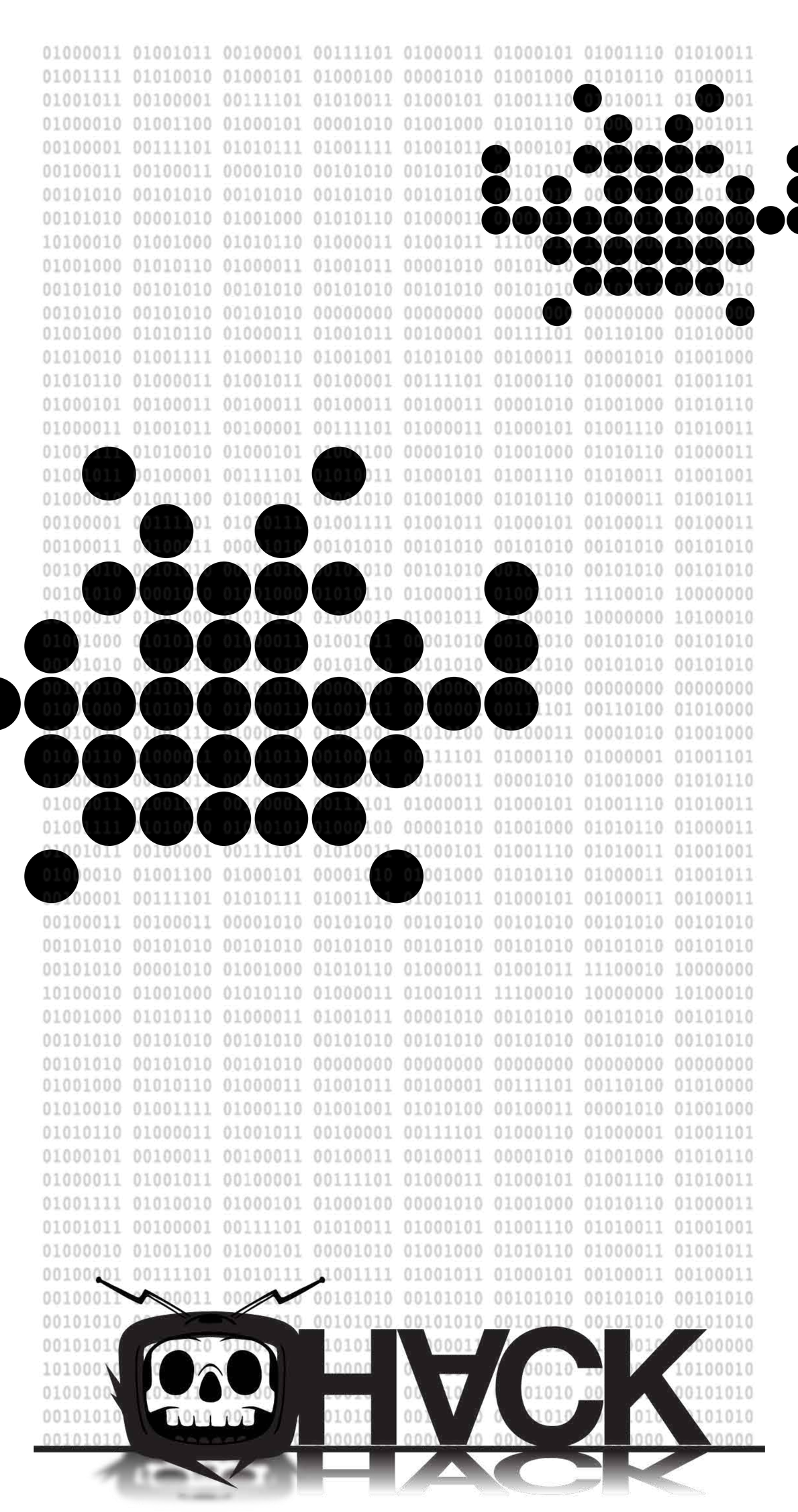
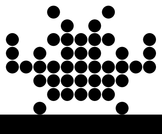


VOL.1 “ITS A LIFESTYLE CHOICE”

NOT ANOTHER HAK PUBLICATION



contents

#freshmeat
#rightbrain
#leftbrain
#futureprimitive
#refuseresist
#hacks
#tracks
#bitchslap

fresh meat

nooblife

Everyone starts somewhere. Freshmeat is a platform for those walking the walk to share their experiences and maybe even a little advice. This section is for those who want it and won't take no for an answer.

Thw words that follow are not gospel. Make up your own mind. Forge your own path. We are with you.

that time I went outside of scope and it bit me in the ass!

A how-not-to guide by D8RH8R

Undersell and overdeliver

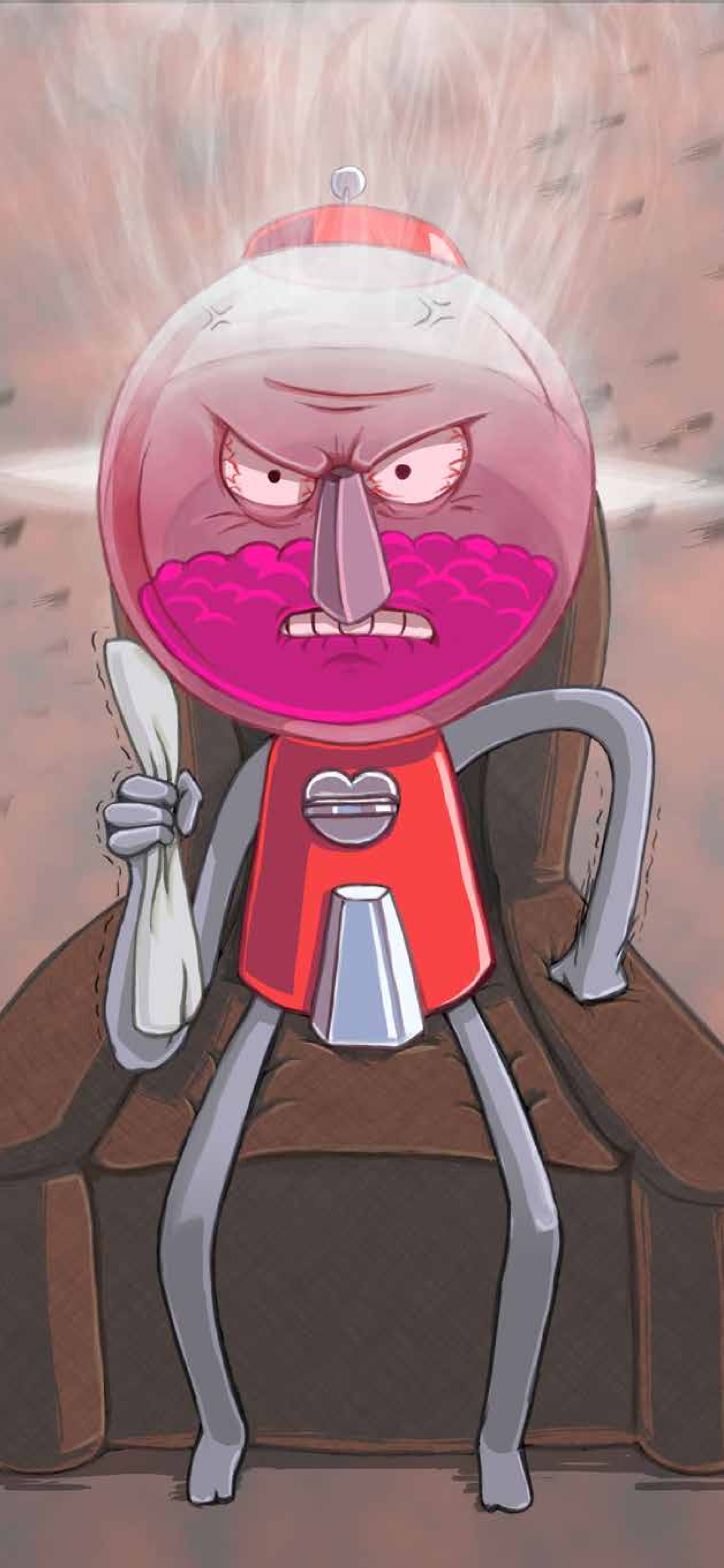
Those words, spoken with the sage like patience only a hands on experience can bring have been echoing in my head for the past week.

This simple concept is apparently the key to growth and longevity on the business side of this industry I love. Its also I great mantra from the superkeen newcomer to consider when tackling their first solo engagement.

The scope was cut & dry, very narrow, perfect really for a first spin around the block but with new skills up my sleave, I was keen to impress not only the client but the big cheese.

So I flexed, found gold and thought, time for a raise

Negative




thanks
but..
you're
fired

the takehome

don't do what donnie don't does

I won't get into the nitty gritty of what happened but for those of you out there just starting out in this game here's a few hard earned pearls of wisdom.

1. Stay within scope. It doesn't matter how interesting the information you found is, going outside it could derail the whole engagement or even land you in hot water.

2. Know your limitations. There is a big difference between knowing how to do something and being proficient.

3. Don't be affraid to ask for help. You're new to this. You can't know everything on day one.

4. Don't be affraid to make mistakes. It seriously is the best way to learn

breaking news

LARS STRIKES AGAIN

WIth sales at an all time low and COVID preventing acts from touring to create income, Metallica drummer Lars Ulrich has once again taken it upon himself to protect copyright holders everywhere.

Getting the taste for the takedown with file sharing giant NAPSTER, Ulrich explained that his NOWYAGOTTABUYIT malware protected Joe Average from himself and his urge to hear the sweet sweet sounds of “Enter Sandman” for free.

“Hundreds of Universal artists go without kitchen renovations every year due to these torrent sites and the heartless poor people that use them” said Ulrich.

“Getting my #OSCP and learning some Malware Dev chops is one of the best things I’ve ever done.. Now I can take the fight to them, on their level”

It remains to be seen if more A list musicians will turn to vigilante offensive security to protect their nest egg but till then copyright holders of the world, “Lars is lookin’ out for you”

right brain

analog

The right brain is more visual and intuitive. It has a more creative and less organized way of thinking.

imagination
holistic thinking
intuition
arts
rhythm
nonverbal cues
feelings
visualization
daydreaming

poetry as resistance

These are aperture voices, indefatigable, defiant in silent spaces….

There is a poetic tradition in Afghanistan that binds women together, connects them like a red thread that weaves into one cloth past, present and future, and offers a way to speak of ‘dangerous’ things and subvert a monolithic patriarchy.

The tradition is called Landay, meaning short poisonous snake. It is analogous to the Japanese Haiku tradition but emanates from the region of southern Afghanistan and north-western Pakistan, the traditional homeland of the Pashtuns, an Iranian ethnic group.

The Landay poetry is written in Pashto, and, according to those who continue the tradition, belongs to women, for women.

Landays take the form of narrative fragments that

contain what would be considered by the broader community as taboo subject matter i.e., sex, desire, gendered violence, love, grief, and the dynamics of power in the context of intimacy.

In whispers they betray a punitive patriarchy and subvert the power wielded against them.

Two lines, twenty-two syllables. Words woven in such a way as to strike, inject their poison/medicine, and disappear into the silences between what is spoken and what is heard.

Behind the burka, Afghan women have sharp tongues, and they can speak the truth in such a way as to slice the heart of any man who is foolish enough to believe that he has control.

In the heart of what is, once again, a Taliban-ruled country, the secret susurrations of women speaking to each other of love, desire, sex, loss, and freedom, escape through the pores of veils that may cover their faces but can never silence their fierce courage.

I sing even under my blue hood. My mother says I am a most determined songbird..

Your eyes aren't eyes. They are bees. I can find no cure for their sting

You are not alone

Stay wild even when made invisible. Stay to let your voices be hear even when they try to silence you
You are not alone

We see you. We hear you.
We will not forsake you.

I kneel before you, my strong, wild sisters of the wilderness,

my sisters of an ancient land,
my sisters of the dark night,
my sisters of the cradle of life,

and honour your courage despite the terror.

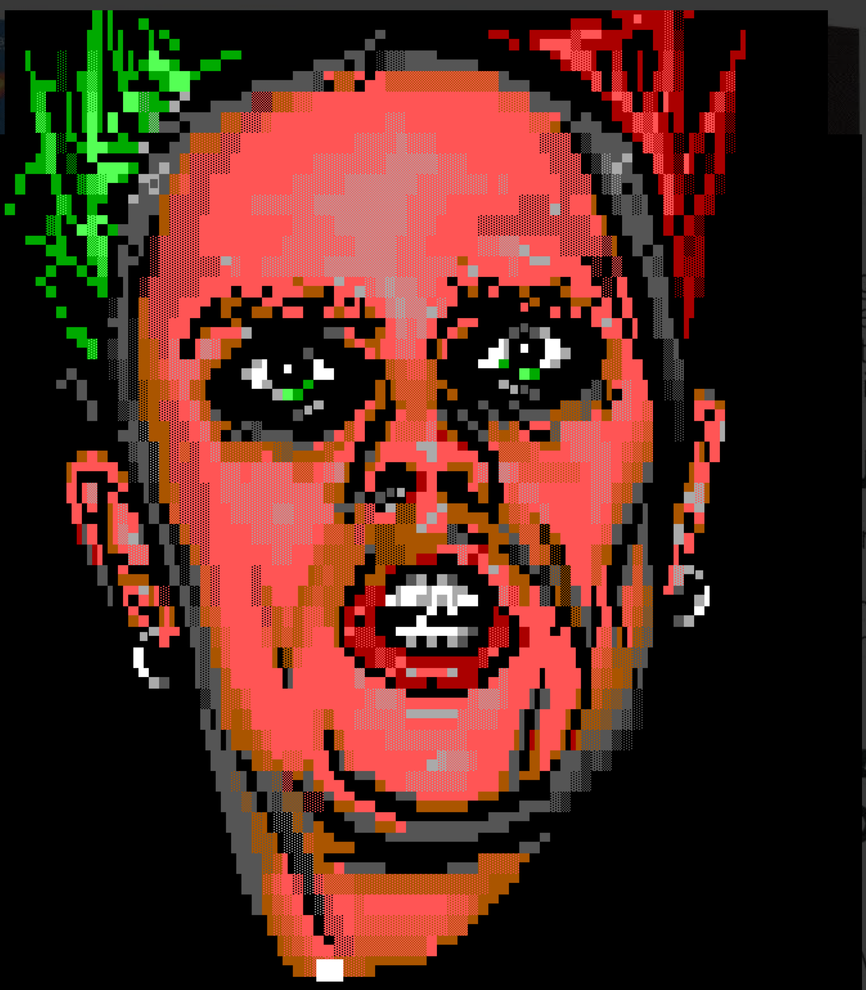
I bow my head before you, sacrificed sisters, indomitable warrior women poets.

written with love by

LIL' RED

Frank Reding

GABBA GABBA *HEY*



ansi

art from the days of yore

“Back in the early 90s, a few friends and I decided to start what was then labelled an “art group.” This was a digital collective out to create ANSI and ASCII artwork for the computer communication medium of the day: bulletin board systems. A BBS was kind of like a website, but you dialled directly into it (its address being a phone number), and all it could serve you was text, with a hint a color.

