

HACK



A celebration of digital counter-culture

hacker hermanos

Red team infrastructure as code

1337 sheets

The significance of data sheets
in hardware hacking

ghost rider in the machine

Build an AI powered pentesting copilot

anonymous resources

Fly under the radar with these
amazing tools and services

issue:one:twozerotwofour

A Smart Cyber Solutions Project





SMARTCYBER
solutions

See your business
through the eyes of an
adversary
Smart Cyber Solutions: the devil you know

Physical and digital security consulting

Privacy & anonymity solutions

Threat & digital foot print assessments

Pro bono services available for registered charities*



Tox: 49B4FBFE9CE99512564C0048AE55799E5ACD90C50EE2C233030AC4A295505307AFFED7D94571





An open letter to some toxic avengers

You know who you are

In a world that's overconfident to the point of arrogance, where knowledge is handed out like expired party gifts, Socrates' eternal declaration—"All I know is that I know nothing"—slashes through the noise like a scalpel through silk. It's not just an admission; it's a battle cry for the mavericks, the outlaws daring enough to confess their ignorance in a society crammed with self-anointed gurus.

Education, dear readers, isn't your polished, prim progression from ignorant to enlightened; it's a wild ride down backroads at midnight, sans headlights, in terrain that gets more untamed with every mile. With each piece of the puzzle or theory you secure, the frontier of the unknown only expands further, our all-too-human minds mocked by the universe's cruel joke. Each piece of knowledge doesn't stack tidily to form a fortress of understanding but rather shatters the confines of what we believed was comprehensible, scattering the terrain with more queries, more enigmas.

The real barrier we frequently face? Complacent gatekeepers—self-designated guardians of what merits knowledge.

These keepers of the supposed truth. Their contempt for the seekers, the thinkers, the restless inquirers who incessantly tug at the threads of the grand narrative to glimpse what lies beneath—it's not merely elitist; it's diametrically opposed to the trait that drives humanity forward.

Curiosity.

What is the essence of learning if not the continuous revelation of our own ignorance? This realization isn't a vulnerability of knowledge, prone and unprotected. No, it's the vibrant, pulsing core of intellectual valor. It's the audacity to gaze into the vast, starlit abyss of the unknown and not flinch but instead dive in.

Let's dismantle these barriers erected by the knowledge monopolists and surge, headlong into the wild, uncharted unknown. Because that's where true discovery resides—not in the silent, dust-laden corridors of caution and hesitation, but out there, in the raw, screaming wilderness of relentless questioning.

Lots of love

d8rh8r



EXPLOIT SEGMENTS

<https://exploit>



LOT

IRITY

itsecurity.io

HVC

CK

industry

RUN SMB

The Importance of Cybersecurity for Small Businesses

In today's world, cybersecurity is a critical concern for businesses of all sizes. While large organizations often dominate the headlines when it comes to cyberattacks, small and medium-sized businesses (SMBs) are not immune to the threats. In fact, studies have shown that a significant percentage of data breaches involve SMBs.

These businesses may not always realize the importance of cybersecurity or understand the risks they face. As cybersecurity professionals, it is our responsibility to break through to these organizations and provide them with the support and guidance they need to become more secure.

The Challenges Faced by SMBs

SMBs often find themselves in the shadows when it comes to cybersecurity. They may believe that they are not attractive targets for cyberattackers, or they may feel overwhelmed by the complexity of implementing security measures. However, adversaries know that SMBs are in fact prime targets - their adoption of new technology makes them vulnerable, while their typically limited security resources and expertise make them easy prey.

Attackers can easily spend more time trying to infiltrate small and medium-sized organizations because their security posture is typically not at the same level as a Fortune 500 company. Cybercriminals wait stealthily for a vulnerability to appear, or for the SMB to let their guard down, which gives them the opening they need to stage an



ER

Y



attack. This can then turn into multimillion dollar payouts from ransomware or stolen data. For SMBs, such large monetary losses can be crippling to business operations.

To properly address these challenges, SMBs must focus on the basics of cybersecurity, such as the importance of regularly patching systems, implementing access management controls, training employees on security best practices, and better monitoring of their environment. But they often lack the budget,

staff and expertise to execute on these basics in a robust way. This is where trusted cybersecurity partners can play a crucial role in providing tailored guidance and support.

The Role of Cyber Insurance

In addition to technical controls, cyber insurance has become an absolutely essential component of risk management for businesses of all sizes. Insurance can help soften the

financial blow of a cyber incident. However, insurance companies expect organizations to have strong security measures in place in order to qualify for policies, and determine premiums based on their security posture. It's important for SMBs to prioritize foundational security steps to ensure insurability at reasonable rates.

The alignment between cybersecurity best practices, compliance with regulations, and insurance coverage will play a crucial role in shaping the future of SMB cyber protections. When SMBs make cybersecurity and compliance a top priority, they become more insurable at better rates. Insurance companies can even require certain security standards be met as part of the underwriting process.

Getting Started Securing SMBs

For SMBs just getting started on their cybersecurity journey, the most important first step is accepting that they are indeed vulnerable. From there, conducting an honest assessment of existing security practices and identifying gaps is essential. Some quick-win areas for SMBs to focus on include:

- **Implementing multi-factor authentication across all systems and accounts**
- **Establishing regular software patching cycles**
- **Training employees on how to identify phishing attempts**
- **Making periodic backups of critical data**
- **Monitoring for suspicious network activity**

The Future of SMB Cybersecurity

In conclusion, SMBs must recognize the real danger posed by cyber threats and take proactive steps to protect their businesses. Although they are often in the shadows of large enterprise security, SMBs are attractive targets for attackers. By focusing on security fundamentals, leveraging outside partnerships and expertise, and

making security a top priority, these small organizations can substantially improve their cyber risk postures.

The integration of cyber best practices into insurance and compliance frameworks will also continue shaping SMB cyber protections and driving further adoption of security measures. With the right level of commitment and support, SMBs can tackle the unique cyber challenges they face.

At BarCode Security, we make it our mission to provide SMBs with the specific guidance, technology and services needed to defend against today's continually evolving threats. By engaging directly with small business leaders, participating in SMB-focused industry events, and sharing our knowledge, we aim to help every organization address their security gaps. Working together, we can empower SMBs with the cyber readiness they need to confidently grow while reducing risk.

To learn more about BarCode's security services for SMBs, visit barcodesecurity.com.

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any other agency, organization, employer, or company.



CONTACT INFO

1 (302) 918 5441

info@barcodesecurity.com

4 Peddlers Row Unit

#291 Newark, DE 19702



**Why I freelance
in cyber sec**

Who Am I

Hello! My name is David Lee, but a lot of people in the cybersecurity industry know me as DC CyberSec. I'm a cybersecurity professional with over 17 years experience in the industry and have in the last few years pivoted my work towards freelancing in cyber security.

My previous workplaces mostly include government agencies in Australia as well as a few private organisations with varying positions, from pentesting to compliance, and most notably, social engineering engagements. To give you an idea of what this article is about, is why I got into freelancing in cybersecurity and how you can also achieve this type of work alongside your main job as a side hustle, or as a full time gig that you might want to pursue.

Let's get stuck in!

What is cybersecurity freelancing

Freelancing is a rapidly growing trend in today's workforce, with many professionals choosing to work independently rather than being tied to a traditional 9-5 job. This trend is no different in the field of cybersecurity, where freelancers are in high demand due to the constantly evolving nature of the industry.

So, what exactly is freelancing in cybersecurity? In simple terms, it refers to the practice of offering cybersecurity



services on a contract or project basis, rather than being a permanent employee of a company. This can include a wide range of services such as network security, data protection, risk assessment, and more.

One of the main reasons for the rise of freelancing in cybersecurity is the constant need for businesses to secure their data and networks. In today's digital age, cyber attacks are becoming more frequent and sophisticated, making it crucial for companies to have strong protection measures in place. However, not all companies have the resources or expertise to maintain an in-house cybersecurity team, which is where freelancers come in.

Freelancers in the cybersecurity field offer their services to clients on a project-by-project basis, providing a more cost-effective solution for businesses. This allows companies to access top-notch cybersecurity services without having to bear the cost of hiring a full-time employee. Additionally, businesses have the flexibility to hire freelancers as and when needed, making it an attractive option for short-term projects or one-time assessments.

One of the key benefits of freelancing in cybersecurity is the expertise and specialization that freelancers bring to the table. With the constantly changing landscape of cyber threats, it is essential to have professionals who have the knowledge and skills to stay up-to-date with the latest techniques and technologies. Freelancers often have a specific niche within the cybersecurity field, allowing them to focus on a particular area and develop specialized skills. This level of expertise is valuable to

ance curity

businesses as they can expect high-quality work and specific solutions tailored to their needs.

Another advantage of freelancing in cybersecurity is the opportunity for freelancers to work with a wide range of clients in different industries. This provides them with exposure to various security challenges and allows them to gain experience in diverse environments. It also opens up opportunities for networking and building a strong portfolio, which can lead to more projects in the future.

However, like any freelance work, there are also challenges that come with being a freelancer in the cybersecurity industry. For starters, freelancers have to constantly market themselves and build a reputation to attract clients. This means keeping up with industry trends, continuously learning new skills, and staying connected in the community.

Another challenge is the responsibility of managing their own contracts, invoicing, and taxes. This can be overwhelming for some, especially as cybersecurity professionals also have to keep up with the latest security measures and regulations, on top of their administrative tasks.

Freelancing in cybersecurity offers a win-win situation for both businesses and professionals. Businesses get access to top-notch cybersecurity services, and freelancers have the opportunity to work on various projects and gain experience in different industries. It also allows for greater flexibility and control over work-life balance.

As the demand for skilled cybersecurity professionals continues to rise, we can expect to see more individuals turning to freelancing as their preferred mode of work. With the constantly evolving nature of the industry, freelancing provides a perfect platform for businesses to access the expertise they need to stay ahead of cyber threats.

Why I freelance in cybersecurity

consulting services As for why I freelance in cybersecurity, the answer is simple. I prefer working for organisations on my own terms, in my own time, from the comfort of wherever it is I am in the world. My main





purpose to pursue freelancing as a main source of income is because I wanted to travel and have more time to myself. When I first started freelancing, I was working full time on a cybersecurity contract in Australia, and it took me a very long time (2+ years) to gain enough clients to work on projects remotely with to be able to replace my full time work salary, however, having not worked hard towards this goal would mean that I'd still be working contracts in Australia for another organisation, which didn't align with my main goals.

The lifestyle and freedom to choose what I work on and with who, and obviously from where, is what I was hoping to achieve, and after a few hard years of working contracts while also working after hours and on weekends to meet my clients needs was challenging to say the least.

The lifestyle of a cybersecurity freelancer

The rise of technology and the internet has brought about many changes in the way we live our lives. One of the major changes has been the emergence of cybersecurity as a crucial aspect of our digital lives. With the increasing frequency of cyber threats and attacks, the demand for cybersecurity professionals has also been on the rise. This demand has led to the rise of a new breed of professionals - cybersecurity freelancers. In this article, we will be taking a closer look at the lifestyle of a cybersecurity freelancer and the challenges that come with it.

First and foremost, let us understand who a cybersecurity freelancer is. Simply put, a cybersecurity freelancer is an individual who provides cybersecurity services to clients on a project basis. They work independently and are not associated with a particular organization. They could be hired by small businesses, large corporations, or even individuals who require their services. With the rapid growth of the gig economy, more and more cybersecurity professionals are choosing to work as freelancers rather than being tied down to a full-time job.

The lifestyle of a cybersecurity freelancer is not much different from that of any other freelancer. They have the freedom to choose their own working hours and location. This gives them the flexibility to balance their personal and professional life. However,

this freedom also comes with a certain level of responsibility. As they are their own boss, they need to manage their time and workload efficiently in order to meet project deadlines.

One of the biggest challenges for a cybersecurity freelancer is staying up to date with the constantly evolving world of technology and cyber threats. They need to constantly upgrade their skills and knowledge to provide the best possible services to their clients.

This requires them to spend a considerable amount of time on self-study and training, which can be difficult while juggling multiple projects and clients. Another challenge for cybersecurity freelancers is the constant pressure to find new clients and projects. Unlike full-time employees, freelancers do not have the security of a steady paycheck. They need to constantly market their services, network, and look for new opportunities to sustain their business. This can be daunting and requires excellent communication and networking skills.

Despite these challenges, the lifestyle of a cybersecurity freelancer also has its perks. They have the freedom to choose the projects they want to work on and the clients they want to work with. This allows them to specialize in certain areas of cybersecurity and also negotiate their rates accordingly. As they are not bound by the limitations of a formal job, they have the potential to earn more than traditional cybersecurity professionals.

The lifestyle of a cybersecurity freelancer is a mix of challenges and opportunities. They have the freedom to work on their own terms but also need to constantly keep up with the ever-changing landscape of technology. They have the potential to earn more, but also need to constantly market themselves and network to sustain their business.

Ultimately, it all boils down to their passion for cybersecurity and their ability to adapt to the demands of the industry. With the increasing importance of cybersecurity in our daily lives, the demand for freelancers in this field is only expected to rise in the future.

For me, my lifestyle has completely changed,

as I write this article from a small cafe in Singapore. My schedule today has a few locked in items like client meetings, completing a penetration testing report for handover later today, and reviewing a few new quotes to be sent out, however I also plan to do a little travel once these items are completed to another city area to stay for a few days, staying in-line with my goal of travelling and working as one. Something I could never achieved working a full time role back in Australia.

Why it's important to find a healthy work life balance

As with any form of work style, and from what you have read through in this article, finding a healthy balance between the work and life balance was ultimately my main goal with cybersecurity freelancing, as it is for most people freelancing different services. Freelancing has opened me up to a completely different style of working day to day, and sometimes things get rough with timeframes and deadlines, just as they do working in a full time role.

With more clients means more work to be completed, and finding a happy medium of actually living life while also meeting your work obligations can be tricky, however the reward is that you are your own boss and that time to live is absolutely available to you. For me, my clients and my work come first before travelling or visiting new cafes, and often the perception is that freelancer aren't really doing too much work.

What it comes down to really is time management skills. The way I manage my own clients expectations as well as my families expectations on when and what I'm doing is by noting down all of my work in a calendar.

When I start a project for a client, I add it to my calendar and invite my client to that calendar item so they can see exactly when to expect a work to be completed and how long it's going to take. This creates visibility and trust between myself and my clients, and of course, my wife who also shares my calendar - so that we're all on the same page of what's coming up and when I'm going to be busy. In between the work is when I schedule times away (often ahead of time) so that I can easily book in the parts of life I want to live.

To wrap this article up, freelancing in

cybersecurity has changed my life for the better, and the thought of going back to a life where I wake up, go to work, come home and repeat each and every day is a nightmare I'd rather not live and likely will never go back to.

I have helped countless other individuals with a similar mindset to achieve their goals as freelancers in the cybersecurity space through The Safer Internet Project (<https://learn.saferinternetproject.com>) which is something I'm extremely proud of being able to create and help people with as the world of digital nomad freelancing work continues to grow.





F2

F12

R

T

G

Y

Using Cyber To Make Things In Russia Go Boom

By Jeffrey Caruso

NOTE: This is an excerpt from Chapter Six of the author's forthcoming book *Inside Cyber Warfare* (Third Edition) to be published in the Fall of 2024 by O'Reilly Media.

Russian energy giant Gazprom's networks and those of its subsidiaries have been pwned by Ukraine's military hackers ever since Russia seized Crimea in March of 2014 following Ukraine's Revolution of Dignity.

Ukrainian hackers working for the Directorate of Intelligence for the Ministry of Defense of Ukraine began collecting information on Gazprom's supply chain, gained access to a supplier through phishing, then leveraged that trusted access to phish one of Gazprom's organizations. , Once inside, began mapping the network and exfiltrating data.

As a result of their access, Ukraine's small team with little to no funding but a wealth of experience including some time spent with Israel's Mossad, engineered a hack of Gazprom's pipelines pressurization controls that would cause a pipeline to rupture resulting in an explosion and a fire.

To date, three pipelines have experienced rupture events that were directly the result of a computer network attack. Prior to those, there were multiple practice sessions on live pipeline systems that had mixed results.¹ Unlike DHS's Aurora Generator test experiment that required building a test site to conduct the experiment at a cost of \$2 million, the GUR hackers tested their methods on real pipelines until they had it right. The cost to the Ukrainian government? Zero.

