

THE PACKET

SUMMER

JULY 2021

IN THIS ISSUE

HACKS OF THE MONTH	4
CYBER NEWS UPDATES	6
CYBERSECURITY HISTORY	20
HACKING “POC”	21
CYBER TIPS & TRICKS	26
JOBS & INTERNSHIPS	27
QUICK PROJECT	35



A MESSAGE
FROM
PROFESSOR
MICHAEL
GALDE

LETTER FROM THE EDITOR

--- BEGIN MESSAGE ---

Welcome to the JULY issue of "The PACKET" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and we are just weeks away from DEFCON 29 and I am very excited. One of the things I look forward to are the workshops and DEFCON will be hosting quite a selection during the week as well as many in-person and virtual events. I am eyeing the "Hacking the Metal" workshop to brush up on my assembly knowledge and to interact with others who share the love of learning. Windows 11 was also announced last month which looks visually stunning and I am excited to find out how many ways I can break it once it comes out to help make it even better by finding vulnerabilities which will later turn into CVE bulletins. Finding a Windows 11 Remote Code Execution with "no-click" could give you a nice 1 million dollar pay out. That is nothing compared to mobile device payouts which are sitting around 2.5 million for an Android exploitation. The last few weeks we have also seen numerous news stories about ransomware attacks taking place and it looks like this trend will continue. A company with a good cybersecurity program will help navigate these disturbing trends and the knowledge you gain within the Cyber Operations program will help you become part of this important team. Many organizations are discovering that cybersecurity insurance provides very little protection and, in many cases, refuse to pay out if the organization has failed to protect themselves as well.

--- END MESSAGE ---

A MESSAGE
FROM
OKTETT

--- BEGIN MESSAGE ---

HELLO (DIGITAL) WORLD!

YOU CAN REFER TO ME AS OKTETT AND I AM EXCITED TO HAVE THE OPPORTUNITY TO SHARE SOME OF THE CYBER-RELATED TOPICS, THAT CATCH MY ATTENTION, IN BYTE SIZES. LET ME SHARE JUST A FEW THINGS ABOUT MYSELF.

I JUST JOINED [UA'S CYBER OPS PROGRAM](#), BUT I AM NOT ENTIRELY NEW TO THE CYBER WORLD. I RECENTLY GOT A DOUBLE ASSOCIATES IN CYBERSECURITY AND SOCIAL AND BEHAVIORAL SCIENCES.

I SERVED IN THE MILITARY FOR EIGHT YEARS. PRIOR TO THAT, I HAVE A FEW LANGUAGES UNDER MY BELT, AND I AM NOW EXTREMELY EXCITED AND INVESTED IN SEVERAL CYBER TOPICS. A FEW OF THEM ARE NATIONAL AND SPACE DEFENSE SYSTEMS, OPEN-SOURCE

INTELLIGENCE, SOCIAL ENGINEERING, GLOBAL AND DOMESTIC CYBERTERRORISM, LINGUISTIC AND CULTURAL NUANCES IN CYBER MITIGATION, DIGITAL FORENSICS, AND JUST HOW CAN I BREAK SOMETHING JUST SO THE "BAD APPLES" WON'T IN THE FUTURE. THIS CERTAINLY DOES NOT SPELL OUT THE ENTIRE SCOPE OF MY INTERESTS, BUT AS I LEARN MORE ABOUT IT ALL, MY HOPE IS TO ALSO SHARE SOME OF THAT WITH YOU.


AS I STUDY FOR MY [COMPTIA SECURITY+](#), I'M ALSO GETTING READY TO START A COUPLE OF CLASSES IN JULY AND THEN ON TO THE REGULAR SEMESTERS. WITH THE GLOBAL PANDEMIC A BIT MORE UNDER CONTROL AND ALL OF US REINTEGRATING BACK TO SOME OF THE PREVIOUS NORMS, I'M LOOKING FORWARD TO SEEING WHAT WE HAVE LEARNED FROM IT ALL AS A SOCIETY. YOU KNOW, BESIDES THE FACT THAT CYBERSECURITY IS PARAMOUNT, AND CYBERCRIME IS HERE TO STAY. HOW DO WE CONTINUE TO EDUCATE THE PUBLIC OF DIGITAL HYGIENE, BOTH AT HOME AND AT WORK? HOW DO WE KEEP OURSELVES MORE AWARE AND SAFER IN THE EVER-INTRUDING SOCIAL MEDIA REALM? BUT MOSTLY, HOW DO WE MOLD THE NEW NORMS OF THE DIGITAL ERA INTO OUR EVERYDAY IN A SAFE AND PRODUCTIVE WAY?

--- END MESSAGE ---

REVIEWING
THE LAST 30
DAYS OF
REPORTED
HACKS

HACKS OF THE MONTH

THE TYLER TECHNOLOGY RANSOMWARE ATTACK



The Tyler Technology Ransomware attack is one of the most important attacks that happened in the past years as Tyler Technologies, Inc. represents the largest provider of software to the United States public sector. At the end of September 2020, the company disclosed the fact that it suffered a ransomware attack with its customers apparently finding suspicious logins and previously unseen remote access tools on their networks. The Tyler Technologies ransomware attack happened on September 23 when the threat actors breached the network of the company and managed to deploy the malware. Very soon after the intrusion, Tyler turned its website into an information portal for news about the attack. The company did not disclose who was behind the attack but, reports circulating online believe that the company was infected with the RansomExx ransomware.



BLACK KINGDOM RANSOMWARE

The use of a ransomware family dubbed Black Kingdom in a campaign that exploited the CVE-2021-27065 Microsoft Exchange vulnerability known as ProxyLogon was publicly reported at the end of March. The ransomware can be executed without parameters and will start to encrypt the system, it is possible to run Black Kingdom with a number value, which it will interpret as the number of seconds to wait before starting encryption. Black Kingdom will encrypt a single file if it is passed as a parameter with the key to encrypt it. If the system has been infected by Black Kingdom twice, files in the system will be encrypted twice, too, which may prevent recovery with a valid encryption key. All Black Kingdom notes contain the same Bitcoin address; sets it apart from other ransomware families, which provide a unique address to each victim. After decompiling the Python code, the code base for Black Kingdom has its origins in an open-source ransomware builder available on Github.

**REVIEWING
THE LAST 30
DAYS OF
REPORTED
HACKS**

HACKS OF THE MONTH

NEW MALWARE TARGETS GOVERNMENTS IN THE MIDDLE EAST



Proofpoint researchers identified a malware called LastConn distributed by TA402, a threat actor also known as Molerats. The malware targeted government institutions in the Middle East and global government organizations associated with geopolitics in the region. TA402 is a Middle Eastern advanced persistent threat group that often targets entities in Israel and Palestine, in addition to other regions in the Middle East. Researchers assess with high confidence that LastConn is an updated version of the SharpStage malware that was first reported by Cybereason in December 2020. TA402 has been active since at least 2011 and is believed to be operating out of the Middle East. TA402 is a highly effective and capable threat actor that remains a serious threat, especially to entities operating in and working with government or other geopolitical entities in the Middle East.