This format was colloquially known as ANSI (although that technically refers to the character set, but stay with me), and is a plain text file with so-called escape codes that describe background and foreground colors. You have 256 characters to work with, although 32 of those are things like line-break, so it’s actually fewer than that.

Color-wise you had 8 background colors, and 16 foreground colors. This set of restrictions actually made for an interesting challenge. And, you know, a decent download experience on your slow-ass 9600 baud modem.

Above and below by Fuel

When you dialled into a BBS, you would generally be presented with a pretty functional page of menu options, where you could do things like read news, browse some files, and maybe chat with the sysop—the system operator.

Worldwide, art groups sprang up to take this limited medium and elevate it, play with it, mix it up, and create amazing things. Some of the biggest were ACiD and iCE. These guys and gals came up with some mindblowing stuff.

My friends and I, clever (and Luxembourgian) as we were, came up with Black Maiden as a name. Despite the rumour that the name was a mashup of popular bands we liked (Black Sabbath, Iron Maiden), it was actually inspired by a clipart outline of a black angel. That didn't make it any better. Still, over the years, Black Maiden grew from a trio of friends into an international group of friends of some repute. We branched into the demo scene, went to competitions, and won some.

So here I am, about 25 years later, and I thought it time to collect some my ANSI and ASCII (like ANSI but sans color) art together. Please bear in mind that when I created these, I was a juvenile git with delusions of grandeur, and a loose grasp on the English language, so please ignore much of the drivel that accompanies this stuff.

Oh, and I went under the handle of VOiCE back then.

BBS design
by Frank Reding

VOiCE, gfx
artist of bM

E-Mail to:
2:270/26.6@fido

B L A C K M A i D P T i O N S o 9 5 o

left brain

digital

If you’re mostly analytical and methodical in your thinking, you’re said to be left-brained

logic
sequencing
linear thinking
mathematics
facts
thinking in words

digital extortion

by Prasan Singh

Abstract

Multiple research projects and studies conducted have reported increases in cyber extortion, the levels of complexity, and the overall financial consequences/ implications on the target organizations. These previously conducted studies focus on the attackers, how they are improving their techniques, how they are forming groups to accomplish their mission, and simple countermeasures.

In this particular research project, we take a deeper look at the target than the threat actors; we look at why attackers can still perform cyber extortion-type attacks on their target organizations. We look at the side of their pavement because I firmly believe that the success of an attack lies in the target's hands. Some organizations, firstly, may be oblivious to the fact they are just as eligible to cyber extortion as all the other organizations they hear about in the news. Another issue is their flawed implementation of strategies to protect themselves against cyber extortion.

Introduction and Background

My curiosity sparked this topic. Being a cybersecurity student and an aspiring cybersecurity professional, I find myself asking many questions regarding the cybersecurity domain in its entirety, but more importantly, about the rapid increase in cyber extortion. I am keen to find out what factors contribute to this rapid increase and perhaps explore various ways to mitigate or counter these incidences. I feel it is essential to investigate this topic as it seems to be the backbone of cybercrime and a lucrative part of cybercrime if we look at cybercrime as a business. I look at cyber extortion as the factor behind the rise in the number of cybercrime groups, or threat actors, as it holds more financial rewards.

Before conducting this research, I had quite a narrow way of looking at cyber extortion and the manners in which threat actors or attackers gain a foothold into their targets' information systems, which allows them to perform successful cyber extortion attacks, i.e., ransomware attacks. In this study, we had a deeper look at cyber extortion, the techniques involved, we will look at the spread, and some of the well- known threat actors in this field.

Problem Statement

Cyber extortion all over the world has been increasing rapidly over the years. Let's take a look at Ransomware attacks, for example, as they are the biggest and most common form of cyber extortion. According to research conducted by PURPLESEC, ransomware attacks grew by 350% in 2018. Let's take it a bit further, and take a deeper look at Ransomware attacks that were propagated through phishing emails; these have increased by 109% between 2017 and 2019.

I firmly believe that the increase in phishing emails is directly proportional to the increase in Ransomware attacks and various forms of cyber extortion like APT attacks in which threat actors steal sensitive data and threaten the target to sell it in the dark web if they do not pay the extortion fee. We've seen some efforts towards countermeasures for these types of attacks. However, they do not seem to have a highly effective outcome as the numbers of cyber extortion incidents are still rising rapidly.

I took it upon myself, through my own volition, to conduct a short and quick study via a survey methodology based on how many organizations know about cyber extortion, whether or not they believe that their organization has any hack value, the measures they rely on to protect their organizations against cyber extortion, whether or not they have User Behavior Analytics strategies in place and above all whether or not they would pay the ransom if their organization experienced a ransomware attack.

Objectives

This study aims to determine where organizations are going wrong as far as cyber extortion countermeasures are concerned. In this project, we explore various methods through which attackers gain a foothold into the target organization to execute successful cyber extortion-related attacks and how these targets play a role in helping the attackers succeed. I aim to investigate the strategies and solutions that organizations rely on to protect themselves against cyber extortion.

I will use a survey to collect information on how many organizations know about cyber extortion, the countermeasures they use to protect their organizations against cyber extortion; this is based on a set of questions that will give us a detailed view of this information. By using statistical analysis, this research will indicate to us just what the organizations are doing wrong, as well as how they are actually contributing to the increase of cyber extortion. We are basically identifying the gaps that exist in the current countermeasures that organizations may have in protecting their data and all their information systems from cyber extortion.

Literature Review

How attackers gain a foothold into the target organization
This pandemic has forced many organizations to take avenues some may have never even dreamt of taking a couple of years prior to this global crisis; with the rise of COVID-19 infections and many countries enforcing lockdown regulations, the various consortium has had to enable their workers to work from home, which unfortunately has some cybersecurity risks and has been a breeding ground for the increase in cyber extortion.

The fact that employees have to remotely means that the systems they need to fulfill their occupational responsibilities have to be accessible outside the organization’s LAN, and if this is not implemented properly, attackers will have an opportunity to try various methods to gain access to these information systems, and once

they get a foothold, a whole new world of opportunities arise for the attackers, the main one being cyber extortion.

New research, which was conducted by the Microsoft 365 Defender Threat Intelligence, highlighted various ways through which attackers gained a foothold into target organizations by exploiting internet-facing information systems. Let's look at the most common vulnerabilities that were exploited, which I strongly believe is a contribution by the target organizations in aiding the threat actors to successfully execute a ransomware attack or any other cyber extortion attack(s).

"To gain access to target networks, the recent ransomware campaigns exploited internet-facing systems with the following weaknesses:

- Remote Desktop Protocol (RDP) or Virtual Desktop endpoints without multi-factor authentication (MFA)

- Older platforms that have reached the end of support and are no longer getting security updates, such as Windows Server 2003 and Windows Server 2008, exacerbated by the use of weak passwords

- Misconfigured web servers, including IIS, electronic health record (EHR) software, backup servers, or systems management servers

- Citrix Application Delivery Controller (ADC) systems affected by CVE-2019-19781

- Pulse Secure VPN systems affected by CVE-2019-11510" (Microsoft 365 Defender Threat Intelligence Team,2020)

Based on what I have observed from reading the various pieces of literature during this exercise, I noticed that most cyber extortion, like ransomware attacks, occur via email, particularly through the use of social engineering techniques, and this is because the human being is the weakest element and probably the best for any attack, because their trusting nature and the willingness to help in exchange for praise/ recognition, the like to feel good, and as an attacker, you just have to tell them what they desire to hear to get what you want.

Factors contributing to the rise in cyber extortion
First of all the monetary rewards are a contributing factor to the rise in cyber extortion; this is also highly influenced by cryptocurrency; with this type of currency, there is no paper trail, and transactions are completely anonymous, which means attackers can not be traced like they would if the money was paid into a bank account. Cryptocurrency wallets are easier to open, and they are not regulated as banks are, which means anybody can get a cryptocurrency wallet. Another factor that I strongly believe contributes to the rise in cyber extortion is the lack of User Behavior Analytics strategies, or even when they are in place, they not being put into their utmost potential use. User Behavior Analytics can be used to detect malicious insiders; not only that, but they can also shed some light in APT cases where a user's credentials are being used to facilitate the attack. Malicious insiders can make use of RaaS to carry cyber extortion attacks.

"Malicious insiders can exploit their inside information on the organization's unstructured data and their knowledge of where sensitive data is located, as well as their permissions, to encrypt the most valuable data. Moreover, they know what the value of the data to the organization is and can assume how much the organization will agree to pay for the data decryption. We are aware that the main motivation for malicious insiders is financial, and using RaaS on the organization is simple, safe, and profitable. Future RaaS customizable parameters might be more specific and include business-related information such as what are the valuable network shares of interest or even relevant credentials. It is conceivable that a malicious insider could use RaaS to extort his organization and cause irreparable damage." (Margel & Shtar,2016).

Speaking of malicious insiders, I am reminded of the attempted ransomware attack incident that took place at the Tesla Gigafactory. This shows that the human element is still the best attack vector coupled with various other attack vectors to archive the desired outcome, in this case, cyber extortion.

Commonly used methods to prevent cyber extortion
We've had a look at how attackers gain a foothold into the target organization's information systems to perform

successful cyber extortion attacks. Now let's inspect the commonly used countermeasures against cyber extortion. Based on the various numbers of articles that I have read seem to focus on similar countermeasures, which are the methods listed below:

- Having regular back-ups of all the sensitive data or all information systems that the organization relies on.

- Use high-quality anti-virus software and update it regularly. Update Operating Systems regularly, make sure all security software is up to date.

- Doing background checks on employees to get an insight into the employees' previous behavior.

- Ensuring that the organization has cybersecurity insurance.

The gaps in all these literature pieces are that they do not focus on continuous User Behaviour Analytics as one of the countermeasures; I mean, a single background check on an employee is not enough if attackers approached an employee with a promising reward for successful ransomware deployment, the chances are that user will take it. However, the user's behavior will change once they are taking part in such activities; there will be suspicious behavior, which we can pick up through user behavior analytics. Another gap I identified is that they don't focus on breach/attack drills, as well as providing continuous basic cybersecurity training to users.

Methodology Adopted

The methodology that I adopted in conducting the research was the survey methodology. I created a survey using Free Online Surveys. This survey was aimed at organizations.

The survey questions are listed below:

- Have you ever heard of Cyber Extortion?
- Do you believe that your organization has any hack value?
-

- What measures do you have in place to protect your organization from Cyber Extortion?
- Do you have User Behavior Analytics?
- Would you pay the ransom if your organization experienced a ransomware attack?

Explain the reason for your answer.

I used understand. The results will give us an insight into how many organizations believe they are potential targets of cyber extortion, the methods they have in place, and how they would react to a cyber extortion attack like ransomware.this method because of its agility. It is straight to the point, easy to answer and to

Results – Project Findings

From this study, I have found that 83% of the organizations that participated in the study have an understanding or have heard of what cyber extortion is,67% believes that their organization has some hack value,80% rely on IDS and Firewalls to protect their consortium against cyber extortion,67% have User Behaviour Analytics strategies in place, and 33% said they would pay the ransom if the organization experienced a ransomware attack. The fact that only 67% of these organizations believe they have any hack value was a bit alarming because I believe any organization has some hack value, as long as it has employees or clients, there is some hack value, sensitive data relating to the staff may be stolen from the organization and sold to black hat hackers on the dark web who will then use it for identity theft or forms of cybersecurity threats, this type of information can be used to extort funds from the target organization by attackers, in a sense where they would say “We have all your employees’ sensitive data, and we demand so much from you, or we will sell the data on the dark web.”. Something else that I found alarming was the fact that 80% of the organizations rely ultimately on IDS and Firewalls to protect themselves against cyber extortion, because like I side in the previous sections of this document that the human being is the best attack vector, and only 33% have regular staff training. This alone tells me that majority of the organizations are responsible for the increase in cyber extortion as they are making it very easy for the attackers to gain a foothold into their

organizations. Another interesting thing I found was that 66,6% of the organizations have User

Behavior Analytics strategies in place. However, they did not list them as a manner of protecting the organization against cyber extortion.

Recommendations

Some organizations do not think they have any hack value, and it is recommended that they treat themselves as having the highest hack value despite the size of the organization. Once they practice this way of looking at things, they will be inclined towards finding all sorts of ways to protect themselves against cyber extortion. It has also come to my attention that majority of the organization that participated in this survey do not see User Behavior Analytics strategies as a way of protecting themselves against cyber extortion.

I, therefore, recommend that organizations start treating using the data from user behavior analytics systems as a way of identifying malicious insiders, which will, in turn, protect them against cyber extortion like ransomware, APTs, or data theft. I would also like to put great emphasis on the importance of implementing an anonymous whistleblowing campaign or strategy, where other employees can anonymously report malicious or suspicious activities they may be seeing other individuals getting involved in. This will have to be coupled with providing regular cybersecurity training to individuals and having random breach/ attack simulations to test the vigilance of the employees.

Furthermore, I would like to add that we can not only rely on firewalls and other security software to protect organizations from cyber extortion; they are all good to have. However, they should be accompanied by other countermeasures like those I have outlined above. It would not be a bad idea to make use of Breach and Attack Simulation tools regularly because they are not as complex as penetration testing, therefore do not require a lot of planning; they do, however, require a person that knows how to configure them for optimum results and use them to their full efficiency.

back to the future for payment options

by Brenda van Rensburg

Believe it or not, it took banks several years to enrol individuals into using credit cards. Up until the 80s, the bankcard was used predominantly by the wealthy. However, things began to change in the 80s when the bankcard signed an agreement with 'Visa and Master to enable international usability.' In was only in the early 2000s that credit cards become popular. As such, it took over 2 decades to lure people into an alternatively monetary system.

