THE PACKET

THE UNIVERSITY OF ARIZONA

SUMMER

JUNE 2020

IN THIS ISSUE

THE UNIVERSITY OF ARIZONA

THE PACKET
JUNE 2020

--- BEGIN MESSAGE ---

Welcome to the **JUNE** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. My name is Professor Galde and it is my pleasure to produce this next issue. We now mark the start of Summer in this new COVID-19 world and many of us will be stuck inside and avoiding large groups. DEFCON has been officially canceled and this time it is not a joke.

The infosec community is adjusting to this new reality and so are all of us at the University of Arizona. So we may ask ourselves how do we cope in this world and I do not have a answer for everyone but for me it is finding projects. It is one day at a time and finding ways to make the most of everything. At the University of Arizona we will teach you not just the basics of cyber security we teach you the dark arts in cyber security to give you that edge in the infosec community. Last month our main project was showing readers how to develop there own malware using python as a exercise of what malware really is. You can take as many classes as you want about malware research at other locations but the Cyber Operations program will tear the vail away from your eyes and show you what makes malware work and why. Last month was the anniversary of WannaCry and the ILOVEYOU malware which both hold a special bond to my awakening into cybersecurity and this month is showing us the start of the cybersecurity community coming together in 1993 for the first time at DEFCON. In 2005 a team of security researches showed how mobile malware would work by developing malware for mobile devices. We will continue that path this month by showing how malware is packaged into trusted programs we know and love. Tell next time!!!!

--- END MESSAGE ---

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

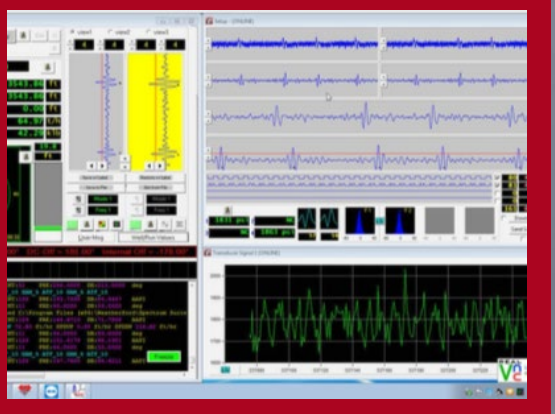
HACKS OF THE MONTH

BLACKOUT, BROWNOUT OR CYBER ATTACK…

So I have a passion for critical infrastructure and the cyber security issues unique to these networks as they are not the same IT issues and solutions. Everyone relies on these critical infrastructure and as the UK recently discovered at the Elexon administrator they are targeted with sophisticated attacks.

HIDE YOUR MALWARE IN A 2 FACTOR AUTHENCATOR … AWESOME MOVE!

So just looking at it from a techniques perspective, if you want to hide malware, using a 2FA application is a interesting choice. Infecting the MAC OS with malware has its own distribution challenges but choosing a 2FA app is a interesting choice and have to give them credit when due. That would get quite a few unsuspecting victims. Now for what that malware was used for… shame on you Lazarus!



HE WHO CONTROLS THE SPICE ER… WATER CONTROLS THE UNIVERSE

Critical infrastructure again, this time unknown attackers targeted the industrial control systems (ICS) involved with water management. The attack were discovered after the compromised PLCs caused suspicious valve changes, but it's unclear if the attackers were trying to cause damage by tampering with valves or if they made an error that led to their discovery.

CYBER NEWS UPDATES

US PORTS AND INFRASTRUCTURE PROVIDERS COME TOGETHER ON CYBER SECURITY

A group of US ports and infrastructure organizations have come together to share information on cyber security under the umbrella of The Maritime Transportation System Information Sharing and Analysis Centre (MTS-ISAC). The Department of Homeland Security recognizes the Maritime Transportation System (MTS) as one of the seven critical subsectors within the Transportation System Sector.

DISCOVER MORE | CYBV 480 CYBER WARFARE | CYBV 435 Cyber Threat Intelligence | CYBV 385 INTRODUCTION TO CYBER OPERATIONS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY

THREAT RESEARCH TTPS ASSOCIATED WITH MAZE RANSOMWARE INCIDENTS

Malicious actors have been actively deploying MAZE ransomware since at least May 2019. The ransomware was initially distributed via spam emails and exploit kits before later shifting to being deployed post-compromise. Since November 2019, FIREEYE has seen the MAZE ransomware being used in attacks that combine targeted ransomware use, public exposure of victim data, and an affiliate model.

