# THE PACKET

THE

# PACKET

CYBER SERVICE

April 2022

Packet Prodigy Clone
v0.39

QUESTIONS?
Contact Us

520-GLUT-CPU
(520-458-8278)
EXT: 2155

1 Select News Source

- HACK OF THE MONTH
- CYBER NEWS UPDATE

2 Select Internal Topic

- CYBER SECURITY HISTORY
- HACKING POC
- QUICK PROJECT

3 Select External Topic

- JOBS / SCHOLARSHIP

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

? Exit

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
THE UNIVERSITY OF ARIZONA
CAE IN CYBERSECURITY COMMUNITY

# >. HELLO_WORLD_☺

≥ ----- ESTABLISHING CONNECTION -----

≥ ≥ Welcome to the April 2022 issue of "THE PACKET", produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. With a heavy heart, I must address that this will be the very last packet ever made by Professor Galde. Last month we still observed advances in the cyberwar against the Ukraine and threats against Europe and the United States. Russia is losing backbone connections to the global internet, making it harder for the Russian Federation to maintain connectivity but much easier to monitor. This year is turning into a fascinating one so far, and it will likely become even crazier this month in April. In March, the United States formally declared that the Russian military has committed war crimes in Ukraine and expects a response from the Russian Federation, which may come from the cyber realm. The Federal Bureau of Investigation revealed that known malicious addresses connected to Russian campaigns were observed scanning networks of five US energy firms ahead of Biden's Russia cyberattack warning in March. This month we have a great April Fools' Prank involving windows batch files and a network visibility program you would run on your network to monitor devices at the hardware MAC level. Enjoy the pranks and fun while it lasts because this April fools it will be more than a joke about me leaving this publication. I have also included a short description explaining the cover for those of you too young to have used the Prodigy internet service. I wish to be the first to say Happy April Fools' Day, and I hope April remains a month of fun and laughter. Also, don't forget to scan your QR codes!

# OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

# JOIN CYBER SAGUAROS TODAY

Cyber Saguaros

CYBER_SAGUAROS

# Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

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

www.twitter.com/UWicys

f www.facebook.com/UAZWicys

www.instagram.com/uarizonawicys/

THE UNIVERSITY OF ARIZONA

WiCyS women in cybersecurity

UNIVERSITY OF ARIZONA STUDENT CHAPTER

AZ CYBER® initiative

# 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:*

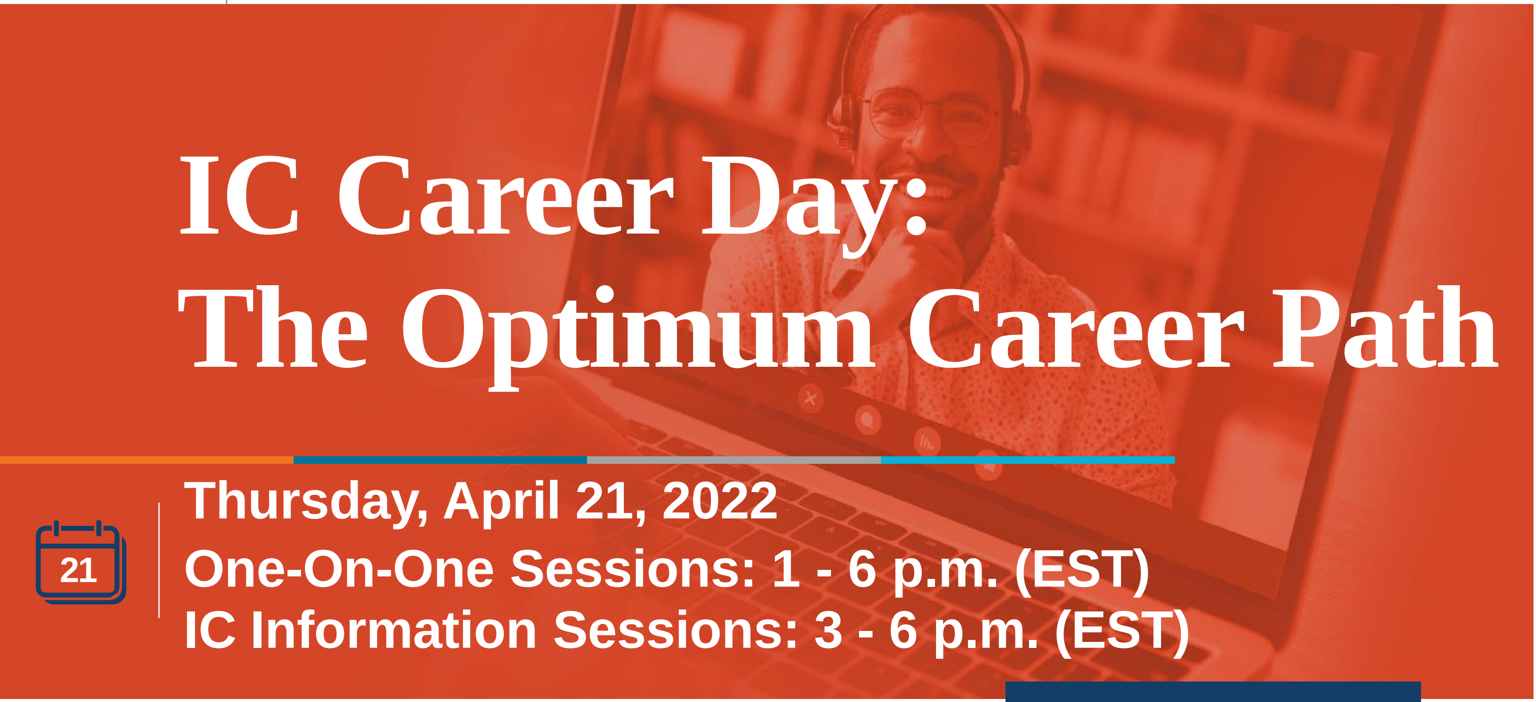
| | | |
|---|---|---|
| 01. | MAY 31- JUNE 03 | LOCATION: PIMA JTED, BRIDGES CAMPUS, TUCSON, AZ |
| 02. | JUNE 06- JUNE 10 | LOCATION: PIMA COMMUNITY COLLEGE, EAST CAMPUS, TUCSON, AZ |
| 03. | JUNE 13- JUNE 17 | LOCATION: CHANDLER HIGH SCHOOL, CHANDLER, AZ |
| 04. | JUNE 20- JUNE 24 | LOCATION: VIRTUAL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