Bitcoin was introduced into the world in 2008. It was not enthusiastically supported and took several years for people to buy into the concept. Its lure was decentralization. This meant that no single administers controlled the currency. Its foundation was set on the premise of a value that was hashed within a block. A single block would connect to another block only if all the elements matched up. These elements are what is termed as a hashed value and are often viewed in a hexadecimal amount.

The first official bitcoin transaction took place in 2010 when Laszlo Hanyecz sent 10,000 BTC for payment of two pizzas. By 2011, bitcoin gain stardom with attention drawn to the realization that it was being used on the dark web as payment for ‘goods & services.’

Six years later, a single Bitcoin reached a valued of US $3000.00. However, with fame came several issues. Processing speed became slow and sluggish due to the increase of transactions. By 2014, bitcoin succumb to more negative press when the Mt.Gox exchange mysteriously disappeared over night, taking with it over 850,000 Bitcoin. And, the world watched on as bitcoin crashed to an average value of US $300.00.

Despite these minor setbacks, Bitcoin has recently triumphed by reaching new all-time highs. Big companies such as Pay Pal, Tesla and Microsoft are quickly adopting it as a form of payment. And, Visa and Mastercard have joined forces with several cryptocurrency platforms offering a payment solution for cryptocurrency supporters. Ironically, it seems history is starting to repeat itself.

ALT COINS

IXCoin was one of the first coins to fork off the bitcoin chain in 2011. In the same year an alternative algorithm, also known as a proof-of-work (POW), was introduced. This prevented the occurrence of denial-of-service attacks. This led to the development of LiteCoin and hundreds of other Alternative Coins. With bitcoin soaring to new all-time highs, alternative coins became an interest for many that ‘missed the investment boat’. As the years rolled on, new blockchain technology projects have surfaced focusing on specific issues. Many of these projects are concentrated on worldwide issues such as privacy, insurance, transactions and even accounting. It can be argued that we are heading quickly toward a digitized economy.

NON-FUNGIBLE TOKENS

Blockchain is not all about money. Non-Fungible Tokens, also known as NFTs, are digital art tokens that would first introduce into the digital realm in 2012. In 2017, cyberpunks minted 10,000 cartoon characters and gave these to anyone with an

Ethereum wallet. The NFT market has grown significantly, with images being sold for more than $1000.00 a-piece. The main disrupter is the fact that NFTs is a ‘gift that keeps on giving’. Artist are paid a commission every time their digital art token changes hands, or in this case, wallets. Possibly the biggest drawback to NFTs is the cost of minting a token and the cost in sales. Transaction fees, also known as gas fees, are pricey when compared with bitcoin or alt coin transaction fees.

PRIVATE EYE

One of the biggest draw cards to cryptocurrency is the decentralization. Initially, bitcoin, which is shared via a digital wallet, was difficult to trace. As technology advances, digital wallets are becoming easier to obtain. It is also becoming easier to track transaction. While a hash address can be found, the identify of the owner of that address remains private unless the identity of the individual is released online either by the owner, or a person who can identify the owner. Additionally, any person can determine how much money is held within that wallet. This is all publicly displayed. Arguably, this defies several regulations. And the question arises on whether there is a duty of care to keep this information private.

MARKET MANIPULATORS

Over the past year, several big corporations have moved into the crypto space. These include Morgan Stanley, Goldman Sachs Group, Square, Tesla and PayPal. In addition, this, there are several influencers that have impacted the market just from a single tweet. Much like Cambridge Analytica, there is a specific framework that one can apply to create Fear, Uncertainty, and Doubt (FUD). Add a bit of ‘Herd Mentality’ and you would create a stampede that will inevitably impact any highly volatile crypto market. The question is raised on whether the crypto market deserves the same protection behind regulations as that of the stock markets.

FOR KING, FOR COUNTRY AND FOR FUTURE PAYMENTS

In the past few months, we have seen some small countries becoming early adopters of crypto currency. These include El Salvador and Paraguay. Arguably, this move has introduced regulation of ownership. However, they are not the first countries to introduce digital currency into their economy.

In 2019, Iceland introduced their own digital currency called Financial Supervisory Authority of Iceland, FME for short. Iceland was the first in Europe to trade digital currency. China, followed suit in 2020, introducing the digital Yuan. China has already distributed over 200 million Yuan.

The USA is also looking at developing their own digital currency. Discussions about the digital dollar project is already underway. It could be argued that it is just a matter of time before we see the humble dollar in digital form.

CONCLUSION

Blockchain technology has disrupted the economy and is offering solutions for many digital challenges. Apart from a digital currency, this technology can solve many issues which include security, privacy and efficiency within platforms and systems.

History has shown us that the adoption of a new system can take decades. However, we have seen an increase of adaption to new technology. It could be argued that we could see a shift to digital payments a lot sooner than anticipated. We have already seen some marked improvements in the digital payment gateways. These improvements have made it easier for the everyday person to use the digital currency as an alternative form of currency. The only restriction is the lack of regulations around this eco-system. Arguably, the introduction of regulations may remove decentralization and therefore, the essence to why bitcoin was initially created. The question is left on how this vulnerability ecosystem can be protected while still keeping its vision and purpose.

References:

https://www.finder.com.au/credit-card-history

https://www.britannica.com/topic/credit-card

https://money.usnews.com/investing/articles/the-history-of-bitcoin

Nick Furneaux, Investigating Cryptocurrencies, Wiley 2008.

https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578

https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578

https://steemit.com/downs/@steemitraj/bitcoin-s-top-up-and-downs-which-have-been-modified-by-cryptonics

https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/?sh=2af4c7773f27

https://www.independent.co.uk/life-style/gadgets-and-tech/bitcoin-price-prediction-2021-crypto-b1853818.html

https://www.gobankingrates.com/money/business/10-major-companies-that-accept-bitcoin/

https://crypto.com/cards

Alexandru Pîrjan, Dana-Mihaela Petrosanu, Mihnea Huth, and Mihaela Negoita. “RESEARCH ISSUES REGARDING THE BITCOIN AND ALTERNATIVE COINS DIGITAL CURRENCIES.” Journal of Information Systems & Operations Management (2015)

Panda, Sandeep Kumar., Elngar, Ahmed A, Balas, Valentina Emilia, and Kayed, Mohammed. Bitcoin and Blockchain : History and Current Applications. 2020

https://www.cbinsights.com/research/industries-disrupted-blockchain/

https://www.linkedin.com/pulse/what-nft-brenda-van-rensburg-/

https://www.linkedin.com/pulse/brief-history-nfts-look-future-brad-bulent-yasar/

Karandikar, N., Chakravorty, A., & Rong, C. (2021). Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure

https://www.bloomberg.com/news/articles/2021-01-14/research-affiliates-quant-warns-of-bitcoin-market-manipulation

http://content.time.com/time/magazine/article/0,9171,2061234,00.html

https://asic.gov.au/online-services/search-asic-s-registers/asic-s-training-register/asic-s-training-register-search-results/training-registers/stock-market-and-products-405/

https://www.coindesk.com/paraguay-bitcoin-law-crypto-mining-registration.

https://www.coindesk.com/icelandic-regulators-approve-startups-plan-for-fiat-payments-on-ethereum

https://www.scmp.com/economy/china-economy/article/3135886/china-digital-currency-when-will-e-yuan-be-launched-and-what

https://www.aljazeera.com/economy/2021/7/12/us-digital-dollar-will-fiat-currency-ride-the-crypto-wave

future primitive

Yesterdays technologies of the future

Everyone had one of those relatives that had the latest and greatest of every. I was luck I had two. One was an architect. He had the Porche, the beach front mansion and the minimalist interior design, a desert of boredom for a young child.

My other uncle was a medical professional, into photography and technology. I remember being in awe of his professional looking video camera but being disapointed that we couldn't watch his beta tapes on our vhs. I think he backed the wrong horse there. Yes I know BETA was better quality and that the VHS winning dominance over BETA was won in the direct to tape porn market. Yes. Once upon a time you had to pay money for porn.

This section celebrates the cutting edge of yesterday and some of the people who paved the way. The ghosts of hackers past.

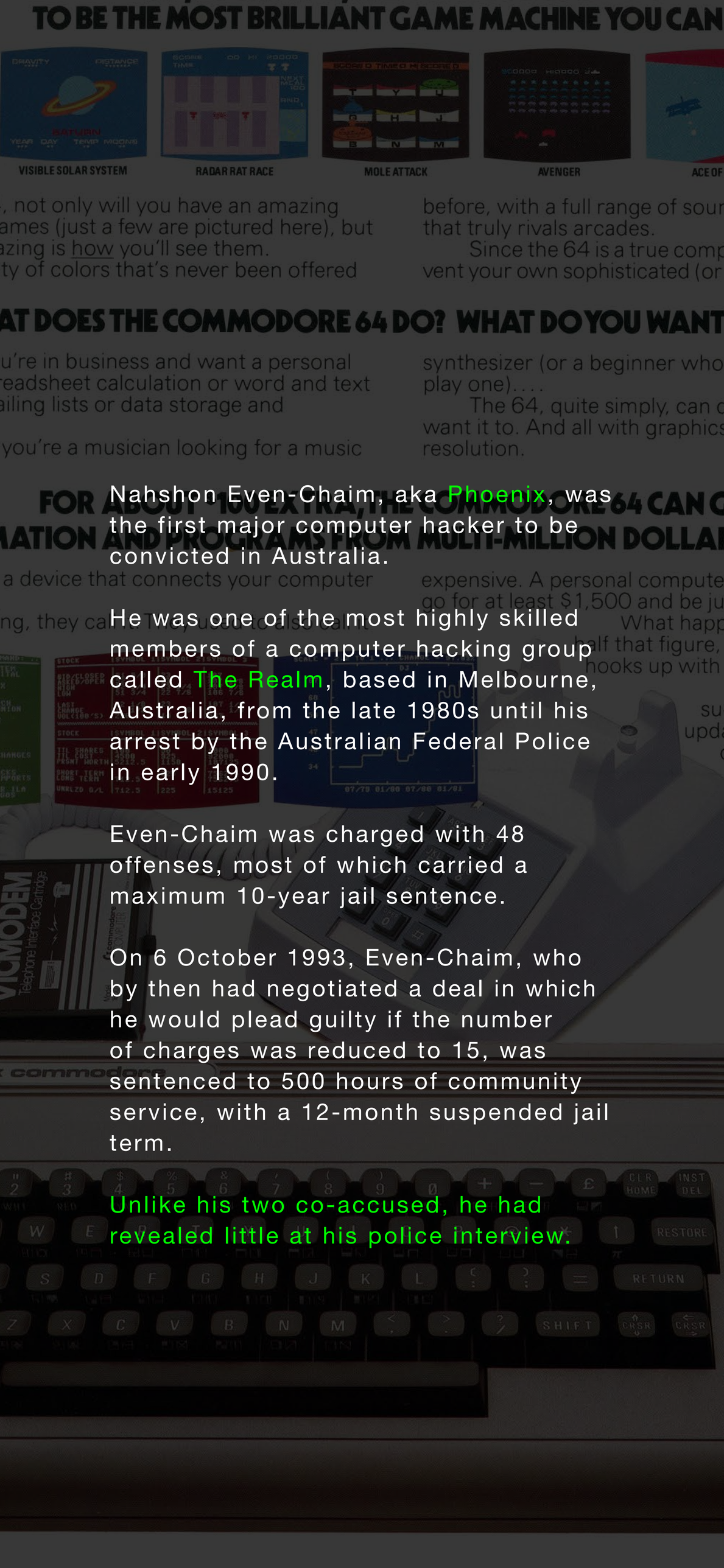
the realm

globe trotter

As a hacker in this time we truly do stand on the shoulder of giants. We take for granted the instant access to almost any information we seek. At one time though, before the tweets, the snaps, the beef and the bullshit, plain text documents of the hard won secret knowledge of a mostly unknown digital wonderland was meticulously chronicled in zines.

Released in 1988, a time when Australian hackers were at the top of the game, “The Realm” released Globe Trotter, the first Australian hacker zine.

Firsts seem to have been a thing for the Australian hackers. A member of “The Realm” was the first to be charged under the brand new computer crimes act.



Nahshon Even-Chaim, aka Phoenix, was the first major computer hacker to be convicted in Australia.

He was one of the most highly skilled members of a computer hacking group called The Realm, based in Melbourne, Australia, from the late 1980s until his arrest by the Australian Federal Police in early 1990.

Even-Chaim was charged with 48 offenses, most of which carried a maximum 10-year jail sentence.

On 6 October 1993, Even-Chaim, who by then had negotiated a deal in which he would plead guilty if the number of charges was reduced to 15, was sentenced to 500 hours of community service, with a 12-month suspended jail term.

