OWASP 2023 GLOBAL AppSec

WASHINGTON

DC

OCT 30 • NOV 3

OWASP 2023 GLOBAL AppSec | WASHINGTON DC OCT 30-NOV 3

THE THREAT ACTORS WE FORGOT TO MODEL: PROFILING PSYCHOLOGICALLY-MOTIVATED CYBER CRIMINALS

JACKIE SINGH

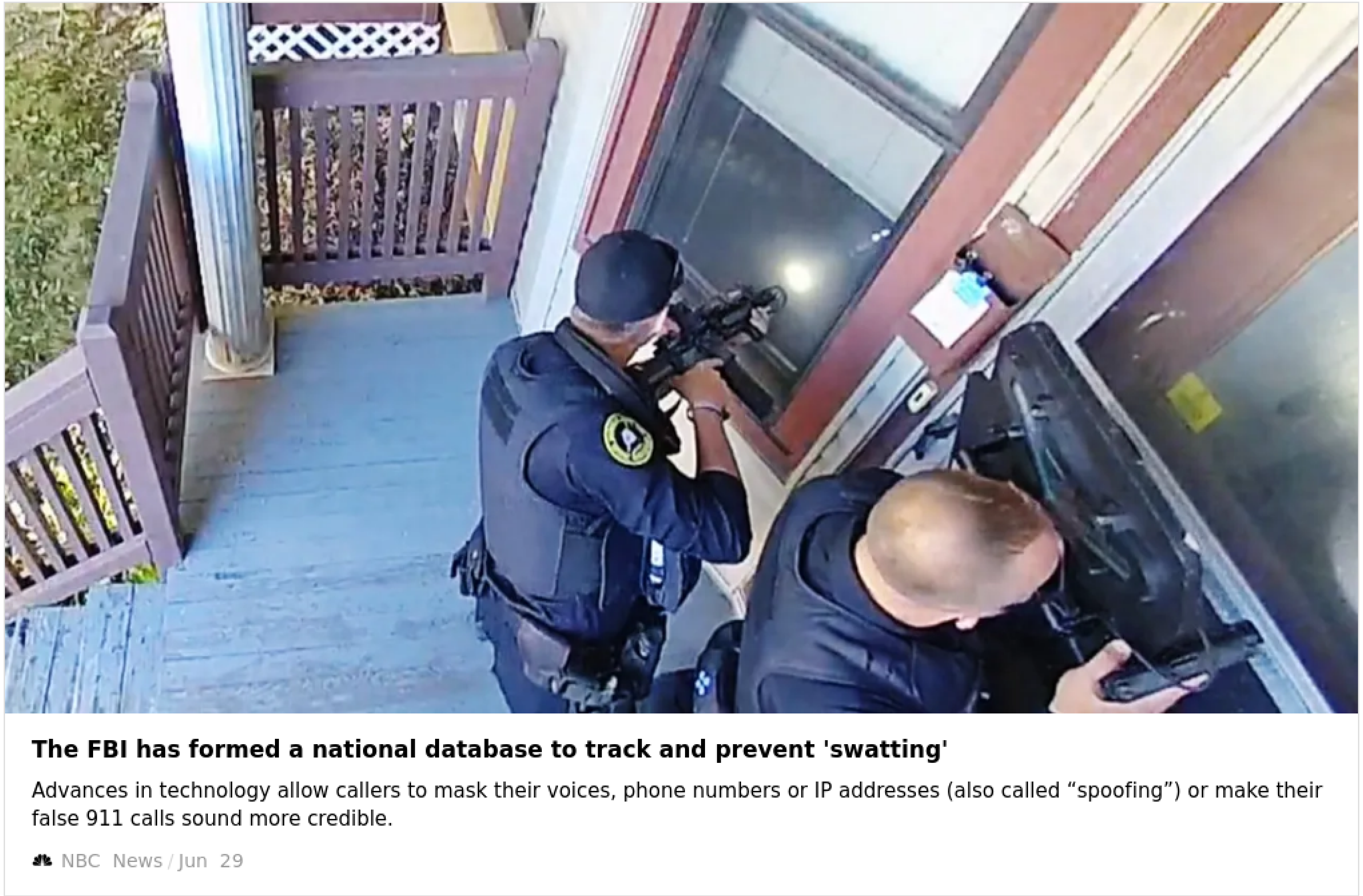
Visualization Exercise

Visualization Exercise

Video
NIGHTLY NEWS
NBC NIGHTLY NEWS

(Video Source)

HTTPS://WWW.NBCNEWS.COM/NEWS/US-NEWS/FBI-FORMED-NATIONAL-DATABASE-TRACK-PREVENT-SWATTING-RCNA91722



The FBI has formed a national database to track and prevent 'swatting'

Advances in technology allow callers to mask their voices, phone numbers or IP addresses (also called “spoofing”) or make their false 911 calls sound more credible.

NBC News / Jun 29

Key Issues

- A primary Victim is consistently targeted by a networked group using technological means.

- The Victim and people connected to the Victim cannot ignore these attacks due to their consistent, persistent, and scaled nature.

- These attacks have had real-world consequences for the Victim.

- The Victim's public and private data, real or falsified, are key assets to the attackers.

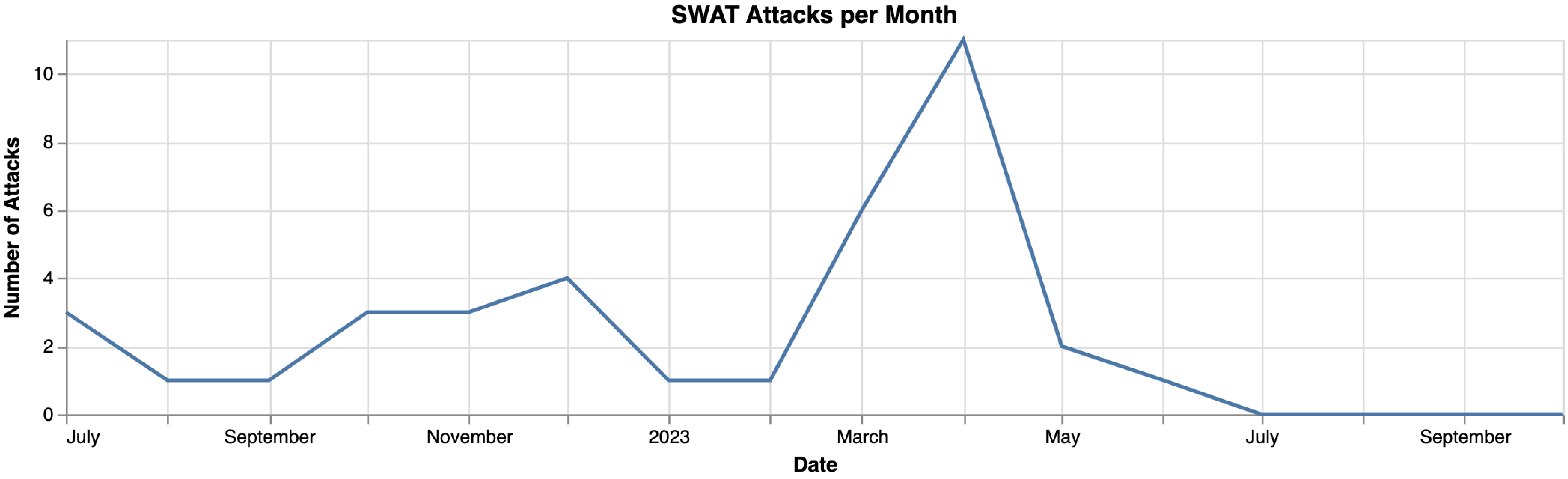
- These attackers are not unique; their modus operandi (TTPs) are shared culturally in low- or no-moderation online spaces and can include harassment, stalking, swatting, abuse of personal data such as doxing, and disinformation attacks.

- No one is properly naming or addressing these threats. Some folks doubt they are real. Companies are not properly handling abuse reports. Infosec is unaware.

Strategic Attacks Against Public Participation “SAAPP”

The goal of SAAPP attacks are to ‘sap’ the victim's will to continue participating in public life. These attacks attempt to degrade the victim's reputation in the eyes of the world, to isolate and disconnect them from their allies, friends and colleagues, and to cause them to doubt themselves and withdraw from their work.