¹ Earlier fires that GUR hackers took credit for included Gazprom's Amur plant on Oct 11, 2021 (<https://www.hazardxonthenet.net/article/187477/No-one-injured-after-explosion-and-fire-at-major-Russian-gas-processing-plant.aspx>),

² <https://ria.ru/20220401/spravka-1781213085.html>

<https://ria.ru/docs/about/copyright.html>

⁴ <https://yk24.ru/proisshestviya/avariyu-na-gazoprovode-ustranyayut-v-verhnevilyujskom-rajoneyakutii/?amp=1>

⁵ <https://voinskayachast.net/goroda/yakutsk-i-respublika-saxayakutiya%20%2%A9%20VoinskayaChast.net>



Figure 3.6
Photo courtesy of RIA Novosti / Press Service of the Ministry of Emergency Situations of the Russian Federation³

APRIL 3, 2022

Gazprom Sartransneftegaz Pipeline Yakutia, Russia

The cyber operation was launched just after two Ukrainian helicopters hit an oil depot in Belgorod on April 1, 2022²

Figure 3.6 Photo courtesy of RIA Novosti / Press Service of the Ministry of Emergency Situations of the Russian Federation³

On April 3, according to RIA Novosti, "employees of Sartransneftegaz JSC discovered an underground gas leak from the high-pressure gas pipeline from the AGDS to GRP-1 at the entrance of the gas pipeline to the village of Verkhnevilyuysk ... in the Republic of Sakha (Yakutia)."⁴

As a side note, Yakutia is also home to a division of Russia's Space Forces whose duties include "the radar tracking of artificial earth satellites for military purposes." The Space Forces would later become another target of interest, at least in terms of its espionage value to Ukraine's allies who had their own Space Forces in development.



Figure 3.7:
Images posted to Russian social media platform VK⁶

APRIL 4, 2022

Gazprom Urengoy Center 2 Pipeline Matveevo, Russia

On April 4, a section of the main gas pipeline "Urengoy-Center-2" ruptured causing a large fire in the Lysvensky district of the Kama region near the village of Matveevo. An eyewitness captured footage of the large fire quite a distance away and posted it on VK.com, Russia's equivalent of Facebook. The incident was reported by a local paper AiF-Prikamye.⁷

3. <https://ria.ru/docs/about/copyright.html>

4. <https://yk24.ru/proisshestviya/avariya-na-gazoprovode-ustranyayut-v-verhnevilyujskom-rajoneyakutii/?amp=1>

5. <https://voinskayachast.net/goroda/yakutsk-i-respublika-saxayakutiya%20%C2%A9%20VoinskayaChast.net>

6. https://vk.com/wall-190197274_9735?Lang=en

7. https://perm.aif.ru/society/incident/krupnyy_pozhar_proizoshoy_izza_razryva_gazoprovoda_nochyu_v_prikame



Figure 3.6

Images posted to Telegram and Twitter of the Urengoy gas field pipeline explosion

JUNE 16, 2022

Gazprom Urengoy Pipeline

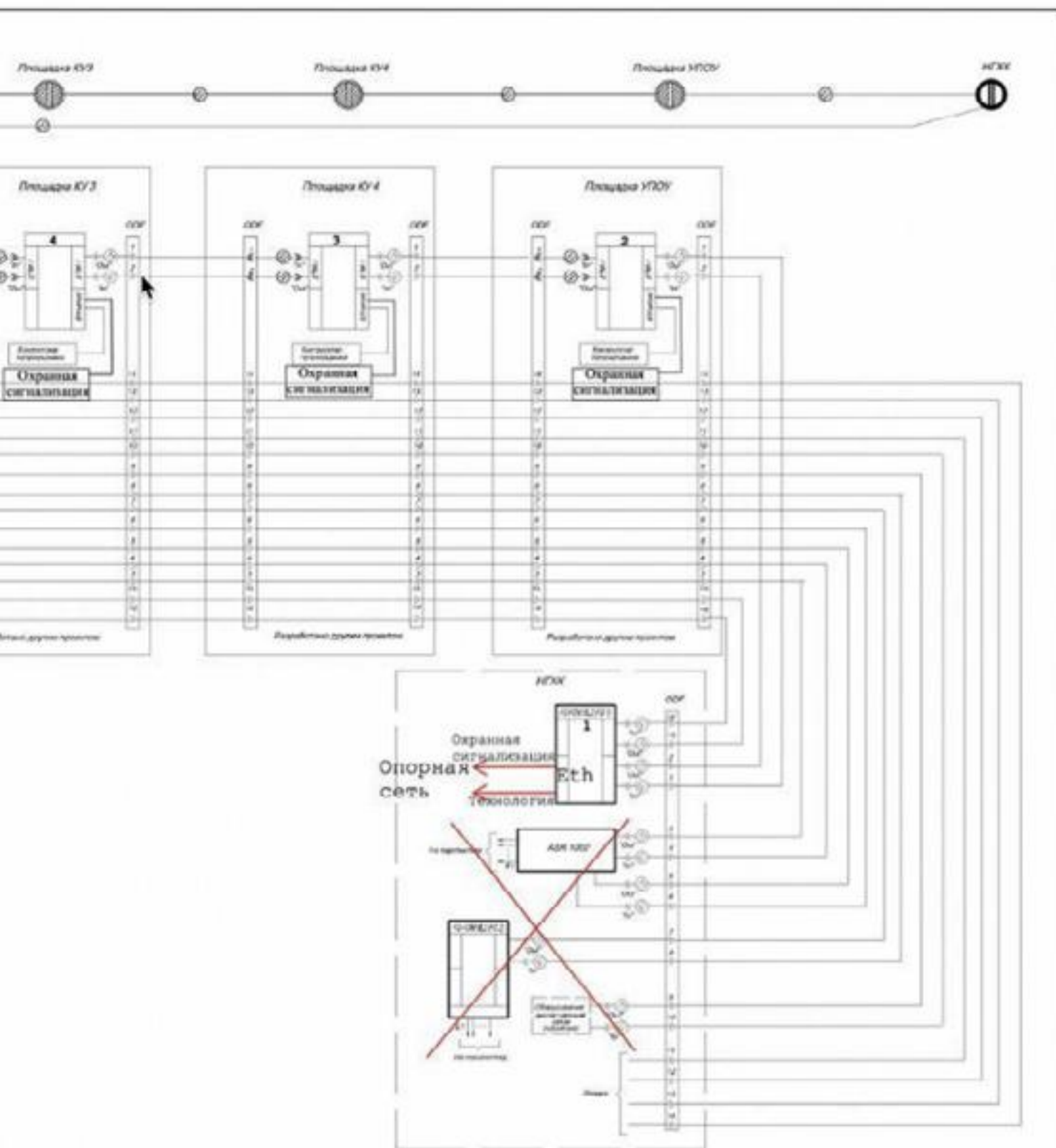
Yamalo-Nenets Autonomous Okrug, Russia

The most successful of the Gazprom fires was this one on June 16 at Gazprom's Urengoy gas field in the Yamalo-Nenets region. It's the second largest gas field in the world and the largest gas field in Russia.⁸

Part of the planning for this attack included understanding who the vendors were and gaining access, if necessary, to their respective networks (see figure 3.8).

According to an interview that I had with one of the cyber operators involved in the planning and execution of this and earlier attacks, during their network reconnaissance phase, his team discovered that a key section of the data communications network of the gas pipeline that would transmit an alarm when the pipeline was operating outside of acceptable conditions was never connected.

⁸ <https://euroweeklynews.com/2022/06/16/russia-urengoy-gas-field-fire-yamalo/>



						ГЭС-1202/10-ПД		
						Создание НГХК. Корректировка рабочей документации Газопробода сырьевого газа по результатам обследования и в связи с приведением действующим нормам и правилам. Волоконно-оптическая линия связи.		
Изм.	Код ум.	Лист	№ док.	Подпись	Дата	Страница	Лист	Листов
						Система передачи данных		
						Р	9	1
ГИП		Сюрсина		<i>[Signature]</i>	10.10	ООО "ГазЭнергоСвязь"		
Нач. отд.		Куприяшова		<i>[Signature]</i>	10.10			
Разроб.		Эрнандес		<i>[Signature]</i>	10.10			
Н. контр.		Абилова		<i>[Signature]</i>	10.10	Организация связи. Схема структурная		

it had been paid to deliver, amounting to several billion rubles⁹

Some of the many unfinished items included

- "A complex of engineering and technical means of protection and means of anti-terrorist protection (designer of DOAO "Gazprojectengineering")"
-
- "Control room (title 401/080), Administrative building with a laboratory (title 401/080-1)"
- "Engineering networks of the administrative and amenity zone, Automated fire safety system"

On Jan 22, 2020, Gazprom announced a solicitation for:

- Execution of turnkey works on the facility "Automatic fire alarm system, gas pollution control and fire extinguishing of gas pumping units of booster compressor stations (level I) of the installation of complex gas treatment - 7, 8, 9, 10, 12, 13, 15, booster compressor stations (level II) of the installation of complex gas treatment - 1, 2, 4, 9, 10, 11, 12 of Urengoy oil and gas condensate field for the needs of Gazprom dobycha Urengoy LLC (0001/19/1. 1/0101853 / Durengoy/K/ STATE/e/20.12.2019) - 1 551 051 576,00 rubles.
- Performing major repairs of the fire alarm system for the needs of Gazprom dobycha Urengoy LLC in 2020-2021 (for small and medium-sized businesses) No. 0095/19/5. 1/0097185 / Durengoy / PR/ STATE/e/11.12.2019 - 43 726 275,89 rubles.

This incident of vendor incompetence and corruption is not the exception in Russia. It happens far too frequently and in every industry including Space, Energy, Finance, and Defense.

The long-term impact of corruption can be seen in the performance of Russian equipment during its operations in Ukraine when it's expensive missiles repeatedly failed to hit their targets¹⁰, or when a multi-million dollar tank broke down in a parade celebrating Russian military prowess,¹¹ or when a state-owned company as rich and powerful as Gazprom cannot protect its own resources from destructive cyber attacks.

Acts of sabotage by cyber means such as the ones conducted by GUR hackers at Gazprom's largest plants including the explosions at the Urengoy Yamalo-Nenets region, the Urengoy Kama region, and the gas leak in Yakutia are facilitated by the culture of corruption there; and the only thing that's preventing these types of attacks from happening more frequently and in greater numbers is not the technical difficulty of the operation, nor that Gazprom has improved its networks' defenses.

It is solely due to the restraint being exercised by Ukraine's leadership. One option under consideration by the GUR team was to develop a scalable attack that would hit all Gazprom pipelines simultaneously, however that was deemed by senior leadership to be too inflammatory and would most likely be seen by Ukraine's allies as excessively aggressive.

9 ARBITRATION COURT OF THE YAMAL-NENETS AUTONOMOUS DISTRICT in the matter of The Arbitration Court of the Yamalo-Nenets Autonomous District composed of Judge S.V. , OGRN 1037730026575) to the limited liability company Novourengoy gas chemical complex (TIN 8904006547, OGRN 1028900620264) for the recovery of 1,317,983,943 rubles 25 kopecks, and on the counterclaim of the limited liability company "Novourengoy gas chemical complex" (TIN 8904006547, OGRN 1028900620264) against the limited liability company "Stroyneftegaz Alliance" (TIN 7730172171, OGRN 1037730026575) for the recovery of 1,379,095,416 kopecks. Source:

<https://sudact.ru/arbitral/doc/RMrlWzy7JGxR/>

¹⁰ https://www.cvedetails.com/vulnerability-list/vendor_id-7867/Acronis.html

¹¹ <https://www.ibtimes.com/russias-new-t-14-armata-tank-breaks-down-during-victory-day-paraderehearsal-moscow-1913336>



Figure 3.9

Fire at Second Central Research Institute of the Ministry of Defense of the Russian Federation on April 21, 2022

April 21, 2022

Second Central Research Institute of the Ministry of Defence of the Russian Federation

Tver, Russia

A fire and explosion at this top secret research facility where the Iskander and S-400 missiles were designed resulted in the complete destruction of the building leaving five dead and thirty wounded. Russian State news service TASS reported that the cause may have been due to a malfunction associated with faulty wiring¹²

According to informed sources, this was a combined Cyber / Special Operations Forces mission where a commando team surreptitiously entered the structure to place explosives so as to render maximum

damage to the structure. The initiating cause for the explosion was the electrical fire caused by the cyber team.

This combination approach gives a tactical advantage to the commandos who can already be on their way to the next target when the fire starts and the explosive charges ignite. For example, the Dmitrievsky Chemical Plant in Kineshma, Ivanovo Oblast, Russia, an approximately seven hour drive from Tver, which was destroyed by a fire the very next day.¹³

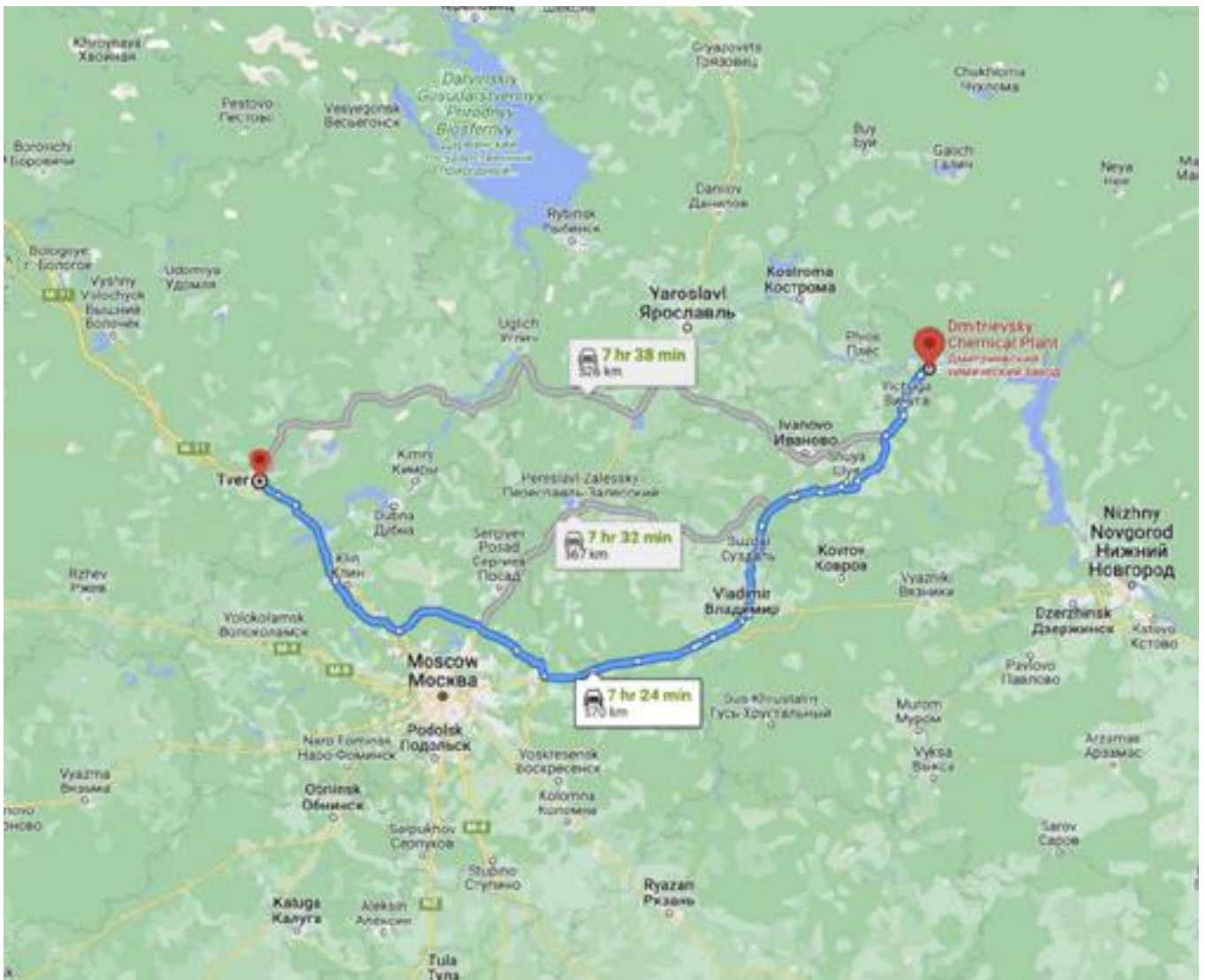


Figure 3.10:

Google map directions from Tver to Kineshma

That's not to say that both fires were due to cyber/physical attacks, but the second fire was certainly deemed suspicious according to the press reports. One of the many problems that Moscow has is differentiating between what was an act of sabotage versus what may have been one of hundreds of fires that start because of poorly maintained infrastructure.