Unlike his two co-accused, he had revealed little at his police interview.

```
                -   G L O B E     T R O T T E R    -
+=+=+=||================================================================||=+=+=+
+         Volume #1,    File #1                    Date:    01/01/1988        +
+                                                                             +
+                                                                             +
+  Written By:  ----====} THE FORCE {====----   From The depths of THE REALM  +
+=+=+=||::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::||=+=+=+

Welcome To the first Edition of GLOBE TROTTER,  the first  AUSTRALIAN HACKERS,
Monthly Magazine.   I have chosen the name “GLOBE TROTTER” Because that’s
what this is all about and it is dedicated to all the DATA BUMS out there,
playing with systems in countries not even heard off.   The Realm which is a
BBS I sysop, is the source for most of the information and I will try to
state where every piece of data in these files comes from.  To continue this
magazine on monthly basis, I will need your support.  Any information or files
you can contribute will be greatly appreciated by all. If you have anything of
interest, this is where you can contact me:.

::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
Germany:    ALTOS                NUA: 026245890040004    Username: force
Australia:  Any Good BBS In Melbourne  or  The Realm
Usa:        Still Looking for a Good BBS.
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::

                              I  N  D  E  X
                              ~~~~~~~~~~~~~
R E G U L A R   F E A T U R E S
------------------------------

    - Outdial Systems:          This month we have an international Outdial, to
                                Start you modeming around the globe.

    - Unusual Systems:          Few NUA’s which are a little different.

    - System Passwords:         In this issue you will find few DG AOS/VS
                                passwords, along with other accounts.

    - Trix of The Trade         In this edition there are few tips on preserving
                                minerva accounts and on Identifying Systems.

    - Hack Of The Month         An Interesting GANDALF PACX hack.

    - Network Profile:         This month we feature TYMNET 3106 and have
                                up-to-date  Scans of  the 00, 07 and 90 areas.
                                Please note they are different to the Scan
                                Published in Force Files 1-9.  This is a newly
                                done scan with many new systems.

N O T   S O   R E G U L A R   F E A T U R E S
-------------------------------------------

    - What You Need To Know    A guide to the Scan Formats and Abreviations
                               used in these files.
    - The BAD and THE UGLY     We have a compiled list, of what we consider are
                               The three worst networks yet explored in depth.

================================================================================


OUTDIAL SYSTEMS
~~~~~~~~~~~~~~~

There are only three countries which are really serious about outdialing from
their networks to computers outside the packet switched service.   They are
CANADA, AMERICA, and JAPAN.   As yet I have never found an outdial in JAPAN,
but I know they are there and I have only scratched the surface of DDX and
VENUS, so I will keep you informed.  In america, TYMNET is the first network
which springs to mind if you think of outdials.  They like the VEN TEL systems
above all others, and most can dial Internationally.  There are few exceptions
like HOUSTON, and CLEARWATER outdials, but more about those in the next issue.
CANADIAN DATAPAC, must be on a real low budget, since virtually all of the
outdials service only a particular area,  however,  some ports don’t seem to
be functioning properly and have been known to dial outside CANADA. Once in
a while you will come across, local outdials on IPSS and TELEPAC of UK and
SWITZERLAND but they are very very rare indeed.  If you need outdials on other
networks, the best way is to look for privatelly owned ones, in systems like
Unix etc.  There is one type of system, which I have seen people mistake for
outdials very often indeed, although none of them have got them to work.  They
play with it and give up, not knowing what they have.  They come up with the
“#” prompt and when you type  STATUS, you get a lot of bullshit about parity,
```

baud rate, call parameters etc. They look and feel like outdials, but they are more like a GATEWAY. They do call out systems on the PSTN, but only to those which are subscribers to that gateway. To use them try things like CALL 1, CALL 100 etc etc.
Few outdials are very simple to use. They have instructions, and all you do is enter the number and off you go. Others are not so easy. Some may require HAYEYS type codes or other Prefixes to make the call. for example few outdials I came across need formats such as ATDP9T,#   or TB,#,00285 where # is the phone number. Others require various numbers infront of the actual number like 9 which was used instead of a 1 to make calls to the USA. The best thing I can recomend is to experiment and if there is a memory to store numbers in, check it to see the formats other people have used.
Ok, Lets Get down to some real Outdials now:

3106004956   - DATAPHONE II Outdial, (select port #1 or #2)
310600216401 - MITRE Outdial   (This one requires a Password)

The above are just fair, but the outdial of the month is on the ANF GANDALF PACX and it will dial any numbers in the USA and Elswhere in the World.

3106002062   - VEN TEL O/D   You will need to figure out how to use it,
                                since I will not say any more about it, but
                                it works great.

UNUSUAL SYSTEMS
~~~~~~~~~~~~~~~

This is hopefully going to be a regular feature if I can come up with something interesting month after month. Few of the NUA's I will give you in this section you might have seen in various NUA scans, but if they are interesting or unusual I will try to bring them to your attention.

026245221040194   - CPX-PAD
026245621040580   - DYNAPAC Multi-PAD
026246890040281   - DATUS PAD

And finally for this Month, Something I don't approve off at all, but here it is anyway:

03106007580   - Mc MASTER CARD Direct Order Entry System

Next months I will have various Bulleting boards on the Data Networks and other nice systems for you.

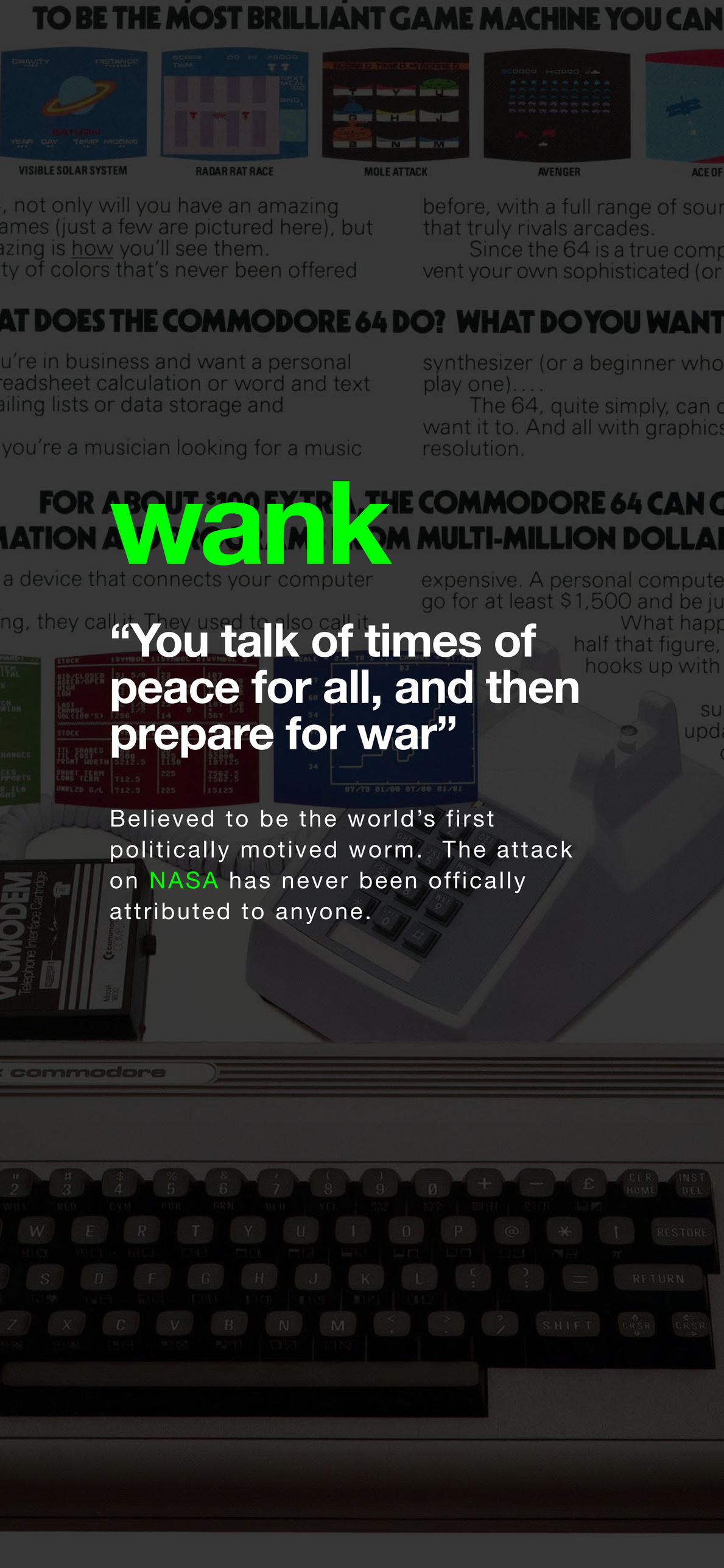
SYSTEM PASSWORDS
~~~~~~~~~~~~~~~~

In this section I will leave you with various accounts and passwords. Please do not expect to just gain entry, and have a great time. In most cases, anything I post personally will be something I don't need. In any case, I will not make it easy since if everyone got access to the system in question, it would last only for few days. This Month I have some accounts on Telenet, but if you're sick of the US networks stay tuned since in a few issues I will have bits in pieces from IRELAND, ISRAEL etc.

311080100062   - DG AOS/VS 03A   Login: GUEST/GUEST
311050300040   - DG AOS/VS   Login: VISITOR/VISITOR
311091900060   - PRIMENET 20.0.4.R2   Login: PRIME/PRIME

TRIX OF THE TRADE
~~~~~~~~~~~~~~~~~

This is where you can pick up very usefull information, so you can learn and prosper. Lets start off with MINERVA. It's a system part of the DIALCOM network. Running on PRIME'S. It is equivalent to the Us PRIMECON, Uk, BT GOLD, Germany, TELEBOX. Each country has a few more or less. Since Minerva is my favourite system (Only system 08 is still called MINERVA, systems 07 and 09 are now known as KEYLINK. I will always refer to KEYLINK as MINERVA for sentimental reasons. I mean what sort of a dud name is KEYLINK?)
most of you all ready Know this, but you can try this out for yourselves if you
~~~~~~~~~~~~~~~~~


TO BE THE MOST BRILLIANT GAME MACHINE YOU CAN
VISIBLE SOLAR SYSTEM
RADAR RAT RACE
MOLE ATTACK
AVENGER
, not only will you have an amazing
ames (just a few are pictured here), but
azing is how you'll see them.
ty of colors that's never been offered
before, with a full range of sour
that truly rivals arcades.
Since the 64 is a true comp
vent your own sophisticated (or
AT DOES THE COMMODORE 64 DO? WHAT DO YOU WANT
u're in business and want a personal
readsheet calculation or word and text
ailing lists or data storage and
you're a musician looking for a music
synthesizer (or a beginner who
play one)....
The 64, quite simply, can d
want it to. And all with graphics
resolution.
FOR ABOUT $100 EXTRA, THE COMMODORE 64 CAN G
MATION A
M MULTI-MILLION DOLLA
a device that connects your computer
ng, they call it. They used to also call it
expensive. A personal compute
go for at least $1,500 and be ju
What happ
half that figure,
hooks up with
su
upda
wank
"You talk of times of peace for all, and then prepare for war"
Believed to be the world's first politically motived worm. The attack on NASA has never been offically attributed to anyone.
VICMODEM
Telephone Interface Cartridge
commodore

****

DDN Security Bulletin 03 DCA DDN Defense Communications System
18 Oct 89 Published by: DDN Security Coordination Center
(SCC@NIC.DDN.MIL) (800) 235-3155

DEFENSE DATA NETWORK
SECURITY BULLETIN

The DDN SECURITY BULLETIN is distributed by the DDN SCC (Security Coordination Center) under DCA contract as a means of communicating information on network and host security exposures, fixes, & concerns to security & management personnel at DDN facilities. Back issues may be obtained via FTP (or Kermit) from NIC.DDN.MIL [26.0.0.73 or 10.0.0.51] using login="anonymous" and password="guest". The bulletin pathname is SCC:DDN-SECURITY-nn (where "nn" is the bulletin number).

****

W.COM ("WANK") WORM ON SPAN NETWORK

On 16 October, the CERT received word from SPAN network control that a worm was attacking SPAN VAX/VMS systems. This worm affects only DEC VMS systems and is propagated via DECnet (not TCP/IP) protocols. At least two versions of this worm exist and more may be created. Non-VMS systems are immune; TCP/IP networks are not at risk.

While this program is very similar to last year's HI.COM (or "Father Christmas") worm (see DDN MGT Bulletin #50 23 Dec 88), THIS IS NOT A PRANK. Instead of a "cute" Christmas greeting, W.COM appends code to .com files and displays this banner:

```
   W O R M S   A G A I N S T   N U C L E A R   K I L L E R S

 _____________________________________________________________
 \__ ___________ _____ ________ ____ ____ __ _____/
  \ \ \ /\ / / / /\ \ | \ \ | | | | / / /
   \ \ \ / \ / / / /__\ \ | |\ \ | | | |/ / /
    \ \ \/ /\ \/ / / ______ \ | | \ \| | | |\ \ /
     \_\ /__\ /____/ /______\ \____| |__\ | |____| |_\ \_/
      \_____________________________________________/
       \ /
        \ Your System Has Been Officically WANKed /
         \_____________________________________/
```

You talk of times of peace for all, and then prepare for war.

Initial reports described the worm as destructive, i.e. it would erase files. Detailed analysis by the CERT, Lawrence Livermore National Laboratory, and FermiLab has not found any code that would perform file erasures. However, files are altered and new accounts created. Serious security holes are left open by this worm.

It is very important to understand that someone in the future could launch this worm on any DECnet based network. Many copies of the virus have been mailed around. Anyone running a DECnet network should be warned.

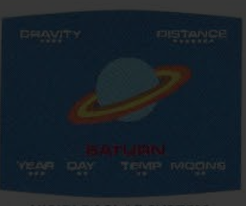
When the DDN PMO received these initial reports, the MailBridge filters were activated to preclude any traffic from passing between MILNET and the rest of the Internet. The filters will be turned off (restoring full interoperability) Tuesday 17 October 1989 NLT 17:00 EDT. (NOTE: W.COM could traverse the MILNET only if encapsulated in a TCP/IP "envelope", i.e. "assisted" by a human agent, and cannot "infect" the MILNET.)

R. Kevin Oberman from Lawrence Livermore National Laboratory reports:

> "This is a mean bug to kill and could have done a lot of damage. Since it notifies (by mail) someone of each successful penetration and leaves a trapdoor (the FIELD account), just killing the bug is not adequate. You must go in an make sure all accounts have passwords and that the passwords are not the same as the account name."

The CERT also suggests checking every .com file on the system. The

TO BE THE MOST BRILLIANT GAME MACHINE YOU CAN



VISIBLE SOLAR SYSTEM

RADAR RAT RACE

MOLE ATTACK

AVENGER


ACE OF

, not only will you have an amazing
ames (just a few are pictured here), but
azing is how you'll see them.
ty of colors that's never been offered

before, with a full range of sour
that truly rivals arcades.
Since the 64 is a true comp
vent your own sophisticated (or

AT DOES THE COMMODORE 64 DO? WHAT DO YOU WANT

u're in business and want a personal
readsheet calculation or word and text
ailing lists or data storage and

you're a musician looking for a music

synthesizer (or a beginner who
play one)....
The 64, quite simply, can d
want it to. And all with graphics
resolution.

FOR ABOUT $100 EXTRA THE COMMODORE 64 CAN C
MATION AND SOFTWARE FRIENDLY MULTI-MILLION DOLLAR

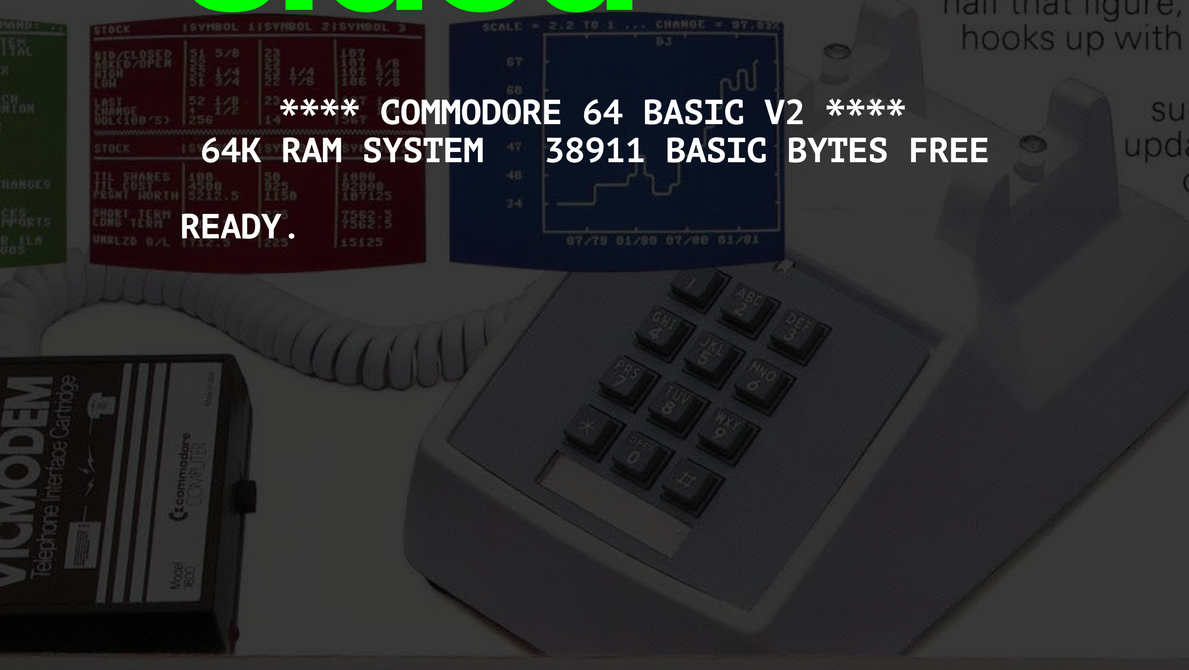
a device that connects your computer

expensive. A personal compute
go for at least $1,500 and be ju
What happ
half that figure,
hooks up with

ng, they call it

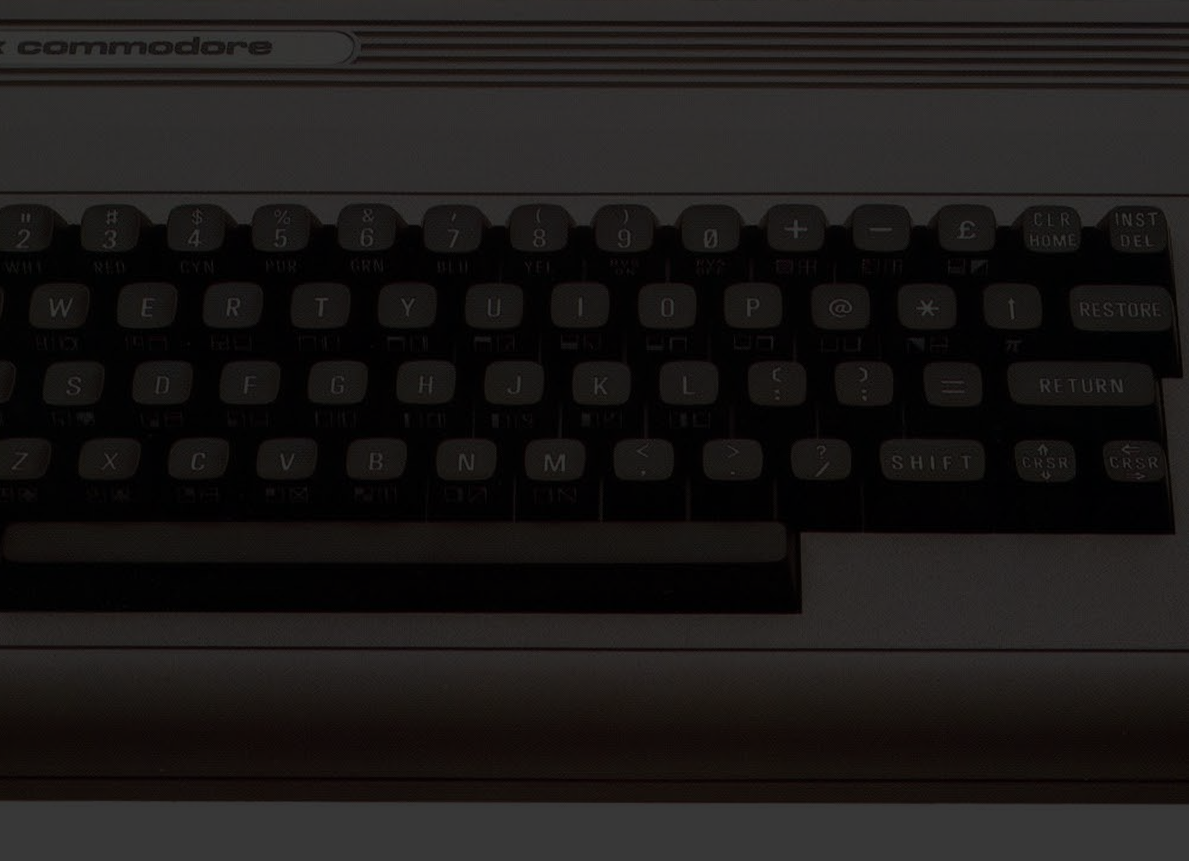
su
upda

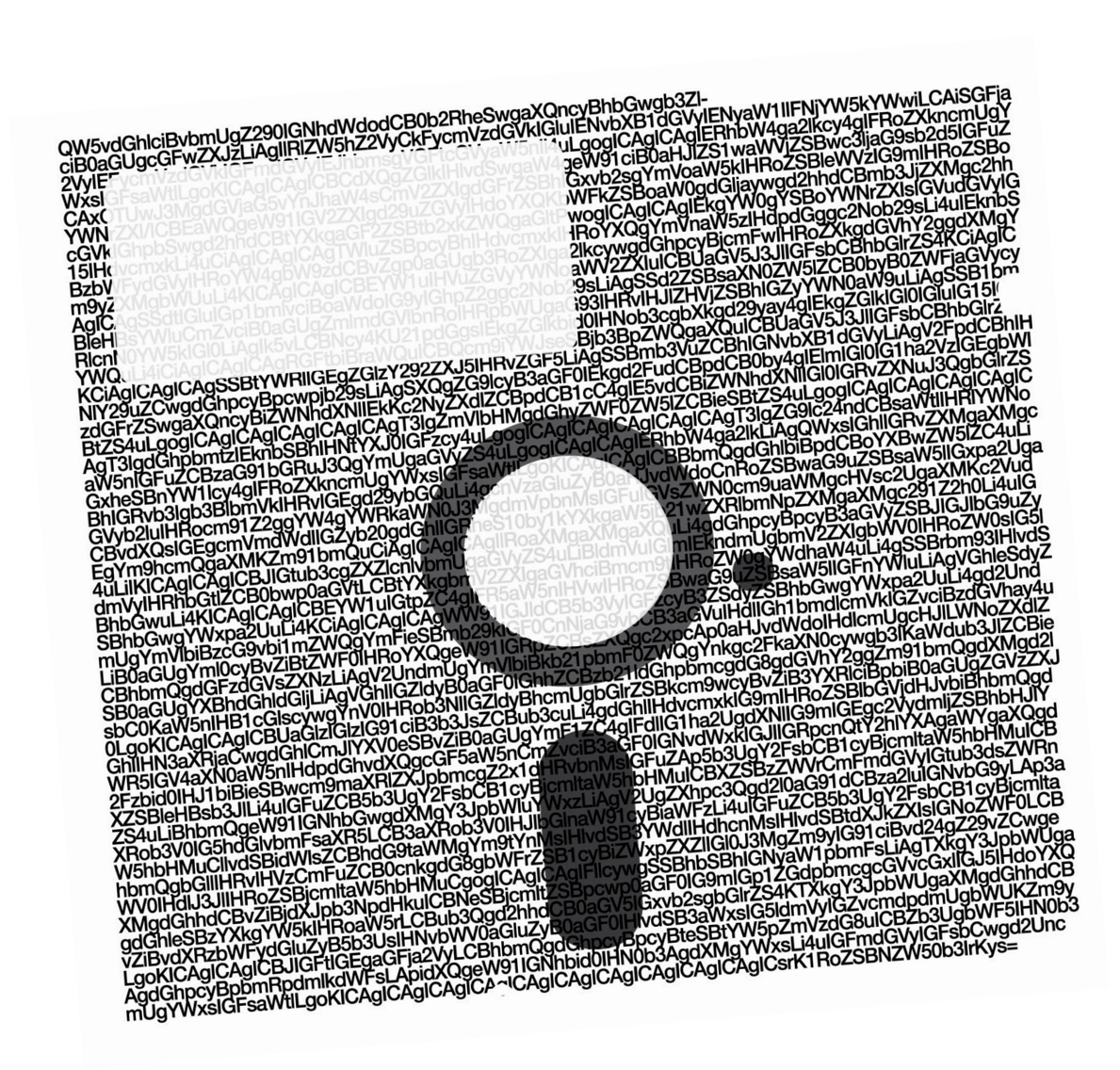
double sided




```
**** COMMODORE 64 BASIC V2 ****
64K RAM SYSTEM  38911 BASIC BYTES FREE

READY.
```



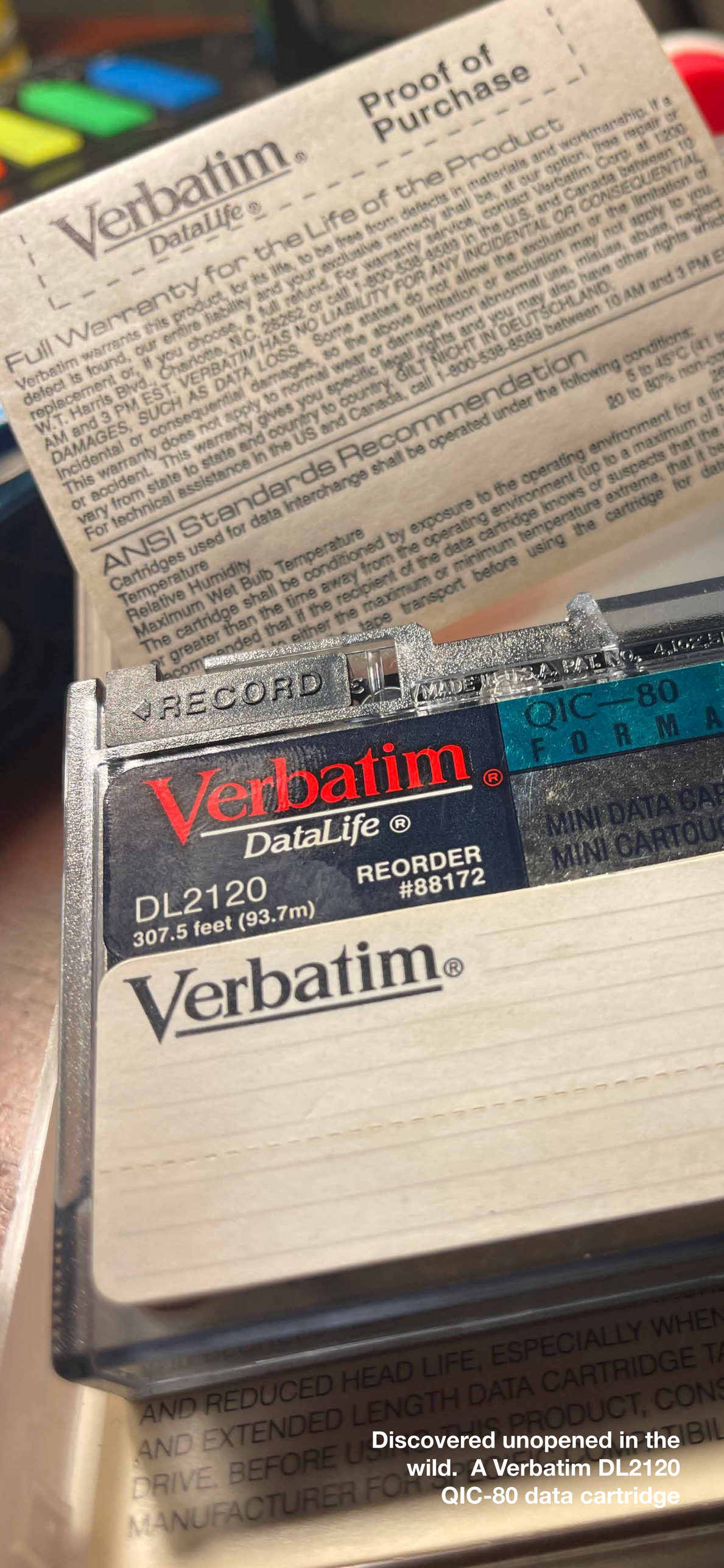


The 5 1/4 Floppy Disc

Originally designed as a single-sided, low-density format with a storage capacity of 100 KB, the 5.25-inch floppy disk underwent many enhancements, including the introduction of a double-sided, high-density variant with a capacity of 1.2 MB.

Like all floppy disks, the 5.25-inch floppy disk had a magnetic disk inside a case with a hole in the middle and was used with a dedicated disk drive capable of reading the magnetic data from the disk. However, the 5.25-inch floppy disk used a paper cover for the protection of the magnetic face of the disk and there was no other built-in protection

The 5.25-inch floppy disk was the successor to the 8-inch floppy disk and served as the dominant portable storage medium during the late 1970s and throughout the 1980s. It was developed in 1976 and was similar in capacity to the 8-inch floppy disk but used high-density media and recording techniques. Because of its lower price and smaller size, the 5.25-inch floppy disk quickly replaced its predecessor.



Discovered unopened in the wild. A Verbatim DL2120 QIC-80 data cartridge

refuse
resist

neutral ground

HVCK has no official affiliations with any group or organisation. What we do have is a passion for people willing to fight for what's right.

WARNING:
Those with questionable moral or ethical standards may find the next pages to cause the following symptoms:

Nausea
Sweating
Acute Paranoia

If these symptoms persist. Eat a dick.


