Active Cyber Defense Section 101 - 104	Thomas Jewkes
CYBV 400	Active Cyber Defense Section 105 - 106	Colin Brooks
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 101 - 104	Thomas Jewkes
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 102 & 104	Harry Cooper
CYBV 436	Counter Cyber Threat Intelligence (7 Week Class)	Harry Cooper
CYBV 440	Digital Espionage (7 Week Class)	Kate Mabbett
CYBV 441	Cyber War, Terror and Crime (7 Week Class)	Kate Mabbett
CYBV 454	Malware Threats & Analysis	Luis Mendieta

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 470	C Programming for Security Professionals	Keith Rezendes
CYBV 471	Assembly Language Programming for Security Professionals	Mohamed Meky
CYBV 473	Violent Python	Chester Hosmer
CYBV 474	Advanced Analytics for Security Operations	Chester Hosmer
CYBV 479	Wireless Networking and Security	Jordan Vanhoy
CYBV 480	Cyber Warfare Section 101 - 102	Rock Stevens
CYBV 480	Cyber Warfare Section 103 - 104	Roy Luongo
CYBV 496	Special Topics in Cyber Security - Introduction to Security Programming I & II (7 Week Class)	Keith Rezendes
CYBV 498	Capstone in Cyber Operations	Jordan Vanhoy Heidi Calhoun-Lopez

POC Or GTFO

Part 1/3

Bypass Windows 10 User Group Policy

Group Policy is a Microsoft feature that allows Domain Administrators to manage settings and enforcements for users on their network. An administrator can configure these Group Policy settings at the computer level and/or for the user level.

For user policies, these settings are pushed out to a domain user's account upon login and stored in the "%USERPROFILE%\ntuser.dat" hive. These user policies are read-only for Domain Users, preventing them from being changed.

Since we can swap out an entirely new hive, we can bypass or modify any of these "protected" user group policy enforcements.

We simply need to:

- Craft our own User Registry hive named "ntuser.man",
- Remove or apply whatever policies key/values we want in the hive.
- Drop the file in target machine's %USERPROFILE% path
- Logout and log back in.

CAUTION — THIS CAN DAMAGE A WINDOWS ACCOUNT, do NOT try this on a Domain machine that you are not Administrator for. I recommend trying this in a test virtual machine if you are curious. If you do end up trying this on a personal machine, don't try it on an Administrator account, as an Administrator account will be required to go in and delete the ntuser.man file when done

Crafting Ntuser.man

- On an entirely separate (same version) Windows machine which you have Administrator access to, copy any user's registry hive from %USERPROFILE%\ntuser.dat file to a different folder. Note, you will need to make sure this user is not logged in so that you can actually copy this file.
- Under the Administrator account, start regedit.exe, load this copied registry hive by selecting HKEY_LOCAL_MACHINE key, and clicking File->Load Hive…
- Under the newly loaded reg hive, clear or add any policies under the appropriate policy reg path, for example, many user policies are stored in \Software\Microsoft\Windows\CurrentVersion\Policies\.
- At the root of the hive you loaded in regedit, change permissions to allow "Everyone" full control (read/write/etc) and propagate these permissions for all subkeys.
- Depending on the "Policy" you want to override or add, you will need to find the corresponding subkey related to it, as they are not all stored under one key in the User's registry. For example, in the "Remove Task Manager '' scenario, the value that defines this is in the \Software\Microsoft\Windows\CurrentVersion\Policies\System key. So "System" subkey is where you would add a "DENY" rule, to deny SYSTEM "Write/Create" privileges for that key. This ensures GpSvc can't overwrite it.

PoC or GTFO

Part 3/3

Drop Ntuser.man

- Before continuing, ensure sure you have a backup account on the machine with Administrator privileges separate from the account you are testing on. If not — create one now, as this will be needed to delete the PoC file.
- Copy the registry hive you crafted as “%USERPROFILE%\ntuser.man” to the machine which you want to override User Group Policy for.
- Log off and Log back on. You may see a Windows welcoming screen, let this finish and now all User Group Policies have been overridden with what you have in ntuser.man.