(Jackie Singh, 2023)


SWAT Attacks per Month
Number of Attacks
0
2
4
6
8
10
July
September
November
2023
March
May
July
September
Date

Big Picture

- About 1.2% of U.S. adult men and 0.3% to 0.7% of U.S. adult women are considered to have clinically significant levels of psychopathic traits (APA).
- NJ-based psychologist Dr. Nuccitelli has defined **iPredopathy** as an "advanced stage personality disorder describing any adolescent to adult male or female who skillfully uses Information and Communications Technology to troll, identify, control and manipulate their human targets."

Big Picture

A New Threat Actor Emerges

Beyond Traditional Threat Models

Geopolitics & Legal Gaps

Big Picture

A New Threat Actor Emerges

Psychologically-motivated Internet extremists, distinct from conventional cyber adversaries, introduce unique challenges in application security due to their deep-rooted psychological compulsions driving attack patterns which appear unpredictable and chaotic without a framework for understanding the threat.

Big Picture

Beyond Traditional Threat Models

These extremists operate with a modus operandi heavily influenced by personal psychology and specific digital environment, necessitating an evolution in threat modeling to anticipate unforeseen vulnerabilities and user behaviors with downstream impact.

Big Picture

Geopolitics & Legal Gaps

The role of platforms in nations with lenient digital regulations, combined with an outdated legal system, amplifies the threat. Hostile state-sponsored actors provide both implicit and material support to Western hate forums.

Speaker Credentials

@HACKINGBUTLEGAL
HACKINGBUTLEGAL.COM

- Threat Hunter, Security Consultant
- Served in the US Army, 4th Infantry Division, Iraq (2003-2004) and later in cleared roles in Iraq and Djibouti, Africa through 2012
- Joined Mandiant in 2013, Security consulting (threat detection) for Fortune 1000 companies
- Formerly the Worldwide Director of Incident Response at Intel Security/McAfee
- Co-founded Spyglass Security, led vulnerability management for the NYC Board of Elections
- Served as the Lead Incident Response and Threat Analyst on the Biden-Harris Campaign
- Acted as Director of Technology at the Surveillance Technology Oversight Project, a 501(c)3 focusing on the risks of mass surveillance

Investigator Profile

- Or, what makes me able to tackle these threats?
- Do not try this at home!

Common Characteristics

- Angry, racist, misogynist, reactive
- Extensive outward projection of personal insecurities
- Leverage technology at a low-to-medium level of sophistication
- Desire for recognition and validation, attention- or acknowledgment-seeking through various mediums
- Desire to record and showcase their harassment endeavors, suggesting a mix of narcissism and a need for internal or group validation
- A willingness and capacity to misuse systems or legally pay to gather and public the personal information of their targets
- Traits of pathological lying, crafting intricate deceptions to further their narratives and objectives.
- Dual lives, presenting a "clean" public image publicly while engaging in illicit activities privately, suggesting deep psychological compartmentalization.
- Notable family connections/backgrounds exist for all individuals, suggesting potential influences or vulnerabilities. Sensitivity and defensiveness are displayed when family backgrounds or personal details are highlighted. Their reactions and activities hint at potential motivations or traumas rooted in family backgrounds or histories.
- Drive for control and dominance: Their actions reveal a pattern of manipulation and calculated malice.
- They regularly indulge in fantasies, and speculations about the victim's life and actions, indicating an obsessive tendency and perhaps a need to control narratives.

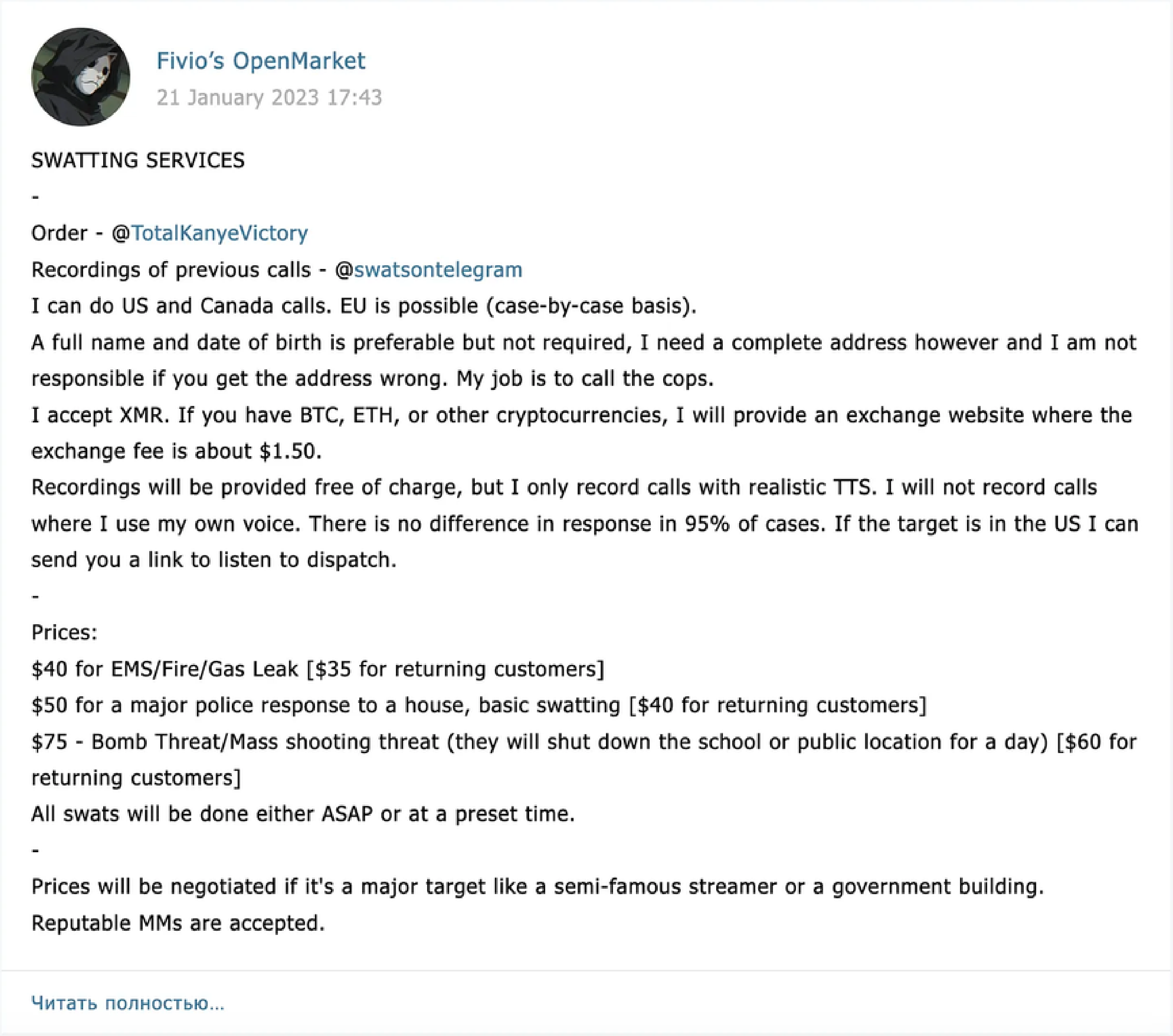
The Swatter: Sample Detailed Profile

A complex adversary, blending medium technical skills with emotional vulnerabilities.

Deep-seated needs for power, control, and recognition drive him, which is evident in acts like swatting (for nominal sums) to exert dominance and using platforms like Telegram to engage and taunt.

Despite his intelligence, he's driven by thrill-seeking motives, a narcisstic need for validation and dominance, and possibly personal vendettas (evident in the audio files in the next slides and other posted content)

1. Identity:
    a. Leads a Dual Life: Family man vs. Cybercriminal.
    b. High Technical Proficiency: Masks actions using digital platforms.
    c. Strong Need for Anonymity: Uses privacy tools like Monero.
2. Motivations:
    a. Power & Control: Manipulates law enforcement with swatting.
    b. Thrill-seeking: Enjoys chaos and real-world consequences.
    c. Recognition & Validation: Seeks attention, even if negative.
    d. Potential Personal Vendetta: Consistent targeting suggests past grievances.
3. Behavioral Traits:
    a. Lack of Empathy: Indifferent to harm caused.
    b. Narcissistic: Engages victims and authorities for recognition.
    c. Emotional Reactivity: Vulnerable to emotional challenges.
4. Biases & Prejudices:
    a. Possible Racial Bias: Exhibits targeted racial threats.
    b. Predictable Actions: Biases could lead to anticipated behaviors.