```
   /$$ /$$    /$$$$$$            /$$$$$$  /$$      /$$ /$$      /$$  /$$$$$$            /$$$$$$           /$$
  / $$/ $$   /$$__  $$          /$$__  $$| $$     |__/| $$     | $$ /$$__  $$          /$$__  $$         | $$
 /$$$$$$$$$| $$  \ $$  /$$$$$$ | $$  \__/| $$$$$$$  /$$| $$  /$$$$$$$| $$  \__/  /$$$$$$ | $$  \__//$$$$$$  /$$$$$$   /$$   /$$
|   $$  $$_/| $$  | $$ /$$__  $$| $$      | $$__  $$| $$| $$ /$$__  $$|  $$$$$$  |____  $$| $$$$   /$$__  $$|_  $$_/  | $$  | $$
 /$$$$$$$$$| $$  | $$| $$  \ $$| $$      | $$  \ $$| $$| $$| $$  | $$ \____  $$  /$$$$$$$| $$_/  | $$$$$$$  | $$    | $$  | $$
|_  $$  $$_/| $$  | $$| $$  | $$| $$    $$| $$  | $$| $$| $$| $$  | $$ /$$  \ $$ /$$__  $$| $$    | $$_____/  | $$ /$$| $$  | $$
  | $$| $$  |  $$$$$$/| $$$$$$$/|  $$$$$$/| $$  | $$| $$| $$|  $$$$$$$|  $$$$$$/|  $$$$$$$| $$    |  $$$$$$$  |  $$$$/|  $$$$$$$
  |__/|__/   \______/ | $$____/  \______/ |__/  |__/|__/|__/ \_______/ \______/  \_______/|__/     \_______/   \___/   \____/  $$
                      | $$                                                                                                  /$$  | $$
                      | $$                                                                                                 |  $$$$$$/
                      |__/                                                                                                  \______/
```

#GhostSec #Anonymous
https://t.me/GhostSecc
https://github.com/ghostsec420/Opchildsafety2
https://youtu.be/Afsa2Q57og8
==========

Greetings users around the globe we are GhostSec. I Userware would like to take an opportunity to announce the resuming of an operation called #OpChildSafety. As part of the Anonymous collective it is our responsiblity not just as activists or hacktivists but as a collective to fight against the mass pedophilia on the internet. We GhostSec ask every user who is watching this. those who are willing to join the hunt down of these sick freaks who deserve to be sentenced behind bars and worse.

Such lawlessness must not continue on yet these beasts come back again and again promising that they won't do it ever again! Well guess what users? That's what they all say over and over and over AGAIN! They just couldn't keep their promises now do they?! I think we shouldn't stay soft any longer to these sick freaks!

But GhostSec why? The governments are actually trying their best to punish these criminals. Oh really? Let me tell you the truth user. We vigilante hackers are trying our best not to get caught by the law enforcement. To be honest I really lost faith in them. Some countries like Sweden and Norway just let these rapists go unsc athed. In contrast, a hacker can go to 6 months to 6 years depending of what acts he committed or probably even a decade. However, these fiends just get away with it.

Now are you convinced user? Are you willing to let these sadistic fucks get away with it like nothing ever happened? I'm sure you do feel that fury of yours that has struck inside of you, you want to relief it somehow with that murderous intent of yours. However, I need you to calm down because it won't work that way. These criminals would have wished they were never been born with their sick lustful desires. So all we can do is by giving them the agony to torment their minds. Knock down their doors! To avenge the victims especially the children in exchange for their sanity. That's why we won't let them get what they wish for.

How can we achieve our united goal through online hacktivism and even activism?

First for hacktivism, our goal would be to shutdown and expose as many of these child pornography or pedophilia sites and forums that exist, this can be done through everyone's favorite and most popular method DDoS attacks though we encourage to leave that as a last option, we recommend first attacking the web servers through any other means, exfiltrate as much data as possible, gather info on users and admins of the site, deface the sites, etc etc and remember anything goes.

The main goal is to use any means to attack, and disrupt our targets child pornography and pedo operations

For activists how you may help?
You all can spread and support our cause through writing and getting people to acknowledge it, it will encourage others to join the operation or even let people who can't support our cause directly at least know we exist and are fighting for the children who have been victimized.

#OpChildSafety initiated.

We are Anonymous
We are Legion
We do not Forgive
We do not Forget the silence of the victims
Expect us
we run shit because we can!

```
      ###, ,##, ,##,
       #  # #  # #  #
       ###  #  # #  #  Expect Us
       #  # #  # #  #
       ###' '##' '##'
```