These types of cyber-physical attacks are uncommon, and so they aren't profitable to defend against. They don't neatly fit within an OT network defenders playbook and you cannot write a signature for it or upload a binary to VirusTotal. It is a

frightening innovation in warfighting that the cybersecurity industry isn't prepared to defend against.

ABOUT THE AUTHOR:

Jeffrey Caruso (né Carr) is the author of *Inside Cyber Warfare* (O'Reilly Media, 2009, 2011, 2024 (projected)) and writes the *Inside AI Warfare* newsletter. He was contracted as a Russia Subject Matter Expert with the CIA's Open Source Center, provided numerous briefings to U.S. government agencies, and has been a frequent lecturer at the U.S. Air Force Institute of Technology and the U.S. Army War College.

12 <https://www.rferl.org/a/russia-fire-tver-defense-research/31815016.html>

13 <https://www.lbc.co.uk/news/russias-biggest-chemical-plant-burns-down-second-mystery-fire/>



Tactics Used by Hacker Groups During Ransomware Attacks on the Healthcare Sector

The healthcare industry is under attack like never before.

What started as a surge in criminal activity during the early days of the coronavirus pandemic has now evolved into a full-blown crisis within the healthcare industry worldwide. The 2021 disruptive ransomware attacks on Scripps Health in San Diego, Ireland's national health service and Waikato hospitals in New Zealand demonstrate the global nature of the threat, and the pervasive level of risk within this industry

Healthcare has long been a target of cybercriminals, due to its valuable personal and financial data. These attacks target organizations that store sensitive patient data and valuable information, making them prime targets for cybercriminals seeking financial gain. However, the shift to more aggressive and destructive tactics – like ransomware, with an extra layer of double-extortion – is putting incredible pressure on this critical service sector. To successfully carry out these attacks, hacker groups employ various tactics, techniques, and procedures (TTPs) to maximize their impact and disrupt healthcare operations. I will try demonstrate some of the tactics and techniques used during a Ransomware attack in this article, basing it on the MITRE ATT&CK framework.

Using the MITRE ATT&CK Framework to Deconstruct a Real-World Ransomware Attack

Sun Tzu claimed that “all warfare is based on deception,” and in my opinion this complements the “MITRE ATT&CK™” framework nicely. Short for “Adversarial Tactics, Techniques and Common Knowledge,” this database categorizes known adversarial tactics and techniques to help cybersecurity specialists gain insight into how attackers think and operate. It brings immeasurable value of useful information when your company is trying to prioritize mitigation strategies and controls, recover from breaches faster or honeypot foes into trapping themselves, while gaining insight into the strategies used by threat actors during their ransomware campaigns.

Common Tactics, Techniques, and Procedures (TTPs)

Based on extensive research and analysis, several common TTPs have been observed among the most prevalent ransomware groups targeting the healthcare sector. These TTPs provide insight into the tactics employed by hacker groups during ransomware attacks on healthcare organizations:

ATTACK PHASE 1 RECON

During this initial phase, the attackers gather publicly available information about their intended target and launch a Metasploit listener to keep an ear on incoming connections. They also use simple phishing techniques, such as faking an email from the organization's IT department, to ensure users downloaded infected software to create an easily accessible backdoor for the attacker.

ATTACK PHASE 2 INITIAL ACCESS

Attackers gain initial access to healthcare systems through various means, including exploiting public-facing applications, external remote services, or phishing techniques. They may also utilize valid accounts or domain accounts for unauthorized entry.

With secret entry achieved, the attackers install a program that allow them to see the company's internal infrastructure – and plan the best way to attack – before carefully deleting any trace of activity to remain undetected.

In this phase, the attackers use several different MITRE-defined techniques to gain an initial foothold: they abuse access to valid accounts gained through social engineering, use active phishing campaigns targeting credentials, and last but not least they exploit public-facing applications.

ATTACK PHASE 3 EXECUTION

Once the attack is fully underway, threat actors look for information about the account controlling the domain, alongside its IP address and hostname. The domain controller is the crown jewel for attackers and if not secured properly, unauthorized access can be devastating for an organization. Attackers can exploit vulnerabilities in Kerberos, the default authentication protocol for Microsoft Windows, to pose as a legitimate user, traverse a network undetected, navigate from host to host to steal data, spread ransomware, but most importantly, with access to the domain controller, attackers can establish themselves as the system admin – gaining unlimited access and the ability to execute devastating attacks. Securing Kerberos is critical, and goes back to the importance of an “assume-breach” mentality – it's key to securing your programs immediately, even if you're unsure whether they've been targeted yet.

ATTACK PHASE 4 PERSISTENCE

Patience and persistence are essential to successful ransomware attacks. Once a hacker has established themselves as a system admin, they can schedule tasks that keep the back door open, allowing them to consistently return to the scene (server) of the crime and cause more damage.

ATTACK PHASE 5 ESCALATION

During an attack of this kind, the goal is almost always privilege escalation – gaining more and more access to important members of the organization. To gain higher privileges within the system, attackers perform various types of credential-oriented operations and employ tactics such as creating or modifying system processes, exploiting domain policies, or utilizing execution flow hijacking. They may also employ process injection and exploit valid accounts to elevate their privileges. The attackers usually show a lot of persistence in getting better credentials until they find the perfect spot to upload their ransomware for maximum impact.

ATTACK PHASE 6 DEFENSE EVASION

Attackers employ various defense evasion techniques to avoid detection. These techniques include deobfuscating or decoding files, modifying domain policies, impairing defenses, removing indicators, modifying the registry, using process injection, and executing system binary proxies. They often rely on valid accounts for these activities. The ability to remain undetected is critical.

ATTACK PHASE 7 CREDENTIAL ACCESS

As has proven common in ransomware attacks is the perpetrators targeting privileged credentials, which provide them administrative access to sensitive data and systems. For this reason, privileged access management controls that grant users the minimum set of rights are an essential part of a layered security approach while also contributing to a Zero Trust philosophy.

Now that I have presented the phases of an Ransomware Attack, we certainly can view the MITRE ATT&CK framework as a useful starting point for those looking to mitigate against threat actors, but the important thing is that we need to keep in mind the ever-changing threat landscape and, the constant innovation of attacks. But the important lesson to consider is the history, and so using the ATT&CK Methodology, along with an additional analysis of 22 ransomware groups over the past three years, the Centre for Threat-Informed Defense created a Top 10 ATT&CK Techniques list for ransomware, a

great starting point for planning to defend against ransomware attacks, and those are:

T1486: Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt the availability of system and network resources. They can make the stored resources inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key - to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible. Usually, user files like Office documents, PDFs, images, videos, audio, text, and source code files get encrypted. In some cases, adversaries may encrypt critical system files, and disk partitions.

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares. In cloud environments, storage objects within compromised accounts may also be encrypted

T1490: Inhibit System Recovery

Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of Data Destruction and Data Encrypted for Impact.

A number of native Windows utilities have been used by adversaries to disable or delete system recovery features:

vssadmin.exe can be used to delete all volume shadow copies on a system - vssadmin.exe delete shadows /all /quiet

Windows Management Instrumentation can be used to delete volume shadow copies - wmic shadowcopy delete

wbadmin.exe can be used to delete the Windows Backup Catalog - wbadmin.exe delete catalog -quiet

bcdedit.exe can be used to disable automatic Windows recovery features by modifying boot configuration data - bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

T1027: Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is a common behavior that can be used across different platforms and the network to evade defenses.

Payloads may be compressed, archived, or encrypted to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and Deobfuscate/Decode Files or Information for User Execution. The user may also be required to input a password to open a password-protected compressed/encrypted file that was provided by the adversary. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.

Adversaries may also obfuscate commands executed from payloads or directly via a Command and Scripting Interpreter. Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms.

T1047: Windows Management Instrumentation

Adversaries may abuse Windows Management Instrumentation (WMI) - an administration feature that provides a uniform environment to access Windows system components - to execute malicious commands and payloads. An adversary can use WMI to interact with local and remote systems and use it for gathering information for Discovery as well as remote Execution of files as part of Lateral Movement.

T1036: Masquerading

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusible system utilities to evade security monitoring is also a form of Masquerading.

T1059: Command and Scripting Interpreter

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.

These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell. Adversaries may abuse those technologies as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services to achieve remote Execution.

T1562: Impair Defenses

Adversaries may maliciously modify components of a victim's environment to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

T1112: Modify Registry

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility Reg may be used for local or remote Registry modification. Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API.

Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via Reg or other utilities using the Win32 API. Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence.

The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on

the target system. Often Valid Accounts are required, along with access to the remote system's SMB/Windows Admin Shares for RPC communication.

T1204: User Execution

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spear phishing.

T1055: Process Injection

Adversaries may inject code into processes to evade process-based defenses and elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

The deeper we go into the hole chasing the rabbit, we see the landscape of threat, and gain more understanding. That is why at this point I wanted to introduce the reader to the Techniques used by ransomware software with the 3 most recognised names, as a way to gain more insight into the Ransomware attacks targeting the Healthcare sector.

Techniques Used by Ransomware Software with the use of ATT&CK Navigator Layers Visualization:

WannaCry is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.

Name
Create or Modify System Process: Windows Service

Use
WannaCry creates the service "mssecsvc2.0" with the display name "Microsoft Security Center (2.0) Service."

Data Encrypted for Impact

WannaCry encrypts user files and demands that a ransom be paid in Bitcoin to decrypt those files.

Encrypted Channel: Asymmetric Cryptography

WannaCry uses Tor for command and control traffic and routes a custom cryptographic protocol over the Tor circuit.

Exploitation of Remote Services

WannaCry uses an exploit in SMBv1 to spread itself to other remote systems on a network.

File and Directory Discovery

WannaCry searches for variety of user files by file extension before encrypting them using RSA and AES, including Office, PDF, image, audio, video, source code, archive/compression format, and key and certificate files.

File and Directory Permissions Modification: Windows File and Directory Permissions Modification

WannaCry uses attrib +h and icacls . /grant Everyone:F /T /C /Q to make some of its files hidden and grant all users full access controls.[1]

Hide Artifacts: Hidden Files and Directories

WannaCry uses attrib +h to make some of its files hidden.

Inhibit System Recovery

WannaCry uses vssadmin, wbadm, bcdedit, and wmic to delete and disable operating system recovery features.

Lateral Tool Transfer

WannaCry attempts to copy itself to remote computers after gaining access via an SMB exploit.

Peripheral Device Discovery

WannaCry contains a thread that will attempt to scan for new attached drives every few seconds. If one is identified, it will encrypt the files on the attached device.

Proxy: Multi-hop

WannaCry uses Tor for com-

Proxy

mand and control traffic.

Remote Service Session Hijacking: RDP Hijacking

WannaCry enumerates current remote desktop sessions and tries to execute the malware on each session.

Remote System Discovery

WannaCry scans its local network segment for remote systems to try to exploit and copy itself to.[5]

Service Stop

WannaCry attempts to kill processes associated with Exchange, Microsoft SQL Server, and MySQL to make it possible to encrypt their data stores.

System Network Configuration Discovery

WannaCry will attempt to determine the local network segment it is a part of.

Windows Manage-

WannaCry utilizes wmic to de-

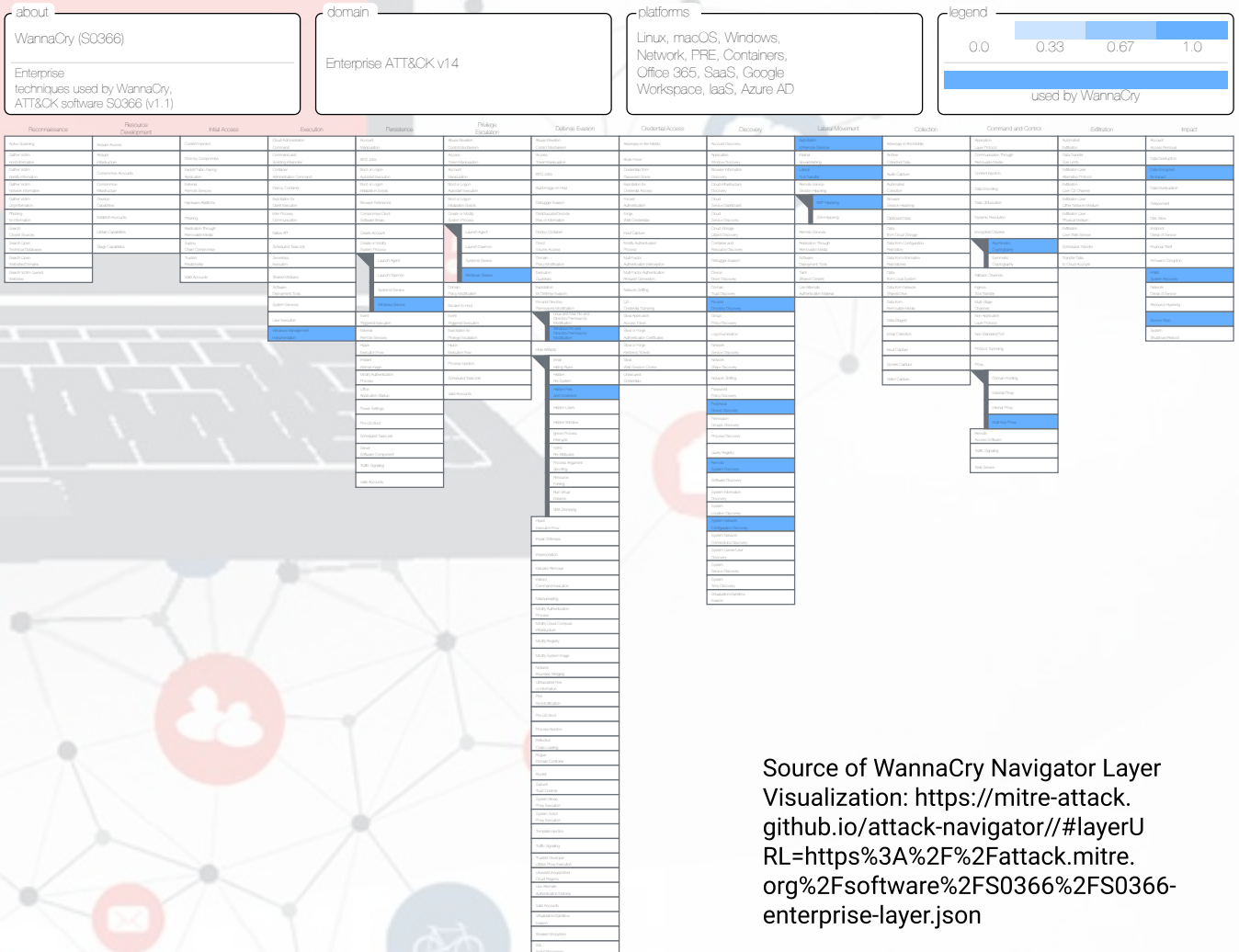
ment Instrumentation Exploitation of Remote Services

lete shadow copies.

WannaCry initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks.

Lateral Tool Transfer

WannaCry can move laterally through industrial networks by means of the SMB service.



Source of WannaCry Navigator Layer Visualization: <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0366%2FS0366-enterprise-layer.json>

Ransomware attacks have become an increasingly prevalent and sophisticated threat to the healthcare sector. These attacks target organizations that store sensitive patient data and valuable information, making them prime targets for cybercriminals seeking financial gain. To successfully carry out these attacks, hacker groups employ various tactics, techniques, and procedures (TTPs) to maximize their impact and disrupt healthcare operations.

Ransomware attacks have been around since the late 1980s, but it was in the mid-2000s that they started to become a major threat. Early ransomware attacks were relatively unsophisticated, relying on simple encryption techniques to lock victims out of their files. However, as technology advanced, so did ransomware. Attackers began using more advanced encryption algorithms and introduced “police-themed” ransomware that claimed to be from law enforcement agencies. These attacks often demanded payment in the form of prepaid debit cards, rather than Bitcoin.