TEN-YEAR HACTIVIST FUGITIVE COMMANDER X ARRESTED IN MEXICO

A decade after Chris "Commander X" Doyon skipped out on a federal hacking charge and fled the country, the long arm of US law enforcement stretched out its hand and plucked him from Mexico City, where he had claimed political asylum. Doyon now faces the original charges for coordinating a 2010 DDoS attack, plus a serious new charge for jumping bail. Strangely, the US government seemed to accept some version of this story—that is, that Doyon was someone worth tracking down, at great expense, rather than an extremely minor miscreant who spent seven years in Toronto begging for money on the street, eating at McDonald's, and hanging out on Twitter, before trekking down to Mexico and claiming asylum there. In any event, Doyon is back in California and has already had two brief hearings, over Zoom, before a federal judge. His pro bono attorney from a decade back, Jay Leiderman, has agreed to represent Doyon once more.



HEALTHCARE DEVICE SECURITY FIRM COO CHARGED WITH HACKING MEDICAL CENTER

A shocking indictment unsealed this week by the Justice Department reveals a security vendor executive has been indicted for hacking into a Georgia medical center - allegedly disrupting telecommunications and network printer services as well as breaking into a computer to steal information for both "Commercial" and private financial gain. Vikas Singla, 45, whose company was not named by DoJ but was described as a metro-Atlanta network security company serving the healthcare industry, has been charged with 17 counts of intentional damage to a protected computer plus one count of taking information from a protected computer. On Sept. 27, 2018, Singla and others allegedly conducted an attack that involved transmitting a "Program, information, code, and command" that ultimately disrupted and damaged Gwinnett's computers that run the phone system at one of its hospitals, as well as systems that run its network of printers for its hospitals. Neither the DoJ nor the grand jury indictment specify details or the form of the attacks, so it's unclear how it unfolded. "Criminal disruptions of hospital computer networks can have tragic consequences," said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division. "The department is committed to holding accountable those who endanger the lives of patients by damaging computers that are essential in the operation of our healthcare system." "This cyberattack on a hospital not only could have had disastrous consequences, but patient's personal information was also compromised," said Chris Hacker, Special Agent in Charge of FBI.



MEATPACKER JBS PAID EQUIVALENT OF \$11 MILLION IN RANSOMWARE ATTACK

Meatpacker JBS USA paid a ransom equivalent to \$11 million following a cyberattack that disrupted its North American and Australian operations, the company's CEO said in a statement. The subsidiary of Brazilian firm JBS SA halted cattle slaughtering at all of its U.S. plants for a day last week in response to the cyberattack, which threatened to disrupt food supply chains and further inflate already high food prices. The JBS meat plants, producing nearly a quarter of America's beef, recovered faster than some meat buyers and analysts expected. The Brazilian meatpacker's arm in the United States and Pilgrims Pride Corp, a U.S. chicken company mostly owned by JBS, lost less than one day's worth of food production. Third parties are carrying out forensic investigations and no final determinations have been made.



HOW COULD THE FBI RECOVER BTC FROM COLONIAL'S RANSOMWARE PAYMENT?

Even though law enforcement groups around the world urge ransomware victims not to pay up, Colonial apparently decided to hand over what was then \$4.4 million in bitcoins anyway. Sadly, the value of Bitcoin has taken a tumble since last month, so even though 85% of the bitcoins involved in the blackmail payment were recovered, they're now worth about 50% of what they cost when Colonial purchased them to do its deal with the criminals. Every Bitcoin payment ends up in someone's Bitcoin wallet, and every wallet has a private key by means of which the contents of that wallet can be spent, i.e., transferred onwards to someone else's Bitcoin wallet. That, simplified yet further, is very loosely how BTC transactions work: your Bitcoin wallet address, derived from your public key, can be used by anyone to "Lock away" funds so that they "Belong" to you. If the FBI were able to get hold of the private key of the Bitcoin wallet or wallets where Colonial's ransom payment ended up, then it could simply transfer those funds to itself, whether it knew who owned those wallets or not. As alleged in the supporting affidavit, by reviewing the Bitcoin public ledger, law enforcement was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI has the "Private key," or the rough equivalent of a password needed to access assets accessible from the specific Bitcoin address.



COLONIAL PIPELINE REPORTEDLY PAID MILLIONS FOR SLOW DECRYPTION SOFTWARE

Colonial Pipeline, which operates more than 5,500 miles of fuel pipelines in the United States, found out the hard way that paying the ransomware authors is not always the best policy. The decryption software provided by the hacking group DarkSide, notes Bloomberg, was reportedly "So slow" that Colonial Pipeline "Continued using its own backups to help restore the system." Ransomware is malware that encrypts victims' computers and demands payment in exchange for the decryption key. Bloomberg reports that Colonial Pipeline paid the almost \$5 million ransom - in other words, almost immediately after it says it detected the infection. Nicole Perloth, a noted cybersecurity reporter for the New York Times, confirmed that the payment was 75 bitcoin - nearly \$5 million, to recover stolen data. A few days following the attack, Colonial Pipeline announced that its systems were back up and running - with very little thanks, it would seem, to that payment of 75 bitcoin.

HOW THE FBI CONDUCTED THE MOST SOPHISTICATED GLOBAL STING OP**NEWS REVIEW
AND
ANALYSIS BY
OKTETT****HOW IT STARTED:**

According to [unsealed court documents](#), in 2017, [San Diego FBI field agents](#) started to investigate an organization called Phantom Secure, which they believed to have been selling “hardened encrypted devices” solely to transnational criminal organizations (TCOs). These devices allowed for an assortment of services that ensured hindrance to any law enforcement legal surveillance over any criminal conduct carried out using such devices due to its encryption capabilities. At the closing of this investigation, it was clear that the reach of Phantom Secure was global and used by a variety of international criminal syndicates. In 2018, Southern District of California procured an indictment against the CEO of Phantom Secure company, Vincent Ramos. Consequently, shutting down the service and creating a void in the encrypted communications market share.

Following the unraveling of Phantom Secure, FBI recruited an unnamed informant who was “developing the ‘next generation’ encrypted communications product”, according to the search warrant affidavit provided by the agency. In exchange for a reduced sentence, the Confidential Human Source (CHS), offered his new device, Anom, to the FBI and agreed to distribute it to his already established criminal network (specifically TCOs). Because such intricate business relied heavily on trust and reputation, this was vital for FBI to insert these devices, organically, into the hands of as many TCOs as possible without suspicion. This was the start of the covert surveillance operation dubbed Operation Trojan Shield, which eventually involved 16 international partners, including Australian Federal Police (AFP).