DISCOVER MORE | CYBV 454 MALWARE THREATS & ANALYSIS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 388 CYBER INVESTIGATIONS AND FORENSICS | CYBV 385 INTRODUCTION TO CYBER OPERATIONS

APPLE'S COPYRIGHT LAWSUIT HAS CREATED A 'CHILLING EFFECT' ON SECURITY RESEARCH

Last year, Apple accused a cybersecurity startup based in Florida of infringing its copyright by developing and selling software that allows customers to create virtual iPhone replicas. During the lawsuit's proceedings, Apple has sought information from companies that have used the tool, which emulates iOS on a computer, allowing researchers to probe potential iPhone vulnerabilities in a forgiving and easy-to-use environment.

DISCOVER MORE | CYBV 474 ADVANCED ANALYTICS FOR SECURITY OPERATIONS | CYBV 435 CYBER THREAT INTELLIGENCE | CYBV 329 CYBER ETHICS | CYBV 301 FUNDAMENTALS OF CYBERSECURITY

JOB BOARD

Network Professional (Network Engineer, Network Architect)

NSA is in search of top-notch cyber professionals with technical expertise and driving desire at the forefront of their field. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satellite communications networks) that are deployed across NSA worldwide. Help protect national security interests as part of the world's most advanced team of cyber professionals!

Cyber Network Professional (Offensive/Defensive Operations)

NSA is in search of top-notch cyber professionals with technical expertise and driving desire at the forefront of their field. We have positions in penetration testing, defensive operations, identifying cyber threats and vulnerabilities and building defensive capabilities, designing, developing, deploying, sustaining and monitoring state-of-the-art network solutions (WAN, CAN, LAN, DCN and Satellite communications networks) that are deployed across NSA worldwide. Help protect national security interests as part of the world's most advanced team of cyber professionals!

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

Associate Proxy Administrator - Arizona

Works with customers analyzing, troubleshooting, and isolating network protocol issues and hardware/software problems using various network tools. Tools include, but not limited to, the build, configuration, full end-to-end traffic analysis, migration and deployment of Blue Coat Proxy. Provide recommendations to customers for rapid restoration of services. An understanding of the Transmission Control Protocol/Internet Protocol (TCP/IP) and the IP address scheme and understand Secure Socket Later (SSL) Protocol. Be able to provide written and oral communication within a team structure and operate as an individual under some supervision. Perform Log analysis, DNS entry coordination, ACL management and multi-system configuration control as required work within a team structure. Research and identify means for detection of malicious activity toward Army web resources.

Associate- Help Desk Technician - Illinois

As a Help Desk Technician, you provide phone and in-person technical support for end users in an enterprise level environment. This is a full-time position to support and maintain in-house computer systems, desktops, and peripherals. This includes installing, diagnosing, repairing, maintaining, and upgrading all hardware and equipment while ensuring optimal workstation performance. Troubleshoot problem areas in a timely and accurate fashion and provide end user training and assistance where required.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

Network Administrator - Illinois

The ideal candidate will be responsible for administration and day-to-day operation of organization's local area network (LAN). The Network Administrator will provide integrated team support and maintenance of LAN hardware and software. The ideal candidate will have experience with protocol analysis, knowledge of common network protocols, satellite networks, and Cisco ASA and Palo Alto firewalls.

Information Security Engineer - Maryland

Responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within their Computing Environment (CE). Assesses architecture and current hardware limitations, defines and designs system specifications, input/output processes and working parameters for hardware/software compatibility. Provides recommendations on information assurance engineering standards, implementation dependencies, and changing information assurance related technologies.

Software Engineer - Maryland

Provides functional and empirical analysis related to the design, development, and implementation of software systems, including, but not limited to application software, utility software, development software, and diagnostic software. Participates in the development of test strategies, devices, and systems. Solving engineering problems (or managing the solution of engineering problems) in the functional area to which assigned.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

JOB BOARD

Software Configuration Management Specialist - Maryland

Must be able to write Configuration Management (CM) Plans and audit software change procedures, software development, software testing, and software documentation to verify compliance with software CM plans and procedures. Must be capable of participating in design reviews, configuration audits, and evaluations of software products to ensure proper identification, control, and status accounting of the software baseline for each system. Working on code management, audits, baseline identification, and preparation and control of documentation for software projects.

Senior Network Administrator (SME) - Arizona

The selected candidate will assist with daily leadership and technical guidance for a team of network analysts while performing daily management network assets from various vendors to include firewalls, routers, switches, load balancers and VPNs on behalf of the United States Army. Writing documentation to include SOPs and TTPs. Utilizing a diverse suite of network monitoring technology, troubleshoot a dynamic and complex environment while assisting third parties to solve various network connectivity problems.