## *INTERESTED IN BECOMING AN INSTRUCTOR?*

Send an email at *mfelix@azcyber.org*

Join the Intelligence Community
for a Virtual Recruiting Fair

Intelligence Community
Centers for
Academic
Excellence
*Diversity. Knowledge. Excellence.*



# IC Career Day:
# The Optimum Career Path

21

## Thursday, April 21, 2022

## One-On-One Sessions: 1 - 6 p.m. (EST)
## IC Information Sessions: 3 - 6 p.m. (EST)

**Calling all IC CAE Students**

Join us online to launch your career with the U.S. Intelligence Community's elements. The Intelligence Community recognizes IC CAE Scholars as the next generation of Intelligence Community professionals.

Freshman and sophomores: join this event to gain the opportunity to understand the key roadblocks that impede students from landing an Intelligence Community internship.

Rising junior, senior, and graduate-level IC CAE Scholars: connect with hiring managers and recruiters to prepare to join the Intelligence Community. You will receive several Intelligence Community career opportunities to apply to in advance of the event - coming your way soon! We encourage you to review the career opportunities prior to the event, to be better prepared for a one-on-one career discussion with the Intelligence Community recruiters.

WWW

**Register Now at**

**https://tinyurl.com/y97cy898**

**by April 4, 2022**

**A resume is required.**

**Questions**

**Contact ICCAE@dni.gov**

*U.S. citizenship is required. The United States Intelligence Community is an Equal Opportunity Employer.*

## AVOSLOCKER RANSOMWARE TARGETS US CRITICAL INFRASTRUCTURE

"AvosLocker is a Ransomware as a Service (RaaS) affiliate-based group that has targeted victims across multiple critical infrastructure sectors in the United States including, but not limited to, the Financial Services, Critical Manufacturing, and Government Facilities sectors," the FBI said. AvosLocker first surfaced during the summer of 2021, promoting their Ransomware-as-a-Service (RaaS) operation on underground forums and calling for ransomware affiliates to join them. According to deepweb research by Cyble Research Labs, the Threats Actors of AvosLocker ransomware groups are exploiting Microsoft Exchange Server vulnerabilities using Proxyshell, compromising the victim's network. Before starting the encryption process, the malware drops ransom notes with the name README_FOR_RESTORE.txt in the specific drive. Then, like other ransomware groups, the attackers instruct the victims to visit the TOR website. When the victim visits AvosLocker's TOR website, it asks for the ID given on the ransom note to proceed with the payment process. Once the victim enters the ID, the website redirects to the payment page where TAs instructs victims to pay, the ransom amount would double if the victim does not pay the ransom before the deadline. The ransomware groups are looking for support to expand their cybercrime ransomware business in the countries such as the USA, Canada, the United Kingdom, and Australia.

- **ARTICLE LINK**
- **TECHNICAL DETAILS**
- **FBI ALERT**
- **CYBLE DEEP WEB RESEARCH**

## MULTIPLE AUTOMOTIVE MANUFACTURERS INFECTED WITH EMOTET

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment. Conti cyber threat actors remain active and the number of reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike. The auto industry however has seen an increase with Emotet ransomware. While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds used by affiliate cyber actors and receives a share of the proceeds from a successful attack. Considered the most widely distributed malware, Emotet acted as a malware loader that provided other malware operators initial access to infected systems that were assessed as valuable. Qbot and TrickBot, in particular, were Emotet's main customers and used their access to deploy ransomware (e.g. Ryuk, Conti, ProLock, Egregor, DoppelPaymer, and others).