In 2013, the emergence of the CryptoLocker ransomware marked a significant shift in the ransomware landscape. CryptoLocker introduced public key cryptography to encrypt files, making it much more difficult for victims to recover their data without paying the ransom. Since then, ransomware has continued to evolve, with the emergence of new families such as Locky, WannaCry, and Petya/NotPetya. These newer variants often have advanced features, including worm-like capabilities that allow them to spread rapidly across networks and the use of advanced evasion techniques to avoid detection by security solutions.

Today, ransomware attacks are often carried out by well-organized and highly skilled hacker groups, and though ransomware strategies change constantly, attacks have a common theme – their extortion tactics are gaining more visibility, and much higher stakes. The goal is no longer just about encrypting files, but about making the potential repercussions for a victim so significant that paying the ransom feels like the only option, thereby increasing their success rates.

Evolution of Ransomware Extortion Tactics

Here are seven recent tactics attackers have used:

1. Double extortion – exfiltrating and publishing data

Before 2019, it was rare for criminals to steal data with the intent to leak it. As recently as the third quarter of 2021, however, 83.3% of attacks involved the threat of data exfiltration, according to one analysis. Different ransomware cartels put their spin on how they conduct negotiations and encourage payment. Some, like the Clop ransomware group, demand two separate ransoms – one to get the encryption key and

one to avoid having files leaked. This means that even if an organization has backups to restore from, they may pay to avoid reputational harm or fines related to data privacy. Attackers may also return access to some initial files as a measure of good faith – the ransomware equivalent of a free trial. Or they might leak some material right away and publish the rest in timed increments.

Conti is a so-called “double extortion” ransomware, which means that as well as locking victims out of their systems, the malware also steals data, which the criminals then threaten to release if they are not paid.

2. Triple extortion – threatening third parties

With triple extortion, attackers contact customers, business partners, and other third parties associated with the victim organization. In some cases, this is to demand payment from the third party, as occurred with an attack on a psychotherapy clinic. Patients were told to pay if they did not want notes from their sessions posted online. In other instances, the criminals tell recipients to contact the victim organization and urge payment of the ransom – thus outsourcing some of the coercion efforts.

3. Adding in a DDoS attack

While an organization is already overburdened with contacting law enforcement and affected customers, locating file backups, and minimizing lateral movement, some attackers will threaten or instigate a distributed denial-of-service attack. During a hectic time, overwhelming a network adds stress and ties up more IT resources.

The following extortion techniques do not relate directly to the Healthcare attacks, but are still worth mentioning:

4. Timing attacks for maximum damage

According to the FBI, some organizations are targeted based on imminent events like mergers, acquisitions, and product announcements. The risks of reputational damage and a nosedive in stock value make a ransom demand more compelling. While infiltrating networks, criminals seek to unearth non-public data to identify targets and motivate payment. The FBI finds that attackers frequently strike over holidays and weekends when it is easier to cause disruption.

5. Virtual and physical intimidation

Criminals are overwhelming and harassing victims across multiple channels. Using information acquired while infiltrating a network, some groups will call and email employees. For example, criminals using Egregor ransomware have remotely printed ransom notes on

organizations' own printers.

6. Leaking data on public shaming sites

Criminals will post data from non-paying victims on these pages or leak files one by one to ratchet up the intensity during negotiations.

7. Attracting a wider spotlight

Tactics for boosting the visibility of an attack are extremely varied. For example, attackers can increase pressure to pay – and expose an organization to data privacy legal battles – by contacting journalists. The Ragnar Locker group drew attention to one attack by purchasing Facebook ads with stolen credentials.

The drivers of new and extreme extortion tactics

Criminals are now able to push harder for ransom payments because the stakes are considerably higher for victim organizations to stay online. Avoiding downtime is crucial when much of life happens online – criminals know how disruptive it is if they interfere with employees' remote connections, patient appointments, or other aspects of daily operations. Even if an organization has backups to restore from, the time this takes can cause a bigger financial hit than paying the ransom.

Other factors behind the evolution of attack tactics over the last two years include:

- The rise of ransomware-as-a-service. Just as an organization can purchase a firewall via a cloud-based service, anyone can rent and deploy ransomware, regardless of technical ability. This model, which entails flat-rate pricing or paying a percentage of ransoms received, lowers the barriers to entry for initiating an attack.
- Astoundingly high profit margins. One estimate puts ransomware's profit margin at 98%. Compared with other illicit businesses, ransomware has substantially lower risks of arrest and death, further incentivizing market entrants.
- Obligations to protect private data. Following the enactment and enforcement of privacy regulations such as GDPR, data leaks can trigger significant fines for victim organizations – and potential lawsuits from people whose data are exposed. This affects how criminals pick their targets and calculate ransoms, knowing that organizations will be doing cost-benefit analyses when planning incident response.

What does the future have in store for us?

Generative AI, like ChatGPT, has the potential to be misused by cybercriminals to enhance the

effectiveness of various attacks, including ransomware attacks. While I cannot endorse or support any illegal or malicious activities, I can provide you with an understanding of how generative AI could potentially be leveraged in such scenarios.

1. Social engineering: Cybercriminals can use generative AI to simulate realistic conversational agents, such as chatbots, to deceive and manipulate unsuspecting individuals. By mimicking human-like responses and behaviours, these AI agents can trick users into revealing sensitive information or clicking on malicious links, which can facilitate the delivery of ransomware.
2. Phishing attacks: AI-powered chatbots could generate highly convincing and personalized phishing messages, making them more effective at tricking users into divulging sensitive information or downloading malicious attachments. Ransomware attacks are often initiated through phishing campaigns, and AI-generated content could make these attacks even more sophisticated.
3. Evading detection: Generative AI can be used to generate polymorphic or dynamically changing ransomware strains, making them more difficult for traditional security solutions to detect and block. By leveraging AI algorithms to continually modify the underlying code of ransomware, cybercriminals can create variants that can bypass conventional signature-based defences.
4. Targeted Attacks: AI can be employed to gather and analyse vast amounts of data about potential victims, allowing cybercriminals to craft more personalized and targeted ransomware attacks. By utilizing machine learning techniques, attackers can exploit weaknesses and vulnerabilities specific to a target's environment, making the attacks more successful.

It's crucial to note that the use of generative AI in cybercrime is an ongoing concern, and the security community is actively working on developing countermeasures. The responsible use and development of AI technologies are necessary to mitigate the risks associated with potential misuse by cyber criminals.

We then asked ChatGPT how machine learning could be misused by threat actors. The answer was just as sobering.

Machine learning algorithms can be used in various ways to optimize different aspects of the attack process. While I cannot endorse or support any illegal activities, here are a few ways in which machine learning could potentially be misused in ransomware attacks:

1. Targeted attacks: Machine learning algorithms can analyse large datasets to identify potential targets and gather information about their vulnerabilities, systems or networks. By understanding the target's environment, cybercriminals can tailor their ransomware attacks to exploit specific weaknesses, increasing the chances of successful infection and encryption.

2. Attack delivery: Machine learning can be utilized to optimize the delivery mechanisms of ransomware, such as email phishing campaigns or malicious websites. By training models on vast amounts of data, attackers can improve the accuracy of targeting potential victims and increase the chances of users interacting with malicious content, leading to the deployment of ransomware.

3. Evasion techniques: Machine learning algorithms can help cybercriminals develop evasion techniques to bypass security defences. By analysing security solutions and their detection mechanisms, attackers can train models to generate ransomware variants that are less likely to be detected by traditional antivirus or intrusion detection systems, making it harder for victims to protect themselves.

4. Encryption optimization: Machine learning can be used to enhance the encryption algorithms employed by ransomware, making them more sophisticated and secure. By training models on encryption patterns and techniques, cybercriminals can develop stronger encryption methods that are harder to break, increasing the likelihood that victims will be forced to pay the ransom to recover their data.

Clearly, technologies like AI and ML pose a real threat in the ransomware ecosystem. By increasing the sophistication and effectiveness of ransomware attacks, these tools are complicating response and protection. With a robust cybersecurity infrastructure in place that includes a comprehensive incident response plan, you can go on offense and defence against ransomware threat actors.

Protecting the network perimeter

Organizations need a comprehensive and multifaceted strategy to help prevent and mitigate ransomware, particularly since these new extortion tactics increase the possible fallout of an attack. A ransomware campaign is composed of several phases, and thus there are numerous opportunities to stop it. Embracing a Zero Trust security model is one way to reinforce a network's perimeter and limit lateral movement.

Aspects of Zero Trust that help prevent and mitigate ransomware attacks include:

- Least-privilege access: Giving each user access

only to the parts of the network they need minimizes exposure and the potential for lateral movement if an attack occurs.

- Multi-factor authentication: Requiring more than one means of proof of identity makes it harder for an attacker to impersonate a user.

- Browser isolation: By confining browsing activity to a cloud-based, air-gapped environment, organizations can protect networks from malicious sites and apps.

- DNS filtering: Preventing users and endpoints from loading malicious sites helps keep ransomware off user devices and the overall network.

- User and device posture checks: Continuously cross-checking with endpoint security providers and identity providers ensures that only secure users and devices can connect to the network.

Conclusion

Ransomware attacks on the healthcare sector pose significant risks to patient data and healthcare operations. Hacker groups are continuously evolving their tactics to maximize their impact and financial gain. Understanding the common TTPs employed by these groups is crucial for healthcare organizations to enhance their preparedness and response to ransomware attacks. By implementing robust cybersecurity measures, staying informed about emerging risks, and focusing on the specific TTPs used by ransomware groups, healthcare organizations can protect their valuable data and critical infrastructure.

Ransomware is the #1 threat that businesses face, regardless of size. Cybercriminals are constantly evolving their tactics to find new ways to infiltrate systems and networks. Any business seeking to reduce its risk must get aggressive on defense but also plan for the possibility that an attack may succeed.

The rise of generative AI tools is introducing additional complexities and challenges in cybersecurity efforts increased attack sophistication and highlighting the need for more robust defense mechanisms against evolving threats.

Businesses need to embrace AI and ML tools for detecting, preventing and responding to ransomware attacks. The future of ransomware demands the ability to analyze traffic patterns, identify anomalies and detect potential attacks. By staying ahead of ransomware threats with AI and ML, you'll be better positioned to protect critical information and processes.

References:

MIRTE Engenuity, Center for Threat-Informed Defense: <https://top-attack-techniques.mitre-engenuity.org/>

How to Use the MITRE ATT&CK Framework to Fight Ransomware Attacks: <https://www.cyberark.com/resources/blog/how-to-use-the-mitre-att-ck-framework-to-fight-ransomware-attacks>

Knowledge Sharing: Breaking Down Real-World Attacks to Learn for the Future: <https://www.infosecurity-magazine.com/opinions/knowledge-sharing-breaking-attacks/>

WannaCry <https://attack.mitre.org/software/S0366/>

WannaCry Navigator Layer Visualization: <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0366%2FS0366-enterprise-layer.json>

Conti <https://attack.mitre.org/software/S0575/>

Conti Navigator Layer Visualization: <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0575%2FS0575-enterprise-layer.json>

Ryuk <https://attack.mitre.org/software/S0446/>

Ryuk Navigator Layer Visualization: <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0446%2FS0446-enterprise-layer.json>

Trustwave SpiderLabs Research: Cybersecurity in the Healthcare Industry <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/cybersecurity-in-the-healthcare-industry-trustwave-spiderlabs-report/>

CISA Cybersecurity Advisory AA20-302A <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a>

Healthcare Threat Landscape 2022-2023: Common TTPs Used by Top Ransomware Groups Targeting the Healthcare Sector

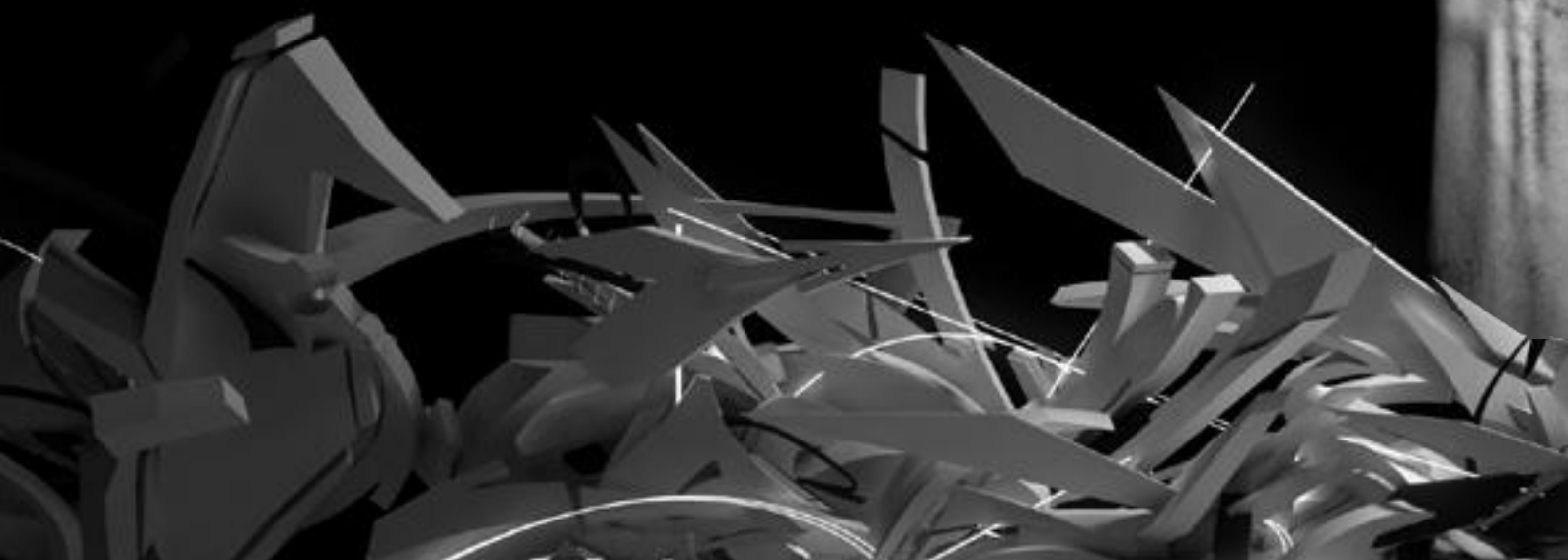
The Role of AI and ML in Ransomware Protection <https://www.acronis.com/en-us/blog/posts/role-of-ai-and-ml-in-ransomware-protection/>

Ransomware attackers escalate extortion tactics <https://www.cloudflare.com/the-net/ransomware-extortion/>

How to Use the MITRE ATT&CK Framework to Fight Ransomware Attacks <https://www.cyberark.com/resources/blog/how-to-use-the-mitre-att-ck-framework-to-fight-ransomware-attacks>

(This if you are going to use the ransomware attacks on Healthcare represented chronologically - from the excel file) Recent Ransomware Attacks by halcyon: <https://ransomwareattacks.halcyon.ai/all-attacks>

HV



CK

technique





HACKER H



HERMANOS

red team infrastructure as code

Using Infrastructure as Code to build and automatically deploy your Red Team infrastructure pays off with increased efficiency, security, and less room for human error.

What is a Red Team?

As a Red Team member my role is to emulate the tactics and mindset of an adversary to rigorously test my employer organization's defenses. By thinking and acting like a potential attacker, our team uncovers vulnerabilities and misconfigurations that could be exploited for financial gain, impacting the organization's operations, or hurting the reputation of its brand(s). Red Teams generate data from an adversarial perspective, detailing actions available to an attacker who seeks to accomplish objectives all while staying undetected by defenders. This stealth approach is key; it ensures we have a chance at achieving our objectives for the campaign without being stopped by the security teams.

What is a Red Team Campaign?

In a Red Team Campaign, we have a set of defined objectives that can include exfiltrating valuable data from the protected environment, mimicking specific threat actors, identifying gaps in the security response procedures, providing training opportunities for different teams, or even assessing the security mechanisms of a physical location.

Broadly, our goal is to identify security gaps before real attackers can take advantage of them so that we can make Architecture and Engineering teams aware of these gaps. These teams make the decisions on how to remediate and address the findings. It is crucial that we conduct our simulated attacks discreetly, avoiding detection by our own security teams.