DUE TO THE CURRENT ISSUES SURROUNDING THE COVID-19 PANDEMIC, SOME GOVERNMENT AGENCIES ARE EXPERIENCING HIRING FREEZES, BUT WILL STILL PROCESS APPLICATIONS FOR HIRE. PLEASE REMAIN FLEXIBLE WITH HIRING OFFICIALS DURING THIS TIME.

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 301	Fundamentals of Cybersecurity (7 Week class 1 & 2)	Paul Wagner
CYBV 326	Introductory Methods of Network Analysis Section 101 - 106	Jordan Vanhoy
CYBV 326	Introductory Methods of Network Analysis Section 107 - 110	Michael Galde
CYBV 329	Cyber Ethics (7 Week Class 1 & 2)	Heidi Calhoun-Lopez
CYBV 354	Principles of Open Source Intelligence (7 Week Class 2 only)	John McCary
CYBV 385	Introduction to Cyber Operations (7 Week Class1 & 2)	Michael Galde
CYBV 388	Cyber Investigations and Forensics Section 101 - 104	Troy Ward
CYBV 388	Cyber Investigations and Forensics Section 105 - 106	Steven Wood
CYBV 393	Internship in Cyber Operations	Jason Denno

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 399 CYBV 499	Independent Study	Jason Denno
CYBV 400	Active Cyber Defense Section 101 - 104	Thomas Jewkes
CYBV 400	Active Cyber Defense Section 105 - 106	Colin Brooks
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 101 - 104	Thomas Jewkes
CYBV 435	Cyber Threat Intelligence (7 Week Class) Section 102 & 104	Harry Cooper
CYBV 436	Counter Cyber Threat Intelligence (7 Week Class 2 only)	Harry Cooper
CYBV 440	Digital Espionage (7 Week Class 1 only)	Kate Mabbett
CYBV 441	Cyber War, Terror and Crime (7 Week Class 2 only)	Kate Mabbett
CYBV 454	Malware Threats & Analysis	Luis Mendieta

CYBER OPERATIONS FALL SCHEDULE

CAT #	Course	Instructor
CYBV 470	C Programming for Security Professionals	Keith Rezendes
CYBV 471	Assembly Language Programming for Security Professionals	Mohamed Meky
CYBV 473	Violent Python	Chester Hosmer
CYBV 474	Advanced Analytics for Security Operations	Chester Hosmer
CYBV 479	Wireless Networking and Security	Jordan Vanhoy
CYBV 480	Cyber Warfare Section 101 - 102	Rock Stevens
CYBV 480	Cyber Warfare Section 103 - 104	Roy Luongo
CYBV 496	Special Topics in Cyber Security - Introduction to Security Programming I & II (7 Week Class 1 & 2)	Keith Rezendes
CYBV 498	Capstone in Cyber Operations	Jordan Vanhoy Heidi Calhoun-Lopez

THE UNIVERSITY OF ARIZONA

The Intelligence & Information Operations (IIO) Program *Presents:*

ICCAE **SPEAKER SERIES** 2020

The Intelligence Community Center of Academic Excellence (ICCAE)

2020 Student, Staff & Faculty Professional Development Speaker Series (April – June 2020)

A designated Intelligence Community Center of Academic Excellence, The College of Applied Science & Technology's Intelligence & Information Operations program affords its students, staff, and faculty exclusive professional development opportunities. Event attendees learn from and engage with the leaders and practitioners of the United States IC and private sector.

The IIO program culminates the 2020 academic calendar year with a professional development speaker series that will deep dive into issues such as cybersecurity, military intelligence analysis, politics, topics of national security and more.

All sessions will be streamed live via Zoom **(Meeting ID: 605 128 853): https://arizona.zoom.us/j/605128853.** Topics and speakers will be announced as they are confirmed; upcoming speaker segments will be posted on the *CAST IIO's ICCAE Academic and Professional Development webpage*. We encourage you to join us for live interactive events, as not all session will be available for a later viewing.