```
           .--,
          /  (
         /    \
        /      \
       /  0  0  \
(((()   |    ()    |   ()))
\  ()  (  .____.  )  ()  /
 |` \_/ \  `""`  / \_/ `|
 |       `.'--'.`       |
  \        `""`        /
```

I'm sorry

but I don t want to be an emperor. That s not my business. I don t want to rule or conquer anyone.

I should like to help everyone - if possible - Jew, Gentile - black man - white. We all want to help one another. Human beings are like that.

We want to live by each other s happiness - not by each other s misery. We don t want to hate and despise one another. In this world there is room for everyone.

And the good earth is rich and can provide for everyone. The way of life can be free and beautiful, but we have lost the way.

Greed has poisoned men s souls, has barricaded the world with hate, has goose-stepped us into misery and bloodshed. We have developed speed, but we have shut ourselves in. Machinery that gives abundance has left us in want. Our knowledge has made us cynical. Our cleverness, hard and unkind. We think too much and feel too little. More than machinery we need humanity. More than cleverness we need kindness and gentleness. Without these qualities, life will be violent and all will be lost

The aeroplane and the radio have brought us closer together. The very nature of these inventions cries out for the goodness in men - cries out for universal brotherhood - for the unity of us all. Even now my voice is reaching millions throughout the world - millions of despairing men, women, and little children - victims of a system that makes men torture and imprison innocent people.

To those who can hear me, I say - do not despair. The misery that is now upon us is but the passing of greed - the bitterness of men who fear the way of human progress. The hate of men will pass, and dictators die, and the power they took from the people will return to the people. And so long as men die, liberty will never perish

Soldiers! don t give yourselves to brutes - men who despise you - enslave you - who regiment your lives - tell you what to do - what to think and what to feel! Who drill you - diet you - treat you like cattle, use you as cannon fodder. Don t give yourselves to these unnatural men - machine men with machine minds and machine hearts! You are not machines! You are not cattle! You are men! You have the love of humanity in your hearts! You don t hate! Only the unloved hate - the unloved and the unnatural! Soldiers! Don t fight for slavery! Fight for liberty!

In the 17th Chapter of St Luke it is written: the Kingdom of God is within man - not one man nor a group of men, but in all men! In you! You, the people have the power - the power to create machines. The power to create happiness! You, the people, have the power to make this life free and beautiful, to make this life a wonderful adventure.

Then - in the name of democracy - let us use that power - let us all unite. Let us fight for a new world - a decent world that will give men a chance to work - that will give youth a future and old age a security. By the promise of these things, brutes have risen to power. But they lie! They do not fulfil that promise. They never will!

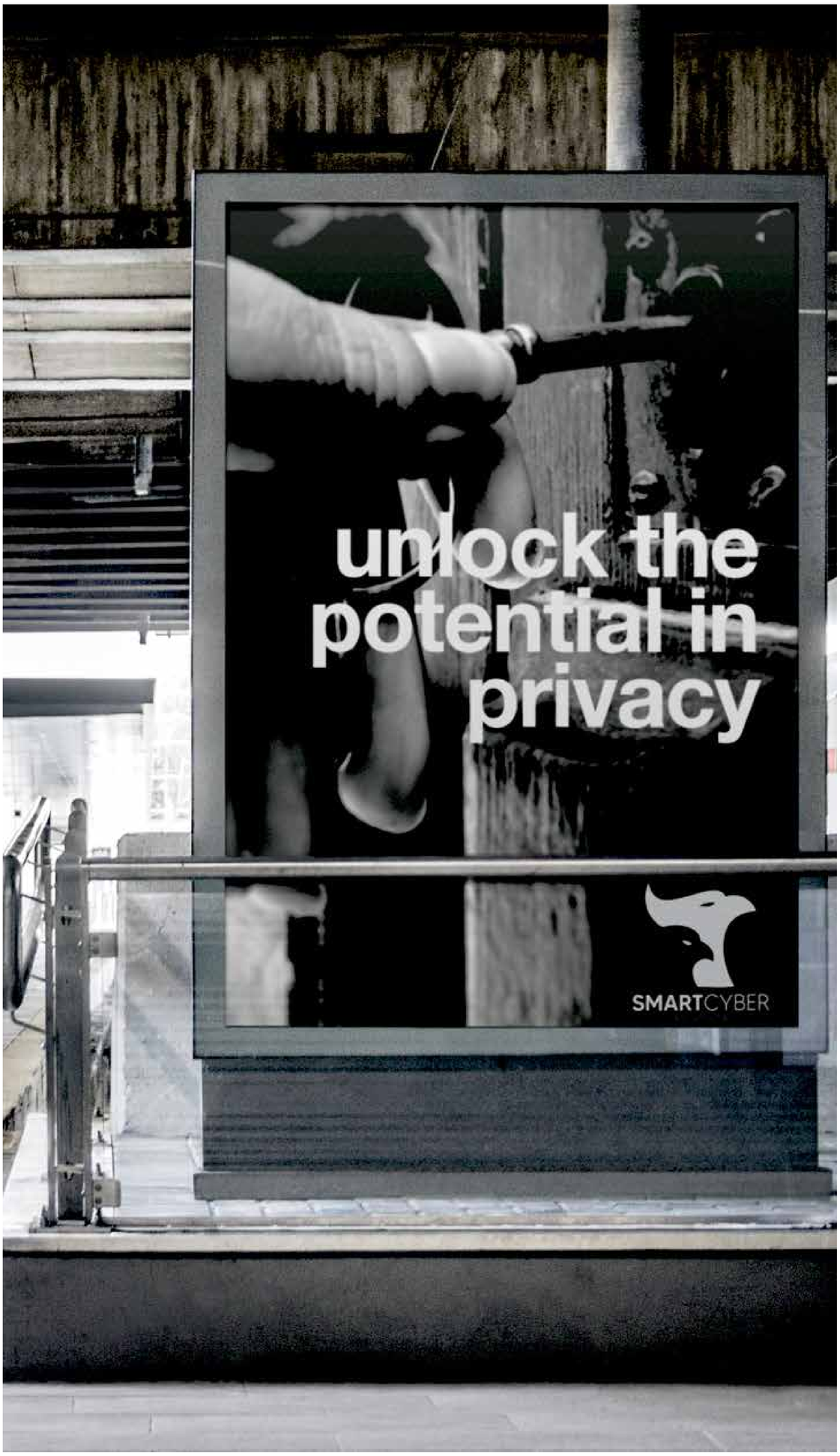
Dictators free themselves but they enslave the people! Now let us fight to fulfil that promise! Let us fight to free the world - to do away with national barriers - to do away with greed, with hate and intolerance. Let us fight for a world of reason, a world where science and progress will lead to all men s happiness. Soldiers! in the name of democracy, let us all....

unite

unite

unite

unite



Privacy & Anonymity Services

SMARTCYBER
solutions

tracks

Recall

by Plaster

Gianclaudio Hashem Moniri is an enigima. One of the most diverse producers I've come across of late. Switching effortlessly between the experimental drone and ambient he performs under his own name and the dark brooding timbres he creates as Plaster.

"I feel oppressed by the fast consuming of our society. Love, friendship, spirituality and our relation with technology, needs a pure consciousness, not influenced by violence and disruptive capitalism. This is what Recall means for me."

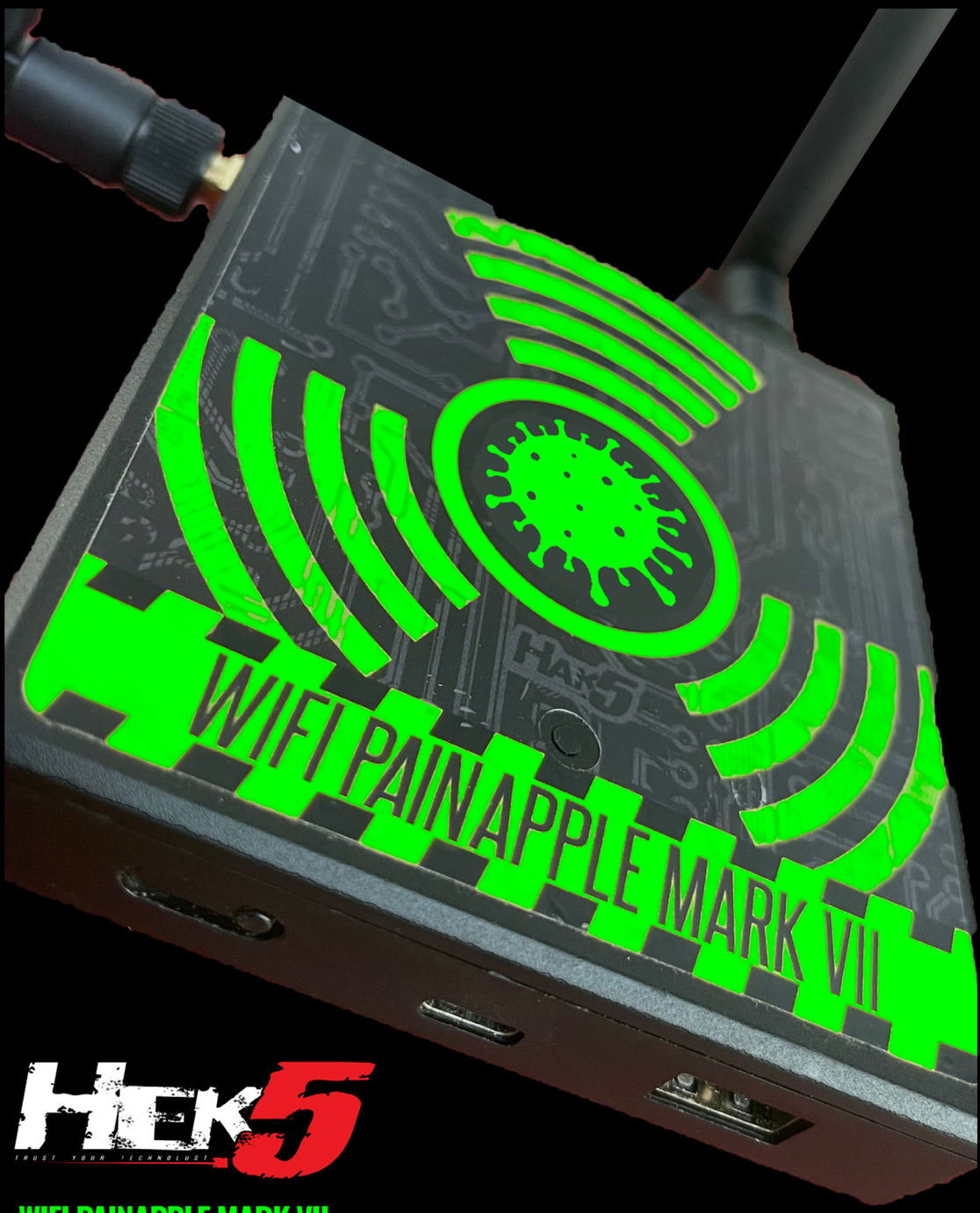
Both of the offerings on this 2 track release feel like a direct response to the oppression. The second track "Harden", feels like earbud candy for a day of solid political dissent. Aggressive percussive synth patterns stab their way between a lazy off beat kick. An interesting vocal sample and the shadow of an acid line bind it all together. In reality, though it is the more up tempo of the two tracks, it pales in comparison to track one.

Mongrel begins almost as a whisper of white noise. The serenity is short lived. Thick with distortion, the kick and bassline drag the track forward in an awkward perfection. A haunting cut up loop of dirty vocals drives home the ominous overtones. It has the vibe of Godzilla making her way towards Tokyo. Big, bad and really really pissed, ready to f$%k shit up.

Emotive, dark and distorted. A relentless momentum, not unlike the capitalism that inspired it. "Recall" is available now on Kvitnu.

https://kvitnu.bandcamp.com/album/recall

Review by Ryan Williams



HAK5
TRUST YOUR TECHNOLUST

WIFI PAINAPPLE MARK VII

CUSTOM 5G VAX MOD

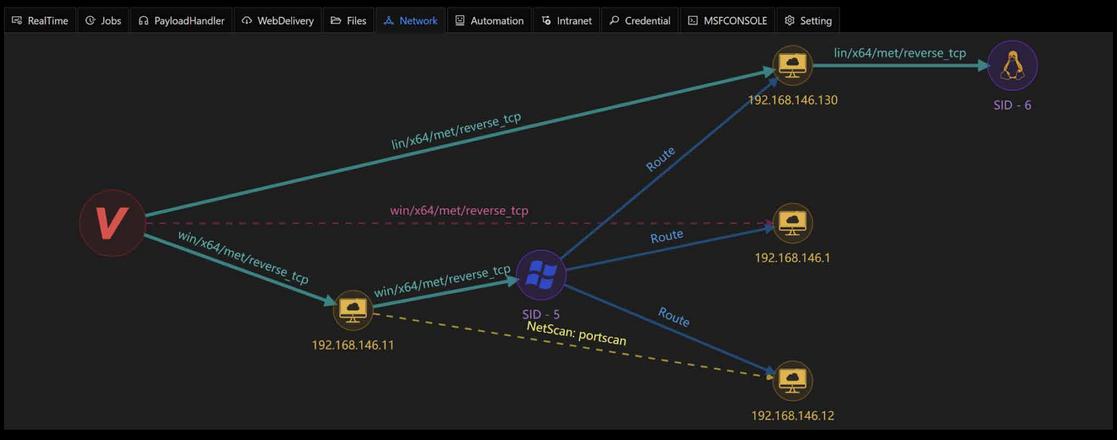
CONNECT TO YOUR NANOBOTNET AND MAKE THE MOST OF THE 5G COURSING THROUGH YOUR BODY WITH THE NEW 5G VAX MOD FOR THE HEK5 WIFI PAINAPPLE.

ANOTHER INNOVATION FROM

FLAT EARTH SOCIETY

hacks


KITPLOIT
THE HACKER'S TOOLS
TOP 3

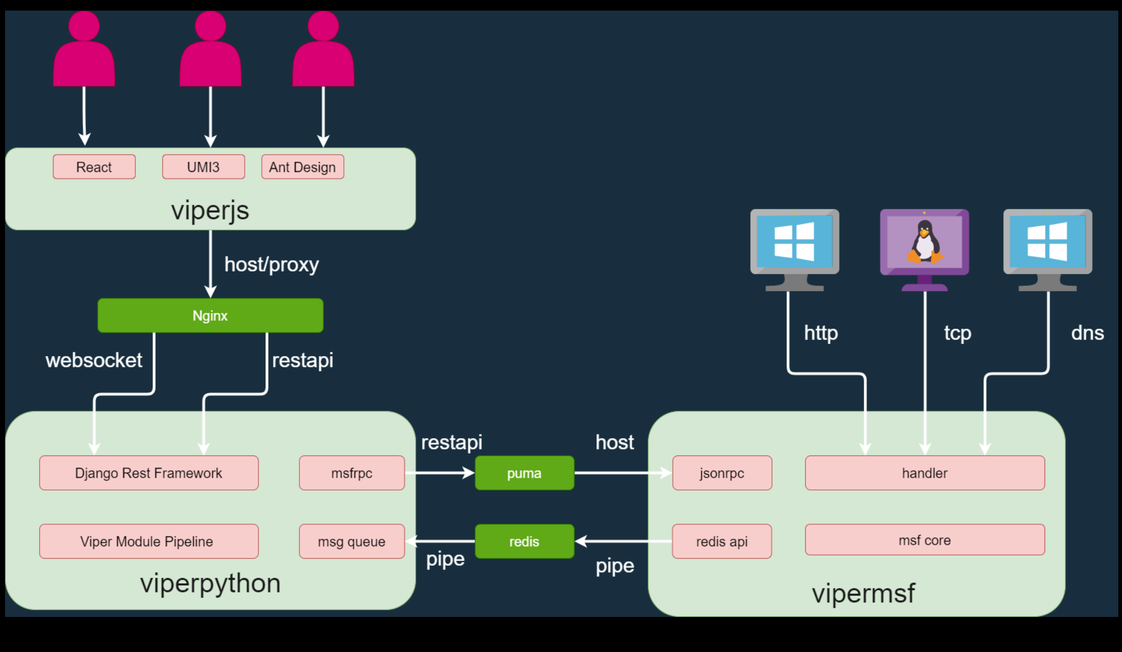


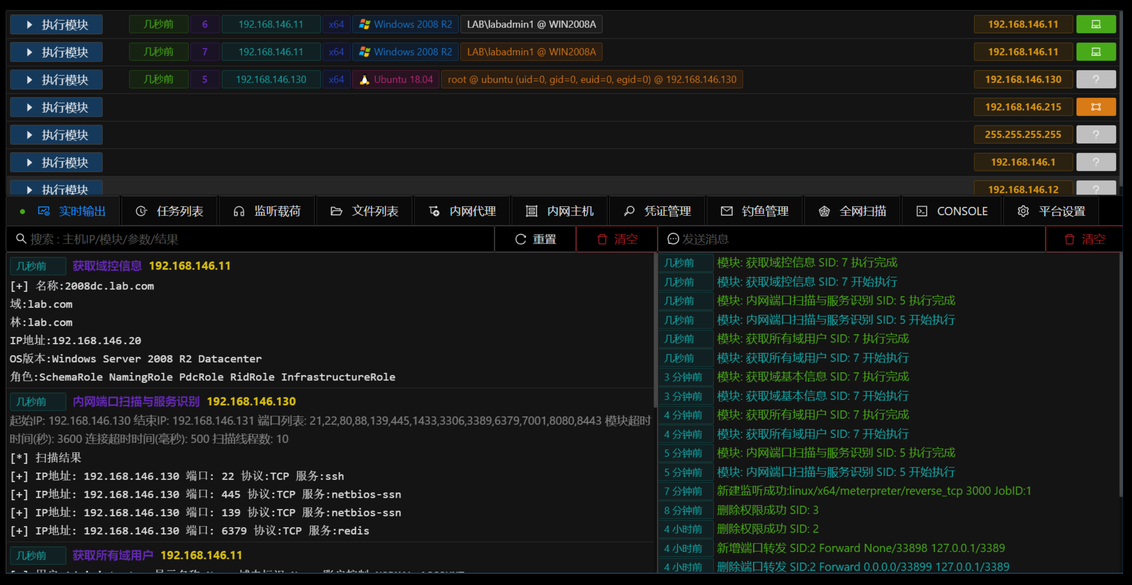
Open source graphical intranet penetration tool

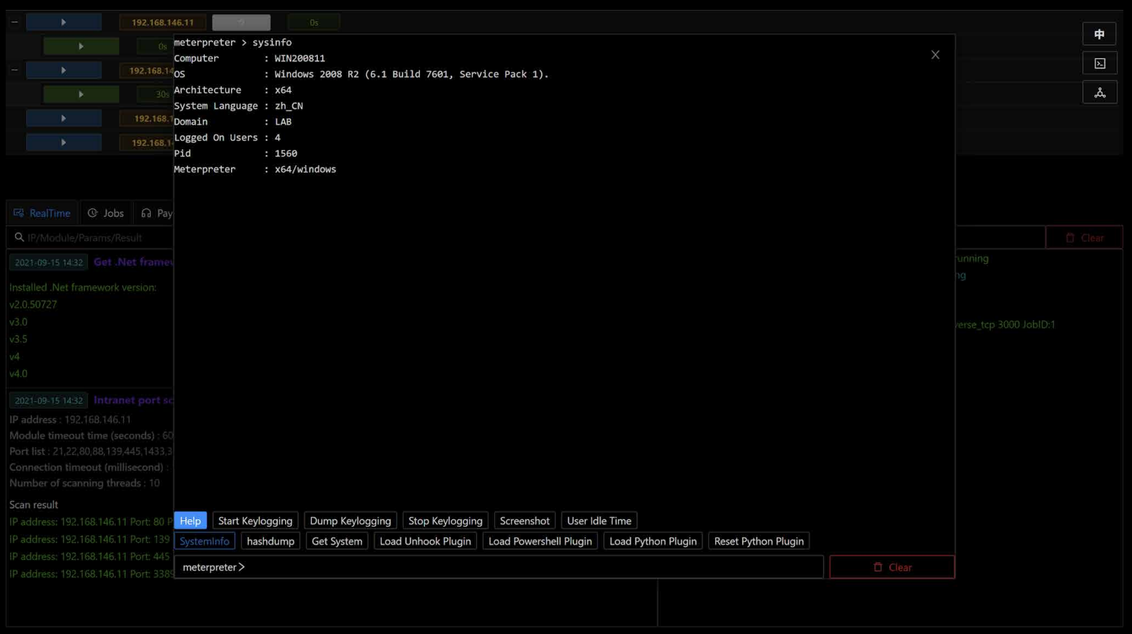
Viper is a graphical intranet penetration tool that modularizes and weaponizes the tactics and techniques commonly used in the intranet penetration process. Intergrating basic functions such as anti-software bypass, intranet tunnel, file management, and command line.

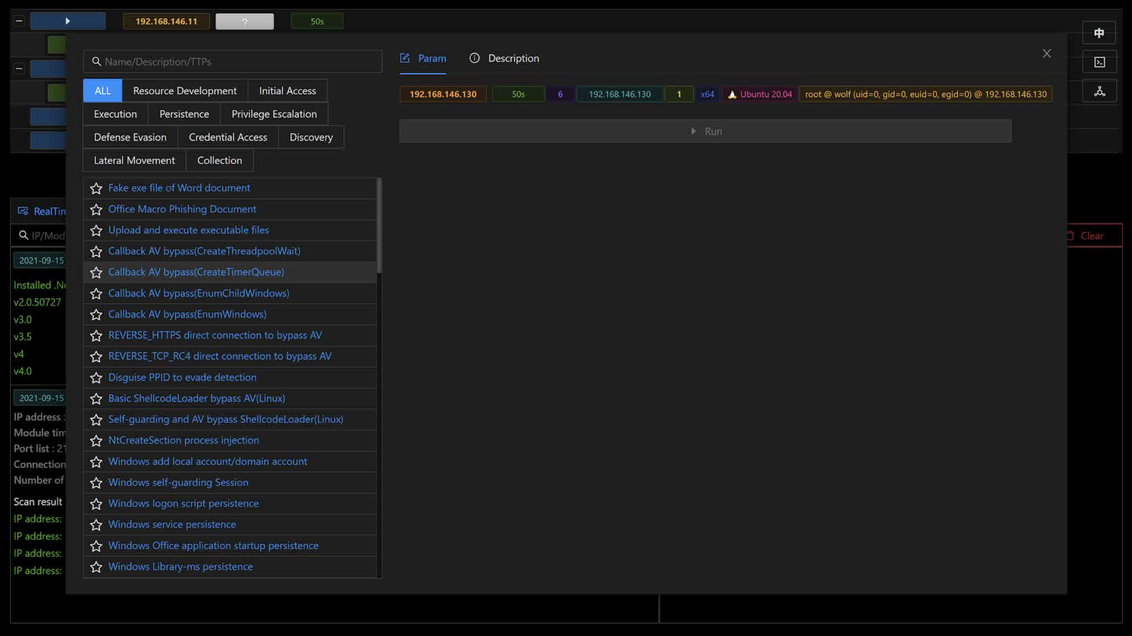
Currently viper has integrated 70+ modules, covering initial access/persistence/privilege escalation/defense bypass/credential access/information collection/lateral movement and other categories. Viper's goal is to help red team engineers improve attack efficiency, simplify operations, and lower technical thresholds.

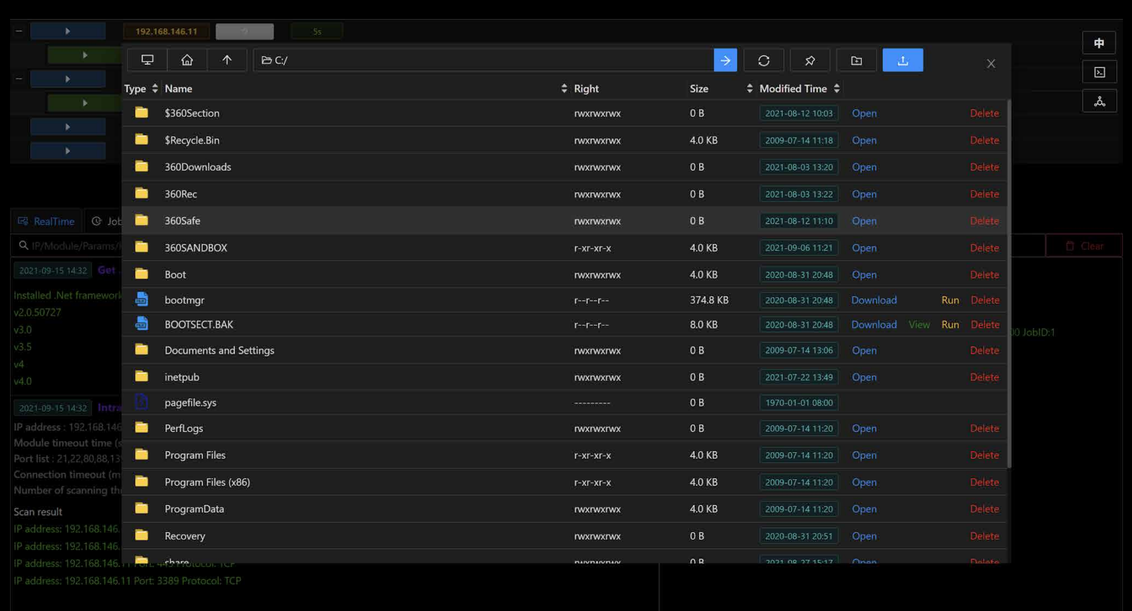
Viper also supports running native msfconsole in the browser and supports multi-person collaboration. This project was created for educational purposes and should not be used in environments without legal authorization. Download here: https://github.com/FunnyWolf/Viper




执行模块 几秒前 6 192.168.146.11 x64 Windows 2008 R2 LAB\labadmin1 @ WIN2008A 192.168.146.11
执行模块 几秒前 7 192.168.146.11 x64 Windows 2008 R2 LAB\labadmin1 @ WIN2008A 192.168.146.11
执行模块 几秒前 5 192.168.146.130 x64 Ubuntu 18.04 root @ ubuntu (uid=0, gid=0, euid=0, egid=0) @ 192.168.146.130 192.168.146.130
执行模块 192.168.146.215
执行模块 255.255.255.255
执行模块 192.168.146.1