- **ARTICLE LINK**
- **CISA ADVISORY**
- **MALWARE ANALYSIS**

# RUSSIAN COMMS IN UKRAINE: A WORLD OF HERTZ

When the Ukrainian invasion first started, American military sources expressed surprise that Russian electronic warfare had not been more heavily deployed as is expected of a modern military. To put this surprise into more context, on paper, the Russian military can jam civilian V/UHF communications, including two-way radios and cell phone networks, as you would expect a military to be capable of controlling and limiting the flow of information. To do this, the Russian military, in general, places a high premium on high-frequency communications as the signal transmits over long distances and keeps their communication secure. It is a favorite mechanism for long-range trunk communications in any modern military, having equal importance to SATCOM in NATO forces. However, online sources like Twitter reveal that Russian military HF radio transmissions have been relatively easy to find using elementary tools and are made without built-in encryption capabilities, making them nothing more than regular civilian radios.

- There are a few ways this makes military sense.
  First, Russian military HF users may not care if eavesdropping occurs during warfare. Second, Russia has many capabilities, so why bring out the "expensive" toys to lose or damage if these are not needed?
- The second possibility is that HF may be used to transmit false information deliberately poison the well with incorrect information. However, anecdotal evidence from the Ukraine theatre hints that intercepted traffic correlates with Russian actual tactical actions.

Ukrainian electronic warfare forces have also exploited Russian HF nets and jammed them to impede command and control. Ukraine has also claimed to use these networks as a conduit for false, misleading, and demoralizing traffic. Determining the location of HF transmission sources has also let Ukrainian forces determine the position of Russian units. The seemingly dire state of Russian communications has created an opportunity that has been taken advantage of by Ukrainian troops. Ukrainian electronic warfare cadres can exploit lax communications discipline and deficient COMSEC/TRANSEC.

# RUSSIAN COMMS IN UKRAINE: A WORLD OF HERTZ

While the Ukrainian forces may be numerically inferior on the battlefield, they had an opportunity to be superior in the electromagnetic spectrum, and they jumped on it. At the same time, via the use of communications intelligence (COMINT) equipment, Ukrainian forces exploited Russian networks for intelligence and battlefield deception. The goal now is to preserve Ukrainian use of the electromagnetic spectrum while denying it to their opponents as long as possible.

The Security Service of Ukraine (SBU) has claimed to have captured a hacker who was helping to provide communications services for Russian troops inside Ukrainian territory. The hacker was helping to route calls from within Russia to the mobile phones of Russian forces in Ukraine and send text messages to Ukrainian security officers and civil servants proposing they surrender.

The hacker made use of a device called a SIM box. In this case, it is a Hypertone SMB-128 that can control 128 separate sim cards. This server then communicates with a GSM gateway. The SBU claims the hacker used four gateway devices to cover the 128 sim cards. The SBU claims the captured Russian equipment was for communication with top leadership in the Russian forces. Any military should never use methods like this for military comms due to the lack of encryption and how these points are actively able to be hunted by simple capabilities. Ukraine has been vigorously defending their mobile network communication space.

## SUCH A SIMPLE VIRUS, THE VIENNA VIRUS

The Vienna virus was an extremely simple virus and became a template for more complex and innovative viruses like Ghostballs, Chameleon and (possibly) Zerobug as the source code was published in many places. Damage done by this virus was probably minimal regardless of how widespread it became. Vienna was the first virus to be neutralized by an antivirus program written by German hacker Bernd Fix, this event also marks the first documented antivirus software ever written.

**April 1, 1988**

## HEARTBLEED VULNERABILITY PUBLICLY DISCLOSED

Heartbleed was a security bug in the OpenSSL cryptography library, which was 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 could be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client. It resulted from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension. The Canada Revenue Agency reported a theft of Social Insurance Numbers belonging to 900 taxpayers and said that they were accessed through an exploit of the bug during a 6-hour period on 8 April 2014. The UK parenting site Mumsnet had several user accounts hijacked, and its CEO was impersonated. The site later published an explanation of the incident saying it was due to Heartbleed and the technical staff patched it promptly. Anti-malware researchers also exploited Heartbleed to their own advantage in order to access secret forums used by cybercriminals. The problem can be fixed by ignoring Heartbeat Request messages that ask for more data than their payload need.