For questions or concerns, please contact: Professor Craig Nazareth at cnazareth@arizona.edu or 520-458-8278 ext. 2185

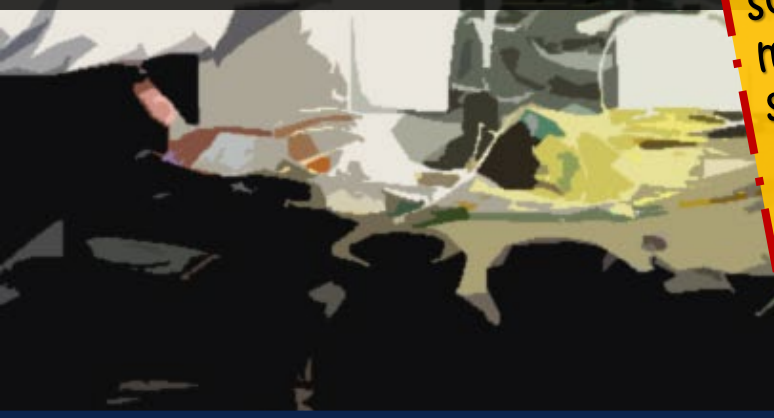
HACKING POC

Part 1/3

LETS PACK MALWARE FOR FUN!!

Last month we developed a simple malware example using python. Now while that was fun to test and develop it would be hard to have your victim open up a python file and even more of a risk if they looked at the code to figure out what it did. So we will need to package our malware into a innocent looking program or “pack” it.

So first we want to choose what program do we want to choose to be our way in to the victim. The beauty of this is that the program will still work, we are just adding our file to the process as it launches. So what we are creating in this instance is a Trojan Horse which is disguised as a legitimate piece of software. We can use any executable program that will run on the victims computer. We would want something that is enticing enough to be opened from a unknown source and able to be believed as coming from a untrusted or unvetted source. For our example we will just simply use Microsoft Calculator.



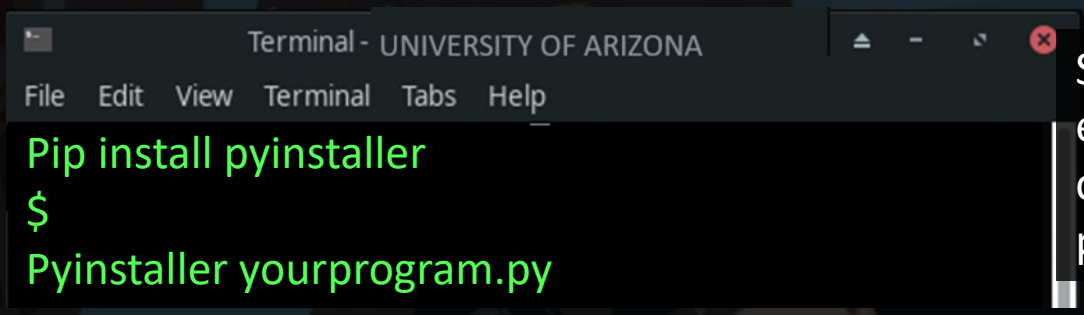
CAUTION — This article shows you how to create a piece of software some may misuse and/or misunderstand. This malware series is intended for academic purposes only and is intended to provide education to cyber security professionals... Plus you will likely be caught if you don’t make major changes. You assume any risk of using the information in this article.

HACKING POC

Part 2/3

CREATE CONTROL PROGRAM IN EXE

In order for this to work we need to turn our python program into a executable program that can be ran as a exe. The process is very simple to get started.



Set up your environment and covert your program

So we are going to download the launcher conversion program

We will create the exe file of our malware and make a note of its location. There is also a backup option we can include at this point as well on the GitHub repo.

Now we identify the front Program we will use to make our program work on the victims computer.

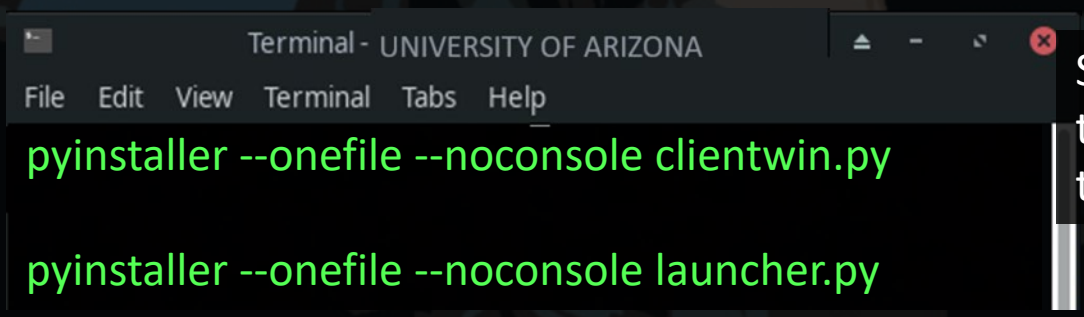
```
import os
import threading

scriptpath = "C:/Users/..." # MODIFY ME -> this will be the backdoor (clientwin.exe)
exepath = "C:/Users/..." # MODIFY ME -> this will be the fron program (minesweeper.exe)
backupexe = "C:/Users/..." # MODIFY ME -> this will be bacup.exe or b2.exe

def front():
    os.startfile(exepath)

def back():
    os.startfile(scriptpath)


def main():
    os.startfile(backupexe)

    bThread = threading.Thread(target = back)
    bThread.daemon = True
    bThread.start()

    front()


if __name__ == "__main__":
    main()
```