Remove Ntuser.man

- After testing PoC, logout and login with the Administrator account to remove the “ntuser.man” file from the user’s profile path.

Other Implications

- Single File Code Execution
- Antivirus/EDR
- Denial of Service

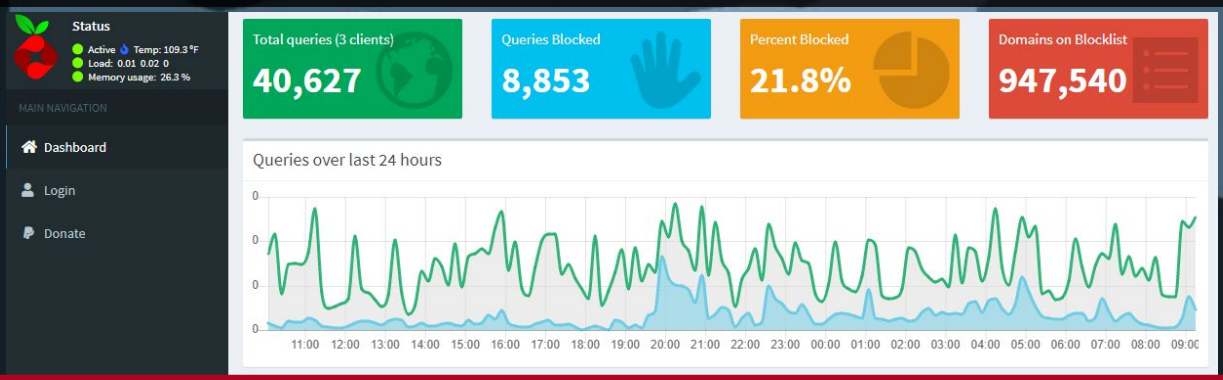
QUICK PROJECT

Block ads at the network level with a Raspberry PI

Ads are everywhere in our digital life and blocking them on your computer can be easy by simply installing a browser pop-up blocker. But what about everything else on your network like your phone, tablet, your TV or even your gaming console?

Well install a network wide ad blocker and live your life ad free in just a few simple steps.

- Setup and configure a Raspberry Pi and place it on your network. Give it a static IP address.
- Run the following command
  - curl -sSL https://install.pi-hole.net | bash
- Go to your home router and set the pi-hole as your DNS server
- Log into your new Pi-Hole and configure it as you would like it
- Enjoy your internet with no ads



CYBER SECURITY HISTORY

CREEPER VIRUS DISCOVERED, MARCH 16, 1971

Creeper was an experimental computer program written by Bob Thomas, a later version by Ray Tomlinson designed to copy itself between computers. This self-replicating version of Creeper is generally accepted to be the first computer virus.

The program was not actively malicious software as it caused no damage to data, the only effect being a message it output to the teletype reading "I'm the creeper: catch me if you can".

Reaper was a similar program created by Ray Tomlinson to move across the ARPANET and delete the self-replicating Creeper. The conflict between Creeper and Reaper served as inspiration for the programming game Core War.

UTAH PASSES THE UTAH DIGITAL SIGNATURE ACT OF 1995

Complex and ambitious, the Utah Act is intended to promote the use of digital signatures on computer-based documents and to facilitate electronic commerce. This influenced the passing of E-SIGN (federal) and UETA (state) which are technology neutral and do not favor digital signatures or secure/advanced signatures.

MELISSA VIRUS RELEASED, MARCH 26, 1999

The Melissa virus was a mass-mailing macro virus. As it was not a standalone program, it was not classified as a worm. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic. The virus would infect computers via Email, the email being titled 'Important Message'. Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook.

David L. Smith was sentenced to 20 months in federal prison and fined $5,000 USD for releasing the virus in May 1999.