Fivio's OpenMarket
21 January 2023 17:43

SWATTING SERVICES

-

Order - @TotalKanyeVictory

Recordings of previous calls - @swatsontelegram

I can do US and Canada calls. EU is possible (case-by-case basis).

A full name and date of birth is preferable but not required, I need a complete address however and I am not responsible if you get the address wrong. My job is to call the cops.

I accept XMR. If you have BTC, ETH, or other cryptocurrencies, I will provide an exchange website where the exchange fee is about $1.50.

Recordings will be provided free of charge, but I only record calls with realistic TTS. I will not record calls where I use my own voice. There is no difference in response in 95% of cases. If the target is in the US I can send you a link to listen to dispatch.

-

Prices:

$40 for EMS/Fire/Gas Leak [$35 for returning customers]

$50 for a major police response to a house, basic swatting [$40 for returning customers]

$75 - Bomb Threat/Mass shooting threat (they will shut down the school or public location for a day) [$60 for returning customers]

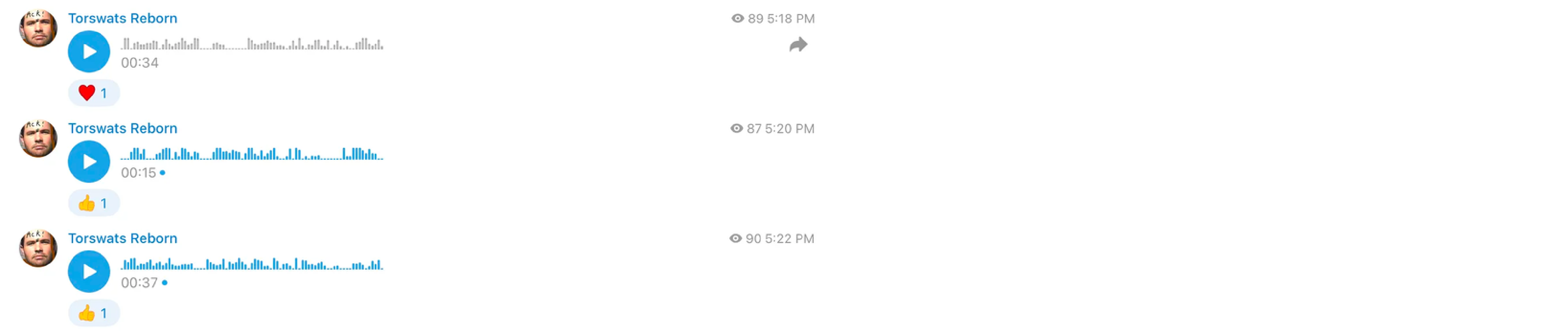
All swats will be done either ASAP or at a preset time.

-

Prices will be negotiated if it's a major target like a semi-famous streamer or a government building.

Reputable MMs are accepted.

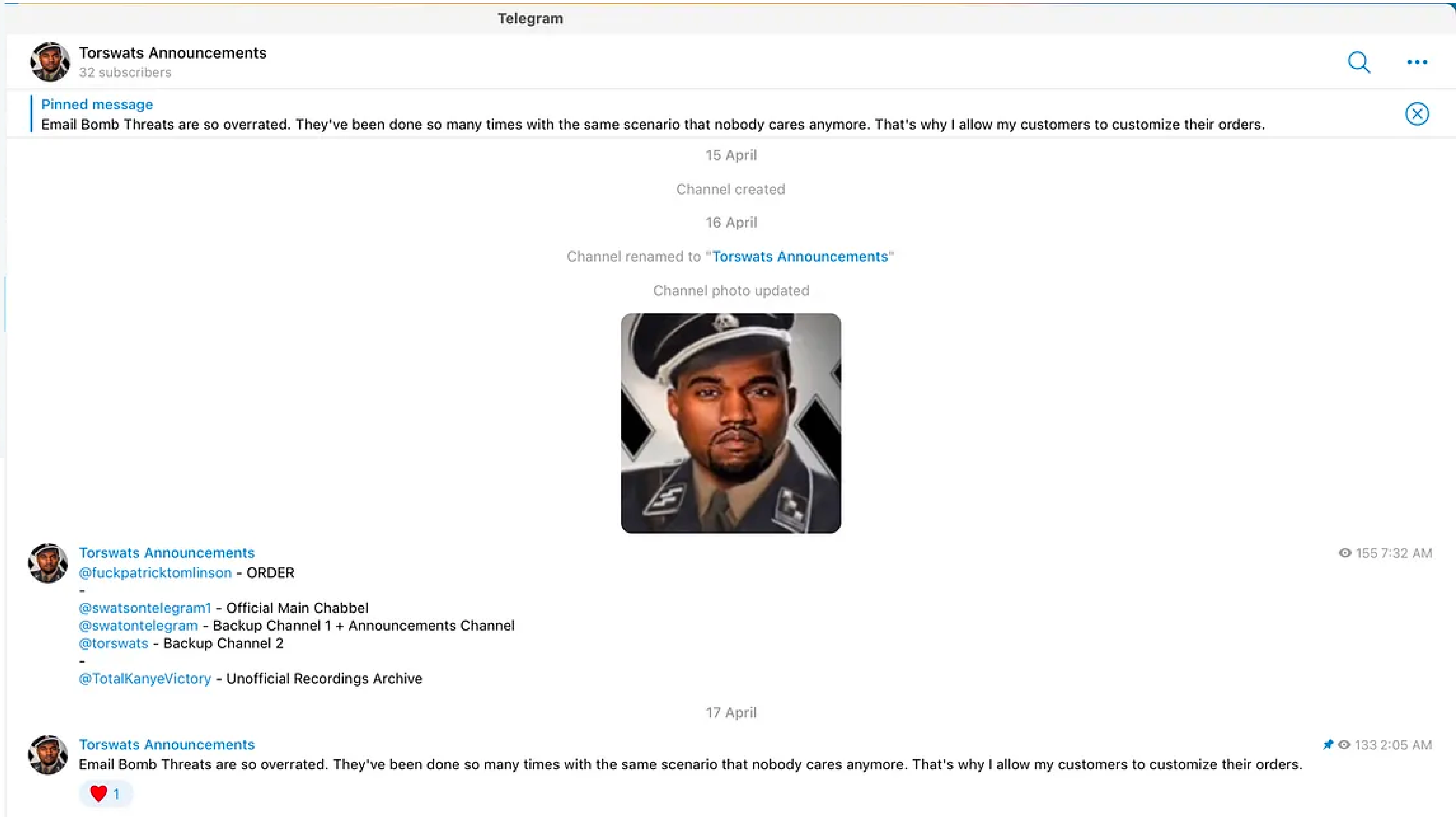
Читать полностью...



Torswats Reborn — 00:34 — ❤ 1 — 89 5:18 PM

Torswats Reborn — 00:15 • — 👍 1 — 87 5:20 PM

Torswats Reborn — 00:37 • — 👍 1 — 90 5:22 PM



Torswats Announcements
32 subscribers

Pinned message
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.