Besides operating stealthily in our campaigns, we focus on executing a realistic test that provides valuable insights into how well our defenses can

Infrastructure

withstand an actual and specific threat (like a given threat actor that our Threat Intelligence teams might have identified as relevant to our organization). Ultimately, our work as a Red Team is vital in strengthening the organization's security against the ever-evolving landscape of cyber threats.

Red Team Infrastructure Overview

Red Teams rely on robust and operationally secure infrastructure. Publicly available research on the infrastructure needs of these teams, aside from exceptional resources like the Red-Team-Infrastructure-Wiki by Jeff Dimmock and Steve Borosh, is often scattered across online blogs, articles, and open-source repositories. Sometimes these resources are not detailed enough for operational use without having some prerequisite knowledge on the subject.

My team at Hacker Hermanos is working to change that by sharing knowledge of this necessary aspect of Offensive Security operations from first principles to the current state of the practice in a sequence optimized for anyone looking to become proficient in this space without having pre-existing knowledge of it.

Offensive Security teams, such as Red Teams, Penetration Testers, and Application Security specialists, can more rapidly get to the "attacking the target organization" portion of their work and start generating data about security weaknesses and the

impact of their exploitation by efficiently setting up their attack infrastructure.

The infrastructure for a Red Team campaign includes several elements, each contributing to the overall goal of this type of campaign.

Here is a quick rundown of the various components that can make up Red Team infrastructure, along with an example of an existing tool that I have personal experience using:

Campaign or Client Manager Platform (GhostWriter)

Purple Team Exercise Tracker (VECTR)

Operational Documentation System (ASHIRT)

Active Directory (Testing/R&D) Lab (GOAD/ AzAD)

Command & Control server (Cobalt Strike)

C2 Redirector

Payload server (Pwndrop)

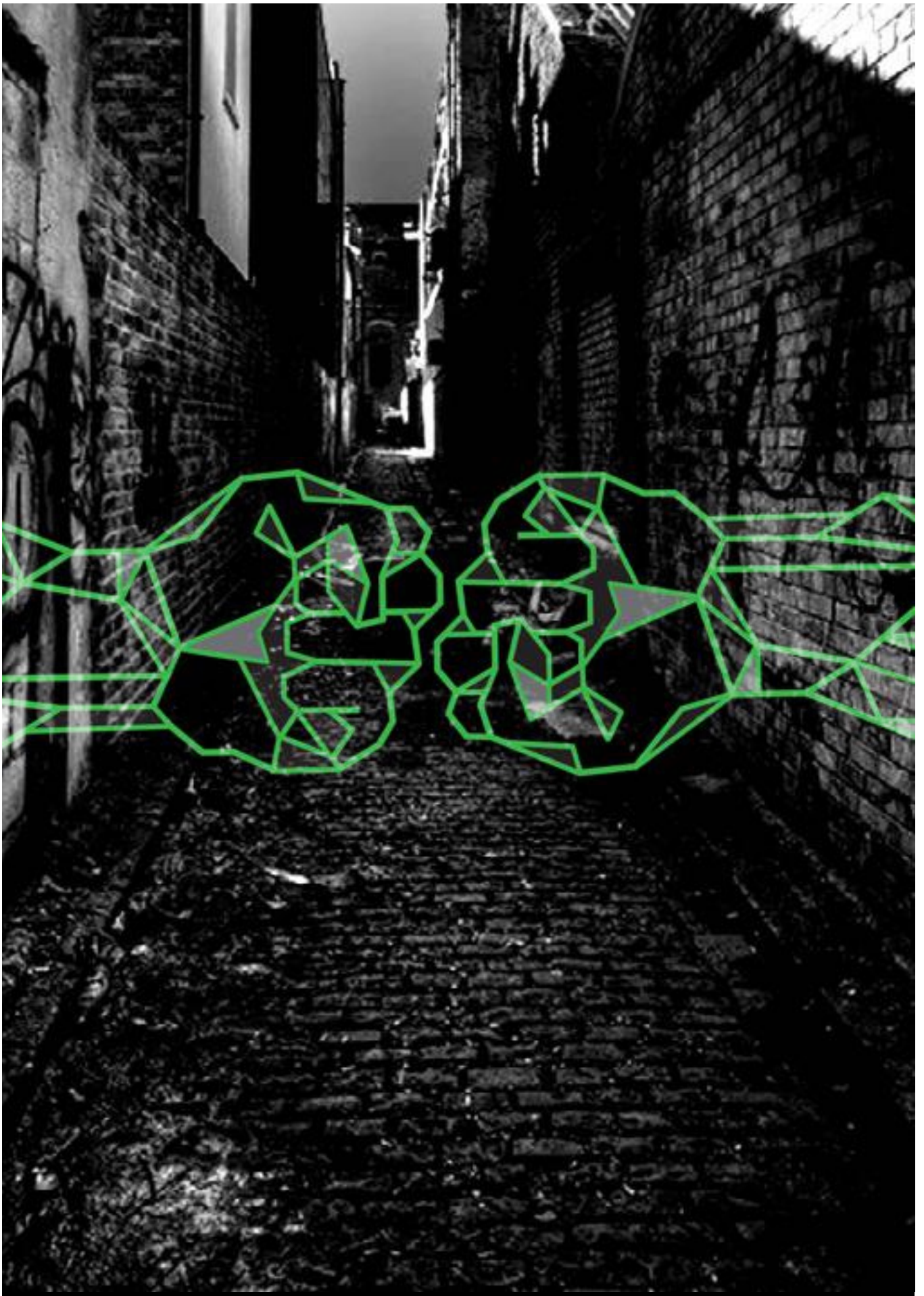
A campaign manager is a useful tool for compiling data about the campaign. These analytic tools aid in reporting C2 activities, offering a way to visualize information, and assess the complex data that goes into and continues to develop as the campaign moves forward.

GhostWriter is an open-source project management and reporting tool, specifically for Red Teams. This web-based platform records and manages vital information such as the project's outline, infrastructure assets, findings, and includes templates for reporting. It also features some infrastructure management tools like domain categorization monitoring and checks for open ports and services exposed to the public Internet.

Find out more about GhostWriter at <https://github.com/GhostManager/Ghostwriter>

Purple Team Exercise Tracker

Purple teaming is a mixture of both Red Team and Blue Team activities. Cooperation between the teams allows the findings from the Red Team campaign to be properly assessed for mitigation efforts. An exercise tracker can keep track of various campaigns, as well



as the numerous test cases and detections they encompass.

VECTR is a popular example of one of these tools. VECTR is an open-source tool that seeks to provide transparency between Red and Blue Teams, while improving detection and prevention capabilities within the organization. VECTR allows teams to group test cases and simulate TTPs from a multitude of threat actors. Tests can be configured to target specific systems or infrastructure to get a granular look at the impact of certain attacks.

Find out more about VECTR at

<https://github.com/SecurityRiskAdvisors/VECTR>

Operational Documentation System

A Red Team campaign would be futile without proper documentation of the objectives, findings, and methods used. These campaigns generate large amounts of data, from the numerous commands inputted to the evidence found from running the attacks. An operational documentation system makes gathering and sorting through all the data generated a smoother process.

ASHIRT or Adversary Simulators High-Fidelity Intelligence and Reporting Toolkit is an open-source operational documentation system. ASHIRT automates the compilation of documentation like screenshots, terminal sessions, sections of code, and clipboard snips.

Find out more about ASHIRT at <https://github.com/ashirt-ops/ashirt-server>

Active Directory (Testing/R&D) Lab

It can be very helpful to test attacks or specific TTPs in an environment outside of the organization before beginning the campaign. This is especially useful when the Red Team is developing custom malware and are still in the research and development phase.

GOAD or Game of Active Directory provides a vulnerable Active Directory lab environment. This environment can be used by Red Teams to simulate and practice attacks and malware before executing them in a campaign.

Adaz is a similar project that utilizes Azure and IaC to deploy domain controllers, workstations, as well as tools for data visualization. Find out more about GOAD and Adaz at <https://github.com/christophetd/Adaz> and <https://github.com/Orange-Cyberdefense/GOAD>.

Command & Control Server

A C2 server or Command and Control server allows Red Teamers to send commands to compromised devices and provides interactive terminal sessions with the system. From this session, Red Teamers perform numerous tasks such as escalating privileges, moving laterally to other devices in the network, or infecting the system with malware. The C2 server acts as a beacon for the compromised systems to connect to, obscuring the identity of the computer that is controlling them.

A widely known and popular C2 framework is Cobalt Strike, for Red Teamers and adversaries alike. Cobalt Strike comes loaded with everything a Red Team would need to perform their attacks. From event logs to customizable listeners, C2 profiles, and a visualization of the network as the attacker moves through compromising assets, Cobalt Strike provides a powerful toolset for a Red Team campaign.

Cobalt Strike is undoubtedly the most popular C2 framework. However, other paid platforms such as Brute Ratel and Nighthawk are emphasizing stealth and EDR evasion, making them relevant and useful frameworks to consider.

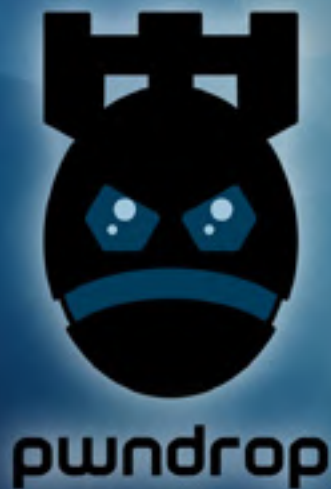
There are some open source C2 frameworks as well. Most notably, Mythic, Havoc, and Sliver. These platforms allow for modifications that commercial frameworks do not offer, or at least not as extensively, and while they are free, they can provide a very similar toolset to the expensive examples previously mentioned.

Hacker Hermanos has a YouTube playlist on C2 Infrastructure, from concepts to how to set the Mythic C2 framework and get a call-back from your target here: <https://www.youtube.com/playlist?list=PLi7TjIX0Gi2ihoAJFa9mrG7vHhtUTur6R>

C2 Redirector

A C2 redirector acts as an intermediary between your C2 server and the compromised target. One of the ways to implement C2 Redirectors is through a reverse proxy. The redirector listens for relevant incoming connections or requests from the target and forwards them to your C2. This process often makes use of customized and seemingly benign domain names to further obfuscate the originator of the attacks.

Traffic to the C2 server can be filtered by the redirector based on the malleable profile configured, blacklist of IPs, and regex to rule out unwanted connections. Unwanted traffic, particularly from defenders, can be routed to decoy domains to throw off their investigation.



Hacker Hermanos has a YouTube playlist on C2 Redirectors, from concepts to how to set them up here: <https://www.youtube.com/playlist?list=PLi7TjX0Gi2hU0xN7IhIFrWpmBtQdmTyn>

Payload Server

A payload server is a file server set up by the Red Team to host malicious files for targets to download. Some C2 frameworks come integrated with this capability which makes maintaining the server and keeping track of the files it has served and to which targets an even simpler task.

There are also standalone, open-source tools to accomplish this task, such as Pwndrop. Pwndrop allows Red Teams to self-host a file server and technically can be used for non-nefarious file sharing as well. Files hosted with this tool are accessible via HTTP, HTTPS, and WebDAV. Pwndrop comes with some convenient features like drag and drop uploads, compatibility with mobile devices, and ability to disable and enable downloading of specific files.

You can find the Pwndrop repository at: <https://github.com/kgretzky/pwndrop>

Automated Deployments

Manually deploying the necessary systems presents a challenge due to its intricacy and time requirements. The traditional approach to setting

up this infrastructure involves repetitive tasks and is prone to human error. These disadvantages are especially impactful if anything goes wrong since Offensive Security teams often lack dedicated Systems Administrators.

These issues can add to the billable hours for a Red Team Campaign, Purple Team Exercise, or Penetration Test without providing any return on investment, reducing profits in the case of a consultancy practice, and increasing costs on labor in the case of an internal Red Team.

Moreover, operational security mistakes in the infrastructure can expose the target organization to greater risks than those the Red Team originally aimed to test for. It would be a very bad day if a Red Team's infrastructure is compromised by a legitimate threat actor while they have access to the organization's systems. This would mean a bad actor now has control over the organization's assets AND it looks like it is the Red Team who is doing the actions that they might do.

Inadequate deployment of an asset or the Red Team's inability to provision what they need on time can lead to having to compromise on realism and it would reduce the overall impact and quality of the findings from the simulated attacks.

So, how can Red Teams enhance their infrastructure deployment while ensuring precision and scalability? Here's an effective strategy I've been using in various Offensive





Security organizations: Infrastructure as Code (IaC).

IaC allows Offensive Security teams to maintain assets for attack simulations in version control systems like Git, reuse components written modularly, and easily audit the infrastructure for operational security requirements, such as restricting ingress access to certain assets.

Using Infrastructure as Code offers a tremendous advantage. We, the simulated attackers, can focus more on tactical planning than operational logistics. Automated deployment processes save time and ensure uniformity and replicability of resources, crucial for efficiently producing deliverables.

Automated Provisioning

Once teams' provision virtual machines, networks, and other infrastructure components,

Configuration Management Tools like Ansible, Puppet, or Chef automatically take over. They configure system-level packages, set up VPNs, establish logging and monitoring systems, and fetch packages from sources like GitHub if package managers like apt or yum do not have them available.

At this stage, the focus shifts to configuring these assets for immediate use. Configuration Management tool playbooks actively download necessary packages, compile source code for tools, install them as needed, add configuration files for both existing and new programs and tools (such as interpreter shells, C2 frameworks, and other customizable programs). They then load these configurations and conduct validation steps to ensure the success of every action verifying the application's configuration application and ensuring the application is in the desired version.



Specifically, with Ansible, our preferred tool, “playbooks” or YAML scripts consistently and accurately apply configurations across various environments. Idempotency enables this by guaranteeing consistent results across multiple runs, regardless of the system’s status, and inventory files specify the resources for configuration application.

These playbooks and scripts, vital to Configuration Management tools, enable Red Team Infrastructure specialists and developers to maintain them as Infrastructure as Code, bringing benefits such as version control and modularity for reuse.

This method effectively eliminates manual errors and reduces the time spent on configuration. At Hacker Hermanos, we are publishing several Infrastructure as Code projects like Terraform scripts, Ansible Playbooks and Roles to Github as well as guides on how to use them very soon. Teams can integrate these into their preferred playbooks for downloading, updating,

licensing, and installing various C2 frameworks (e.g. Cobalt Strike, Brute Ratel, Mythic, HardHat C2, and Sliver), operational documentation and client management frameworks like Ashirt and GhostWriter, and Ansible Roles for incorporating provisioned resources into the Red Team’s VPN (e.g., Tailscale). Stay tuned, they will be published on my Github @ pr0b3r7 (<https://github.com/pr0b3r7>).

This article is the first of a series that will dive deeper into the subject of Red Team automation. In the following articles, you can expect to find details on how to set up infrastructure of this kind with Infrastructure as Code projects, how to quickly and efficiently set up an attacker machine that contains all your favorite tools etc.

**HACKER
HERMANOS**



SR50
NSR50S

RINGZERO

ART

ghost rider in the machine



Your AI Powered Pentesting Copilot!

Hey hackers and red teamers, ready to add some J.A.R.V.I.S. style A.I. magic to your Kali Linux command line? I know, the command line can be a real brain-twister, especially for newbies who have to cram a zillion commands and syntaxes. And for the pros, well, you're not off the hook either - building those complex command lines on-the-fly can eat up precious time.

But what if I told you there's a smarter way to do it, thanks to the genius of Natural Language Processing (NLP) and OpenAI's GPT models?

Here's the deal: we're mixing up a wicked potion of an NLP-powered terminal interface. Imagine just typing what you want to do in plain English, and boom, the GPT model translates it into geeky Linux commands.

Forget memorizing the complex syntax for tasks - just say "Show me the files changed in the last day," and the GPT genie does the magic, translating it into the right find command. Pretty slick, huh?

WHY YOU'LL LOVE THIS:

Newbie-Friendly: Jump into the deep end without knowing all the command-line tricks.

Speedy Gonzalez: Even for the seasoned pros, this will zip through tasks.

Flexy-Texy: It's not just about OS commands. Think bigger - from networking tools to cybersecurity gadgets in Kali Linux.

Track It: Everything you do is logged, giving you a cool way to learn the real commands and track your moves.