**APRIL 1, 2014**

APRIL

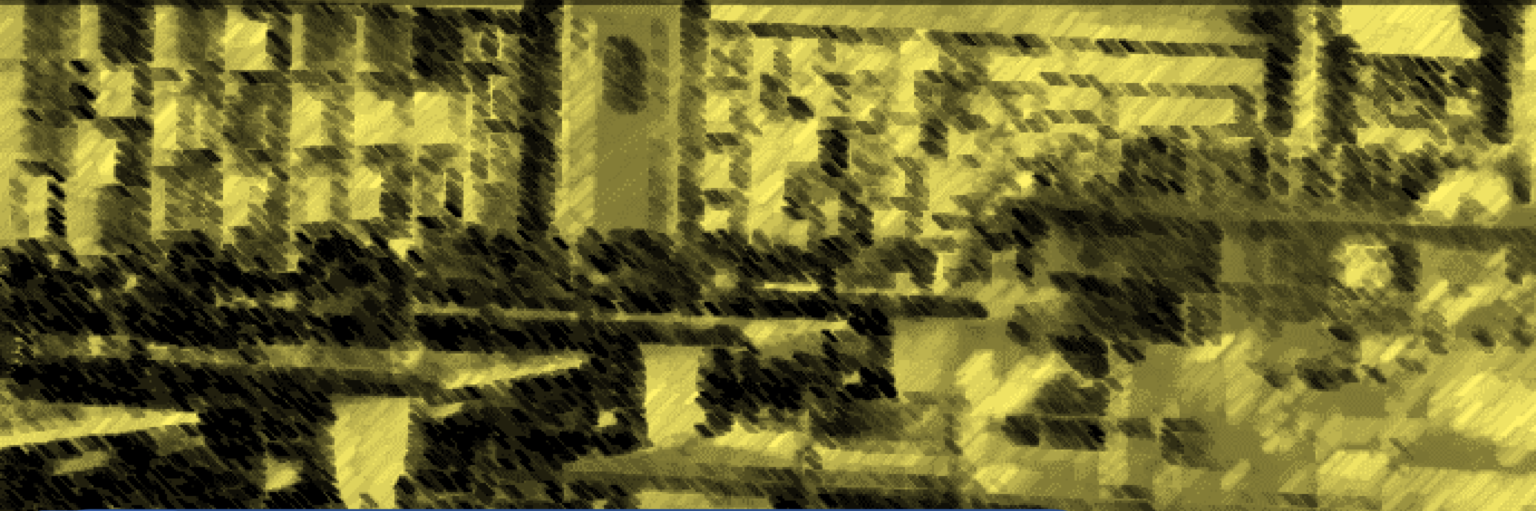
04

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

# CHERNOBYL VIRUS DESTROYS BIOS AS A STUDENT CHALLENGE

CIH, also known as Chernobyl or Spacefiller, is a Microsoft Windows 9x computer virus which first emerged in 1998. Its payload was highly destructive to vulnerable systems, overwriting critical information on infected system drives, and in some cases destroying the system BIOS. The malware filled the first 1024 KB of the host's boot drive with zeros and then attacked certain types of BIOS. This payload served to render the host computer inoperable, and for most ordinary users the virus essentially destroyed the PC. The payload tries to write to the Flash BIOS. Those machines that can be successfully written to by the virus have critical boot-time code replaced with junk. This routine only worked on some machines. The virus made another comeback in 2001 when a variant of the LoveLetter Worm in a VBS file that contained a dropper routine for the CIH virus which was circulated around the internet, under the guise of a picture of Jennifer Lopez. On December 31, 1999, Yamaha released a software update for their CD-R400 drives that was infected with the virus and in July 1998, a demo version of the first-person shooter game SiN was infected by one of its mirror sites.

**April 26, 1999**



APRIL

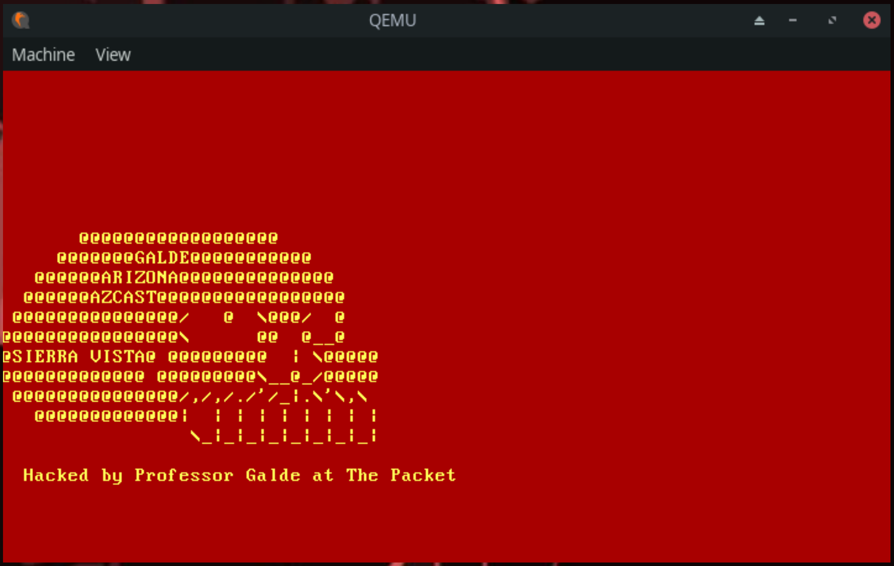
04

| S | M | T | W | Th | F | S |
|---|---|---|---|---|---|---|
| | | | | | | 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 |

# APRIL FOOLS MALWARE

Last year I was very proud to bring you a bootloader prank that you would place on a USB drive and plug into a computer which, when booted, would make it look your device was hacked.