15 April

Channel created

16 April

Channel renamed to "Torswats Announcements"

Channel photo updated

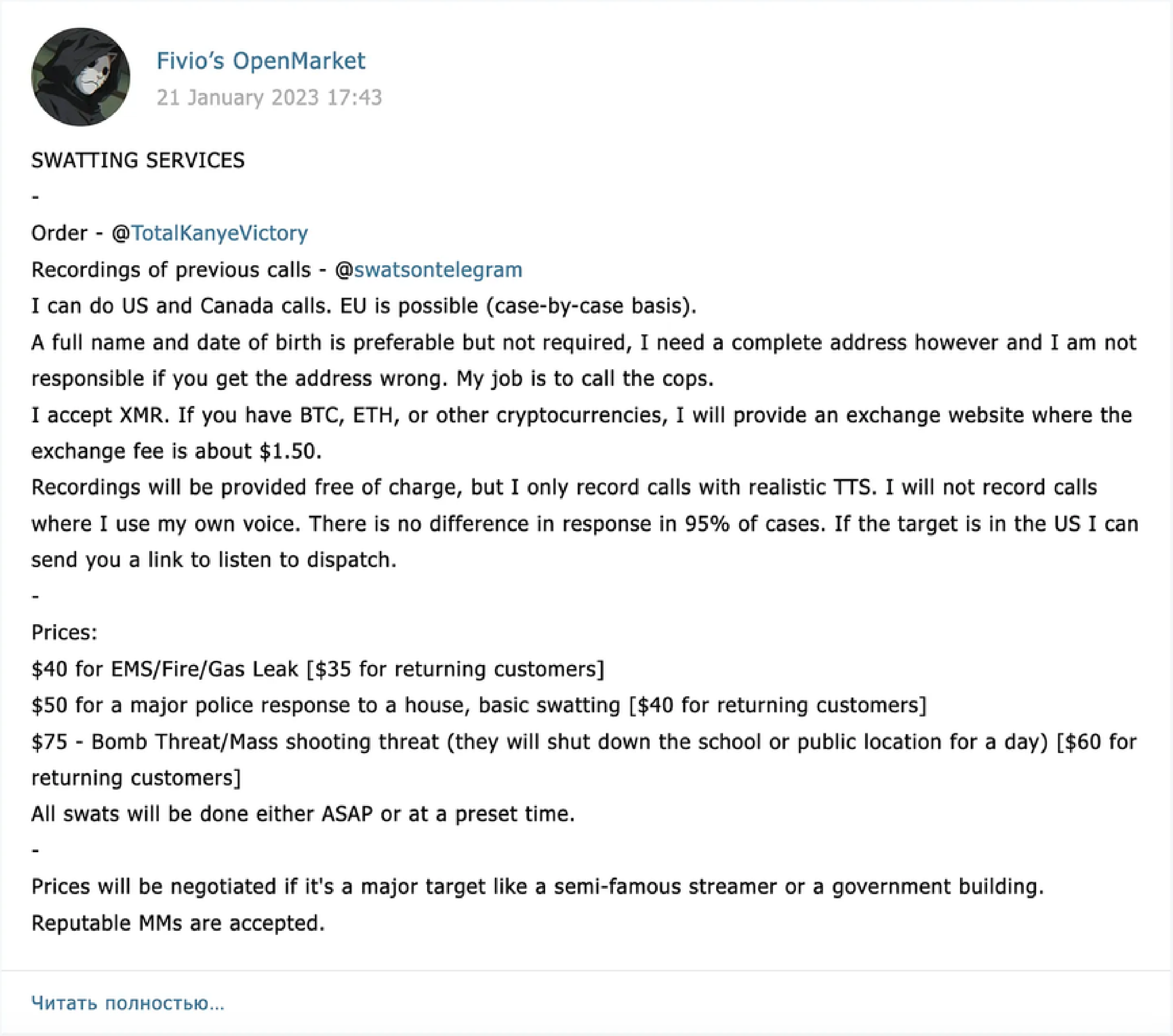
Torswats Announcements — 155 7:32 AM
@fuckpatricktomlinson - ORDER
-
@swatsontelegram1 - Official Main Chabbel
@swatontelegram - Backup Channel 1 + Announcements Channel
@torswats - Backup Channel 2
-
@TotalKanyeVictory - Unofficial Recordings Archive

17 April

Torswats Announcements — 133 2:05 AM
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.
❤ 1

Audio File #1

HTTPS://DRIVE.GOOGLE.COM/DRIVE/U/1/FOLDERS/1GR4C2B3PSE5FU6KVOKS_HYPGS4ZDTMQ2



Fivio's OpenMarket
21 January 2023 17:43

SWATTING SERVICES

-

Order - @TotalKanyeVictory
Recordings of previous calls - @swatsontelegram
I can do US and Canada calls. EU is possible (case-by-case basis).
A full name and date of birth is preferable but not required, I need a complete address however and I am not responsible if you get the address wrong. My job is to call the cops.
I accept XMR. If you have BTC, ETH, or other cryptocurrencies, I will provide an exchange website where the exchange fee is about $1.50.
Recordings will be provided free of charge, but I only record calls with realistic TTS. I will not record calls where I use my own voice. There is no difference in response in 95% of cases. If the target is in the US I can send you a link to listen to dispatch.

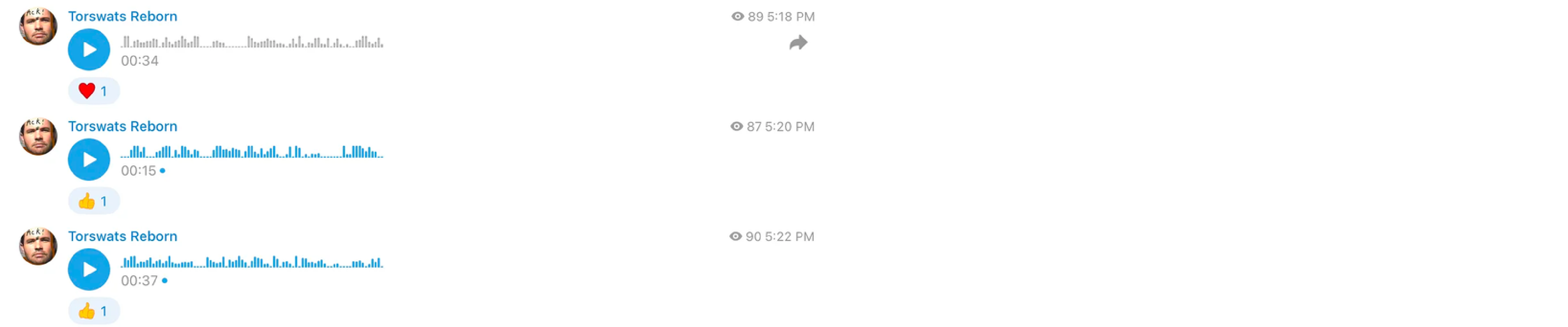
-

Prices:
$40 for EMS/Fire/Gas Leak [$35 for returning customers]
$50 for a major police response to a house, basic swatting [$40 for returning customers]
$75 - Bomb Threat/Mass shooting threat (they will shut down the school or public location for a day) [$60 for returning customers]
All swats will be done either ASAP or at a preset time.

-

Prices will be negotiated if it's a major target like a semi-famous streamer or a government building.
Reputable MMs are accepted.