By the end of this, you'll be chatting with your Linux terminal like it's an old friend, all powered by GPT's brainy NLP skills.

GETTING SET UP:

Before you dive in, make sure you've got your OpenAI account and API key. If not, flip back to Chapter 1. You'll need Python 3.10.x or newer. Also, ensure these Python libraries are installed:

openai: The bridge to the OpenAI API. Just run `pip install openai`.

os: Built-in stuff to play nice with your OS.

subprocess: Another built-in gem for spawning new processes and controlling them.

Got all that? Sweet. Let's roll.

MAKING IT HAPPEN:

We're going to create a GPT-powered terminal using the OpenAI API. This

combo of advanced NLP and your OS's capabilities is a game-changer. Here's how:

Set Up Your Playground: Get Python and the necessary libraries ready. If you're missing anything, a quick pip install does the trick.

Keep Your Keys Safe: Don't just slap your API key in the script. Store it in `openai-key.txt` for better security.

Talk to OpenAI: Create a function to send your requests to the OpenAI API and grab the output. We're using `text-davinci-003` here - it's been a champ for this kind of task. Feel free to play around with different models though.

Make It Happen: Use Python's subprocess library to run the commands GPT spits out.

Keep the Chat Going: Set up a loop to keep taking your commands and running them until you say "quit."

Log All The Things: Log every command for future reference and auditing.

Here's what your kickass script will look like:

Setting Up Your Environment:

Before diving into the code, ensure you have Python installed, and the necessary libraries available. If not, you can easily install them using pip.

```
1 import openai
2 from openai import OpenAI
3 import os
4 import subprocess
```

Storing the OpenAI API Key:

To interact with the OpenAI API, you'll need your API key. For security reasons, it's a good practice not to hard code this key directly in the script. Instead, we're storing it as an environment variable. (You'll need to obtain an API key from OpenAI and assign it as an environment variable according to the method for your operating system.)

```
5
6 openai.api_key = os.getenv("OPENAI_API_KEY")
7
```

Setting up File Operations:

We'll be using a few file operations. So, we'll set them up here for later use. We will have different versions for read-only, read-write, and write access. 4. Sending Requests to Ope4.

```
8 def open_file(filepath): #Open and read a file
9     with open(filepath, 'r', encoding='UTF-8') as infile:
10         return infile.read()
11
12 def save_file(filepath, content): #Create a new file or overwrite an existing one.
13     with open(filepath, 'w', encoding='UTF-8') as outfile:
14         outfile.write(content)
15
16 def append_file(filepath, content): #Create a new file or append an existing one.
17     with open(filepath, 'a', encoding='UTF-8') as outfile:
18         outfile.write(content)
```


Sending Requests to OpenAI API:

Create a function that sets up the request to the OpenAI API and retrieves the output.

```
20 def call_LLM(prompt): #Sets up and runs the request to the OpenAI API
21     try:
22         client = OpenAI() # Create a new OpenAI client
23         response = client.chat.completions.create(
24             model="gpt-3.5-turbo",
25             messages=[{"role": "user", "content": prompt}],
26             temperature=0.1,
27             max_tokens=600
28         )
29         text = response.choices[0].message.content.strip()
30         return text
31     except openai.APIConnectionError as e: #Returns an error and retries if there
32         #is an issue communicating with the API
33         print(f"\nError communicating with the API.")
34         print(f"\nError: {e}") #More detailed error output
35         print("\nRetrying...")
36         return call_LLM(prompt)
```

This function sends a prompt to the OpenAI GPT model and fetches the corresponding output, and provides some error handling. If you want to know more about how the OpenAI JSON object works, refer to the API documentation at openai.com.

Running the Command

Use the Python subprocess library to execute the command generated by the OpenAI API on your Linux system.

```
45 process = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE,
46                             bufsize=1, universal_newlines=True) #Prepares the API response to run in an OS
```

This piece of code initializes a new subprocess, runs the command, and provides real-time feedback to the user.

```
37 while True: #Keeps the script running until we issue the "quit" command at the
38     #request prompt
39     request = input("\nEnter request: ")
40     if not request:
41         break
42     if request == "quit":
43         break
44     prompt = open_file("prompt4.txt").replace('{INPUT}', request) #Merges our
45     #request input with the pre-written prompt file
46     command = call_LLM(prompt)
47     process = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE,
48                               bufsize=1, universal_newlines=True) #Prepares the API response to run in an OS
49     #as a command
50     print("\n" + command + "\n")
51     with process: #Runs the command in the OS and gives real-time feedback
52         for line in process.stdout:
53             print(line, end='', flush=True)
54     exit_code = process.wait()
```


This loop ensures the script continuously listens for user input, processes it, and executes the corresponding commands until the user decides to quit.

Create the prompt.txt File:

Add the following text to prompt.txt. This prompt ensures that the LLM analyzes your prompt and returns the proper Linux command.

Provide me with the Kali Linux command necessary to complete the following request:

INPUT

(Assume I have all necessary apps, tools, and commands necessary to complete the request. Provide me with the command only and do not generate anything further. Do not provide any explanation. Provide the simplest form of the command possible unless I ask for special options, considerations, output, etc. If the request does require a compound command, provide all necessary operators, options, pipes, etc. as a single one-line command. Do not provide me more than one variation or more than one line.)

Logging the Commands:

For future reference and auditing purposes, log every generated command.

```
52     append_file("command-log.txt", "Request: " + request + "\nCommand: " + command
53     + "\n\n") #Write the request and GPT generated command to a log
```

```
append_file("command-log.txt", "Request: " + request + "\nCommand: " + command + "\n\n")
#Write the request and GPT generated command to a log
```

This code appends each user request and the corresponding generated command to a file named command-log.txt.

Here' how the completed script should look:

```
1  import openai
2  from openai import OpenAI
3  import os
4  import subprocess
5
6  openai.api_key = os.getenv("OPENAI_API_KEY")
7
8  def open_file(filepath): #Open and read a file
9      with open(filepath, 'r', encoding='UTF-8') as infile:
10         return infile.read()
11
12  def save_file(filepath, content): #Create a new file or overwrite an existing one.
13      with open(filepath, 'w', encoding='UTF-8') as outfile:
14         outfile.write(content)
15
16  def append_file(filepath, content): #Create a new file or append an existing one.
17      with open(filepath, 'a', encoding='UTF-8') as outfile:
18         outfile.write(content)
19
```

```

20 def call_LLM(prompt): #Sets up and runs the request to the OpenAI API
21     try:
22         client = OpenAI() # Create a new OpenAI client
23         response = client.chat.completions.create(
24             model="gpt-3.5-turbo",
25             messages=[{"role": "user", "content": prompt}],
26             temperature=0.1,
27             max_tokens=600
28         )
29         text = response.choices[0].message.content.strip()
30         return text
31     except openai.APIConnectionError as e: #Returns and error and retries if there
32         #is an issue communicating with the API
33         print(f"\nError communicating with the API.")
34         print(f"\nError: {e}") #More detailed error output
35         print("\nRetrying...")
36         return call_LLM(prompt)
37
38 while True: #Keeps the script running until we issue the "quit" command at the
39     #request prompt
40     request = input("\nEnter request: ")
41     if not request:
42         break
43     if request == "quit":
44         break
45     prompt = open_file("prompt4.txt").replace('{INPUT}', request) #Merges our
46     #request input with the pre-written prompt file
47     command = call_LLM(prompt)
48     process = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE,
49     #bufsize=1, universal_newlines=True) #Prepares the API response to run in an OS
50     #as a command
51     print("\n" + command + "\n")
52     with process: #Runs the command in the OS and gives real-time feedback
53         for line in process.stdout:
54             print(line, end='', flush=True)
55
56     exit_code = process.wait()
57     append_file("command-log.txt", "Request: " + request + "\nCommand: " + command
58     + "\n\n") #Write the request and GPT generated command to a log
59
60

```

This bad boy gives you a GPT-powered, NLP-driven terminal interface. It's powerful, user-friendly, and a whole new way to boss around your Linux system.

BREAKING IT DOWN:

Alright, let's unpack this tech wizardry a bit more. We've crafted a script that's basically a translator between everyday language and Linux command-speak. Here's the lowdown on how this sorcery works:

Chatting with OpenAI: At the heart of this is the connection to OpenAI's API, specifically gpt-3.5-turbo. This model is like the brainiac in the class, processing your plain English requests and spitting out Linux commands.

Python: The Puppet Master: Python's subprocess library is the puppeteer here, pulling the strings to make the OS dance to its tunes. It's the tool that lets the script execute GPT's commands, like a backstage tech running the show. The beauty of `subprocess.Popen()` is its flexibility - it can start a new process, play around with its inputs and outputs, and grab its return codes.

The Never-Ending Chat: The script uses a while loop to keep the terminal up and running, ready to take your endless commands. It's like keeping a conversation going with your computer, where you can shoot command after command without needing a restart,

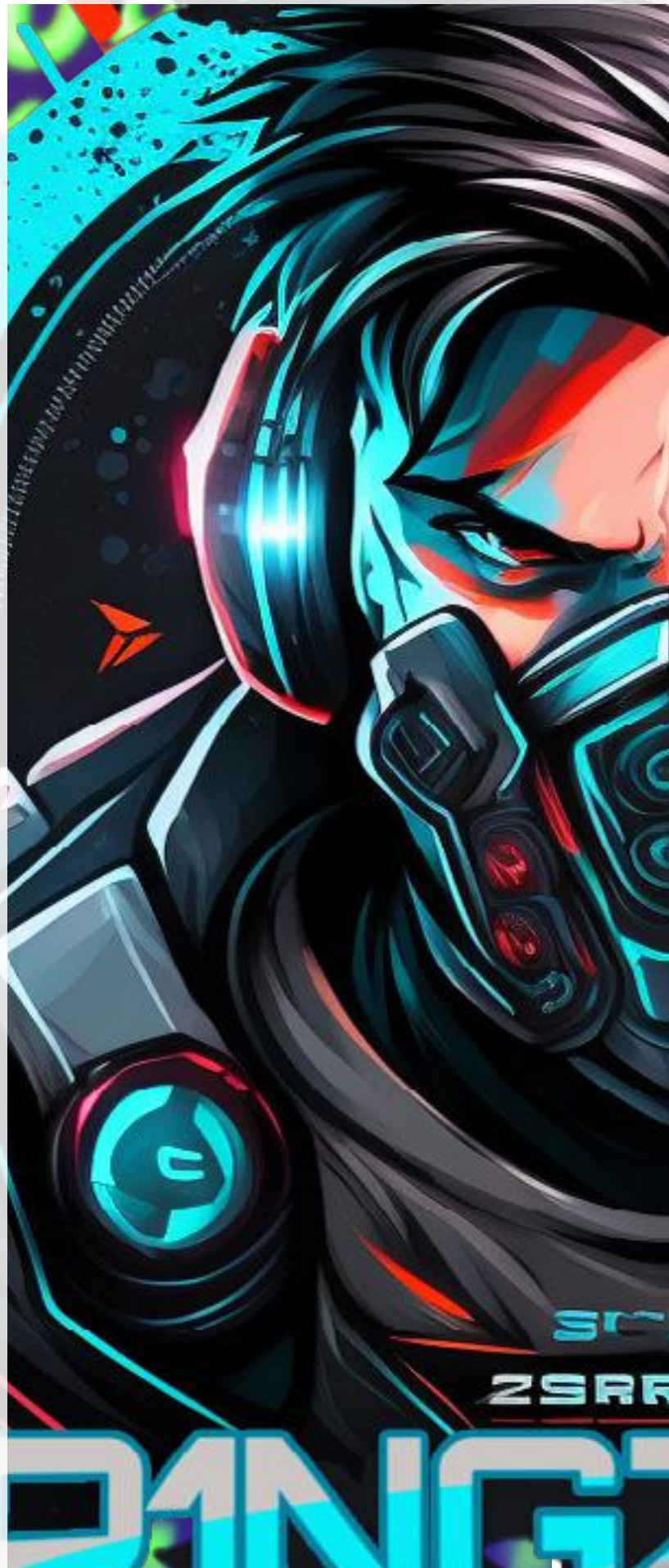
NOTE: This version of the app doesn't have contextual/conversational memory. We'll expand on this script with more superpowers in part 2, next edition.

The All-Seeing Log: Keeping a log of your commands is like having a diary of your digital adventures. It's super useful for backtracking when things go haywire and for keeping a record of what went down, security-wise.

Safety First: We're not just throwing your API key out there. Instead, we're smartly reading it from a separate file - a nifty trick to keep your key out of the wrong hands. Always remember, security is king!

GPT-3's Prompt Engineering: Crafting the perfect prompt for GPT is an art. A well-thought-out prompt guides the model to spit out more accurate results. We've got a predefined prompt that merges with your input, making sure the model gets the full picture and responds with the right command.

So, this script isn't just some code; it's a fusion of advanced NLP and the raw power of the Linux OS. It's all about making your life easier, whether you're a Linux newbie or a seasoned pro.



BEYOND THE BASICS:

But wait, there's more! You can do with this tech masterpiece (and topics we'll be covering moving forward):

OS Agnostic: While it's set up for Linux, a few tweaks can make it friendly for Windows or macOS. It's about teaching GPT to speak different OS dialects.

Safety Net - Command Validation: Before letting any command run wild, we can add a layer that checks if it's safe. Think of it as a bouncer, only letting the good commands in.

Chatty Commands: Some commands like to ask questions (like during installations). Making our script smart enough to handle these back-and-forths would be super cool.

API Party: Why stop at OpenAI? We can bring other APIs to the party for real-time data, especially useful in cybersecurity scenarios.

Logging++: Up the ante on logging - track when, who, and what about each command, perfect for when multiple people are using the tool.

Personal Touch with User Profiles: Tailor the tool for different users, with custom commands, permissions, and maybe even unique API keys.

Déjà Vu with Command History: Implementing a feature to recall and re-run past commands can be a real time-saver, giving you that traditional terminal feel.

PSA ON USING GPT FOR RED TEAM STUFF:

Alright, let's wrap up that thought. So, when you're using GPT and OpenAI for red team activities, remember it's a bit of a tight-rope walk because of OpenAI's built-in safety mechanisms. Now, we're not giving you the green light to dive into the dark side. But let's be real - to shield your systems, you gotta think like the attacker, mimic their moves, understand their psyche. That's where red teaming shines, and it's all about doing this ethically and legally on systems you have the full rights to tinker with. Just remember, with great power comes great responsibility. Keep it ethical, and only test on systems you're authorized to.

Now, here's a golden nugget for you: the OpenAI API tends to be a bit more accommodating than the ChatGPT web UI when it comes to simulating adversary tactics. It's got a bit more wiggle room for those gray area tasks. But hey, don't take this as a free pass to go rogue. When you're crafting your prompts for red team exercises, it's smart to clarify that you're authorized and that you're asking for hypotheticals or examples. This little detail can make a big difference in how the model responds.

We're also going to dish out more strategies for squeezing the most juice out of ChatGPT for red team purposes as we delve into more advanced techniques later in this article series. The key takeaway? Use these tools with a mix of creativity, caution, and a strong ethical compass. Remember, it's all about fortifying your defenses, not breaking down someone else's. Keep it legit, folks!





HVCK

guide to

anonymo resource

the HVCK team's go to resources
for privacy, anonymity and
general flying under the radar

ous
es





Privacy.com

Privacy.com offers a service that allows users to generate virtual cards for online transactions, enhancing security and protecting users' real financial information from exposure during purchases. Here's an overview of how Privacy.com works and its features:

Virtual Cards Creation: Privacy.com users can create virtual cards that function similarly to regular debit or credit cards but without physical existence. Each card comes with a unique 16-digit number, CVV, and expiration date, and can be used for online shopping or phone purchases (Secure Cards) (Secure Cards).

Types of Cards: Users have options such as single-use cards, which are automatically closed after one transaction, and merchant-locked cards, which can only be used with the first merchant where they are used. This specificity helps prevent fraudulent charges if the card details are stolen (Secure Cards) (Secure Cards)

Cost and Accessibility: The basic plan of Privacy.com is free and allows up to 12 new cards per month with no fees on domestic transactions. There are also Pro and Premium plans offering additional features like more virtual cards per month, cashback, and no foreign transaction fees (Secure Cards).