HOW IT WORKED:

For the agencies to be able to conduct surveillance, FBI, AFP, and CHS had to create a master key that could be integrated into the existing encryption system, which affixed to the messages being transmitted. This would allow the agents to decrypt and store this information on their own servers, enabling them to see the

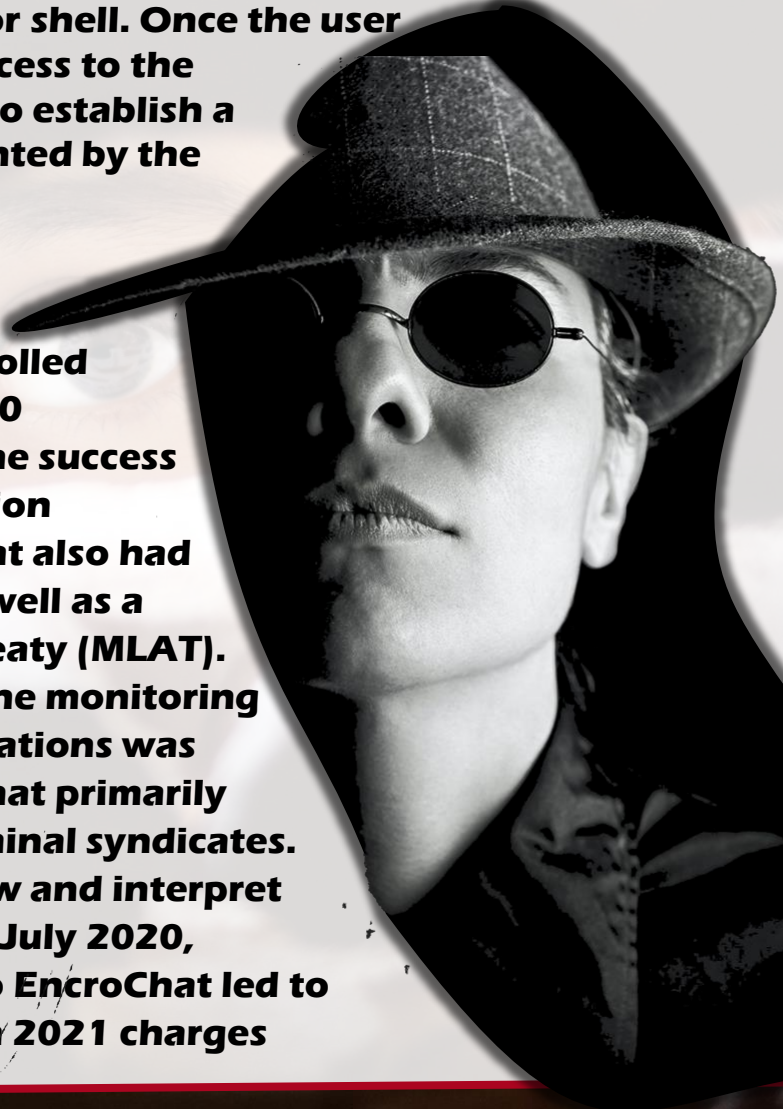
HOW THE FBI CONDUCTED THE MOST SOPHISTICATED GLOBAL STING OP

NEWS REVIEW
AND
ANALYSIS BY
OKTETT

exchanges live and in the clear. When a message was generated by a device outside of the U.S. territory, an encrypted blind copy was generated and sent to an “iBot” server, also outside of the U.S. This is where it would get “decrypted from the CHS’s encryption code and then immediately re-encrypted with FBI encryption code.” It would then get routed to another FBI iBot server and get decrypted for the first time to be viewed by the agents apart of surveillance. This app relied on being uploaded to a stripped Google Pixel phone that was void of the ability to send email or make calls. Its sole purpose was to host the Anom app that was disguised within a calculator shell. Once the user entered a PIN, it allowed access to the services. The user would also establish a Jabber ID which was appointed by the CHS or Anom Admin.

THE OUTCOME:

Australian’s surveillance operation named Ironside rolled out a beta round of about 50 distributed devices. Once the success was evident, the investigation involved a third country that also had to obtain an iBot server as well as a Mutual Legal Assistance Treaty (MLAT). For approximately a year, the monitoring of the encrypted communications was mostly conducted by AFP that primarily consisted of Australian criminal syndicates. In 2019, FBI began to review and interpret the received server data. In July 2020, Europol’s investigation into EncroChat led to its dismantlement. In March 2021 charges



3/3

HOW THE FBI CONDUCTED THE MOST SOPHISTICATED GLOBAL STING OP**NEWS REVIEW
AND
ANALYSIS BY
OKTETT**

against Canadian's CEO of Skylight Global saw yet another encrypted communication platform shut down. This all led to an increased demand for Anom, ultimately resulting in 28 million messages from close to 12,000 devices that were dispersed throughout over 100 countries. According to the court documents, "top five countries where Anom devices are currently used are Germany, the Netherlands, Spain, Australia, and Serbia. The legal inquiry found that Anom devices-initiated government-level corruptions in multiple countries, international drug trafficking, money laundering, obstruction to justice, hire for murder plots, organized crime families, and firearm sales. Once the investigation was made public, the global operation saw over 800 arrests, seizure of varied drugs, currencies, luxury vehicles and homes, and clandestine drug labs. While this operation was made public, many of its dealings are still ongoing.



**BREAKDOWN ANALYSIS OF:
VAN BUREN V. UNITED STATES****THE
CONFUSING
LEGAL
LANDSCAPE
EXPLAINED**

The Supreme Court last month decided a very significant case interpreting the scope and application of the Computer Fraud and Abuse Act (CFAA). As with virtually all Supreme Court cases, reaction to the decision has been mixed. What everyone does agree on, however, is that it is an important case that will limit the ability of the Justice Department to use CFAA to prosecute cases under a trespass theory. The case will also affect how government agencies and private employers craft their authorizations allowing employees / contractors to use work-related computers. If this sounds interesting to you, be sure to register for CYBV 329 (Cyber Ethics, Law, and Policy), where students will have the opportunity to deep dive into the Van Buren case and other cases covering cyber. Be sure to ask your advisor about the Law and Policy track in our department.

ISSUE:

Did the defendant (a police officer) violate CFAA's provision which makes it illegal "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter" when he ran a license-plate search in a law enforcement computer database in exchange for money?

ANALYSIS:

The Supreme Court found that the defendant did not violate CFAA because the defendant, while having improper motives for obtaining the information, otherwise had access to the information. The court noted that CFAA does cover the situation where an individual obtains information from particular areas in the computer - such as files, folders, and databases - to which his/her computer access does not extend. The court found that because the defendant here had access to the information (but used it for an improper purpose), CFAA was not violated.

**BREAKDOWN ANALYSIS OF:
VAN BUREN V. UNITED STATES****THE
CONFUSING
LEGAL
LANDSCAPE
EXPLAINED****FACTS:**

The defendant, Van Buren, was a police sergeant in Georgia. In the course of his duties as a police officer, Van Buren befriended a man, Andrew Albo, known by the department to be "very volatile". Van Buren eventually asked Albo for a personal loan. Albo secretly recorded that request, and took the recording to the local sheriff's office, complaining that Van Buren was shaking him down for cash. The recording made its way to the FBI, which devised a sting operation, whereby Albo would ask Van Buren to run a license plate search on the state law enforcement computer database for a woman Albo had met at a local strip club. In return for the search, Albo would pay Van Buren \$5,000. The sting was carried out, and Van Buren conducted the search, using the law enforcement database with his valid credentials. The United States charged Van Buren with violation of 18 USC Section 1030 (a)(2) (CFAA), alleging that Van Buren violated the "exceeds authorized access" clause of CFAA when he ran the license plate. Van Buren had been trained not to use the law enforcement database for "an improper purpose" defined as "any personal use." The government alleged that Van Buren therefore knew the search breached department policy, and that the violation of department policy also violated CFAA.