HACKING POC

Part 3/3

Putting it all together

So now we have our program in a executable format and our front program we will use to make our malware appear like a legitimate and innocent program.
Even if the victim closes the front program our malware still runs in the background unless the victim closes it by using task manager or we close the connection ourselves.
We now have what many would be considered a backdoor into our victims computer once they launch our malware and open up our program.



Set up the EXE files to be included in the final malware

Next week we will look at the art of distributing our malicious program and trying to get a user to interact with our program. We will look at phishing and the psychology involved with trying to get a user to do something everyone knows they should not do.

QUICK PROJECT

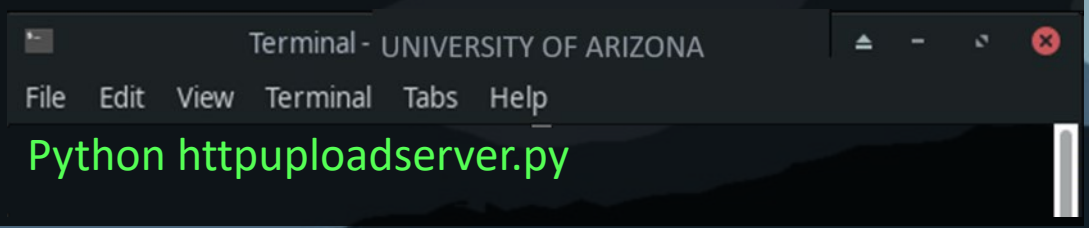
SIMPLE HTTP SERVER

USE PYTHON TO RUN A WEB SERVER AND UPLOAD FILES QUICK AND EASILY

Sometimes you need to set up a quick http server to share files or what not for work or in your personal life. Python has a great built in web server that allows you to do this quickly. If you were to type: *python -m http.server 8000* in the command line you can set up a quick server to share files on port 8000. When you need to share files quickly this has been such a valuable tool.

My problem with this process however is sometimes I want to move files back to my host computer and I did not have a good option. Well I came across a project under a user by bones7456 who put together a really simple HTTP server that allows uploads. Well I modified this code a little bit and have made it available the link **RIGHT HERE**

Once you are ready all you need to do on your host machine is run the following command and you will be running your own upload server.



CYBER SECURITY HISTORY

FIRST DEFCON — JUNE 9, 1993

Dark Tangent who is also known as Jeff Moss put together and founded the DEFCON conference as a farewell party friend from Platinum Net which was Fido protocol based hacking network from Canada. Well travel issues with his friend made it where his friend had to leave early so now with this party planned in Vegas and no friend what is a guy to do? Well lets bring all of our hacker buddies to Vegas and talk about computer security. This consisted of about 100 people in attendance from all over the country. This was considered to be a one time event but because of the positive feedback they decided to bring it back again and eventually it became a annual conference. DEFCON this year is canceled due to COVID-19 but DEFCON will have a virtual conference in place which is called DEFCON Safe Mode with networking. This will take place August 7 to 9 with a introduction day on August 6th. DEFCON 29 however is still planned for August 5 to 8 2021 in Las Vegas and is expected to be a very popular event as this recent one was canceled. My first DEFCON was 27 where a estimated 30,000 people attended the conference and I am excited to go the next time just to take in the fun and exciting hacking culture.

FIRST MOBILE MALWARE – CABIR WORM — JUNE 15, 2005

Cabir or otherwise known as Trojan.SymbOS.Skulls from variant A to F was a security research project to show manufactures and other interested parties how malicious mobile software can be deployed against mobile devices. This was made to target devices running Symbian OS which was a very popular mobile OS under the Nokia branded phones. If you had a phone in 2005 you likely had a Nokia at this time. The iPhone was not released tell 2007 and Nokia was king of mobile devices at the time. Now this worm was never released in the wild but was sent directly to anti-virus companies so that mitigations can be put into place. Now Mabir, a variant of Cabir, is capable of spreading not only via Bluetooth but also via MMS. By sending out copies of itself as a .sis file over cellular networks, it can affect even users who are outside the 10m range of Bluetooth.

THE PACKET

THE UNIVERSITY OF ARIZONA

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

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

Phone: 520-458-8278 ext 2155

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

THE UNIVERSITY OF ARIZONA