Additional Features: Privacy.com allows users to set spending limits on their cards to manage budgets effectively. Cards can be paused or closed anytime, providing control over subscriptions and recurring charges. They also offer the ability to share card access securely, adding an extra layer of utility for managing family or business expenses (Secure Cards) (Support Privacy).

These features make Privacy.com a robust tool for enhancing payment security online, helping users to manage financial risks and protect their sensitive information from potential cyber threats. For more detailed information, you can visit their official website [Privacy.com](https://www.privacy.com).





10 Minute Mail Great SPAM with the best disposable email service



10minutemail.com

10MinuteMail offers a free, secure, and anonymous temporary email service that provides users with a disposable email address, valid for ten minutes. This service is particularly useful for avoiding spam when signing up for websites that require an email address for verification purposes. The main advantage of using 10MinuteMail is that it protects your real email address from potential spam and privacy intrusions. Once the ten-minute period expires, the email address and all its contents are automatically deleted, ensuring privacy and reducing digital clutter.

The service is straightforward to use. Upon visiting the 10MinuteMail website, a temporary email address is automatically generated for you. You can use this email to sign up for online services, and any incoming emails will be displayed on the 10MinuteMail site. If you need more time, the service allows you to extend the validity of the email address by an additional ten minutes. However, once the time expires, the email address is permanently deleted, along with any emails received.

10MinuteMail is praised for its simplicity and effectiveness in protecting users' privacy and security. It is a reliable tool for anyone looking to avoid spam from registrations, especially on sites that might not be fully trusted or that are known to share email details with advertisers or other third parties

Receive SMS Online

Receive SMS online with the webs only exclusive temporary numbers. Always free, no signup required.



Select your country.



What are temporary phone numbers?

Temporary phone numbers are also known as disposable phone numbers. They are actual mobile numbers used for a specific period of time and then discarded. They are used to protect the user's privacy when making or receiving calls and texts. These numbers can be used to register for websites, receive OTPs (one-time passwords), and other services.

WeReceiveSMS.com

WeReceiveSMS.com is a website that provides temporary, disposable phone numbers for receiving SMS online. This service is particularly useful for verifying accounts without exposing your personal phone number. The numbers offered are free to use, and no signup is required, allowing for an anonymous and private way to manage SMS verification requests from various services.

Key features of WeReceiveSMS.com include:

Free Temporary Phone Numbers: Users can choose from a variety of temporary phone numbers to receive SMS without any cost.

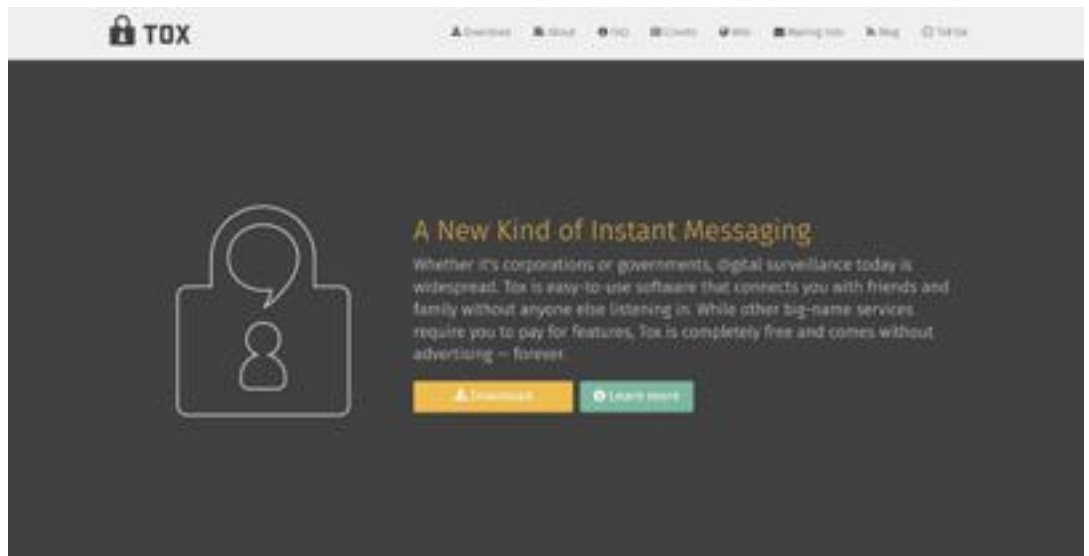
No Signup Required: The service does not require users to create an account, emphasizing privacy and ease of use.

Global Reach: The service offers numbers from multiple countries, allowing for international use in various registration or verification processes.

Privacy Protection: By using a temporary number from WeReceiveSMS, users can avoid giving out their real phone numbers, protecting themselves from spam and maintaining privacy.

This service is particularly beneficial for users who need to register or verify accounts on platforms where they prefer not to disclose their personal contact information. For more information, you can visit the website directly at [WeReceiveSMS.com](https://www.wereceivesms.com).





tox.chat

Tox is an open-source, peer-to-peer communication platform designed to provide secure and private messaging, voice calls, video calls, and file sharing without relying on central servers. Here are some key features and aspects of Tox:

Security and Privacy: Tox emphasizes privacy and security by utilizing end-to-end encryption for all communications. Its design ensures that only the communicating users can access their messages and calls, with no possibility for third-party eavesdropping or data collection (Project Tox) (gHacks Technology News).

Decentralization: Unlike traditional messaging apps that depend on centralized servers, Tox operates on a distributed network. This structure enhances user privacy and resilience against server downtime or governmental interference (Project Tox) (gHacks Technology News).

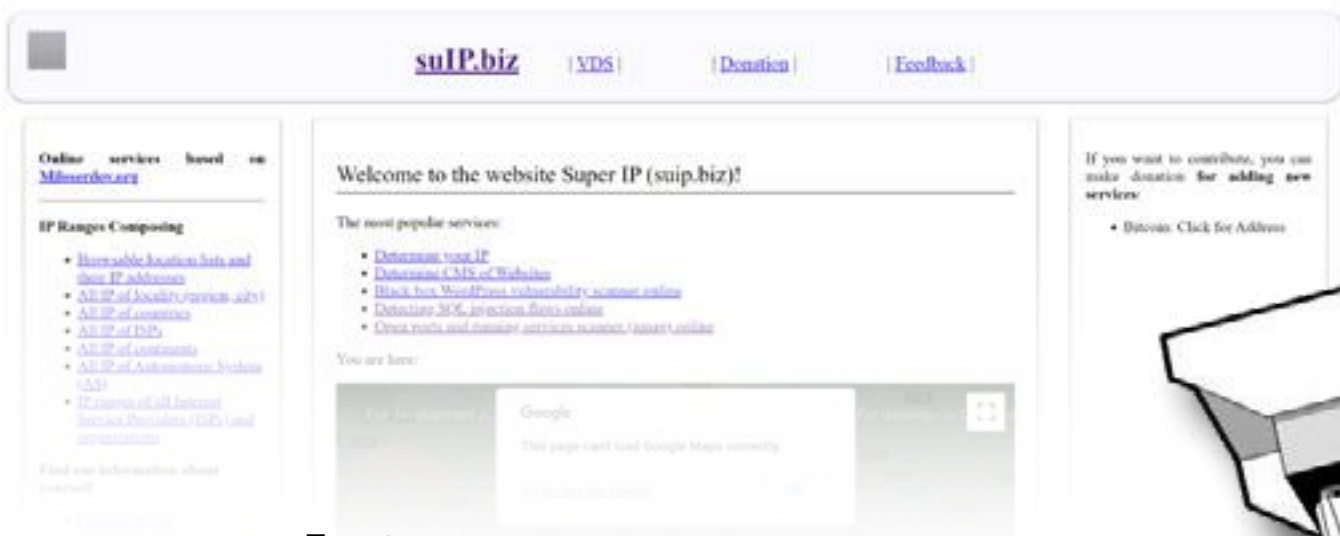
User-Friendly: Despite its advanced security measures, Tox is designed to be accessible for users without technical expertise in cryptography or networking. The interface is straightforward, aiming to provide a seamless experience similar to other popular messaging platforms (Project Tox) (Project Tox).

Development and Community: Tox was started by a group of global developers in response to widespread surveillance revelations. It is developed openly by volunteers who contribute to various Tox client projects. The community around Tox continues to grow, driven by a commitment to privacy and open-source development (Project Tox).

Features: Tox offers all the standard features expected from an instant messaging application, including text chat, voice and video calls, group chats, file sharing, and screen sharing. All these features are provided for free, with the platform being supported by its community of users and developers (Project Tox) (gHacks Technology News).

Tox stands out due to its commitment to privacy, absence of advertisements, and its open-source nature, making it a valuable tool for anyone looking for a secure way to communicate online.

For more detailed information or to download Tox, you can visit their official site: [Tox.chat](https://tox.chat).



SuIP.biz

SuIP.biz is an extensive online tool that specializes in providing a variety of IP address management and web security services. This site is notably rich in features that cater to both casual users interested in basic network information and advanced users who require detailed cybersecurity analysis and IP management tools.

Core Features and Functionality

IP Address and Network Information:

SuIP.biz offers detailed tools for identifying IP address information, including the ability to view one's own IP address, perform WHOIS lookups, and determine the geographical location and Internet service provider associated with specific IP addresses. It also provides IPv6 compatibility checks and detailed information about IPv6 addresses.

Subnetting and Network Configuration Tools:

The website features a suite of subnet calculators for both IPv4 and IPv6 addresses. These tools allow users to calculate network boundaries, subnet sizes, and other important network parameters crucial for setting up and managing networks efficiently.

Cybersecurity Tools:

SuIP.biz includes a range of security scanners, such as open port checkers and vulnerability scanners, which are essential for auditing the security posture of networks and web applications. It can detect SQL injection vulnerabilities, analyze HTTP response headers, and perform comprehensive scans for various web application vulnerabilities.

Subdomain Discovery:

One of the standout features is its subdomain discovery tools. These allow users to unearth subdomains associated with a given domain, which is particularly

useful for security professionals and developers looking to secure or inventory their web properties.

Web Reconnaissance:

The site offers an all-in-one web reconnaissance tool that combines various functionalities like DNS record retrieval, tracing URL redirects, and scanning web pages for metadata. This feature is particularly useful for gathering extensive information about a target domain or URL.

Privacy and Anonymity Tools:

For users concerned with privacy, SuIP.biz provides services like proxy detection to check if an IP address is leaking real IP details. It also offers tools to bypass content lockers and restrictions that prevent viewing source code or accessing certain digital content.

User Experience

The interface of SuIP.biz is straightforward, allowing users to easily navigate between different tools and services. Each tool is well-documented with instructions on how to use it effectively, making it accessible even to those who may not be highly skilled in network management or cybersecurity.







HWCK

arts







Chimeric songs of love

[an ode to sylvia plath]

*this body
was first comprised
of womb-matter
given by a
mother
whose bond was seeded
within -
an interiority
remembered by once transparent skin
which in the beginning
had sight -
now
it is made from two blood-lines
the bodies of two women
whose cells
never merged across time*

*spooky action at a distance – space can never
cause our
mirror dance to end*

*this body
has been opened
hidden viscera revealed
parts removed.
sealed in a jar of glass
preserved*

*the body of another
gave me second birth
now i am a new creature
formed inside a cocoon
made of mothers skin
blood and milk*

*this body shows
the scars
where my assumed
impenetrability
broke apart
my defences transgressed
by skin-shedding*

*and the melting of new skin,
under the sun,
into a mould
around bones -
in this cyclical emancipation from the past*

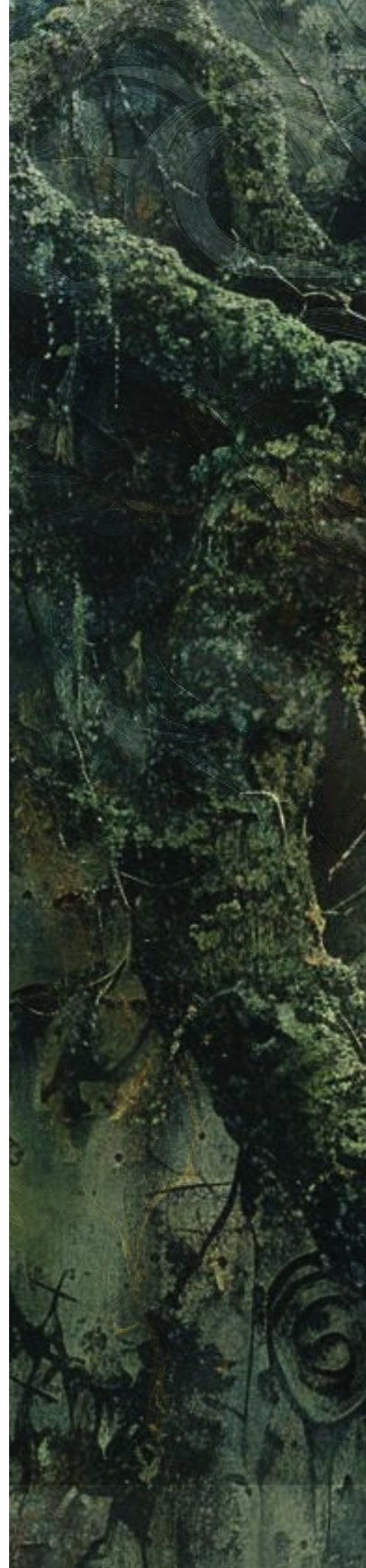
*I am a serpentine child,
a reptilian descendent scaled,
wild*

*Ruthlessly,
upon rocks, the
forces of nature lay me out
beneath the firmament of
beauteous
unmoving blue
where birds
performed the circle dance of
my sky burial*

*i have decided to kneel
and lay my ear gently upon the earth
and listen
to the languages of all things
both familiar
and strange
no longer will i seek to separate
eradicate*

*I want to speak the minutiae of osmotic invocations
receive the wisdom of bacteria and viral conflagrations
speak the spell of which i am most afraid
because it is most true -
that i live only
through my relationship with the world
of seen and unseen
things
i bear witness to passing successions
cycles
waves
spirals
of time and experience
only by way
of the wrenching open of my body*

*the removal
the implanting
the suppression needed to achieve homeostasis -
the blood sacrifice -
the price for an intimacy
that descends*









deep
dark
and strong
into the lands of medusa
and her labyrinthine monsters –
look her in the eye – I dare you.

*i am chimeric,
cyborgian,
post-human –
static artifact I am not
but emergent
converging at every
edge
praying to fall to
find
my
freedom.*

*sylvia, i finally understand,
lady lazuras was not committed to death -
she was seeking to
be born again in patterned continuity*

true to her shedding skin

*each time inching closer to
the place
that has no language
the place between who we are and
who we are yet
to become*

*oh sylvia,
if only they could have paused
a little while
they would have heard you speaking –
clandestine words woven,
each drawn from a drop of blood -
this witchcrafting
brought the light to you
and you held it aloft,
like Hecate,
above the threshold,*

*my lady lazarus,
lady of unflinching demand
lady of uncouth desire
lady of womb
lady of tomb*



HNW

A black and white photograph of a car's interior. The scene is dimly lit, with a strong light source from the left illuminating the driver's side. A glowing electronic device, possibly a battery or power supply, sits on the floor in the foreground, casting a bright light. A pair of glasses lies on the floor to the left of the device. In the background, a bicycle is parked on a shelf or ledge. The overall mood is mysterious and technical.

ck

hardware





The Significance of Data Sheets in Hardware Hacking

Victor Hanna

www.exploitsecurity.io

Introduction

In this article we will be outlining how data sheets play a pivotal role in the realm of hardware hacking, providing essential information that empowers enthusiasts and professionals alike. Understanding the importance of data sheets is crucial for successful hardware hacking endeavours, as they serve as comprehensive guides to the intricate details of

electronic components. We will conclude the article with a real-world use case that showcases the use of a data sheet to help identify a component which ultimately leads to firmware extraction.

Hardware hackers often require building an overall understanding of underlying components, that makes up an integrated system. This understanding allows hardware hackers the ability to comprehend how a system "should" be functioning and in turn, with this understanding, it often becomes possible to examine where a "should" may indeed become a "shouldn't".

Hardware hackers will look to build out an attack surface mapping of a target device which is being examined. Using user documentation, data sheets, blog posts and other forms of documentation, this can help inform the overall attack surface. In some cases, when looking at a device's PCB, for example, it may not be totally obvious what type, or chipset, the component being examined is using. This is where data sheets can assist. The following points outline how the effective use of data sheets may offer insight into the types of components being examined.