PROCEDURAL POSTURE:

Defendant Van Buren was convicted by a jury at the District Court and was sentenced to 18 months in prison. Van Buren appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to those individuals who obtain information to which his / her computer access does not extend, not to those who misuse access they otherwise have. Consistent with Eleventh Circuit Precedent, the Eleventh Circuit Court of Appeals panel held that Van Buren had violated CFAA. The majority opinion was written by Barrett, with Breyer, Sotomayor, Kagan, Gorsuch, and Kavanaugh joining.

LEGAL ANALYSIS

BREAKDOWN ANALYSIS OF: VAN BUREN V. UNITED STATES

THE
CONFUSING
LEGAL
LANDSCAPE
EXPLAINED

SUPREME COURT OPINION:

The majority reversed the Eleventh Circuit's decision, rejecting the broader interpretation of the CFAA. The Court construed the text of the CFAA provisions to create a "gates-up-or-down inquiry" – (1) whether one can or cannot access a computer system and (2) whether one can or cannot access certain areas within that system. The second-part of the inquiry is limited to the question of whether the accessor had authorization to access that information in any circumstance or not. In light of that analysis, the majority makes clear that the CFAA provision criminalizes only those who obtain information from particular areas in the computer, such as files, folders, or databases, to which their computer access does not extend. It does not criminalize those who have improper motives for obtaining information that is otherwise available to them. If a person has access to information stored in Folder Y of a computer from which the person could permissibly pull information, then they do not violate the CFAA by obtaining such information, regardless of whether they pulled the information for an improper motive. However, if the information is instead located in prohibited Folder X, to which the person lacks access, they violate the CFAA by obtaining information from Folder X.

The Government's reading would criminalize every violation of a computer-use policy and terms of service from an online source. Millions of otherwise law-abiding citizens would be criminals. For example, an employee who sends a personal e-mail or visits a non-work-related website, such as a news website, using their work computer would have violated the CFAA.

Therefore, under Van Buren, it would be irrelevant, in obtaining information, whether a person exceeded their scope of access assigned to them so long as they accessed the computer with valid credentials and obtained the information in a computer area which their access allowed them. As a result of the decision, Congress may propose new legislation or elect to redraft the CFAA.

LEGAL ANALYSIS

**BREAKDOWN ANALYSIS OF:
VAN BUREN V. UNITED STATES****THE
CONFUSING
LEGAL
LANDSCAPE
EXPLAINED**

Government agencies and employers may decide to establish clearer restrictions and regulations on computer use and access. Regardless of the Van Buren decision, Van Buren's conduct and other similar conduct may still constitute a violation of other federal and state statutes or a breach of existing computer use, and access policies already exercised by an employer, service provider, institution, etc. The Van Buren decision does not create a free pass so that one can partake in improper or fraudulent conduct with information obtained through valid access or credentials.

The Supreme Court case report can be found [here](#).

ELECTRONIC FRONTIER FOUNDATION OPINION:

The Court's decision was limited in one important respect. In a footnote, the Court left as an open question if the enforceable access restriction meant only "technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies," meaning that the opinion neither adopted nor rejected either path. EFF has argued in courts and legislative reform efforts for many years that it's not a computer hacking crime without hacking through a technological defense. This footnote is a bit odd, as the bulk of the majority opinion seems to point toward the law requiring someone to defeat technological limitations on access and throwing shade at criminalizing TOS violations. In most cases, the scope of your access once on a computer is defined by technology, such as an access control list or a requirement to reenter a password. Professor Orin Kerr suggested that this may have been a necessary limitation to build the six-justice majority. Later in the Van Buren opinion, the Court rejected a Government argument that a rule against "using a confidential database for a non-law-enforcement purpose" should be treated as a criminally enforceable access restriction, different from "using information from the database for a non-law-enforcement purpose" .

LEGAL ANALYSIS

CYBV-474 Advanced Analytics for Security Operations

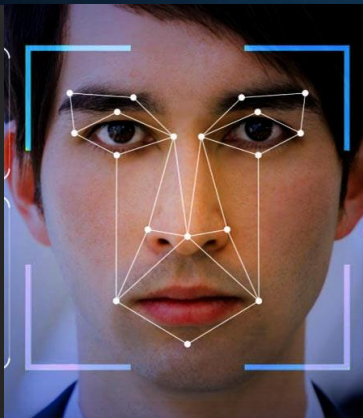
Provides students an in-depth hands-on experience applying Python along with key AI methods (Natural Language Processing, Machine Learning Methods, Expert Decision Making ...) to real-world cybersecurity challenges.



CYBV-475 Cyber Deception

Provides students and in-depth hands-on experience into defensive and offensive cyber deception methods and techniques.

The course investigates the use of fake news, fake images, deep fake video and audio, advanced data hiding methods, covert communications and tagging. Students will learn how to apply decoys, traps and lures in support of active cyber defense.



SUMMER

**SIGN UP FOR
CLASSES
SOON**



**NOTE FROM
YOUR ADVISORS**

FALL 2021 ENROLLMENT IS OPEN. COURSES OFTEN FILL QUICKLY, SO ENROLL EARLY TO GET THE BEST SELECTION! PLEASE TOUCH BASE WITH YOUR ACADEMIC ADVISOR TO VERIFY THE COURSES YOU PLAN ON TAKING ARE IN LINE WITH YOUR DEGREE PLAN. YOU CAN ALSO SCHEDULE AN APPOINTMENT WITH THEM IF YOU NEED ADDITIONAL SUPPORT WITH YOUR SUMMER AND/OR FALL ENROLLMENT. ADVISOR CONTACT INFORMATION CAN BE FOUND HERE:

[HTTPS://AZCAST.ARIZONA.EDU/STUDENT-SERVICES/ADVISING/MEET-YOUR-ADVISOR](https://azcast.arizona.edu/student-services/advising/meet-your-advisor)

FALL SCHEDULE 2021

JULY 2021



THE UNIVERSITY
OF ARIZONA

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

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	BOOK
CYBV 302	LINUX SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 303	WINDOWS SECURITY ESSENTIALS	PENDING BOOK SELECTION
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	BOOK
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	BOOK
CYBV 329	CYBER ETHICS	BOOK
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	BOOK
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	BOOK
CYBV 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 , BOOK 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book 1 , Book 2

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

FALL SCHEDULE 2021

CAT #	COURSE	BOOKS
CYBV 437	DECEPTION & COUNTER-DECEPTION	<u>BOOK</u>
CYBV 450	INFORMATION WARFARE	<u>BOOK 1</u>
CYBV 454	MALWARE THREATS & ANALYSIS	<u>BOOK</u>
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	PENDING BOOK SELECTION
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	<u>BOOK</u>
CYBV 473	VIOLENT PYTHON	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 477	ADVANCED COMPUTER FORENSICS	PENDING BOOK SELECTION
CYBV 479	WIRELESS NETWORKING AND SECURITY	PENDING BOOK SELECTION
CYBV 480	CYBER WARFARE	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION
CYBV 498	CYBER OPERATIONS SENIOR CAPSTONE	PENDING BOOK SELECTION



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

SUMMER

BACK ORIFICE 2000 (BO2K) RELEASED AT DEF CON 7

Cult of the Dead Cow (cDc) member Dildog debuted the program Back Orifice 2000 (BO2k) at DEF CON 7. It was the successor to Back Orifice, released by cDc a year prior. DilDog proclaimed it "a remote administration tool for corporate America". Back Orifice 2000 is a computer program designed for remote system administration. It enables a user to control a computer running the Microsoft Windows operating system from a remote location. The name is a pun on Microsoft BackOffice Server software. Back Orifice and Back Orifice 2000 are widely regarded as malware, tools intended to be used as a combined rootkit and backdoor.