Looking back, that may have been a little intense. So, this year, we will make it more approachable for everyone to do their pranks by making our own windows prank malware which a victim will run and believe they just received malware and hopefully find humorous.



```
       @@@@@@@@@@@@@@@@@@
     @@@@@@@GALDE@@@@@@@@@@@
   @@@@@@ARIZONA@@@@@@@@@@@@@@
  @@@@@@AZCAST@@@@@@@@@@@@@@@@@
 @@@@@@@@@@@@@@@/   @  \@@@/  @
@@@@@@@@@@@@@@@@\      @@  @__@
@SIERRA VISTA@ @@@@@@@@@  | \@@@@@
@@@@@@@@@@@@@ @@@@@@@@@\__@_/@@@@@
 @@@@@@@@@@@@@@@/,/,/./'/_|.\'\,\
   @@@@@@@@@@@@@|  | | | | | | | |
                 \_|_|_|_|_|_|_|_|

  Hacked by Professor Galde at The Packet
```

**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!!**

# APRIL FOOLS MALWARE

For our malware, we will create this by writing what is known as a batch file which is also known as a BAT file, which is a file used to execute commands with the Windows Command Prompt. This is a form of scripting that was popular a while ago but replaced with more powerful scripting platforms like PowerShell. A batch file allows you to perform various tasks, such as starting programs or running maintenance utilities within Windows and can be very powerful. We are going to use this to build our “malicious” script. The first thing we are going to do is open up a notepad document. This will allow us to write the script that we will need.

On the very first line, we are going to write:

```
@echo off
```

We do this to prevent the command prompt and contents of the batch file from being displayed on the screen, so only the output we want the victim to see is visible. The @ makes the output of the echo off command hidden as well.

In the following three lines, we will inform the user that we found a fake danger, and we will use the echo command to make this believable:

```
echo WINDOWS HAS DETECTED A VIRUS, WOULD YOU LIKE TO TERMINATE?
echo -
echo PROCEED WITH VIRUS TERMINATION (Y/N)
```

And with this, the user now believes that some virus or something is on the system.

# APRIL FOOLS MALWARE

Next, we will give the user a choice. They can either type Y or N, Next depending on what they choose, the script will complete the program:

```
set/p "cho=>"
if %cho%==Y goto forward
if %cho%==y goto forward
if %cho%==n goto Shutdown1
if %cho%==N goto Shutdown1
```

Now we defined the choice as cho and we will either go to the function **forward** or to the function **shutdown1**.

Next, we will define the forward function. This will mimic a virus checker that found something and wants to fix your issues:

```
:forward
echo VIRUS HAS BEEN DELETED
Pause
echo PLEASE ALLOW WINDOWS TO PREFORM A SAFETY CHECK
Pause
echo SYSTEM CHECK
echo HARD DRIVE - FAILED
echo -
echo RAM - FAILED
echo -
echo DISK DRIVE - FAILED
echo -
echo CONNECTION - FAILED
echo -
echo WINDOWS SUGGESTS YOU DELETE ALL FILES TO RESUME (Y/N)
```

# APRIL FOOLS MALWARE

Now it looks like the virus has been deleted, but the necessary safety check found some issues. So, we can only assume that the virus did some damage. So, the only solution is to delete all files, and we are given another choice that the user needs to make.

```
set/p "cho=>"
if %cho%==Y goto Sucess
if %cho%==y goto Sucess
if %cho%==n goto Shutdown2
if %cho%==N goto Shutdown2
```

So, the choice again is looking for either a Y or an N, and the functions will be either Shutdown2 or Success.

If the user again selects Y, we will run the rest of our script.

```
:Sucess
echo WINDOWS HAS DELETED ALL FILES
echo -
echo PLEASE ALLOW WINDOWS TO PREFORM A SAFETY CHECK
Pause
echo SYSTEM CHECK
echo HARD DRIVE - FAILED
echo -
echo RAM - FAILED
echo -
echo DISK DRIVE - FAILED
echo -
echo CONNECTION - FAILED
echo -
echo WINDOWS IS SHUTTING DOWN IN 20 SECONDS TO PROTECT FROM DAMAGE
goto Shutdown3
```

# APRIL FOOLS MALWARE

So, now the user is informed that everything has failed and now we will shutdown. The user will be in a panic and now depending on our choices we either continue onto shutdown3 or we go to shutdown2 or 1 depending on an earlier choice.

```
:Shutdown3
shutdown -r -t 20 -c "APRIL FOOLS! HAHAHAHAHAHA"
:Shutdown1
shutdown -s -f -t 60 -c "Windows is shutting down to prevent any
further damage"
:Shutdown2
shutdown -s -f -t 60 -c "Windows is shutting down to prevent any
further damage“
```

And now the prank is complete, the computer would have restarted, and you can now see how easy it is to write a simple script that can get malicious.

This script is available for download as notmalware.bat, feel free to update it or change it how you wish and have fun this April Fools Day

# BUILD YOUR OWN NETWORK PRESENCE DETECTOR

When you walk into a location that you trust, like your home or work environment, you may automatically have your phone set up to connect to the local Wi-Fi. Your family members, roommates, and frequent guests may also automatically connect to the local network for your home network. So, this project will look to determine if someone is "home" or not by looking for these connections on your home network. The simple idea in this project is that if this software sees your device on the network, the software will declare that you are "home." This, of course, will require that the device connects automatically when the Wi-Fi is in range to provide this service. With this software running, we can set up alerts when a device enters or leaves the Wi-Fi. We first need a Raspberry Pi with the latest upgraded software.

The Pi needs to be connected to your device's same network. For example, if you have 2.4Ghz and 5Ghz options on your router, the Pi can only link to the 2.4Ghz option but will still be able to see devices on the 5Ghz band.