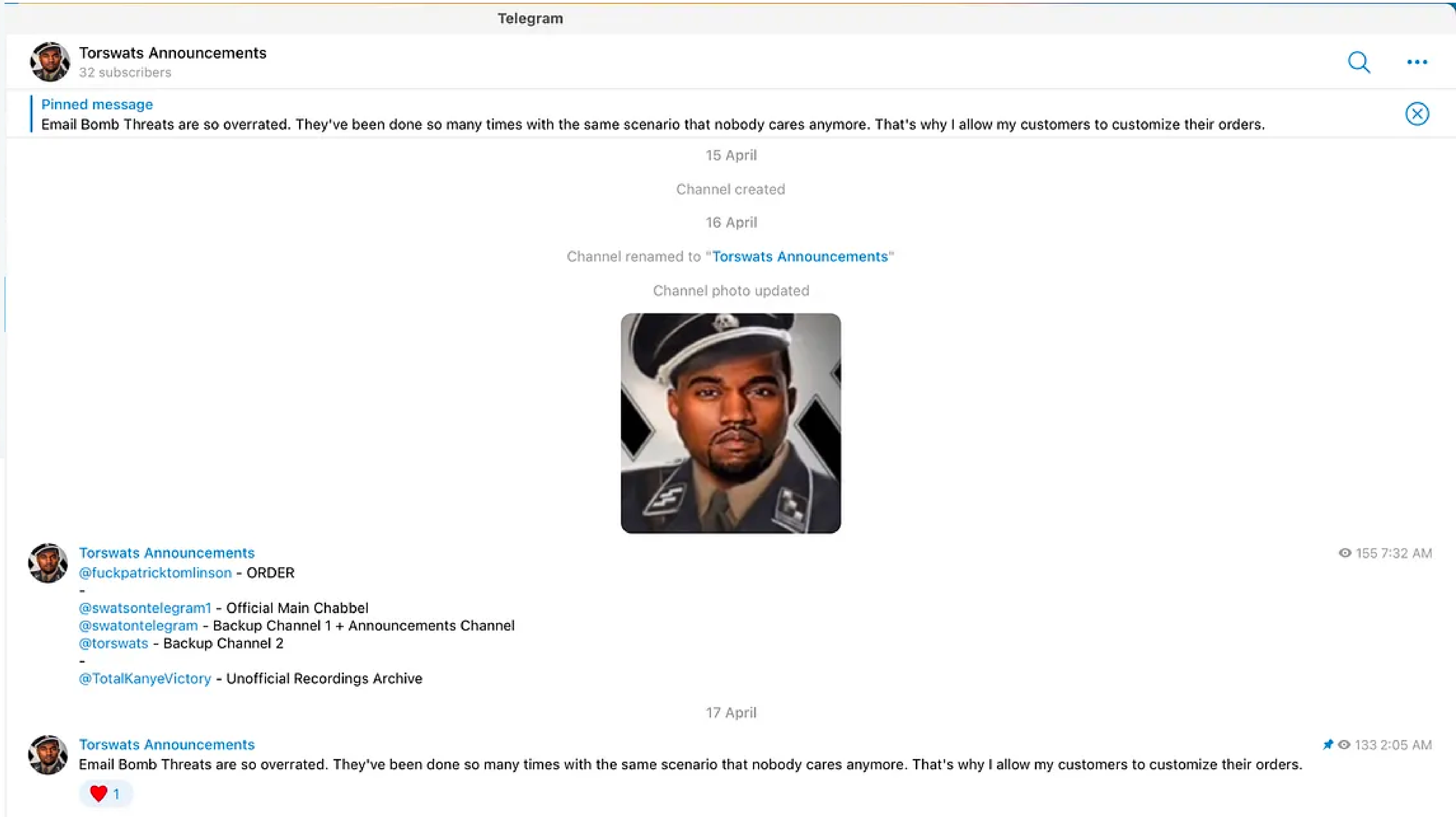
Читать полностью...



Torswats Reborn
00:34
👁 89 5:18 PM
❤️ 1

Torswats Reborn
00:15 •
👁 87 5:20 PM
👍 1

Torswats Reborn
00:37 •
👁 90 5:22 PM
👍 1



Telegram

Torswats Announcements
32 subscribers

Pinned message
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.

15 April

Channel created

16 April

Channel renamed to "Torswats Announcements"

Channel photo updated

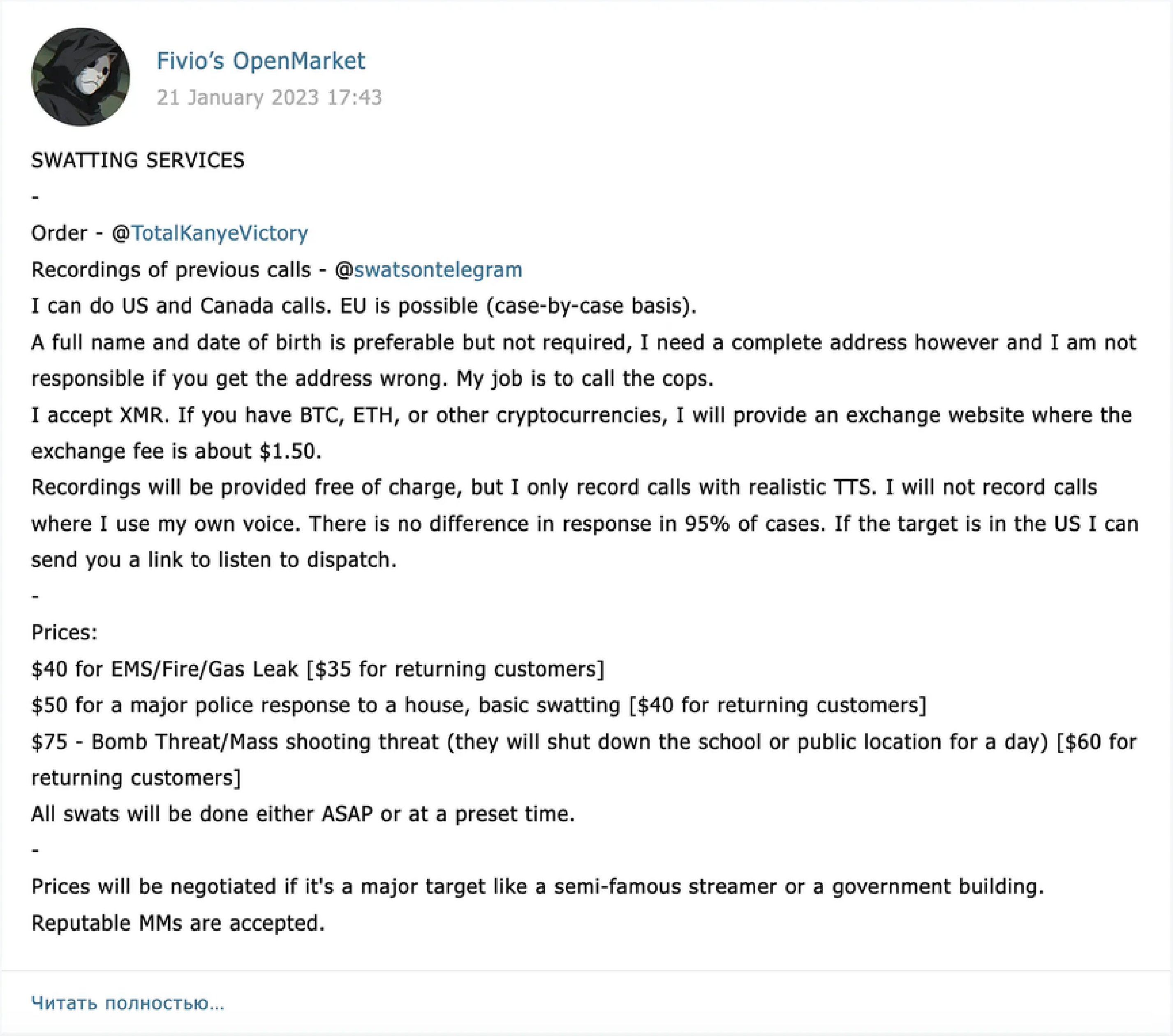
Torswats Announcements
👁 155 7:32 AM
@fuckpatricktomlinson - ORDER
-
@swatsontelegram1 - Official Main Chabbel
@swatontelegram - Backup Channel 1 + Announcements Channel
@torswats - Backup Channel 2
-
@TotalKanyeVictory - Unofficial Recordings Archive

17 April

Torswats Announcements
👁 133 2:05 AM
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.
❤️ 1

Audio File #2

HTTPS://DRIVE.GOOGLE.COM/DRIVE/U/1/FOLDERS/1GR4C2B3PSE5FU6KVOKS_HYPGS4ZDTMQ2



Fivio's OpenMarket
21 January 2023 17:43

SWATTING SERVICES

-

Order - @TotalKanyeVictory
Recordings of previous calls - @swatsontelegram
I can do US and Canada calls. EU is possible (case-by-case basis).
A full name and date of birth is preferable but not required, I need a complete address however and I am not responsible if you get the address wrong. My job is to call the cops.
I accept XMR. If you have BTC, ETH, or other cryptocurrencies, I will provide an exchange website where the exchange fee is about $1.50.
Recordings will be provided free of charge, but I only record calls with realistic TTS. I will not record calls where I use my own voice. There is no difference in response in 95% of cases. If the target is in the US I can send you a link to listen to dispatch.