JULY 10, 1999

CODE RED WORM – ODD PRODUCT PLACEMENTS

The Code Red worm exploited an .ida vulnerability in Windows web server IIS. The vulnerability had been addressed via update MS01-033 a month earlier. The worm spread itself using a common type of vulnerability known as a buffer overflow. It did this by using a long string of the repeated letter 'N' to overflow a buffer, allowing the worm to execute arbitrary code and infect the machine with the worm. Kenneth D. Eichman was the first to discover how to block it and was invited to the White House for his discovery. The worm would deface websites with the text "HELLO! Welcome to <http://www.worm.com>! Hacked By Chinese!" added to the website. The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permech when it exploited a vulnerability discovered by Riley Hassell. They named it "Code Red" because Code Red Mountain Dew was what they were drinking at the time. eEye believed that the worm originated in Makati, Philippines, the same origin as the VBS/Loveletter (aka "ILOVEYOU") worm.

JULY 13, 2001

SIRCAM WORM – THE WORM ASKING FOR ADVICE

Sircam was a computer worm that first propagated in 2001 by e-mail in Microsoft Windows systems. It affected computers running Windows 95, 98, and Me. The worm was able to select 8 message subjects but due to an error in the worm, the message was rarely sent in any form other than "I send you this file in order to have your advice." This subsequently became an in-joke among those who were using the Internet at the time and were spammed with e-mails containing this string sent by the worm. Sircam was notable during its outbreak for the way it distributed itself. Document files on the infected computer were chosen at random, infected with the virus and emailed out to email addresses in the host's address book. Opening the infected file resulted in infection of the target computer. During the outbreak, many personal or private files were emailed to people who otherwise should not have received them. It could also spread via open shares on a network. Sircam scanned the network for computers with shared drives and copied itself to a machine with an open (non-password protected) drive or directory. A simple RPC (Remote Procedure Call) was then executed to start the process on the target machine, usually unknown to the owner of the now-compromised computer.

JULY 17, 2001

CYBER SECURITY HISTORY

JULY 2021



**THE UNIVERSITY
OF ARIZONA**

20

USE PYTHON TO HIDE MESSAGES IN WAV AUDIO FILES

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

Steganography is kind of cool to me, it is the art of hiding a message in plain sight. Cybersecurity focuses on encryption and that is fine, but steganography is more of an art to me. Hiding a message in plain sight has very limited business applications but as a hacker, finding new ways to send information fascinates me. You may be familiar with steganography when you hide messages within images.

This practice makes use of the least significant bit (LSB) of the image file to hide the message without disrupting the image file. The idea being that the image file may not get a second look when a forensic investigation is taking place. An image is fine but what about audio files. So today that is what we are going to focus on. For this project we are going to use a modified version of HiddenWave by Techchipnet and provide something with a little more simplicity. Using Python, we will open a WAV file and edit it to include a secret message. We will then use another Python program to open the WAV audio file and extract the hidden message.

As we mentioned earlier, image file steganography utilizes the least significant bit, and we can use the same in audio. The LSB method (Starting on PDF page 662) gives high embedding capacity for data and is relatively easy to implement and to combine with other hiding techniques. Generally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. The Python program we will be making today will utilize the Lowest Bit Coding method which we will go into more detail on the next page.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THIS SERIES IS INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS... IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

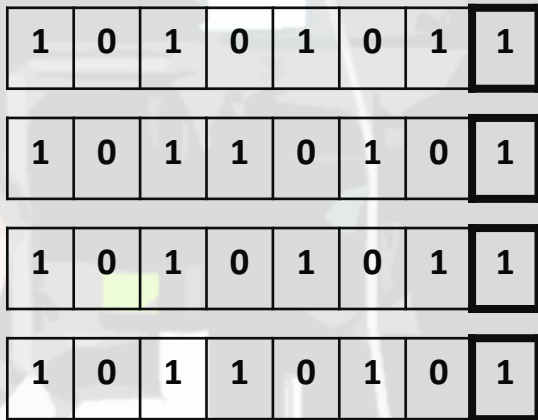
USE PYTHON TO HIDE MESSAGES IN WAV AUDIO FILES

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

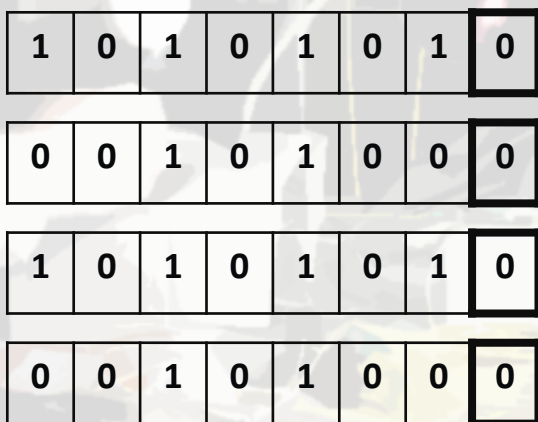
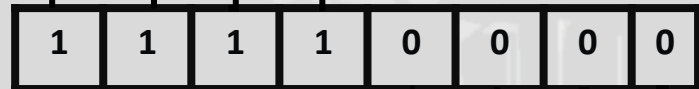
The lowest bit coding is the method that embeds secret data only in the least significant bit (LSB). This method minimizes the transition before and after the audio is embedded. Since the audio data only uses the lowest bit, this method gives embedding capacity up to one eighth or 12.5% of wave file. Below is an example of how the wave data is embedded using the lowest bit method.

express wave data and secret data by binary digits and replace secret data in low bit with the wave data one by one.

AUDIO DATA



SECRET DATA



HACKING POC

USE PYTHON TO HIDE MESSAGES IN WAV AUDIO FILES

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

Now the secret message can be put together from the ends of the other various bytes. This approach has many advantages and disadvantages compared to other steganography approaches. One big disadvantage is that audio steganography is more difficult to utilize compared to visual steganography because your ears are more sensitive than your eyes. So, trying to hide information requires you

to take the source information (The audio file) into consideration before you transmit your message. When considering this issue, maybe you would use an audio source with some already existing background noise or maybe something that is harder to tell what should be normal anyhow.

To begin, we will create an audio file that we will hide our message into. I have created an example that can be [found here](#). To hide data within this file we will break down the Python program which is [found here](#).