The first piece of software we will install is arp-scan, and we can do this with the following command:

```
sudo apt-get install arp-scan
```

Once that has completed installing, we can test the software by running:

```
sudo arp-scan -l
```

I should now get a list of devices that responded to our ARP request. ARP will return the device's physical address or MAC address associated with each IP address that was searched for.

>. QUICK_PROJECT

## BUILD YOUR OWN NETWORK PRESENCE DETECTOR

Now that we know the devices on your network, we can write a straightforward python program to check if a device is on the network or not. We can do a simple check using python and give a read-out. This code can be expanded on, and more logic can be included to do much more.

```
import time
import os

while 1:
    if os.system("ping -c 1 -W 1 192.168.86.27 > /dev/null"):
        print ("Device Not Home")
    else:
        print ("Device Is Home")
    time.sleep(10)
```

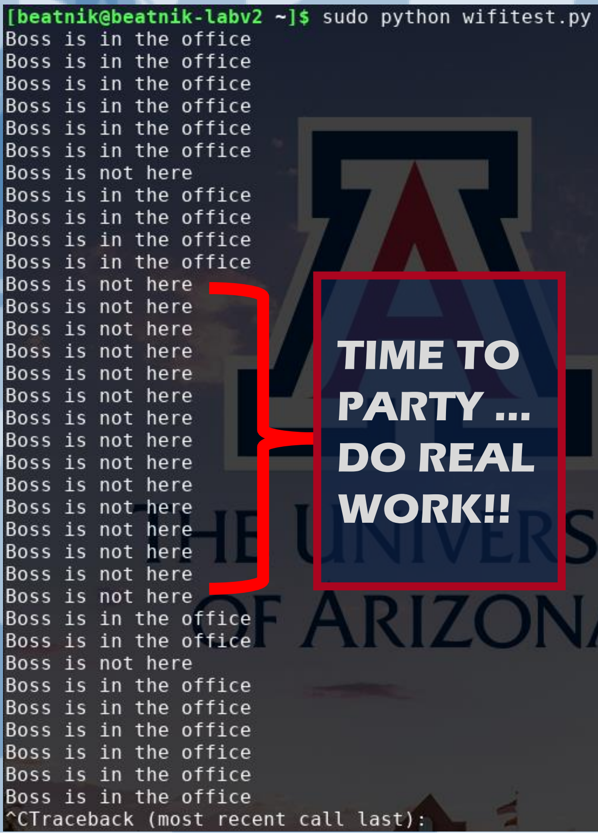
I identified my device as 192.168.86.27. So, I am using python to run the ping command with the flags c and W. The c flag designates how many pings to send out, and for this program, I only need 1 to be sent. The W flag symbolizes how much wait time to issue, and I set this to 1 second to not wait. If the device is online and responds to a ping, the program will print that the Device is Home, but if the ping fails because the device is not on the network or fails to respond to the ping, the program will print the message Device Not Home. This method is just checking for the device's IP address, so we want to check for the device's physical address or MAC address. To do this, we will change the code slightly.

>. QUICK_PROJECT

## BUILD YOUR OWN NETWORK PRESENCE DETECTOR

```
import time
import os
while 1:
    if os.system("arp-scan -l | grep -o ea:05:55:06:cc:be > /dev/null"):
        print ("Device Not Home")
    else:
        print ("Device Is Home")
    time.sleep(10)
```

So, the only change was to the command we ran on the system. We are running the arp-scan command and are looking to see if your device's physical address is listed. So, if a device took our previous IP address, it is unlikely we would have a device also use our device's physical address. This python program will also need to be run with administrator privileges to use the arp-scan command. Now, this is a straightforward Python script, but there is more logic that can be added. When a device enters or leaves the network, the monitor can email a user alerting that this has taken place. If you were utilizing this at work and could identify your coworkers or supervisor's device address, you can be alerted when they enter or leave the office. At the very least, you will know when their mobile device disconnects and connects to the local network. You can even change this program completely to identify all known devices and alert you when an unknown device is seen on the network.



```
[beatnik@beatnik-labv2 ~]$ sudo python wifitest.py
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is not here
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is not here
Boss is in the office
Boss is in the office
Boss is not here
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
Boss is in the office
^CTraceback (most recent call last):
```

TIME TO PARTY ... DO REAL WORK!!

AZ CYBER® initiative

# UPDATE ON GRANT PROGRESS

On behalf of the AZ Cyber Initiative Grant Team, we would like to thank you for your continued support and participation as part of the JFF/Google.org Planning Grant to Develop a Diverse Regional Workforce along the I-19 corridor.

In the spirit of transparency, as promised since our initial kick-off in January, I just wanted to update you on our JFF/Google.org grant progress:

## Needs Assessment

We are conducting labor market research and wrapping up informational interviews this week.

## Visioning Sessions

We will be hosting 1-hour workshops where we will share findings from our needs assessment and facilitate small group discussions to identify opportunities and approaches for digital jobs in the I-19 region.