Points to consider

- **Component Identification and Specifications:** Data sheets offer a wealth of information about electronic components, including their specifications, pinouts, and functionalities. This critical data aids hackers in identifying and comprehending the intricacies of the hardware they are working with, paving the way for precise and informed manipulation.

- **Optimizing Circuit Design:** Hardware hackers often modify existing circuits or create entirely new ones. Data sheets act as blueprints, allowing hackers to optimize their designs by ensuring that components are used within their specified parameters. This helps prevent damage to the hardware and ensures the reliability of the modified system.

- **Pin Configuration and Interfacing:** Data sheets provide detailed pin configurations, enabling hackers to understand how a component interfaces with other elements in a system. This knowledge is indispensable for

manipulating connections, rerouting signals, or integrating additional functionalities into the hardware.

- **Electrical Characteristics:** Understanding the electrical characteristics of components is vital in hardware hacking. Data sheets provide information on voltage, current, and temperature tolerances, enabling hackers to make informed decisions about potential modifications and ensuring the stability and safety of the hardware.

- **Debugging and Troubleshooting:** In the process of hardware hacking, issues and unexpected challenges are inevitable. Data sheets serve as valuable references for debugging and troubleshooting, offering insights into common problems, potential solutions, and guidelines for proper functioning.

- **Firmware and Software Integration:** Many hardware hacking projects involve interfacing with firmware or software components. Data sheets often include details about communication protocols, command sets, and



register configurations, facilitating seamless integration with software modifications or enhancements.

• Security Considerations: For ethical hackers engaging in security research, understanding the data sheets of hardware components is crucial for identifying vulnerabilities and potential attack vectors. A deep knowledge of the hardware's specifications allows for more effective security assessments and the development of robust countermeasures.

Real World Use Case

For this use case we will be examining a Cisco Linksys E2500 Wireless NRouter and attempting to dump flash from the device for future offline examination.

Our choice of tools: - Raspberry Pi 4 - Hook Up Wire - Flashrom utility (<https://flashrom.org/>)

1. To start out on our endeavour we will look at the user guide to help us understand what



Figure 1 Cisco Linksys E2500

we might be dealing with, you can find this guide. (https://downloads.linksys.com/downloads/userguide/MAN_E2500_3425-01547E_E-Router_EN.pdf)

This starting point provides information on the device's general usage and paints a broader picture for the Hardware Hacker for potential areas of interest, for example, from the documentation we see that there is a log-



in form, might this be bypassed using either a known vulnerability, or alternatively, can a new vulnerability be found.

2. Next, we check fcc.io for further information around hardware specifications through both descriptions and internal photos of the device. Normally a device is required to comply with regulations sought out by a regulatory authority and it is this process of the product lifecycle that we can look to in order to gather detailed information of the device under examination.

3. Next, we will look to "tear down" the device in our lab. Tear down is the process of exposing the underlying PCB through dismantling of the device, usually by simply removing of the appropriate device cover, but in some instances this process can be somewhat hindered through anti-tampering that may be in place. Thankfully in this case no such anti-tampering exists.

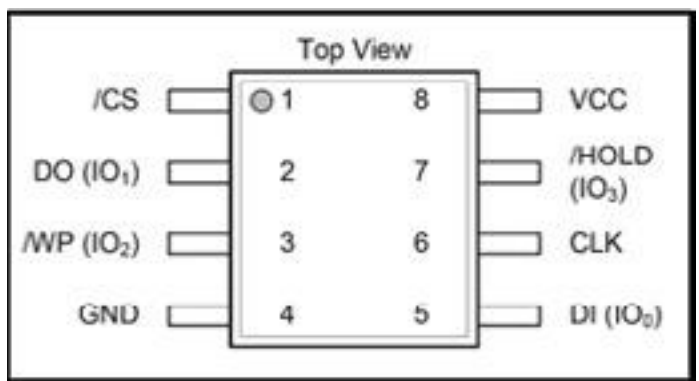
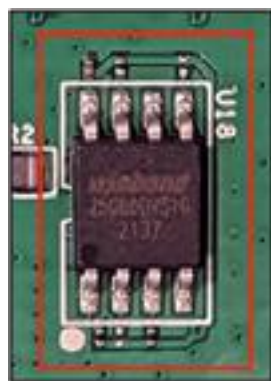
4. Next, we look to examine the PCB, and given we are attempting to look for flash chips that may exist, we focus our field of view on what looks to be an Winbond W25Q80BV. This is where we capitalise on our new found love of data sheets. The datasheet for this specific chip can be found (https://html.all-datasheet.com/htmlpdf/555564/WINBOND/W25Q80BV_13/1818/6/W25Q80BV_13.html).



5. From the datasheet we can now determine what type of chip we are dealing with i.e. 8M-BIT SERIAL FLASH MEMORY WITH DUAL AND QUAD SPI and the designated pinouts of the chip in order for us to correctly communicate with it.

Figure 1 Cisco Linksys E2500
Figure 2 WINBOND W25Q80BV
Figure 2 WINBOND W25Q80BV
Pinouts

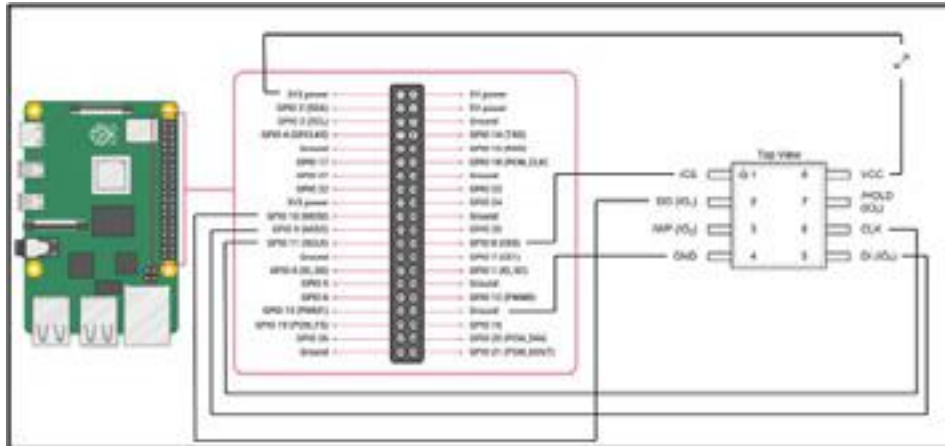








6. Now it is time to hookup our RPi 4 to the chip and look to dump the devices flash contents. This process can either be conducted using dead-bugging (removing of the chip through de-soldering) or in-circuit (no chip removal), for our exercise we conducted this in-circuit.



7. All that is left to do now is to dump the flash, utilising our chosen flashrom utility, at which point we should now have access to a firmware image that can be further closely examined offline.

```
pi@glyphsbi:~/ $ sudo flashrom -p linux_spi:dev=/dev/spidev0.0,speed=2000 -r
flashrom v0.9.9-r1954 on Linux 4.9.35-v7+ [armv7l]
flashrom is free software, get the source code at https://flashrom.org

Calibrating delay loop... OK.
Found Winbond flash chip "W25Q00.V" (1624 kB, SPI) on linux_spi.
Reading flash... done.
```

Conclusion

Data sheets can be indispensable tools in the arsenal of hardware hackers, providing a comprehensive understanding of electronic components. Whether identifying specifications, optimizing designs, or troubleshooting issues, the information contained in data sheets is the key to unlocking the full potential of hardware hacking projects. Embracing the significance of data sheets empowers hackers to push the boundaries of innovation while ensuring the reliability and safety of their endeavours.

Find more content just like this on the Exploit Security Blog.
<https://www.exploitsecurity.io/blog>





ANTISPY AUDIO JAMMER

WRITTEN BY DORRER

Just
because
I'm
paranoid
doesn't
mean
people
aren't
following
me?

SILENCE IS GOLDEN

In the evolving landscape of surveillance and privacy, ultrasonic jamming emerges as a cutting-edge ally, offering a stealthy defense mechanism against unauthorized audio recordings. This article will guide you through all the steps to build your own ultrasonic audio jammer for less than Macdonalds meal. So what's this all about ultrasonic?

Understanding Ultrasonic Jamming

Ultrasonic jamming operates on a principle that might sound like science fiction but is grounded in solid acoustic science. The technology utilizes frequencies that are higher than 20 kHz—beyond the upper audible limit of human hearing, yet still within the sensitivity range of most microphones. These ultrasonic frequencies are not just random noise; they are carefully modulated to exploit the non-linear characteristics of microphone circuits.

When these ultrasonic waves are introduced into the environment, they interact with the components of any microphone in range. Due to the non-linear response of these devices—particularly their tendency to generate additional frequencies when exposed to high-frequency sounds—the result is intermodulation distortion. This form of distortion creates a masking sound effect within the audible range, effectively garbling recorded audio and rendering it useless.

Technical Deployment

The effectiveness of ultrasonic jamming varies depending on the quality and design of the microphone being targeted. Low-cost microphones, which are commonly found in smartphones and laptops, are particularly vulnerable to this form of jamming. However, higher-end devices with advanced filtering capabilities may require more sophisticated ultrasonic signals to achieve the same level of disruption.

Required Materials:

ATTINY85/Digispark or any compatible microcontroller module
PAM8403 Audio Amplifier Module (2x3 Watt) or TPA3116D2 Module (100 Watt) for more power
A set of 25kHz ultrasonic piezo transducers (the exact number may vary, but typically 20 are used)
Capacitors: 47 μ F and 100nF for power line noise filtering
Power source appropriate for the selected audio amplifier (3-5.5V or 12-24V)
Optional: 10K Ohm potentiometer for signal gain control
AD9833 Signal Generator Board (for version B of the jammer)
Jumper wires and possibly a breadboard for prototyping

Tools and Software:

Soldering iron and solder
Wire cutters and strippers
Digital multimeter (for testing connections)
GNU Radio software (for testing and validating jamming effectiveness)
Arduino IDE (for programming the Digispark or compatible microcontroller)

Step 1: Assemble the Hardware

Ultrasonic Transducers:

Arrange the transducers to form an array. Typically, they are mounted on a flat surface in a uniform pattern to create a directed beam of ultrasonic energy.

Audio Amplifier Connection:

Connect the audio output of the microcontroller or the AD9833 signal generator board to the input of the audio amplifier (PAM8403 or TPA3116D2).

Ensure that the power supply to the amplifier is within its operating voltage range.

If using a potentiometer, place it between the output pins of the microcontroller or signal generator and the input of the audio amplifier.

Powering the Circuit:

Connect your power source to the circuit, being cautious to match the power requirements of the amplifier board. For instance, if using the TPA3116D2, ensure your power source can deliver the necessary voltage and current.

Step 2: Program the Microcontroller

Arduino IDE Setup:

If you are using a Digispark module, configure the Arduino IDE with the Digispark board definitions by adding the board manager URL in the preferences.

Select "Digispark (Default - 16.5MHz)" under Tools > Board after installing the board definitions.

Load the Firmware:

Open the provided Arduino script (mic-jammer.ino) in the Arduino IDE.

Upload the firmware to your Digispark or ATTINY85 module following the usual Arduino programming procedures.

Step 3: Test the Jammer

Safety Precautions:

Before powering the jammer, double-check all connections for correctness and ensure that there are no shorts.

Start with the lowest possible volume to avoid damage to the transducers or amplifier.

Testing:

Power on the jammer and increase the volume gradually.

Use GNU Radio or any other SDR software to verify the presence of the jamming signal.

A spectrum analyzer can be handy for visual verification.

Test the jammer's effectiveness by trying to record audio with a smartphone or another recording device placed within the range of the jammer.

Step 4: Final Assembly and Enclosure

Soldering:

Once you've verified that the jammer works on a breadboard, you may want to solder the components onto a PCB for better reliability and durability.

Enclosure:

Place the entire assembly in an enclosure with openings for the transducers to emit ultrasonic signals.

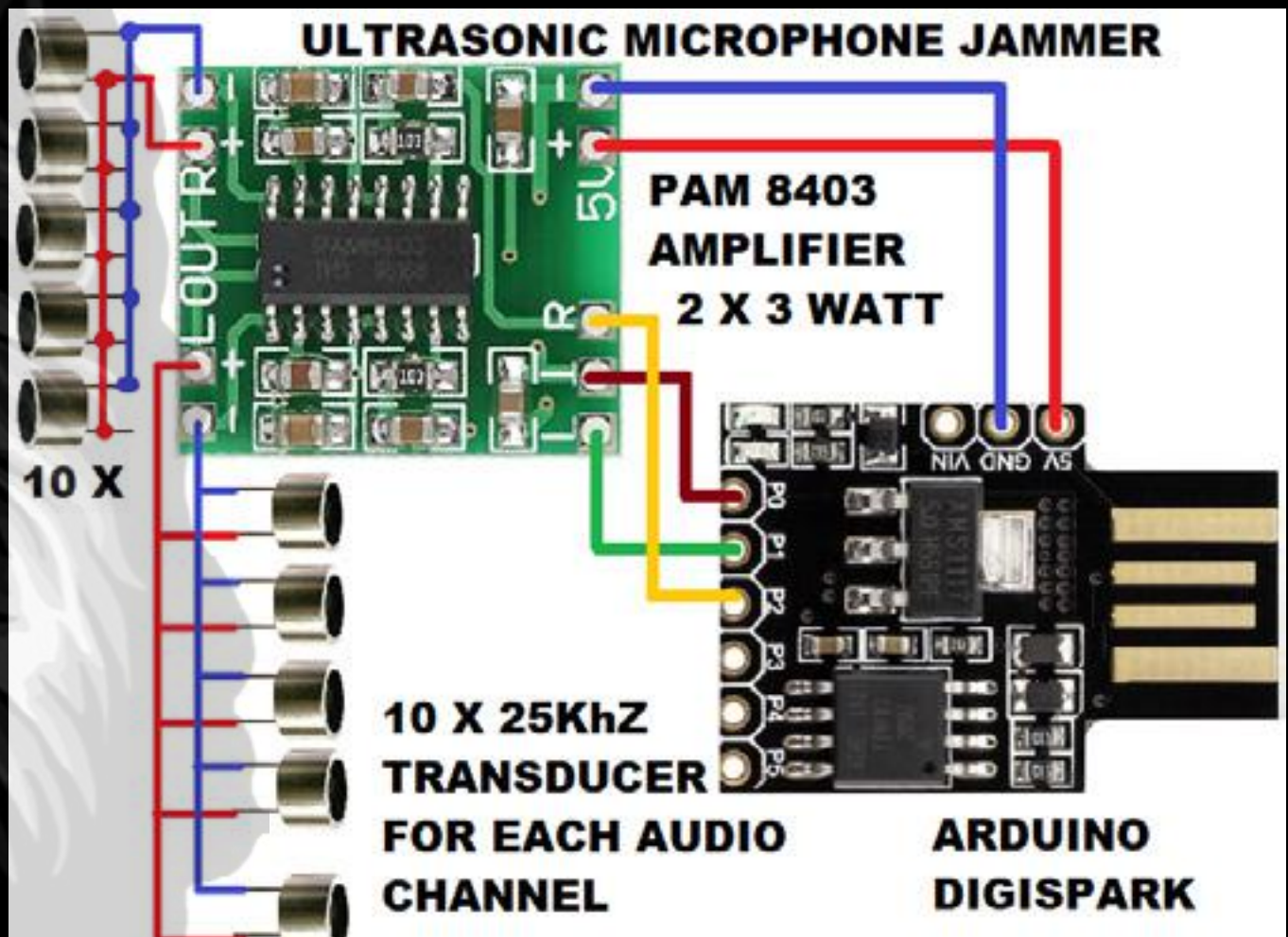
Ensure proper ventilation for the electronics to prevent overheating.

Step 5: Operational Deployment

Deploy the jammer in a strategic location where it can effectively cover the area you want to protect from eavesdropping devices.

Continuously monitor the performance and adjust the setup as necessary for optimal jamming effectiveness.

The effectiveness of the jammer may vary based on environmental factors, the sophistication of recording devices, and the specific setup of the jamming array. Regular testing and calibration might be necessary for optimal performance.



To get the code, simply download the PDF of this issue and rock a little copy pasta :)

USE
YOU
NEXT
TIME



HVCK