The first thing we will need are three imports:

```
import os
import wave
import argparse
```

Next, we want to process the application arguments which will be identified by a, m and o

```
parser = argparse.ArgumentParser()
parser.add_argument('-a', help='(a)udio File', dest='audiofile')
parser.add_argument('-m', help='Secret (m)essage',
dest='secretmsg')
parser.add_argument('-o', help='(o)utput', dest='outputfile')
args = parser.parse_args()
af = args.audiofile
string = args.secretmsg
output = args.outputfile
arged = False
if af and string and output:
    arged = True
```


USE PYTHON TO HIDE MESSAGES IN WAV AUDIO FILES

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

The arguments will be used to tell the program where to look for the audio file (a), What the message is (m) and then where to put the output (o). If all three arguments are provided the program continues as the condition is set to TRUE. Next, we will create our function that we will call `em_audio` and this will take our three arguments and process them.

```
def em_audio(af, string, output):
    if not arged:
        print ("need a, m and o")
        quit("")
    else:
        print ("Please wait...")
        waveaudio = wave.open(af, mode='rb')
        frame_bytes =
bytearray(list(waveaudio.readframes(waveaudio.getnframes()))
        string = string + int((len(frame_bytes)-(len(string)*8*8))/8) *'#'
        bits = list(map(int, ".join([bin(ord(i)).lstrip('0b').rjust(8,'0') for i in
string])))
        for i, bit in enumerate(bits):
            frame_bytes[i] = (frame_bytes[i] & 254) | bit
            frame_modified = bytes(frame_bytes)
        with wave.open(output, 'wb') as fd:
            fd.setparams(waveaudio.getparams())
            fd.writeframes(frame_modified)
        waveaudio.close()
        print ("Complete")
    try:
        em_audio(af, string, output)
    except:
        print ("Please try again")
        quit("")
```

With this function defined we can now try and encode a message into our audio wave file.

USE PYTHON TO HIDE MESSAGES IN WAV AUDIO FILES

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

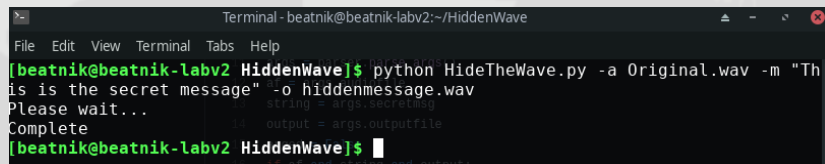
We can add a secret message by modifying the following command:

```
python HideTheWave.py -a Original.wav -m "This is the secret message" -o hiddenmessage.wav
```

This will hopefully add the message "THIS IS THE SECRET MESSAGE" to the audio file. If everything is done correctly then you should get the message Complete in the window.

With this function defined we can now try and encode a message into our audio wave file.

Now we should have a new file created named hiddenmessage.wav.



```
Terminal - beatnik@beatnik-labv2:~/HiddenWave
File Edit View Terminal Tabs Help
[beatnik@beatnik-labv2 HiddenWave]$ python HideTheWave.py -a Original.wav -m "This is the secret message" -o hiddenmessage.wav
Please wait...
Complete
[beatnik@beatnik-labv2 HiddenWave]$
```

Now this filename is not what you would send out but for an example let's compare the original audio file with this new audio file. The original file was 5.6MB and the hidden audio file is also 5.6MB with a difference of 264 bytes and our new audio file being smaller.

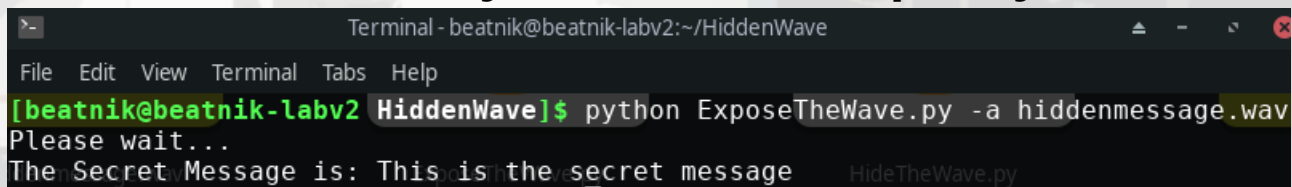
Now to extract our message we will simply reverse the process using the other python program called Exposethewave.py. This will use the command:

```
python ExposeTheWave.py -a hiddenmessage.wav
```

This will reverse the process and will extract the message. Now you can see what text was hidden.

Conclusion:

Take the time and listen to both audio files, you can tell that the original file sounds much clearer and the audio file with the message sounds "dirty" and a little quieter. Now this project can be very easily expanded on, but you can already tell that the concept of hiding messages in audio files is an easy process when you have the tools to do so and now you have one more capability.



```
Terminal - beatnik@beatnik-labv2:~/HiddenWave
File Edit View Terminal Tabs Help
[beatnik@beatnik-labv2 HiddenWave]$ python ExposeTheWave.py -a hiddenmessage.wav
Please wait...
The Secret Message is: This is the secret message
HideTheWave.py
```


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

The industry standard today is to use Virtual Machines (VMs) to run software applications. VMs run applications inside the Operating System, which runs on virtual hardware powered by the server's host OS. Docker however uses containers, and these take a different approach: by leveraging the low-level mechanics of the host operating system, containers provide most of the isolation of virtual machines at a fraction of the computing power.

COMMAND	DESCRIPTION
<code>docker pull APPLICATION</code>	Pull and application image from the Docker registry
<code>docker image ls</code>	List all images that are locally stored with Docker
<code>docker run APPLICATION</code>	Run an image from the local image store
<code>docker ps</code>	Shows you all containers that are currently running
<code>docker run -it APPLICATION</code>	Run a image in interactive mode so you can issue commands while it is running
<code>docker rm CONTAINER_ID</code>	Deletes the docker image by container ID from the ps command
<code>docker container prune</code>	Removes all stopped containers
<code>docker run -p 8888:80 APPLICATION</code>	Runs the container with a defined exposed port
<code>docker port APPLICATION</code>	List ports used by the application that docker has assigned
<code>docker stop APPLICATION</code>	Stop the application



> CYBER PHYSICAL SYSTEMS RESEARCHER

- ≥ INTERNET OF THINGS DEVICES, CRITICAL INFRASTRUCTURE, AND SENSOR AND COMMUNICATION SYSTEMS ALL HAVE ONE THING IN COMMON: THEY INTERFACE THE DIGITAL AND PHYSICAL DOMAINS.
- ≥ THE CYBER-PHYSICAL SYSTEMS GROUP AT MIT LINCOLN LABORATORY CONDUCTS RESEARCH TO UNDERSTAND THE CYBERSECURITY IMPLICATIONS OF THESE PHYSICAL INTERFACES AND USE THE RESULTS OF OUR RESEARCH TO DEVELOP PROTOTYPES THAT SERVE AS PATHFINDERS FOR FUTURE TECHNOLOGICAL SOLUTIONS.
- ≥ THE CYBER PHYSICAL SYSTEMS GROUP TACKLES KEY PROBLEMS IN THE CONVERGENCE OF CYBERSECURITY AND THE PHYSICAL WORLD IN AN INTERDISCIPLINARY RESEARCH AND DEVELOPMENT ENVIRONMENT. WE FOCUS ON DEVELOPING NEW CAPABILITIES IN THE AREAS OF HARDWARE SECURITY AND CYBER-EW FOR THE DOD, INTELLIGENCE COMMUNITY, AND FEDERAL AGENCIES.
- ≥ KEY TECHNOLOGY DEVELOPMENT THRUSTS INCLUDE NOVEL SENSORS, TESTBED DEVELOPMENT AND INTROSPECTION, AND UNCONVENTIONAL METHODS OF SYSTEM EXPLOITATION.
- ≥ WE HAVE POSITIONS OPEN FOR FULL TIME AS WELL AS INTERNSHIP OPPORTUNITIES.