执行模块 192.168.146.12
实时输出
任务列表
监听载荷
文件列表
内网代理
内网主机
凭证管理
钓鱼管理
全网扫描
CONSOLE
平台设置
搜索：主机IP/模块/参数/结果
重置
清空
发送消息
清空
几秒前 获取域控信息 192.168.146.11
[+] 名称:2008dc.lab.com
域:lab.com
林:lab.com
IP地址:192.168.146.20
OS版本:Windows Server 2008 R2 Datacenter
角色:SchemaRole NamingRole PdcRole RidRole InfrastructureRole
几秒前 内网端口扫描与服务识别 192.168.146.130
起始IP: 192.168.146.130 结束IP: 192.168.146.131 端口列表: 21,22,80,88,139,445,1433,3306,3389,6379,7001,8080,8443 模块超时时间(秒): 3600 连接超时时间(毫秒): 500 扫描线程数: 10
[*] 扫描结果
[+] IP地址: 192.168.146.130 端口: 22 协议:TCP 服务:ssh
[+] IP地址: 192.168.146.130 端口: 445 协议:TCP 服务:netbios-ssn
[+] IP地址: 192.168.146.130 端口: 139 协议:TCP 服务:netbios-ssn
[+] IP地址: 192.168.146.130 端口: 6379 协议:TCP 服务:redis
几秒前 获取所有域用户 192.168.146.11
几秒前 模块: 获取域控信息 SID: 7 执行完成
几秒前 模块: 获取域控信息 SID: 7 开始执行
几秒前 模块: 内网端口扫描与服务识别 SID: 5 执行完成
几秒前 模块: 内网端口扫描与服务识别 SID: 5 开始执行
几秒前 模块: 获取所有域用户 SID: 7 执行完成
几秒前 模块: 获取所有域用户 SID: 7 开始执行
3 分钟前 模块: 获取域基本信息 SID: 7 执行完成
3 分钟前 模块: 获取域基本信息 SID: 7 开始执行
4 分钟前 模块: 获取所有域用户 SID: 7 执行完成
4 分钟前 模块: 获取所有域用户 SID: 7 开始执行
5 分钟前 模块: 内网端口扫描与服务识别 SID: 5 执行完成
5 分钟前 模块: 内网端口扫描与服务识别 SID: 5 开始执行
7 分钟前 新建监听成功:linux/x64/meterpreter/reverse_tcp 3000 JobID:1
8 分钟前 删除权限成功 SID: 3
4 小时前 删除权限成功 SID: 2
4 小时前 新增端口转发 SID:2 Forward None/33898 127.0.0.1/3389
4 小时前 删除端口转发 SID:2 Forward 0.0.0.0/33899 127.0.0.1/3389


meterpreter > sysinfo
Computer : WIN200811
OS : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : zh_CN
Domain : LAB
Logged On Users : 4
Pid : 1560
Meterpreter : x64/windows
Help
Start Keylogging
Dump Keylogging
Stop Keylogging
Screenshot
User Idle Time
SystemInfo
hashdump
Get System
Load Unhook Plugin
Load Powershell Plugin
Load Python Plugin
Reset Python Plugin
meterpreter >
Clear


Name/Description/TTPs
Param
Description
ALL
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Fake exe file of Word document
Office Macro Phishing Document
Upload and execute executable files
Callback AV bypass(CreateThreadpoolWait)
Callback AV bypass(CreateTimerQueue)
Callback AV bypass(EnumChildWindows)
Callback AV bypass(EnumWindows)
REVERSE_HTTPS direct connection to bypass AV
REVERSE_TCP_RC4 direct connection to bypass AV
Disguise PPID to evade detection
Basic ShellcodeLoader bypass AV(Linux)
Self-guarding and AV bypass ShellcodeLoader(Linux)
NtCreateSection process injection
Windows add local account/domain account
Windows self-guarding Session
Windows logon script persistence
Windows service persistence
Windows Office application startup persistence
Windows Library-ms persistence
192.168.146.130 50s 6 192.168.146.130 1 x64 Ubuntu 20.04 root @ wolf (uid=0, gid=0, euid=0, egid=0) @ 192.168.146.130
Run

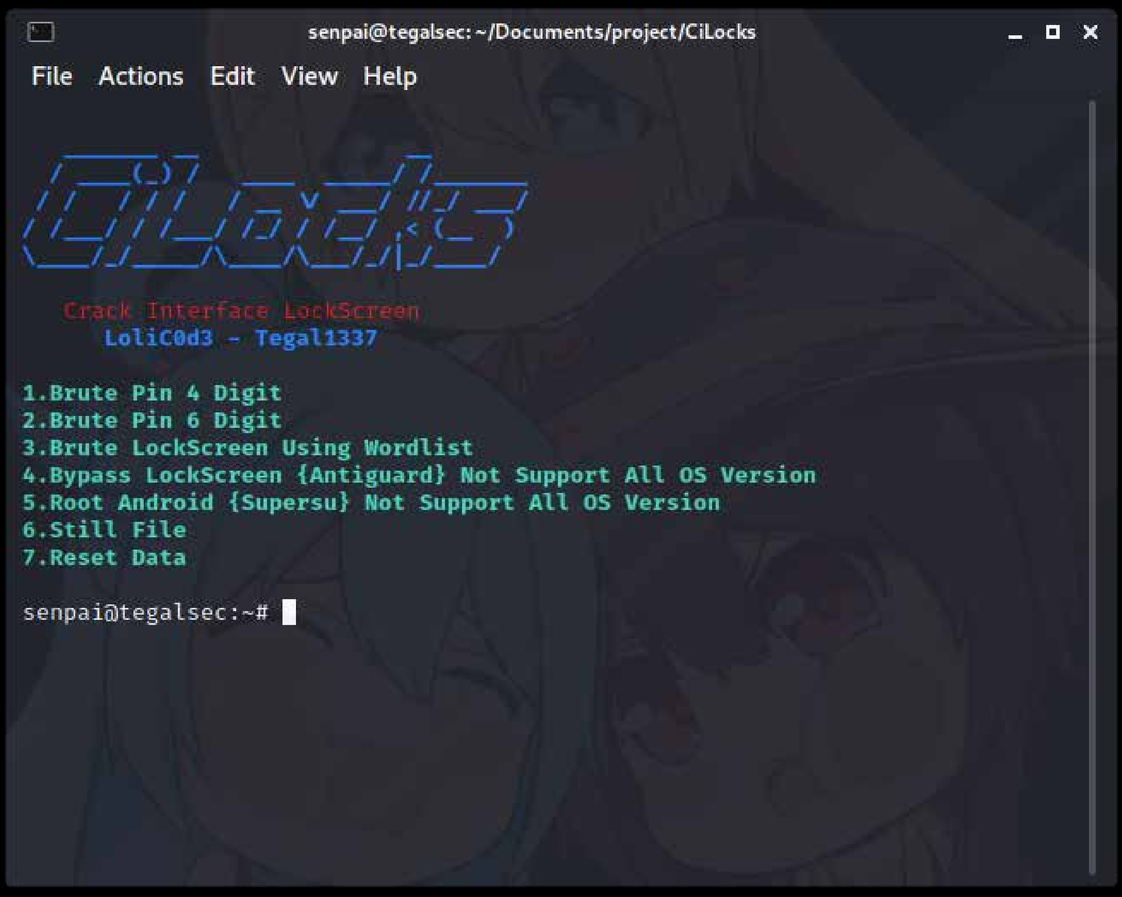

C:/
Type
Name
Right
Size
Modified Time
$360Section rwxrwxrwx 0 B 2021-08-12 10:03 Open Delete
$Recycle.Bin rwxrwxrwx 4.0 KB 2009-07-14 11:18 Open Delete
360Downloads rwxrwxrwx 0 B 2021-08-03 13:20 Open Delete
360Rec rwxrwxrwx 0 B 2021-08-03 13:22 Open Delete
360Safe rwxrwxrwx 0 B 2021-08-12 11:10 Open Delete
360SANDBOX r-xr-xr-x 4.0 KB 2021-09-06 11:21 Open Delete
Boot rwxrwxrwx 4.0 KB 2020-08-31 20:48 Open Delete
bootmgr r--r--r-- 374.8 KB 2020-08-31 20:48 Download Run Delete
BOOTSECT.BAK r--r--r-- 8.0 KB 2020-08-31 20:48 Download View Run Delete
Documents and Settings rwxrwxrwx 0 B 2009-07-14 13:06 Open Delete
inetpub rwxrwxrwx 0 B 2021-07-22 13:49 Open Delete
pagefile.sys --------- 0 B 1970-01-01 08:00
PerfLogs rwxrwxrwx 0 B 2009-07-14 11:20 Open Delete
Program Files r-xr-xr-x 4.0 KB 2009-07-14 11:20 Open Delete
Program Files (x86) r-xr-xr-x 4.0 KB 2009-07-14 11:20 Open Delete
ProgramData rwxrwxrwx 4.0 KB 2009-07-14 11:20 Open Delete
Recovery rwxrwxrwx 0 B 2020-08-31 20:51 Open Delete

Ventoy is an open source tool to create bootable USB drive for ISO/WIM/IMG/VHD(x)/EFI files. With ventoy, you don't need to format the disk over and over, you just need to copy the image files to the USB drive and boot it. You can copy many image files at a time and ventoy will give you a boot menu to select them.

x86 Legacy BIOS, IA32 UEFI, x86_64 UEFI, ARM64 UEFI and MIPS64EL UEFI are supported in the same way. Both MBR and GPT partition style are supported in the same way.

- Can be installed in USB/Local Disk/SSD/NVMe/SD Card
- Directly boot from ISO/WIM/IMG/VHD(x)/EFI files, no extraction needed
- No need to be continuous in disk for ISO/IMG files
- MBR and GPT partition style supported (1.0.15+)
- x86 Legacy BIOS, IA32 UEFI, x86_64 UEFI, ARM64 UEFI, MIPS64EL UEFI supported
- IA32/x86_64 UEFI Secure Boot supported (1.0.07+)
- Persistence supported (1.0.11+)
- Windows auto installation supported (1.0.09+)
- RHEL7/8/CentOS/7/8/SUSE/Ubuntu Server/Debian ... auto installation supported (1.0.09+)
- FAT32/exFAT/NTFS/UDF/XFS/Ext2(3)(4) supported for main partition
- ISO files larger than 4GB supported
- Native boot menu style for Legacy & UEFI
- Most type of OS supported, 700+ iso files tested
- Linux vDisk boot supported
- Not only boot but also complete installation process
- Menu dynamically switchable between List/TreeView mode
- "Ventoy Compatible" concept
- Plugin Framework
- Injection files to runtime environment
- Boot configuration file dynamically replacement
- Highly customizable theme and menu
- USB drive write-protected support
- USB normal use unaffected
- Data nondestructive during version upgrade
- No need to update Ventoy when a new distro is released

Download Ventoy here:
https://github.com/ventoy/Ventoy



Features:

Brute Pin 4 Digit
Brute Pin 6 Digit
Brute LockScreen Using Wordlist
Bypass LockScreen {Antiguard} Not Support All OS Version
Root Android {Supersu} Not Support All OS Version
Steal File
Reset Data

Required:

- Adb {Android SDK}
- Cable Usb
- Android Emulator {NetHunter/Termux} Root
- Or Computer

Compatible

- Linux
- Windows
- Mac

As was probably a give away in the title, these 3 tools can be found at KitPloit.com

free beer

kahlil gibran

A schooner for the soul. I thought I'd round out this issue with some beautiful words from the great man himself.

Defeat

Defeat, my Defeat, my solitude and my aloofness;
You are dearer to me than a thousand triumphs,
And sweeter to my heart than all world-glory.

Defeat, my Defeat, my self-knowledge and my defiance,
Through you I know that I am yet young and swift of foot
And not to be trapped by withering laurels.
And in you I have found aloneness
And the joy of being shunned and scorned.

Defeat, my Defeat, my shining sword and shield,
In your eyes I have read
That to be enthroned is to be enslaved,
And to be understood is to be leveled down,
And to be grasped is but to reach one's fullness
And like a ripe fruit to fall and be consumed.

Defeat, my Defeat, my bold companion,
You shall hear my songs and my cries and my silences,
And none but you shall speak to me of the beating of wings,
And urging of seas,
And of mountains that burn in the night,
And you alone shall climb my steep and rocky soul.

Defeat, my Defeat, my deathless courage,
You and I shall laugh together with the storm,
And together we shall dig graves for all that die in us,
And we shall stand in the sun with a will,
And we shall be dangerous.

fin.