***Please sign up for one of our Visioning Sessions open to the community.***

1

**8:15-9:30 am**
**Tuesday, March 29**

2

**4:15-5:30 pm**
**Tuesday, March 29**

3

**3.6:00-7:15 pm**
**Thursday, March 31**

## Grant Dashboard

We are developing a simple dashboard to share information gathered during our planning grant. We will keep you updated once the dashboard is up and running.

## Youth Development

AZ Cyber is providing paid work experience for over 30 young people in our community through the JFF/Google.org planning grant. Young people are participating in research and design efforts, as well as serving in a leadership capacity. This opportunity provides them with exposure to new networks and personal connections, educational and career development, and hands-on experiences.

We will continue to share updates over the coming weeks, so please be on the lookout for future emails from the AZ Cyber Grant Team. And as always, please reach out if you have any questions or would like additional details on any of the information mentioned above.

Regards,
**Manny**
*Founder & CEO, AZ Cyber Initiative*

JFF Google.org

WWW.AZCYBER.ORG

AZ CYBER initiative

# MENTORING

## PROGRAM

*"Tell me and I forget,*
*teach me and I may remember,*
*involve me and I learn."*

***– Benjamin Franklin***

### OUR PURPOSE

By working with experienced mentors, our program's mentees get a chance to learn what it takes to pursue diverse career paths as well as the challenges and pitfalls they may encounter along the way. The ultimate goal of a mentorship is to help students become more confident and resilient in whatever they choose to pursue.

### OUR PROGRAM

The AZ Cyber Initiative Mentorship Program connects Arizona high school students with qualified professionals in cybersecurity, IT, and other technology fields from all over the country. Through regular interactions with experienced mentors, participating students gain unique insights and important tools to help them find greater success in their path forward.

### OUR PROCESS

AZ Cyber does its best to match program participants based on mutual interests and availability. Most mentoring relationships will consist of one mentor and one mentee. As part of the program, both mentors and mentees commit to initiate, develop, and maintain an effective mentoring relationship.

## ROLES & EXPECTATIONS

### FOR MENTORS

- Dedicate four to six hours of communication over a six-month period with your assigned mentee. May be conducted via phone, video conferencing, email, or in person.
- Serve as a positive role-model and guide to help enhance your mentee's professional growth and learning.
- Assign reading and research materials relevant to your mentee's interests and objectives.
- Enhance your mentee's experience by inviting them to work meetings, connecting them with colleagues, providing information about internships, assigning them tasks that will develop their leadership skills.

### FOR MENTEES

- Dedicate four to six hours of communication over a six-month period with your assigned mentor. May be conducted via phone, video conferencing, email, or in person.
- Discuss your goals, needs, and what you hope to gain from the relationship with your mentor. Speak openly and honestly and seek constructive feedback whenever possible.
- Follow mentor's advice and instruction on eading and research material relevant to your interests and career objectives.
- Ask your mentor for assistance in building a professional network, including introductions to colleagues and other professionals in the field and information about potential internship opportunities.

***For more information visit our website at***
***https://azcyber.org/***

## ENTERPRISE VULNERABILITY SUMMER INTERN

**REMOTE**

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

Avant is looking for an Enterprise Vulnerability Summer intern who is passionate about cyber security and a career in the industry!

Our internships are paid and will likely work a hybrid schedule with time in and out of our downtown Chicago office. We are seeking undergrad students who have completed at least his or her junior year or graduate students pursuing an advanced degree in an information security related field.

Enterprise Vulnerability Management (EVM) is one of the many lines of defense in protecting Avant's technological landscape. EVM proactively detects potential flaws or weaknesses in our systems, assesses the criticality and systematically manages those discoveries through to remediation.

- Discover vulnerabilities within Avant's environment via various methods (scans, audits, penetration tests)
- Assess the criticality of vulnerabilities to prioritize remediation tasks
- Assign remediation tasks to appropriate system owners and manage those tasks within specified criteria and timeframes.
- Continuous improvement of processes and efficiency of the program across the enterprise.

What we're looking for in a good candidate:

- Time Management
- Organization
- Attention to detail
- Ability to critically think through risk scenarios
- Fundamental knowledge of Information Security and Technical systems

## CYBER SECURITY ARCHITECTURE AND ENGINEERING INTERN

**REMOTE**

Avant is looking for talented students passionate about cyber security and a career in the industry!

Our internships are paid and will likely work a hybrid schedule with time in and out of our downtown Chicago office. We are seeking undergrad students who have completed at least his or her junior year or graduate students pursuing an advanced degree in an information security related field.

Our summer intern will work alongside our Cyber Security team as they deploy and maintain the technology that helps monitor and protect Avant infrastructure and employees from malicious or nefarious cyber activity.

- Security Orchestration and Automation Development.
- Endpoint baseline policy configuration and enforcement.
- Log ingestion, aggregation, and correlation.
- Firewall/Network Security Audits.

What we're looking for in a good candidate:

- Understanding of Information Security concepts.
- Knowledge of SIEM, SOAR, EDR, IDS/IPS and how they can be utilized in an organization.
- Technical Problem-solving skills.