MIT
LINCOLN
LABORATORY



THE UNIVERSITY
OF ARIZONA

JULY 2021

27

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY**JOBS & INTERNSHIPS****COMPUTING RESOURCES NETWORK MANAGER**

The Computing Resources Manager/Network Manager will play a unique role in enabling NSA to effectively execute its mission, supplying customers with advanced computing resources, and global networking. The Computing Resources Manager/Network Manager assists in the planning, designing, managing the configuration, identifying network faults, restoring service after faults occur, and the performance and security of operational networks. Entry is with a Bachelor's degree and no experience. The following may also be considered for individuals with in-depth experience that is clearly related to the position: an Associate's degree plus 2 years of relevant experience; or at least 18 semester hours of military coursework/training in networking, computer science, or cyber topics plus 2 years of relevant experience. Salary Range: \$73,076 - \$91,057

COMPUTER NETWORK ANALYST

Computer Network Analysts are hired into positions directly supporting a technical mission office (either on the offensive or defensive side) or one of a few different development programs like the Intrusion Analyst Skill Development Program (IASDP) and the Cybersecurity Operations Development Program (CSODP) (formerly named the Information Assurance and Cyber Development Program (IACDP)). These development programs are 3 years in length and combine formal training and diverse work assignments that may cross both offensive and defensive missions. Entry is with a Bachelor's degree and no experience. The following may also be considered for individuals with in-depth experience that is clearly related to the position: an Associate's degree plus 2 years of relevant experience; or at least 18 semester hours of military coursework/training in networking, computer science, or cyber topics plus 2 years of relevant experience. Salary Range: \$73,076 - \$91,057

**LEARN
ABOUT
CYBER
SECURITY
AND WORK
IN CYBER
SECURITY**

JOBS & INTERNSHIPS

.NET CORE / ASP.NET CORE SOFTWARE ENGINEER

ellisys

Ellisys is seeking brilliant people, who are highly analytical, capable of thinking “out-of-the-box”, and who are motivated to learn from the best. You will bring a strong programming background to the team, coupled with personal enthusiasm and high energy. Your work will be challenging and diverse, and your creativity and proactive approach will be welcomed. You will be contributing to the world's best and most advanced protocol test solutions for technologies such as USB, Bluetooth and Wi-Fi.

- Strong programming background in C# / .NET Core
- Experience with web frameworks such as ASP.NET Core is a plus
- Experience with .NET Core Entity Framework is a plus
- Experience with databases is a plus
- Knowledge of Bluetooth, Wi-Fi or other wireless communication protocols is a plus
- Must be analytical, creative and a good communicator
- Strong team player
- Fluent in English - other languages a plus

FIELD APPLICATION ENGINEER

ellisys

Ellisys is seeking a Field Application Engineer (FAE) with a background in wired and wireless communications technologies, experience in protocol test & measurement tools, and an ability to work closely with customers to expeditiously understand and solve complex technical issues. Our customers include the world's largest technology companies as well as smaller developers, working across a variety of markets and product categories, including silicon developers, makers of consumer electronics, wireless radio manufacturers, IP providers, test labs, government agencies, automotive companies, and more.

- Test verification or validation, or qualification testing
- Knowledge of protocol test solutions and use cases
- Knowledge of USB, Bluetooth, and/or Wi-Fi protocols
- Excellent verbal and written communications skills

CYBERSECURITY AND CRITICAL INFRASTRUCTURE A HISTORIC FOOTNOTE

IMPACTS AND ANALYSIS REPORT OF CYBER ATTACKS

Well to say the least, in these past few months and especially the past few weeks, we have seen the attacks on the US critical infrastructure explode.

HISTORICAL BACKGROUND:

Attacks against critical infrastructure is neither new nor restricted to attacks on the United States. The very first “cyber” attack has been tagged to a British Magician, Nevil Maskelyne, in 1903! Guglielmo Marconi was holding the first public demonstration of his long-distance wireless “secure communications”, in the United Kingdom over a 300-mile distance. Mr. Maskelyne wanted to disprove Marconi’s claim that the wireless telegraph could send messages securely, so he hijacked the demonstration and instead sent the following message:

Rats, rats, rats, rats.

**There was a young fellow of Italy,
Who diddled the public quite prettily.**

Mr. Maskelyne within a few days went public about his role in the “hacking” and that he wanted to revel the security hole presented by Marconi’s technology. It is for this very reason that some also consider his public admission to be the first publicly reported vulnerability in modern technology. The next instance of attacks on critical infrastructure comes out of the Cold War. This specific attack has been partially confirmed, so do remember that it is never been admitted.

In 1982, President Reagan approved the manipulation of various devices, chips, software, etc. that the Soviets were stealing from various companies in blatant acts of corporate espionage. There was a software package that was targeted by the Soviets for stealing, that controlled gas supply systems, such as turbines, pumps, valves, etc. The US altered the software before it was stolen by the KGB, to produce pressures that were far beyond the safe limits of pipeline joints and welds. The result of this software being used by the Soviets was a massive non-nuclear explosion and fire that was picked up via satellites, and even resulted in NORAD identifying the incident as a possible missile launch.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

IMPACTS AND ANALYSIS REPORT OF CYBER ATTACKS

Finally, the most severe incident that brought these types of attacks into sharp focus was the creation and deployment of the Stuxnet malware. Stuxnet was written and specifically aimed at the Iranian Natanz uranium facility in 2010. The goal of Stuxnet was to slow the progress of the Iranian effort to refine uranium for the possible use in nuclear weapons. After the malware made it inside of an industrial network, it used four unpatched

Microsoft vulnerabilities in combination with stolen digital signing certificates from two legitimate Taiwanese companies and multiple rootkits effecting both Windows and Siemens PLCs. No country has officially claimed responsibility for this attack, but to say the threat actor was well funded would be a given.

START OF RANSOMWARE:

Now that we have an idea of the history of cyberattacks, we need to start looking at the latest spate of attacks. Until the past few years, the overall goal of these cyberattacks was the destruction of computer hardware and other industrial equipment. However, this has shifted more toward what we are seeing with these recent events, instead of causing damage, you simply encrypt the data on these systems and demand money for the encryption key. This type of approach is something we are talking about a lot more in your courses, ransomware. Ransomware was first identified in 1989 when an AIDS researcher, Joseph Popp, distributed 20,000 floppy disks to AIDS researchers across the world, that eventually after 90 computer bootups, demanded \$567 to unlock the virus and license the software to keep it unlocked. Dr. Popp never went to trial as he "went insane" according to his lawyer.

The Ransomware that all of us are used to came into play around 2005. But these early ransomware attempts all suffered the same problems that Dr. Popp faced, there was no easy way to anonymously receive funds from the victims of your ransomware. That was until late 2012, when Bitcoin started to become a legitimate and acceptable form of monetary payment.