BACKTRACK RELEASED TO OPEN SOURCE, MARCH 6, 2007

BackTrack was a Linux distribution that focused on security, based on the Knoppix Linux distribution aimed at digital forensics and penetration testing use. In March 2013, the Offensive Security team rebuilt BackTrack around the Debian distribution and released it under the name Kali Linux. Kali Linux was released to open source, March 13, 2013

CYBER SECURITY HISTORY

FIRST APPEARANCE OF VIENNA VIRUS , APRIL 1, 1988

Vienna is a non-resident, direct-action .com infector. When a file infected with the virus is run, it searches for .com files on the system and infects one of them. The seconds on the infected file's timestamp will read "62", an impossible value, making them easy to find. One of six to eight of the files will be destroyed when Vienna tries to infect them by overwriting the first five bytes with the hex character string "EAF0FF00F0", instructions that will cause a warm reboot when the program is run. These files will not actually contain the Vienna virus, they are just corrupted by it. The creator of the Vienna virus has never been revealed. Some sources say that the virus was created by Vienna high school student as an experiment. The first person to detect the virus was Franz Swoboda. Information was leaked that Swoboda received the virus from Ralf Burger, but Burger claimed that he received the virus from Swoboda. Ralf Burger did create a variant that caused the computer to hang rather than a reboot.

CLIPPER CHIP PROPOSED, APRIL 16, 1993

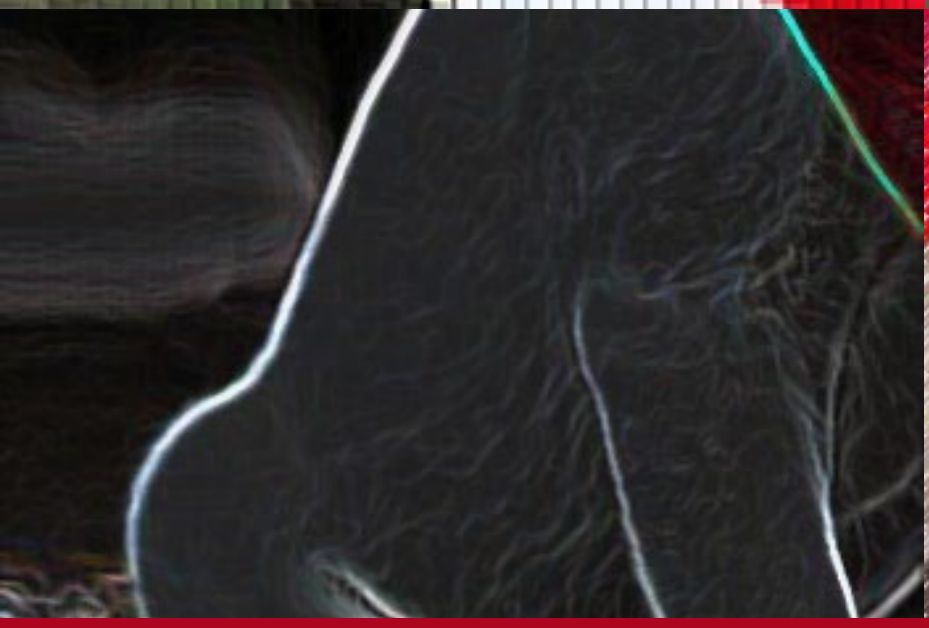
The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency[1] (NSA) as an encryption device that secured “voice and data messages"[2] with a built-in backdoor. It was intended to be adopted by telecommunications companies for voice transmission. It can encipher and decipher messages. It was part of a Clinton Administration program to “allow Federal, State, and local law enforcement officials the ability to decode intercepted voice and data transmissions."

HEARTBLEED VULNERABILITY PUBLIC DISCLOSURE, APRIL 7, 2014

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. Thus, the bug's name derives from heartbeat. The vulnerability is classified as a buffer over-read, a situation where more data can be read than should be allowed. TLS implementations other than OpenSSL, such as GnuTLS, Mozilla's Network Security Services, and the Windows platform implementation of TLS, were not affected because the defect existed in the OpenSSL's implementation of TLS rather than in the protocol itself.

THE PACKET

THE UNIVERSITY OF ARIZONA



CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

http://cyber-operations.azcast.arizona.edu/

THE UNIVERSITY OF ARIZONA