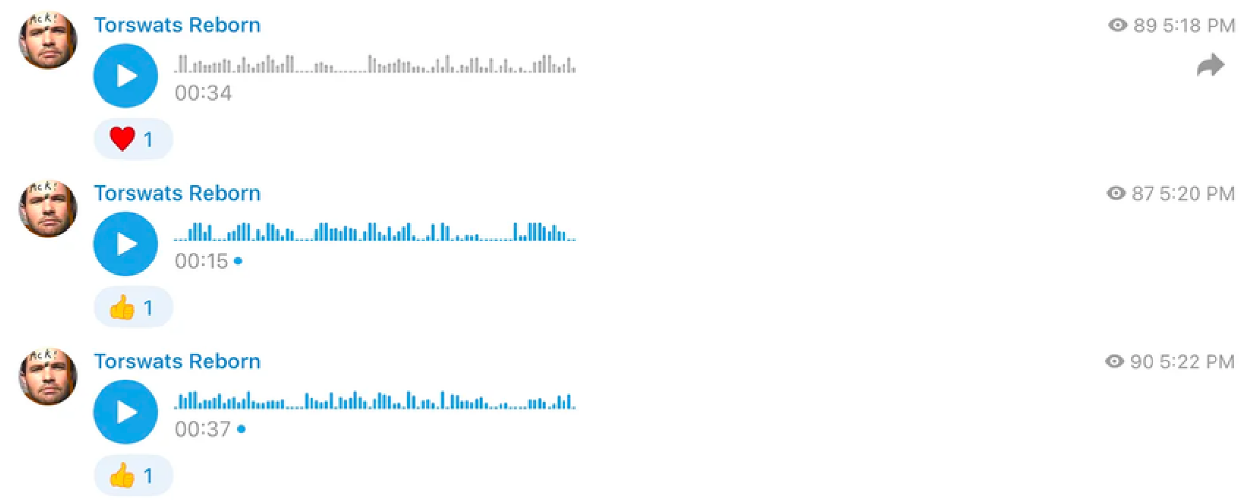
-

Prices:
$40 for EMS/Fire/Gas Leak [$35 for returning customers]
$50 for a major police response to a house, basic swatting [$40 for returning customers]
$75 - Bomb Threat/Mass shooting threat (they will shut down the school or public location for a day) [$60 for returning customers]
All swats will be done either ASAP or at a preset time.

-

Prices will be negotiated if it's a major target like a semi-famous streamer or a government building.
Reputable MMs are accepted.

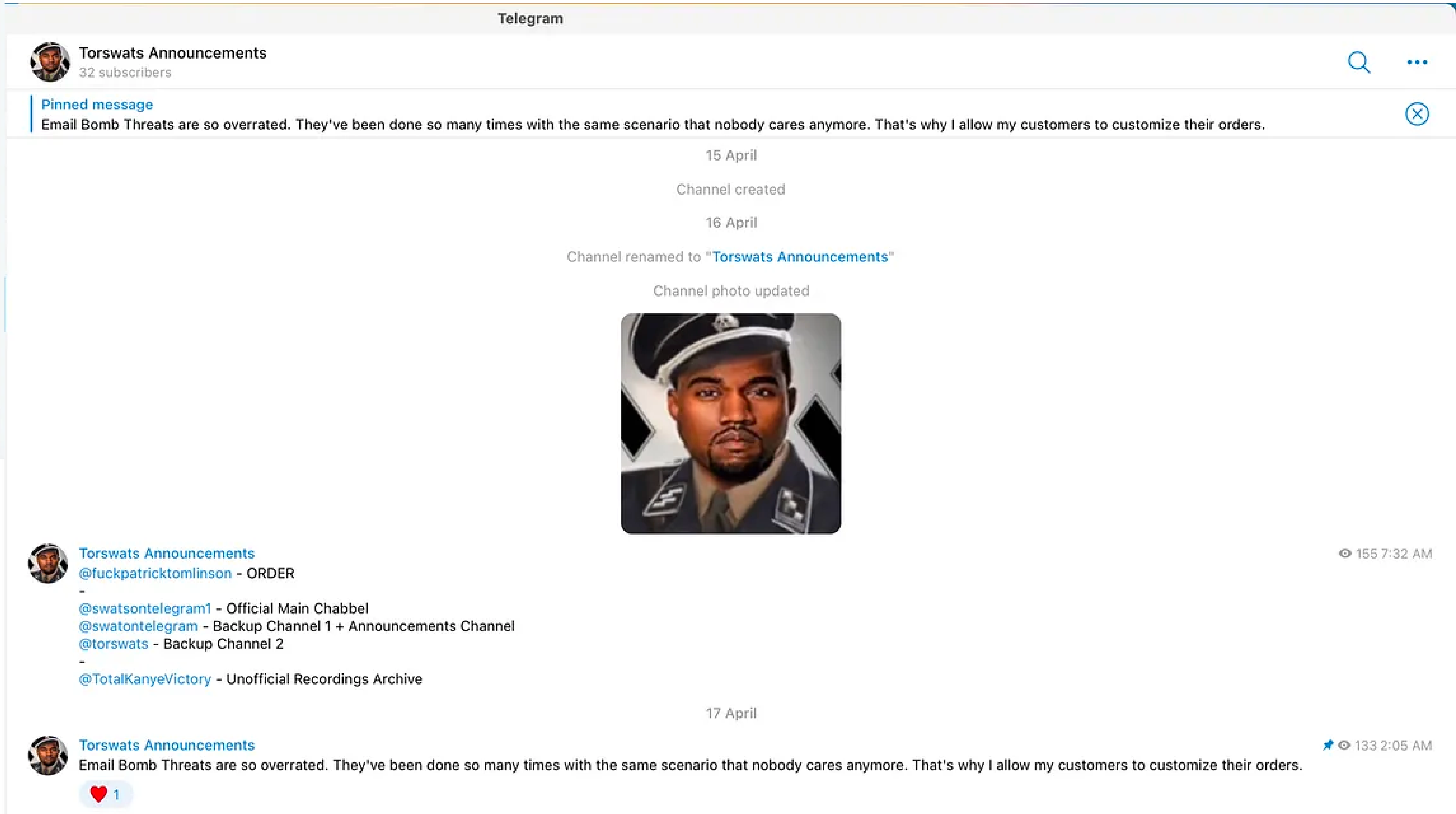
Читать полностью...



Torswats Reborn — 00:34 — 89 5:18 PM — ❤️ 1

Torswats Reborn — 00:15 • — 87 5:20 PM — 👍 1

Torswats Reborn — 00:37 • — 90 5:22 PM — 👍 1



Telegram

Torswats Announcements
32 subscribers

Pinned message
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.

15 April

Channel created

16 April

Channel renamed to "Torswats Announcements"

Channel photo updated

Torswats Announcements — 155 7:32 AM
@fuckpatricktomlinson - ORDER
-
@swatsontelegram1 - Official Main Chabbel
@swatontelegram - Backup Channel 1 + Announcements Channel
@torswats - Backup Channel 2
-
@TotalKanyeVictory - Unofficial Recordings Archive

17 April

Torswats Announcements — 133 2:05 AM
Email Bomb Threats are so overrated. They've been done so many times with the same scenario that nobody cares anymore. That's why I allow my customers to customize their orders.
❤️ 1