ANALYSIS

CYBERSECURITY AND CRITICAL INFRASTRUCTURE**IMPACTS AND ANALYSIS REPORT OF CYBER ATTACKS**

In 2013, we saw the birth of one of the first true Ransomwares as we know them today, CryptoLocker. It is this ransomware and its many clones that started us down the road of having files and data held hostage unless we paid a price in Bitcoins.

RECENT ACTIVITIES:

This brings us to the past few months, and the worrisome trend of ransomware attacking critical infrastructure.

Critical Infrastructures are what make our modern life possible, from the minute we get out of bed till the moment we go back to sleep, we are making use of dozens if not hundreds of these systems to take a shower (water, gas, and electric) to going to work (electric, transportation systems, and communications). Prior to Stuxnet, most hackers stayed away from these sectors, because of the underlying technology used by these systems, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA). ICS and SCADA are programmed using specific coding languages and on very specific hardware that in most cases does not even have an Operating System, like Windows or Linux. But after Stuxnet, hackers realized that there was a lot of money to be made from these systems.

The first incident we are going to look at briefly is the Oldsmar Water Treatment Plant in Florida. This is one of the few recent cases that did not make use of ransomware, but it is key in understanding the seeming redirection of hackers toward the United States and its critical infrastructure. In early February, a hacker gained access to the Industrial Control System of the water treatment plant and increased the lye used in the treatment process from 100 parts per million to 11,100 parts per million. Thankfully, before this change could cause serious health issues, an operator detected the change and modified it back to the correct setting. However, it is the way that the hacker got into the system that is troubling.

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

IMPACTS AND ANALYSIS REPORT OF CYBER ATTACKS

In this facility all the computers used by plant personnel were connected directly to the SCADA system and made use of a 32-bit version of Windows 7 running TeamViewer with the same exact credentials and with no identifiable firewall between the physical plant network and the Internet. It is that last sentence that is the problem and the reason why we are seeing so many attacks coming at these systems, companies are getting lazy or just ignoring security standards, by linking their Operational Technology (OT) networks with their Information Technology (IT) networks. This seemingly innocent link between the networks is serving to give hackers the access that they need to jump from say a receptionist's computer to the computer controlling the chemical mixture for water treatment.

POLITICAL CONCERNS:

So, where are most of these attacks against the United States' critical infrastructure coming from, well one only must look to a few well-known countries that harbor, encourage, and even pay and employ these hackers, Russia, China, North Korea, and Iran. All these countries, have various reasons for their attacks against the US, from political to monetary concerns and even political or religious ideology. The recent Colonial Pipeline incident is believed by the FBI to be the work of Darkside, a hacker group based out of Russia and believed to be backed, off the record of course, by Russia. The Colonial Pipeline ransomware attack caused the 5,500-mile oil pipeline to be shut down for days, leading to gas shortages in parts of the US and even significantly higher prices for the gas that was available. This pipeline supplies almost 50% of the gasoline and jet fuel utilized by 50 million people of the East Coast. Darkside knew this and they set the ransomware at a hefty \$4.4 million dollar ransom.

JBS, one of America's biggest meat processors, is believe by the FBI to be the work of REvil, another hacker group based out of Russia and believed to be backed, off the record of course, by Russia. JBS accounts for the production and processing of one-fifth of the US beef production.

**CYBERSECURITY AND CRITICAL
INFRASTRUCTURE****IMPACTS AND
ANALYSIS
REPORT OF
CYBER
ATTACKS**

Ultimately, JBS had to pay \$11 million dollars to REvil. Unfortunately, that is not the highest ransomware amount paid by a US critical infrastructure company. That honor goes to CAN Financial, the seventh largest commercial insurer in the US, who paid an estimated \$40 million dollars to a group of attackers, who it is believed are attached to the Russian-backed Evil Corp syndicate.

CONCLUSION:

The United States has increased the pressure on the Russian government and its leader, President Vladimir Putin, to put a stop to these types of attacks, regardless of whether they are or are not backed by the Russian government. On June 16th, President Biden in his first meeting with Putin, since taking office, promised that unless these attacks against critical infrastructure do not slowdown and even stop, that America will respond with their own cyber capabilities against Russia.

Only time will tell, whether the Russians will start to work on lessening these attacks, but if the past is any example of Putin's response the future does not look very promising on that front.

**Dr. Harry R. Cooper
Adjunct Instructor
Cyber Operations**

DEPLOY CONTAINERS USING A SIMPLE INTERFACE - PORTAINER

GET UP AND RUNNING TODAY TO START SOMETHING NEW

In our Tips and Tricks section I go over some simple docker commands to help you get started with containers. If you want to hop on the Docker train however there are many tools you can use to make your experience even better and much easier to make use of the power that is containers. The command line can be a little confusing at times but a service like Portainer is here to solve these issues.

By default, Portainer will expose the UI over the port 9000 and expose a TCP tunnel server over the port 8000. We are going to focus on creating Portainer on a Windows environment. To run Portainer in a Windows Server/Desktop Environment, you need to create exceptions in the firewall. These, can be easily added through PowerShell, running the following commands:

```
netsh advfirewall firewall add rule name="cluster_management" dir=in action=allow protocol=TCP localport=2377
```

```
netsh advfirewall firewall add rule name="node_communication_tcp" dir=in action=allow protocol=TCP localport=7946
```

```
netsh advfirewall firewall add rule name="node_communication_udp" dir=in action=allow protocol=UDP localport=7946
```

```
netsh advfirewall firewall add rule name="overlay_network" dir=in action=allow protocol=UDP localport=4789
```

```
netsh advfirewall firewall add rule name="swarm_dns_tcp" dir=in action=allow protocol=TCP localport=53
```

```
netsh advfirewall firewall add rule name="swarm_dns_udp" dir=in action=allow protocol=UDP localport=53
```


DEPLOY CONTAINERS USING A SIMPLE INTERFACE - PORTAINER

GET UP AND RUNNING TODAY TO START SOMETHING NEW

You also need to install Windows Container Host Service and Install Docker. Run the following commands in PowerShell:

```
Enable-WindowsOptionalFeature -Online -FeatureName containers -All
```

```
Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
```

```
Install-Package -Name docker -ProviderName DockerMsftProvider
```

Lastly, you need to restart your Windows Server. After it has restarted, you're ready to deploy Portainer.

Within PowerShell run the following commands:

```
docker volume create portainer_data
```

```
docker run -d -p 9000:9000 --name portainer --restart always -v \\.\pipe\docker_engine:\\.\pipe\docker_engine -v portainer_data:C:\data portainer/portainer-ce
```

Now, you can navigate to <http://localhost:9000> or the IP of the server and start using Portainer. For Linux environments you will just need to run the following commands:

```
docker volume create portainer_data
```

```
docker run -d -p 8000:8000 -p 9000:9000 --name=portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce
```

You are now good to go, enjoy the world of containers!

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE AN AMAZING 4th OF JULY CELEBRATION
>. ---END TRANSMISSION---

THANK YOU

CONTACT US

CIO@EMAIL.ARIZONA.EDU

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

Phone: 520-458-8278 ext 2155

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