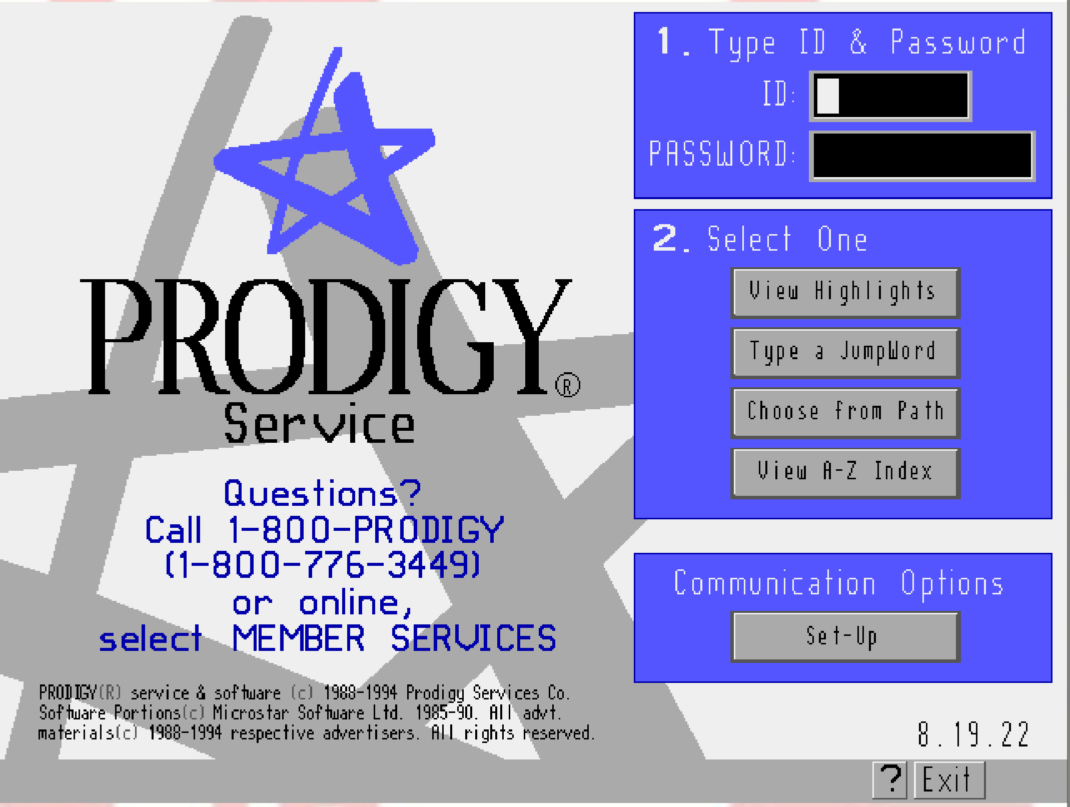
- **APPLY HERE**
- **WEBSITE**
- **GLASS DOOR**

# APRIL COVER DETAILS

Prodigy was an online service from 1984 to 2001 that offered its subscribers access to a broad range of networked services, including news, weather, shopping, bulletin boards, games, polls, expert columns, banking, stocks, travel, and a variety of other features. You may have seen a service like this maybe in AOL depending on when you were first introduced to the Internet. The company claimed it was the first consumer online service, citing its graphical user interface and basic architecture as differentiation from CompuServe, which started in 1979 and used a command-line interface.

Prodigy pioneered the concept of an online content portal or single site offering news, weather, sports, communication with other members, and shopping. The service provided several lifestyle features, including popular syndicated columnists, Zagat restaurant surveys, Consumer Reports articles and test reports, games for kids and adults, in-depth original features called "Timely Topics", bulletin boards moderated by subject matter experts, movie reviews, and e-mail. Prodigy was the service that launched ESPN's online presence. Prodigy's initial business model relied more on advertising and online shopping for cash flow than monthly subscriptions. Subscribers were charged a flat monthly fee that provided unlimited access. Initially, a monthly rate was charged for unlimited usage time and 30 personal messages.

By 1993, Prodigy was developing a network architecture that would become known in the modern Internet age as a content delivery network. The network caches it most frequently accessed content as close as possible to the users. The company sold private versions of this for use within a customer's private corporate network.



Questions?
Call 1-800-PRODIGY
(1-800-776-3449)
or online,
select MEMBER SERVICES

PRODIGY(R) service & software (c) 1988-1994 Prodigy Services Co. Software Portions(c) Microstar Software Ltd. 1985-90. All advt. materials(c) 1988-1994 respective advertisers. All rights reserved.

8.19.22

```
>.  ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE A FUN AND SAFE EARTH DAY, APRIL 22
>.
>. ---END TRANSMISSION---
```

THE
# PACKET
CYBER SERVICE

April 2022

Packet Prodigy Clone
v0.39

QUESTIONS?
Contact Us
520-GLUT-CPU
(520-458-8278)
EXT: 2155

1140 N. Colombo Ave.
Sierra Vista, AZ
85635

1 CONTACT US

CIIO@EMAIL.ARIZONA.EDU

WEBSITE

2 EDITOR / PROOFREADER

MICHAEL GALDE

DR> HARRY COOPER

RUBBER DUCK

3 HAVE A SAFE AND HAPPY

APRIL FOOLS DAY

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

?

Exit

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY