

THE PACKET

NOVEMBER 2021



IN THIS ISSUE

HACKS OF THE MONTH	3
CYBER NEWS UPDATES	7
CYBERSECURITY HISTORY	12
HACKING "POC"	14
JOBS & INTERNSHIPS	17



A MESSAGE
FROM
PROFESSOR
MICHAEL
GALDE

LETTER FROM THE EDITOR

--- BEGIN MESSAGE ---

Welcome to the NOVEMBER issue of "THE PACKET" produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and I would like to start off by congratulating the 8 newest members of Saguaro Pod, each member had to solve a series of challenges during our October tap month and will now work together on a research project to advance the understanding of Cyber Security. This will be revealed over the next few months as the club's research program is being put into place. Now that we are in the month of November, the dust from October is beginning to settle and we have come to learn that Twitch.tv ended up getting hacked and so much internal information became released which included internal source code and content creator payouts. The number of failures that are needed for that type of information to be released is crazy and I am going to be writing about this soon; the "PrintNightmare" attack keeps getting worse and worse as new exploits are being developed to take advantage of this avenue and the patches have so far been ineffective in remove this type of attack. Both are still developing stories and are not small and minor on their own. Oh, and let's not forget that Facebook had all its properties -- to include Oculus, Instagram, and WhatsApp -- off the internet for a day due to a major networking error. I hope November is a little more slow and less active, but I doubt we will get that lucky.

--- END MESSAGE ---

ACER CONFIRMS BREACH OF AFTER-SALES SERVICE SYSTEMS IN INDIA



Taiwanese computer giant Acer has confirmed that its after-sales service systems in India were recently breached in what the company called an isolated attack. Upon detection, we immediately initiated our security protocols and conducted a full scan of our systems. "We are notifying all potentially affected customers in India", an Acer Corporate Communications spokesperson told Bleeping Computer. While Acer didn't provide details regarding the attackers' identity behind this incident, a threat actor has already claimed the attack on a popular hacker forum, saying that they stole more than 60GB of files and databases from Acer's servers. The allegedly stolen data includes client, corporate, and financial data and login details belonging to Acer retailers and distributors from India. As proof, the threat actor provided a video showcasing the stolen files and databases, the records of 10,000 customers, and stolen credentials for 3,000 Indian Acer distributors and retailers. To additional requests for more details, Acer replied by saying that "There is an ongoing investigation and for the sake of security, we are unable to comment on details." Acer is a Taiwanese multinational specialized in hardware and electronics and the world's sixth-largest PC vendor by unit sales, according to Gartner.



NEW "YANLUOWANG" RANSOMWARE VARIANT DISCOVERED

Security researchers are warning of a newly-discovered ransomware variant currently being used in targeted attacks. Yanluowang extension adds to encrypted files; the new ransomware was discovered by Symantec during its investigation into an attack against an unnamed large organization. Before Yanluowang is downloaded, an additional tool creates a .txt file with the number of remote machines to check in the command line and uses WMI to get a list of processes running on these machines. The note purportedly warns victims not to contact the police or any specialized ransomware negotiation firms. "If the attackers' rules are broken the ransomware operators say they will conduct distributed denial of service attacks against the victim, as well as make 'calls to employees and business partners.' The criminals also threaten to repeat the attack 'in a few weeks and delete the victim's data," Symantec revealed in a blog post. While the Yanluowang ransomware appears to be still under development it should by no means be underestimated. Targeted ransomware is one of the biggest cyber-threats faced by organizations today and, as such, all new ransomware threats should be taken equally seriously. The volume of ransomware attacks surged by 288% between the first and second quarters of 2021, according to the most recent data from the NCC Group.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

VISIBLE CONFIRMS ITS CUSTOMER ACCOUNTS HAVE BEEN COMPROMISED



Visible is aware of an issue in which some member accounts were accessed and/or charged without their authorization. As soon as we were made aware of the issue, we immediately initiated a review and started deploying tools to mitigate the issue and enable additional controls to further protect our customers. Our investigation indicates that threat actors were able to access username/passwords from outside sources and exploit that information to log in to Visible accounts. Protecting customer information - including securing customer accounts - is critically important to our company and our customers. As a reminder, our company will never call and ask for your password, secret questions, or account PINs. If you feel your account has been compromised, please reach out to us via chat at visible.com. As XDA Developers reports, yesterday Visible subscribers started reporting large charges to their account for a new phone they didn't order shipping to an unknown address. It looks as though the compromise has happened at Visible rather than individual customers due to how many reports are coming in combined with the fact some users were using random, unique passwords to protect their Visible login. There's currently no word from Visible regarding a possible breach, and the carrier's customer support is proving to be quite poor and very laid back about the concern this is causing its customers. PCMAG reached out to Visible asking for clarification on exactly what's happened and will update when Visible responds and explains the situation.



REvil ACCOUNTS FOR WAY TOO MANY RANSOMWARE ATTACKS

Threat actors don't seem to take a break, especially ransomware operators. Ransomware has evolved to become a massive threat to any business. The Advanced Threat Research Report: October 2021 by McAfee found that REvil accounted for 73% of all attacks in Q2 2021. What did the report find? In Q2, the government sector was the most impacted by ransomware attacks, followed by telecom, energy, and media & communications sectors. Cloud threat campaigns drastically affected the financial services sector in the last quarter. In Q2, Android threats such as adware, banking malware, and spyware observed massive growth. Not only ransomware, but other threats are growing too. Following experienced cyber practices and employing relevant technologies can keep organizations safe from these cyber threats.

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

HACKS OF THE MONTH

CHASE BANK HEAVILY TARGETED VIA XBALTI PHISHING KIT



During the three months from mid-May to mid-August 2021, researchers detected a 300% increase in phishing URLs within their telemetry targeting Chase Bank. During this period, researchers from Cyren, a cloud-based threat intelligence and SaaS company - detected a notable increase in phishing kits designed to mimic the Chase banking portal. Of all the phishing kits collected by Cyren over the last six months, Chase is a close second to only Office 365, and well ahead of Microsoft and PayPal. Phishing kits can be purchased from the internet and used by anyone. Typically, they provide the phishing URL complete with the code necessary to steal the victim's details, leaving the buyer to compose and send the phishing email. Ready-made phishing messages can also be purchased, and email addresses of actual or potential Chase customers can be bought separately. "Many of the phishing kits analyzed since May 2021 are highly sophisticated and built to harvest more than just the victim's email address and password," said the researchers in their report. The purpose, as with all phishing, is to lure the target into clicking a link that will lead to the phishing URL. In an XBALTI example analyzed by Cyren, the malicious link leads to a page looking very similar to the genuine Chase site but hosted on a compromised Brazilian website. As each form is completed, XBALTI emails the details to the attacker, using an email address configured within the phishing kit, in the file email. The phishing kit provider can collect multiple details comprising all the stolen data from all the phishers using the kit across multiple phishing sites.



STATE-SPONSORED IRANIAN HACKERS UPLOADED FAKE VPN APP TO PLAY STORE

The espionage group APT35, also known as Charming Kitten, last year successfully uploaded to Google's Play Store an app that masqueraded as a virtual private network service, claiming the tool would safeguard user data. Google said in an Oct. 14 update that it detected the program "Quickly" and removed it before any downloads occurred. The surveillance app marks an update to existing APT35 tactics. Along with the malicious VPN app, APT35 hackers also compromised a U.K. university site early in 2021, using it as a base to organize a phishing operation. The espionage effort also aimed to collect the codes that users received as part of their second-factor authentication, building on a tactic that Google says Charming Kitten has used since 2017 to hack government officials, journalists, and national security officials. Google detected messages that included link shorteners, click trackers, and attacks that abused Google Drive, Dropbox, and Microsoft services. "We warn users when we suspect a government-backed threat like APT35 is targeting them," Google said.

Kroll is the leading global provider of risk solutions. Kroll's Cyber Risk practice works on hundreds of cases a year, including some of the most complex and highest profile matters in the world. With experts based around the world, supported by ground-breaking technology, we can help protect our client's data, people, operations and reputation with innovative cyber risk assessments, investigations and reporting. We help enable organization to be more cyber resilient by preparing for and detecting incidents through risk assessments, penetration testing and threat detection/intelligence services. Our clients also count on us for quick and expert support in the event of a cyber breach or attack; we help clients – of all sizes – respond to incidents and restore stability through digital forensics, breach notification, and identity monitoring and restoration services for individuals affected by a data breach

In order to be considered for a position, you must formally apply via careers.kroll.com

Cyber Risk

Preferred Majors: Computer Science, Information Security

The Cyber Security Intern will perform technical assessments and auditing of our client's information security programs to assess the maturity of an organization's information security program and make recommendations for improvement.

- Collect, analyze, and investigate information from industry partners and law enforcement to determine various methods and tactics in cyberspace.
- Keep abreast of cyber market trends and competitive intelligence through research and the culling of resources from our partners.
- Use open-source intelligence tools and proprietary technology to conduct research assessments
- Assist with writing presentations for diverse audiences, ranging from private industry to law enforcement.
- Perform statistical analysis of trends in cyber analytics





EVERYDAY CYBERSECURITY PRACTICES INADEQUATE AMONG MANY ONLINE CONSUMERS

Understanding consumer online security behavior trends is crucial for strengthening cybersecurity across society at large, said Bogdan Botezatu, Director of Threat Research and Reporting at Bitdefender. Cybercriminals continuously explore new ways to exploit human weaknesses to steal sensitive data, extort money, or gain a foothold inside systems. By understanding everyday cybersecurity practices, we can better gauge potential risks and vulnerabilities to educate consumers on ways to protect themselves more effectively such as how to use prevention, detection, and digital identity protection technologies to stop attacks from being successful. The report, based on a survey that polled more than 10,000 consumer internet users across 11 countries, examines the use of popular online platforms and services, personal cybersecurity practices, level of exposure to threats, and more. Poor password practices are still common – 50% surveyed said they use a single password for all online accounts, and 32% use just a few passwords and reuse them across multiple accounts. The United States led all other countries in the survey with unsupervised access approaching 50% compared to all other countries reporting less than 40%. Most consumers are highly exposed - When analyzing all respondent behaviors, from password reuse to the number of online accounts and services, to sharing of account details and lack of security services on their devices, almost 60% of consumers were deemed Exposed or Rather exposed. Just 11% of respondents could be described as "Secure" in terms of their cybersecurity practices. Smartphones are used most frequently to access online services - 74% of respondents primarily access online services using a personal smartphone, with 61% of those using the Android operating system. Most have social media and online shopping accounts – 63% of respondents reported having a social media account and 54% an online shopping account.



TURKISH NATIONAL CHARGED FOR DDOS ATTACK ON U.S. COMPANY

A Turkish national has been indicted in the Northern District of Illinois for launching a distributed denial-of-service attack against a hospitality company headquartered in the United States. The man, Izzet Mert Ozek, 32, allegedly used the WireX botnet, which consists mainly of compromised Android devices, to orchestrate a DDoS attack targeting the victim company's website, thus preventing users from completing hotel bookings. Headquartered in Chicago, the hospitality company "Managed and franchised luxury and business hotels, resorts, and vacation properties," the indictment reads. The DDoS attack that Izzet Mert Ozek is responsible for, the indictment reveals, caused damages to multiple computers, Aggregating at least \$5,000 in value. Ozek is charged with intentionally causing damage to a protected computer and a warrant for his arrest will be issued. If found guilty and convicted, Ozek faces a sentence of up to ten years in federal prison. Ozek's indictment was announced roughly two weeks after Matthew Gatrel was convicted for operating the DDoS service named DownThem, which was responsible for over 200,000 attacks.



AUSTRALIA TO TRY A NEW STRATEGY REGARDING RANSOMWARE DATA BREACHES

The Australian Government has approved a massive investment of AU \$1.67 billion across 10 years to mitigate the threat posed by data breaches through Australia's Cyber Security Strategy 2020, which includes a ransomware strategy. We are continuing to observe cybercriminals successfully use ransomware to disrupt services and steal from Australians. Over the past 12 months, Australia has faced a 15% increase in ransomware attacks reported to the Australian Cyber Security Centre. The Ransomware Action Plan takes a decisive stance - the Australian Government does not condone ransom payments being made to cybercriminals. Any ransom payment, small or large, fuels the ransomware business model, putting other Australians at risk. Make a stronger case against countries that aid ransomware attacks or provide safe havens for hackers. The Australian Federal Police and the Australian Criminal Intelligence Commission will be able to delete or remove data linked to suspected criminal activity, gain access to devices and networks, and even take control of online accounts for investigation purposes under this new legislation.



ANALYZING EMAIL SERVICES ABUSED FOR BUSINESS EMAIL COMPROMISE

Attackers seek to compromise email accounts to gain access to financial and other sensitive information related to business operations, and business email compromise (BEC) actors can easily use such access and information for other illicit activities. In the sample routines discussed in the parent article, the attackers' emails do not include the typical malware payload of malicious attachments. As TrendMicro observed professional email services being used for BEC attacks, TrendMicro believe BEC actors will keep adopting new services and tools to optimize their operations flow as email services try to optimize services for their legitimate users. Be wary of irregular emails with suspicious content such as unknown and dubious sender emails, domain names, writing styles, and urgent requests. Report suspicious emails to the respective security and InfoSec teams for analysis, tracking, and blocking. Using enhanced machine learning combined with expert rules, Trend Micro™ Email Security solution analyzes both the header and the content of an email to stop BEC and other email threats.



WHAT YOU NEED TO KNOW ABOUT THE ONEPERCENT GROUP

The FBI recently published a warning stating that ransomware gang OnePercent Group has been attacking companies in the US since November 2020. Ransomware attacks like the ones carried out by OnePercent Group have been crippling businesses across the country since the FBI first reported a 37% uptick in cybercrime in 2018. Although phishing scams have been around for awhile, hackers like OnePercent Group still rely on social engineering to fool high-level members of corporate organizations. If the companies still refuse to pay, then OnePercent sells the data to the Sodinokibi Group to sell at auction on the black market. While the FBI did not explicitly mention that the OnePercent Group was working with any known RaaS providers, some signatures have led professionals to believe that the group could be connected to other hacker groups via this type of service. For security teams to spot this deadly attack before they fully infiltrate the network, organizations must hire backend web and software developers who are aware of the applications that the OnePercent Group typically exploits, according to their past attacks. You can expect to pay around \$80 an hour for an experienced developer who is experienced in cybersecurity and well versed in the applications the OnePercent Group often exploits, including AWS S3 cloud, Cobalt Strike, and PowerShell.



7-ELEVEN BREACHED CUSTOMER PRIVACY BY COLLECTING FACIAL IMAGERY WITHOUT CONSENT

In Australia, the country's information commissioner has found that 7-Eleven breached customers' privacy by collecting their sensitive biometric information without adequate notice or consent. 7-Eleven claimed it received consent from customers who participated in the survey as it provided a notice on its website stating that 7-Eleven may collect photographic or biometric information from users. Angelene Falk, Australia's Information Commissioner and Privacy Commissioner determined that this large-scale collection of sensitive biometric information breached Australia's privacy laws and was not reasonably necessary for understanding and improving customers' in-store experience. In Australia, an organization is prohibited from collecting sensitive information about an individual unless consent is provided. Falk said facial images that show an individual's face is sensitive information. Regarding 7-Eleven's claim that consent was provided, Falk said 7-Eleven did not provide any information about how customers' facial images would be used or stored, which meant 7-Eleven did not receive any form of consent when it collected the images. As part of the determination, Falk has ordered for 7-Eleven to cease collecting facial images and faceprints as part of the customer feedback mechanism.

FALL

**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	<u>BOOK</u>
CYBV 302	LINUX SECURITY ESSENTIALS	<u>BOOK</u>
CYBV 303	WINDOWS SECURITY ESSENTIALS	<u>BOOK</u>
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	<u>BOOK</u>
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	<u>BOOK</u>
CYBV 329	CYBER ETHICS	<u>BOOK</u>
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	<u>BOOK</u>
CYBV 385	INTRODUCTION TO CYBER OPERATIONS	<u>BOOK</u>
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 400	ACTIVE CYBER DEFENSE	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 435	CYBER THREAT INTELLIGENCE	<u>BOOK 1</u> , <u>BOOK 2</u>
CYBV 436	COUNTER CYBER THREAT INTEL	<u>BOOK 1</u> , <u>BOOK 2</u>

NOVEMBER 2021



THE UNIVERSITY
OF ARIZONA

10

FALL

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	BOOK
CYBV 450	INFORMATION WARFARE	BOOK 1
CYBV 454	MALWARE THREATS & ANALYSIS	BOOK
CYBV 460	PRINCIPLES OF ZERO TRUST NETWORKS	BOOK
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	BOOK
CYBV 473	VIOLENT PYTHON	BOOK 1 , BOOK 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	BOOK 1 , BOOK 2
CYBV 479	WIRELESS NETWORKING AND SECURITY	BOOK 1 , BOOK 2
CYBV 480	CYBER WARFARE	BOOK 1 , BOOK 2
CYBV 481	SOCIAL ENGINEERING ATTACKS & DEFENSES	PENDING BOOK SELECTION
CYBV 498	SENIOR CAPSTONE IN CYBER OPERATIONS	BOOK



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

FALL

MORRIS WORM RELEASED AND GETS WIDE MEDIA ATTENTION

The Morris Worm marks a pivotal event in the history of cybersecurity and largely acted as an impetus for legitimizing the formal field of cybersecurity as we know it today. The worm was released over 25 years ago by Robert Morris Junior who, at the time, was a graduate student at Cornell University. The evidence seems to suggest that Morris did not have malevolent intentions, but rather that it was an experiment gone awry. The Morris Worm spread from system to system across the Internet, which in 1987 comprised about 60,000 machines. The mechanisms by which the worm spread included the exploitation of security shortcomings in the Unix Finger program, the Sendmail program, and the Unix utility rsh as well as rexec. In this video, which is the first in a multi-part series, Sourcefire's Chief Scientist, Zulfikar Ramzan, gives an overview of the Morris Worm. In subsequent videos, Zulfikar dives into more detail regarding the worm's inner workings.

NOVEMBER 3, 1988

LEN ADLEMAN USED "VIRUS" FOR THE FIRST TIME FOR COMPUTERS

At a security seminar, Len Adleman used "virus" in connection with self-replicating computer programs. Afterwards, use of the term took off. Hat tip to Gregory Benford's story "The Scarred Man" (1970) and the movie "Westworld" (1973) - prior similar usage of "virus".

NOVEMBER 10, 1983

FBI CONNECTED TO CARNIVORE EMAIL SURVEILLANCE PROGRAM

The Electronic Privacy Information Center, which sued the FBI for the information through the Freedom of Information Act, said the batch of paperwork indicates that Carnivore can capture and archive "Unfiltered" Internet traffic contrary to FBI assertions. Among the information included in the documents was a sentence stating that the PC that is used to sift through email "Could reliably capture and archive all unfiltered traffic to the internal hard drive." The FBI document was dated June 5 and contained scores of deleted words and phrases.

NOVEMBER 16, 2000

EARLIEST KNOWN USE OF THE WORD "HACKER"

The earliest known use of the word "hacker" in connection with computers was in an article in The Tech, MIT's student paper. "Many telephone services have been curtailed because of so-called hackers." Oh no - those pesky "so-called" hackers!

NOVEMBER 20, 1963

CYBER SECURITY HISTORY

NOVEMBER 2021



**THE UNIVERSITY
OF ARIZONA**

12

>. SAGUARO_POD_UPDATE

≥ FINIS CORONAT OPUS: LATIN FOR "THE END CROWNS THE WORK". THE NEW ORGANIZATION CALLED SAGUARO_POD IS INTENDED TO GIVE UNDERGRADUATE STUDENTS, BOTH REMOTE AND LOCAL, THE OPPORTUNITY TO TAKE PART IN RESEARCH TOPICS RELATED TO CYBER-SECURITY. STUDENTS WOULD BE ENCOURAGED TO DEVELOP RESEARCH WHICH WILL BE PRESENTED AT VARIOUS CONFERENCES RELATED TO THE INFORMATION SECURITY FIELD.

≥ UPDATES: REQUIREMENTS

- ≥ RECRUITMENT SELECTED EIGHT MEMBERS DURING TAP MONTH
- ≥ RESEARCH PLAN WILL BE CONDUCTED FIRST FRIDAY OF NOVEMBER STUDENT MUST PUBLISH RESEARCH / ARTICLES
- ≥ CONGRATULATIONS TO ALL OF OUR NEW MEMBERS WHO SOLVED OUR RECRUITMENT CHALLENGE

≥ OCTOBER 31ST APPLICATION DEADLINE

I INVITE ANOTHER BY VO



SAGUARO_POD

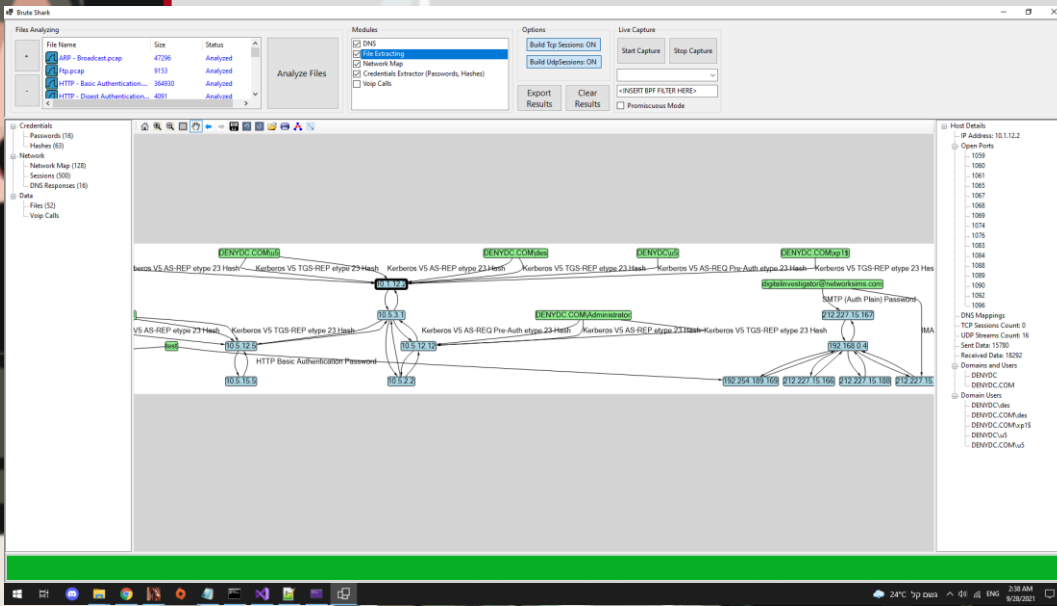
1/3

LET'S CONDUCT NETWORK LEVEL FORENSICS

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

If you have taken CYBV 326, you have experience with Wireshark or at least I hope so. Outside of CYBV 326 you may have come across a tool called Wireshark which allows you to capture network traffic to analyze, diagnose or identify possible malicious activity. Wireshark is a great open-source tool and I encourage everyone to try it out at least once. Wireshark however has a few limitations when it comes to conducting network level forensics and this is where I would like to introduce a tool called BruteShark. The developers recently released version 1.2.5 and added quite a few nice features that would aid you in network forensics. One nice feature is the ability to create a network map based on your network collection. So, if you have an already completed PCAP, you can use this to create a visual representation of which devices are communicating with other devices.

HACKING POC



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!!



LET'S CONDUCT NETWORK LEVEL FORENSICS

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


So now that we can capture traffic, what type of forensics can we conduct at the network level? Well, one possibility is that, given a collected PCAP or just capturing live traffic while a user types in a password or credential information, BruteShark will allow you to see collected hashes.

	Hash	HashType	Protocol	Source	Destination
	0fd7c603fd6f1e89bfc9...	HTTP-Digest	HTTP	192.168.1.5	192.168.1.8
	aGVtbWluZ3dheSAyO...	CRAM-MD5	IMAP	10.0.2.101	10.0.1.102
	6f29cd1f5f5ea0141acf8...	Kerberos V5 AS-REP etype 18	TCP	192.168.124.137	192.168.124.85
▶	e069122b962ddf5ddb8...	Kerberos V5 AS-REP etype 18	TCP	192.168.124.137	192.168.124.85
	0905d791dc14aae2fbc...	Kerberos V5 AS-REP etype 18	UDP	0.0.0.0	127.0.0.21
	0905d791dc14aae2fbc...	Kerberos V5 AS-REP etype 18	UDP	127.0.0.21	127.0.0.21
	72b63bb793fb34ad551...	Kerberos V5 AS-REP etype 18	UDP	0.0.0.0	127.0.0.29

If this is a hash that has been seen before or if password reuse is taking place, you can extract these hashes to later run them through another service like hashcat. BruteShark also allows you to do some simple file carving to identify images, videos or documents that have been transmitted and collected over the network.

Extension	Algorithm	FileSize	Protocol	Source	Destination
png	Header-Header Carving	211	TCP	172.16.133.45	209.99.98.33
jpg	Header-Header Carving	421	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	188	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	41219	TCP	172.16.133.45	209.99.98.33
jpg	Header-Header Carving	6390	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	3086	TCP	172.16.133.45	209.99.98.33
jpg	Header-Header Carving	32188	TCP	172.16.133.16	208.85.46.33
jpg	Header-Header Carving	52431	TCP	172.16.133.16	208.85.41.43
jpg	Header-Header Carving	29950	TCP	172.16.133.16	208.85.44.32
jpg	Header-Header Carving	43813	TCP	172.16.133.16	208.85.44.31
png	Header-Header Carving	118	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	2050	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	548	TCP	172.16.133.45	209.99.98.33
png	Header-Header Carving	204	TCP	172.16.133.45	209.99.98.33
jpg	Header-Header Carving	7403	TCP	172.16.133.116	208.111.161.254
jpg	Header-Header Carving	1095	TCP	172.16.133.116	208.111.161.254
jpg	Header-Header Carving	1073	TCP	172.16.133.116	208.111.161.254
jpg	Header-Header Carving	1122	TCP	172.16.133.116	208.111.161.254

File Preview



Now, all of this is possible within Wireshark but not in an automated way like you'll find within BruteShark. This really helps change the game as you protect or infiltrate a network.

HACKING POC



LET'S CONDUCT NETWORK LEVEL FORENSICS

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

Comparing BruteShark to Wireshark we can explore a few key differences between the two programs. If credentials are transmitted over without any type of security, BruteShark will collect them very nicely.

Username	Password	Protocol	Source	Destination
csanders	echo	FTP	192.168.0.114	192.168.0.193
test	fail	HTTP Basic Authentication	192.168.0.4	192.254.189.169
test	fail2	HTTP Basic Authentication	192.168.0.4	192.254.189.169
test	fail3	HTTP Basic Authentication	192.168.0.4	192.254.189.169
test	test	HTTP Basic Authentication	192.168.0.4	192.254.189.169
digitalinvestigator@networksims.com	napier123	SMTP (Auth Plain)	192.168.0.4	212.227.15.167

Brute Shark will also reconnect network streams together, Wireshark does this easy enough, but it is nice to see it included in this tool as well.

Brute Shark also gives you the ability to collect VOIP calls together which previously has not been a capability within Wireshark and required a bit of fiddling around to make happen. This all makes Brute Shark a great network forensics tool!

Filter Sessions

Destination Port Filter Clear

```

GET /theme/default.css HTTP/1.1
Host: browserspy.dk
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic dGVzdDp0ZXN0
Accept: text/css,*/*;q=0.1
If-Modified-Since: Wed, 29 Oct 2008 21:52:42 GMT
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.69 Safari/537.36
Referer: http://browserspy.dk/password.php
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: __utma=190908281.1560095611.1381843968.1381843968.1381843968.1; __utmb=190908281.2.10.1381843969; __utmc=190908281.20provided); __unam=6b6ab6d-141bc51a81e-4102a661-2

HTTP/1.1 304 Not Modified
Date: Tue, 15 Oct 2013 13:34:13 GMT
Server: Apache
Connection: Keep-Alive
Keep-Alive: timeout=5, max=75

GET /theme/background.gif HTTP/1.1
Host: browserspy.dk
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic dGVzdDp0ZXN0
Accept: image/webp,*/*;q=0.8
If-Modified-Since: Thu, 04 Sep 2008 12:24:28 GMT
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.69 Safari/537.36
Referer: http://browserspy.dk/password.php
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: __utma=190908281.1560095611.1381843968.1381843968.1381843968.1; __utmb=190908281.2.10.1381843969; __utmc=190908281.20provided); __unam=6b6ab6d-141bc51a81e-4102a661-2

HTTP/1.1 304 Not Modified
    
```

From Host	From Ip	To	To Host	To Ip	RTP Port	Call State	RTP Media Type
10.0.2.20:5060	10.0.2.20	test	10.0.2.15:5060	10.0.2.20	26628	Completed	audio:L16/8000/2 audio:telephone-event/8000
10.0.2.20:5060	10.0.2.20	test	10.0.2.15:5060	10.0.2.20	24082	Completed	audio:L16/16000/2 audio:telephone-event/8000
10.0.2.20:5060	10.0.2.20	test	10.0.2.15:5060	10.0.2.20	32682	Completed	audio:L16/11025 audio:telephone-event/8000
10.0.2.20:5060	10.0.2.20	test	10.0.2.15:5060	10.0.2.20	31026	Completed	audio:L16/48000 audio:telephone-event/8000
hostportion	10.35.60.72	061963177	italtel.it	10.35.60.72	16756	Rejected	audio:PCMA/8000 audio:telephone-event/8000 audio:PCMA/8000
hostportion	10.35.40.25	061963177	italtel.it	10.35.40.25	16756	Rejected	audio:PCMA/8000 audio:telephone-event/8000 audio:PCMA/8000
hostportion	138.132.169.101	061963177	italtel.it	138.132.169.101	15580	Rejected	audio:PCMA/8000 audio:telephone-event/8000 audio:PCMA/8000

HACKING POC



THE UNIVERSITY OF ARIZONA

Near You Network

NOW HIRING Student IT Assistant - Maricopa County

Job Details:

- Flexible scheduling - We work around your class schedule. Ideally works in the afternoons/evenings
- Up to 15 hours per week @ \$14/hour
- Primarily located at Chandler, with possible travel to Gilbert or North Valley

Duties/Responsibilities:

- Assists campus community members in the use of technology in the classrooms
- Assist IT with classroom coverage, event support, and projects
- Perform basic clerical duties to help maintain office space
- Have a valid Driver's License

Knowledge, Skills, and Abilities:

- Have excellent customer service
- Knowledge of Microsoft Office Suite
- Ability to problem solve and make decisions
- Skills in use of computers and software

Email your Resumé/Cover letter or any questions to:

Ike Dent (dent@arizona.edu) &
Jackie Mattingly (jmattingly@arizona.edu)



THE UNIVERSITY
OF ARIZONA

NOVEMBER 2021

17



> 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

NOVEMBER 2021

18

INFORMATION SYSTEM SECURITY PROFESSIONAL



Information System Security Professionals at NSA 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 and 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
- conducting security engineering/hardening of the latest operating systems, tailoring them for use in the specific mission area
- reviewing requests for security relevant changes on the mission infrastructures, ensuring risk is adequately mitigated
- working with system owners to accredit/re-accredit critical mission systems

Salary Range: \$73,076 - \$91,057

CYBER MITIGATIONS ANALYST/SYSTEM VULNERABILITY ANALYST



Network cyber mitigations engineers and system vulnerability analysts at NSA analyze vulnerabilities and develop mitigations to strengthen defenses. They produce formal and informal reports, briefings, and guidance to defend against attacks against network infrastructure devices or systems.