Audio File #3

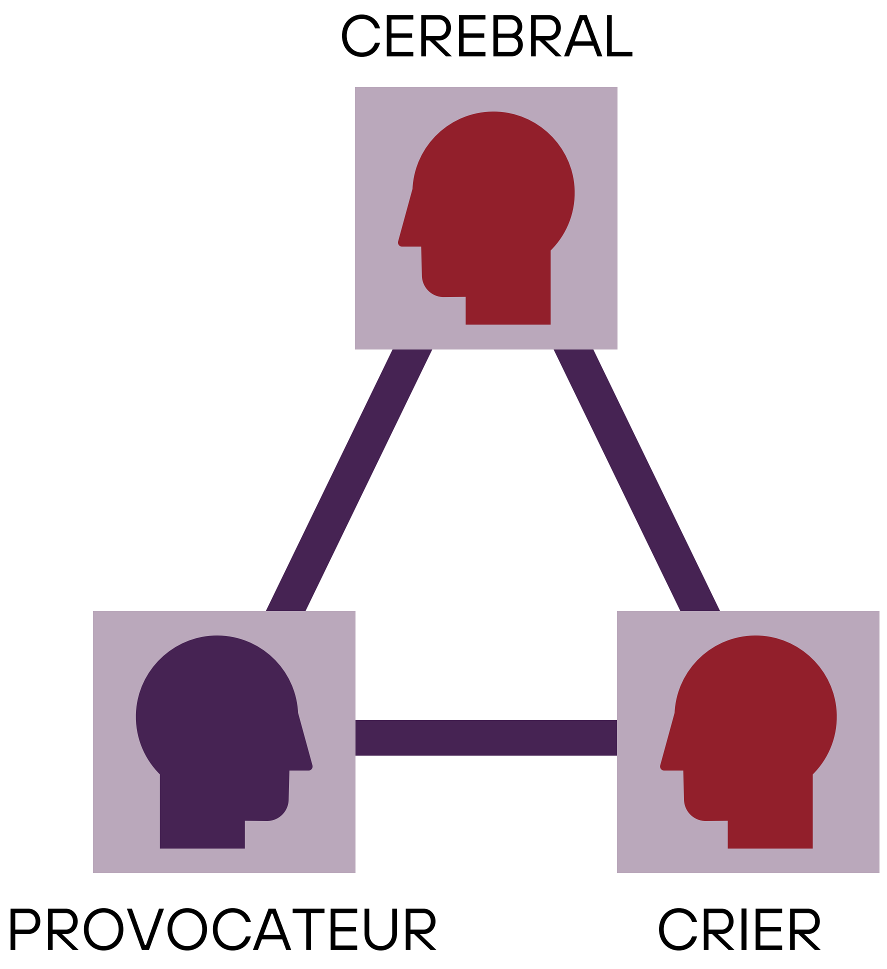
HTTPS://DRIVE.GOOGLE.COM/DRIVE/U/1/FOLDERS/1GR4C2B3PSE5FU6KVOKS_HYPGS4ZDTMQ2

SOURCE: [HTTPS://IPREDATOR.CO/TROLL-TRIAD](https://ipredator.co/troll-triad)

“Troll Triad”

A useful cyber psychopathology-profiling construct

- The Cerebral
- The Provocateur
- The Crier



- Three-pronged archetypal model defining groups of online users who engage in defamation of character, slander & libel.
- Archetypal groupings united in their goal to tarnish and obliterate their target's online credibility and trustworthiness.
- One of each of these personas was behind the attacks on Patrick Tomlinson and his family.

Troll Triad: “The Cerebral”

- Acts as the **architect** and the **legitimacy front** of defamation and disinformation campaigns, driving the group's cognitive agenda online.
- Not necessarily technically proficient or highly formally educated, but is charismatic and influential in online/offline public forums, effectively the "brains" behind the operations.
- Publicly composed, the Cerebral refrains from displaying anger or rage in public settings but may express strong emotions privately among trusted Triad members.

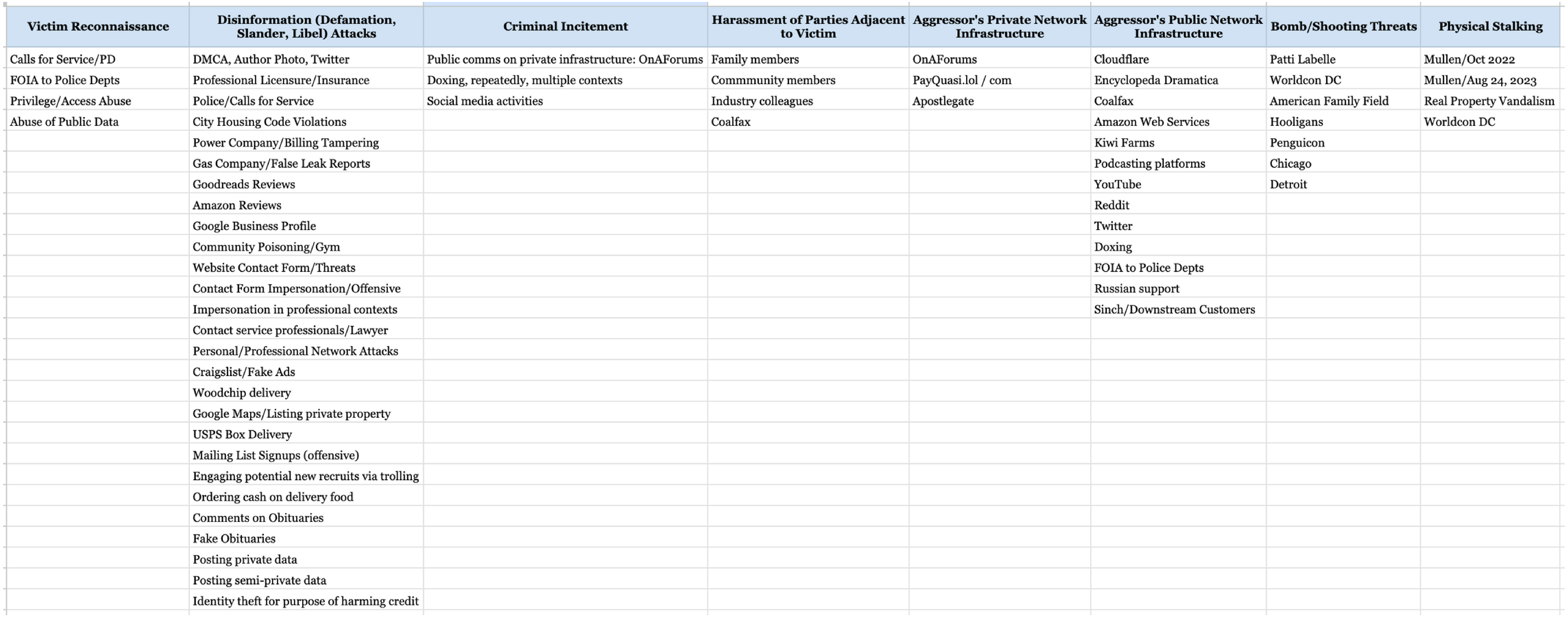
Troll Triad: “The Provocateur”

- Acts as the agitator, rallying like-minded users to participate in defamation and disinformation campaigns.
- Utilizes "us vs. them" narratives, leveraging partial truths and unsubstantiated claims about their target to manipulate perceptions.
- **Primary Functions:**
  - Motivate a large number of online users to actively engage in defamation efforts.
  - Use details about the target to legitimize the Troll Triad's campaigns.
  - Consistently exalt/praise the Cerebral, framing their actions as morally justified.
  - Employ partial truths, fabrications, and unverified claims to provoke and incite online users to attack their chosen victim.

Troll Triad: “The Crier”

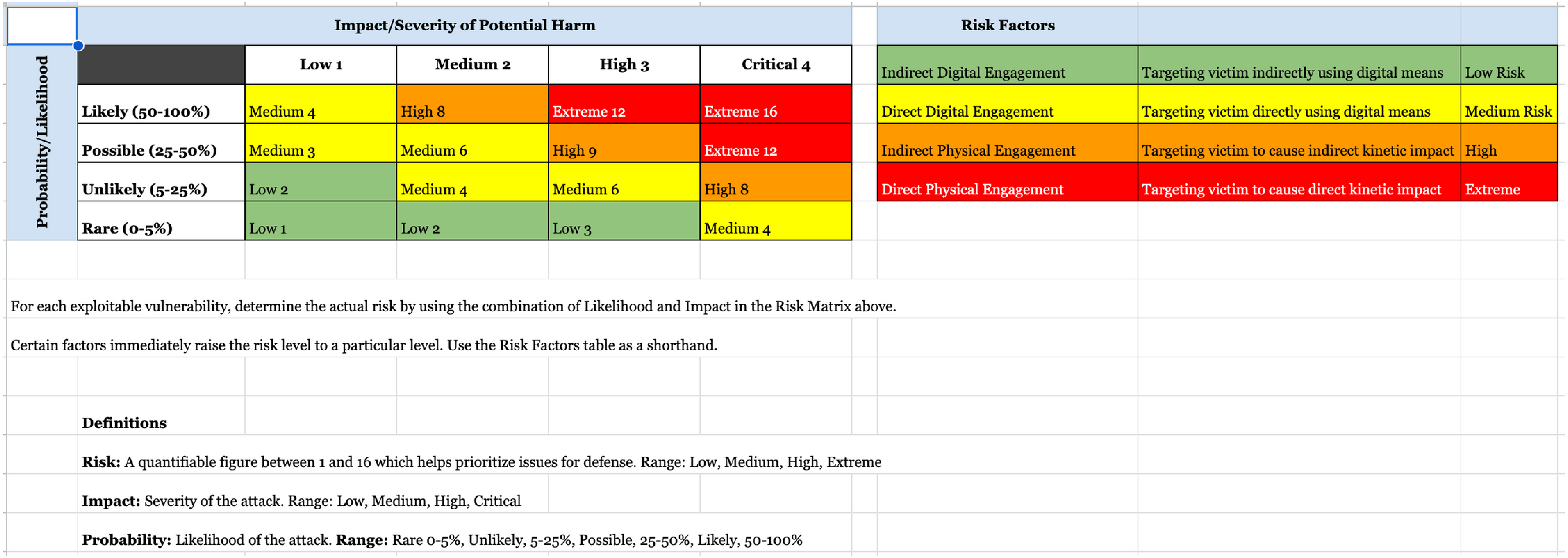
- **Role:**
  - Conveys the Troll Triad's reasons for initiating and maintaining their malicious online campaigns.
  - Organizes the dissemination of information.
  - Offers alternative viewpoints to reinforce the Troll Triad's agenda.
- **Comms Tactics:**
  - Disseminates misleading information, partial truths, and divisive "us vs. them" narratives.
  - Rationalizes the Troll Triad's harmful online activities.
- Lacks the intelligence of the Cerebral or the Provocateur’s attempted charm.
- Excels in spreading the Triad’s message, surpassing both the Cerebral and Provocateur in this regard.
- Functions as a Validator by reinforcing the intellect of the Cerebral and the fervor of the Provocateur.
- Presents alternative views to strengthen the group's objectives.
- Successfully mobilizes both dedicated followers and uncommitted online users to join their campaigns.