Our analysts' competencies run the gamut of data transport possibilities. They work with traditional wired networks, wireless transport, including Wi-Fi and cellular, collaborative platforms such as video teleconferencing, and the hardware and software that support it all. Start your career as a Network Cyber Mitigations Engineer/System Vulnerability Analyst at NSA, where you can become an expert in networking protocols and architectures, cloud security, and Internet of Things protocols, to impact and advance traditional network security

Salary Range: \$73,076 - \$91,057

FALL

LEARN
ABOUT
CYBER
SECURITY
AND WORK
IN CYBER
SECURITY

COMPUTER NETWORK ANALYST/SYSTEM VULNERABILITY ANALYST



System Vulnerability Analysts identify vulnerabilities and attacks to the design and operation of a system (H/W, S/W, personnel, procedures, logistics, and physical security). They compare various system attack techniques and develop effective defensive mitigations. Additionally, System Vulnerability Analysts produce formal and informal reports, briefings, and perspectives of actual and potential attacks against the systems or missions being studied

Salary Range: \$73,076 - \$91,057

JOBS & INTERNSHIPS

TITANS CA CENTER FOR CYBER DEFENDERS - RD UNDERGRADUATE SUMMER



Sandia
National
Laboratories

Sandia California's Center for Cyber Defenders (CCD) is currently hiring for the Summer 2022 internship program!

As part of Sandia's Technical Internships to Advance National Security (TITANS), CCD's mission is to build the next generation of cyber security experts through the identification and mentoring of highly skilled student researchers in the fields of computer science and cyber security. Become a Sandia Cyber Defender and take the first step toward an impactful career in cybersecurity research and development addressing our nation's most challenging issues!

On any given day, you may be called on to:

- Leverage your skills across numerous domains, including software/hardware development, data analysis and machine learning, reverse engineering, and machine and network virtualization.
- Team with Sandia cybersecurity subject matter experts and fellow interns to solve real-world problems with real-world national security impact.

NOVEMBER 2021



THE UNIVERSITY
OF ARIZONA

20



DOD CYBER SCHOLARSHIP PROGRAM (DOD CYSP)

The Department of Defense (DoD) Cyber Scholarship Program (CySP) is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA).

The objectives of the program:

- Promote higher education in all disciplines of cybersecurity
 - Enhance the Department's ability to recruit and retain cyber and IT specialists,
 - Increase the number of military and civilian personnel in the DoD with this expertise, and ultimately
 - Enhance the nation's cyber posture.
-
- The DoD is working with universities like the University of Arizona and other defined National Centers of Academic Excellence (CAE). Interested students need to apply directly with the University of Arizona at CYSP@EMAIL.ARIZONA.EDU
-
- Minimum cumulative GPA of 3.2 (undergraduate)
 - Must be entering junior or senior year.
 - Must be a U.S. Citizen.
 - Must agree to work for the DoD as a civilian for one year for each year of scholarship received.



The NSA CAE-CO designation provides UA graduates access to the CAE Community and all of its resources.



DOD CYBER SCHOLARSHIP PROGRAM MENTORING SESSION

The Department of Defense (DoD) Cyber Scholarship Program (CySP) is sponsored by the DoD Chief Information Office and administered by the National Security Agency (NSA).

JOIN US FOR OUR MENTORING SESSION

- **When: Nov 12, 2021, 05:00 PM Arizona**
- **Register in advance for this meeting:**
- **<https://arizona.zoom.us/meeting/register/tZMsce2grDMpGdwqC7WNKS64ZUrN-xS0Xrgv>**
- **After registering, you will receive a confirmation email containing information about joining the meeting.**



The NSA CAE-CO designation provides UA graduates access to the CAE Community and all of its resources.

>. ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. HAVE AN AWESOME THANKSGIVING
>. 25 NOVEMBER 2021
>. ---END TRANSMISSION---

THANK YOU

CONTACT US

CHIO@EMAIL.ARIZONA.EDU

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

Phone: 520-458-8278 ext 2155

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