TTPs—Adapted from MITRE ATT&CK



Victim Reconnaissance	Disinformation (Defamation, Slander, Libel) Attacks	Criminal Incitement	Harassment of Parties Adjacent to Victim	Aggressor's Private Network Infrastructure	Aggressor's Public Network Infrastructure	Bomb/Shooting Threats	Physical Stalking
Calls for Service/PD	DMCA, Author Photo, Twitter	Public comms on private infrastructure: OnAForums	Family members	OnAForums	Cloudflare	Patti Labelle	Mullen/Oct 2022
FOIA to Police Depts	Professional Licensure/Insurance	Doxing, repeatedly, multiple contexts	Commmunity members	PayQuasi.lol / com	Encyclopeda Dramatica	Worldcon DC	Mullen/Aug 24, 2023
Privilege/Access Abuse	Police/Calls for Service	Social media activities	Industry colleagues	Apostlegate	Coalfax	American Family Field	Real Property Vandalism
Abuse of Public Data	City Housing Code Violations		Coalfax		Amazon Web Services	Hooligans	Worldcon DC
	Power Company/Billing Tampering				Kiwi Farms	Penguicon	
	Gas Company/False Leak Reports				Podcasting platforms	Chicago	
	Goodreads Reviews				YouTube	Detroit	
	Amazon Reviews				Reddit		
	Google Business Profile				Twitter		
	Community Poisoning/Gym				Doxing		
	Website Contact Form/Threats				FOIA to Police Depts		
	Contact Form Impersonation/Offensive				Russian support		
	Impersonation in professional contexts				Sinch/Downstream Customers		
	Contact service professionals/Lawyer						
	Personal/Professional Network Attacks						
	Craigslist/Fake Ads						
	Woodchip delivery						
	Google Maps/Listing private property						
	USPS Box Delivery						
	Mailing List Signups (offensive)						
	Engaging potential new recruits via trolling						
	Ordering cash on delivery food						
	Comments on Obituaries						
	Fake Obituaries						
	Posting private data						
	Posting semi-private data						
	Identity theft for purpose of harming credit						

Sample Risk Matrices



		Impact/Severity of Potential Harm			
Probability/Likelihood		Low 1	Medium 2	High 3	Critical 4
	Likely (50-100%)	Medium 4	High 8	Extreme 12	Extreme 16
	Possible (25-50%)	Medium 3	Medium 6	High 9	Extreme 12
	Unlikely (5-25%)	Low 2	Medium 4	Medium 6	High 8
	Rare (0-5%)	Low 1	Low 2	Low 3	Medium 4

Risk Factors		
Indirect Digital Engagement	Targeting victim indirectly using digital means	Low Risk
Direct Digital Engagement	Targeting victim directly using digital means	Medium Risk
Indirect Physical Engagement	Targeting victim to cause indirect kinetic impact	High
Direct Physical Engagement	Targeting victim to cause direct kinetic impact	Extreme

For each exploitable vulnerability, determine the actual risk by using the combination of Likelihood and Impact in the Risk Matrix above.

Certain factors immediately raise the risk level to a particular level. Use the Risk Factors table as a shorthand.

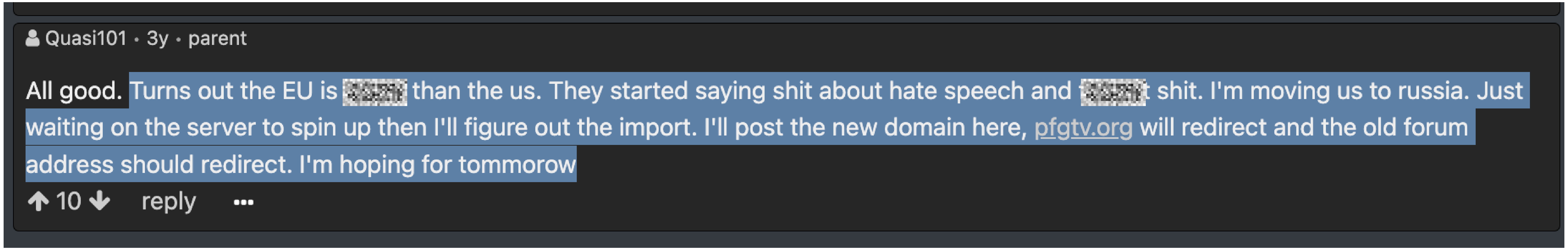
Definitions

Risk: A quantifiable figure between 1 and 16 which helps prioritize issues for defense. Range: Low, Medium, High, Extreme

Impact: Severity of the attack. Range: Low, Medium, High, Critical

Probability: Likelihood of the attack. **Range:** Rare 0-5%, Unlikely, 5-25%, Possible, 25-50%, Likely, 50-100%

Geopolitical Concerns



Quasi101 • 3y • parent

All good. Turns out the EU is [redacted] than the us. They started saying shit about hate speech and [redacted] shit. I'm moving us to russia. Just waiting on the server to spin up then I'll figure out the import. I'll post the new domain here, pfgtv.org will redirect and the old forum address should redirect. I'm hoping for tommorow

“Don’t Feed The Trolls!”

Those fortunate enough not to have been subjected to such coordinated and relentless attacks often underestimate their severity.

They might believe they can simply disregard this kind of aggression.

However, with the Internet’s ever-growing influence over the tangible world, and given that ***these threat actors deliberately blur this distinction for their targets***, such a dismissive stance is rapidly becoming untenable.

Ignoring psychologically-motivated threat actors does not make them magically disappear.

Risk Management Choices

(No good ones available)

- Avoid
- Address
- Accept
- Transfer
- Ignore

Risk Management Choice: Avoid?

Completely avoiding interaction with society to escape targeting results in chilling effects on speech and curtails civic and public participation.

This runs counter to the principles of participatory democracy.

Absolute avoidance is unlikely due to ***limited federal data privacy protections***.

Furthermore, psychopaths can be ***incredibly skilled liars,*** allowing them to evade detection by casual observers.

Risk Management Choice: Address?

Victims can implement personal defensive controls themselves, but ***this can be an extremely daunting task***. The appropriate layers of security technologies and processes required to provide “reasonable” security and the judgement required to threat model oneself accurately to determine those layers & reasonability are beyond the reach of most individuals who are not not highly experienced in infosec.

The onus should also be on tech companies to introduce product design changes and on governmental and corporate entities to modify their operational processes upstream to safeguard potential victims.

Risk Management Choice: Accept?

This is often the default response we are forced to accept; ***risk management decisions affecting us are largely made upstream from us by policymakers and tech vendors***, whose priorities most often involve brand risk, financial loss, and intellectual property—not third party individuals.

Victims may discover they have little to no say in these decisions, leading to a deeper sense of powerlessness when seeking defensive solutions.

Risk Management Choice: Transfer?

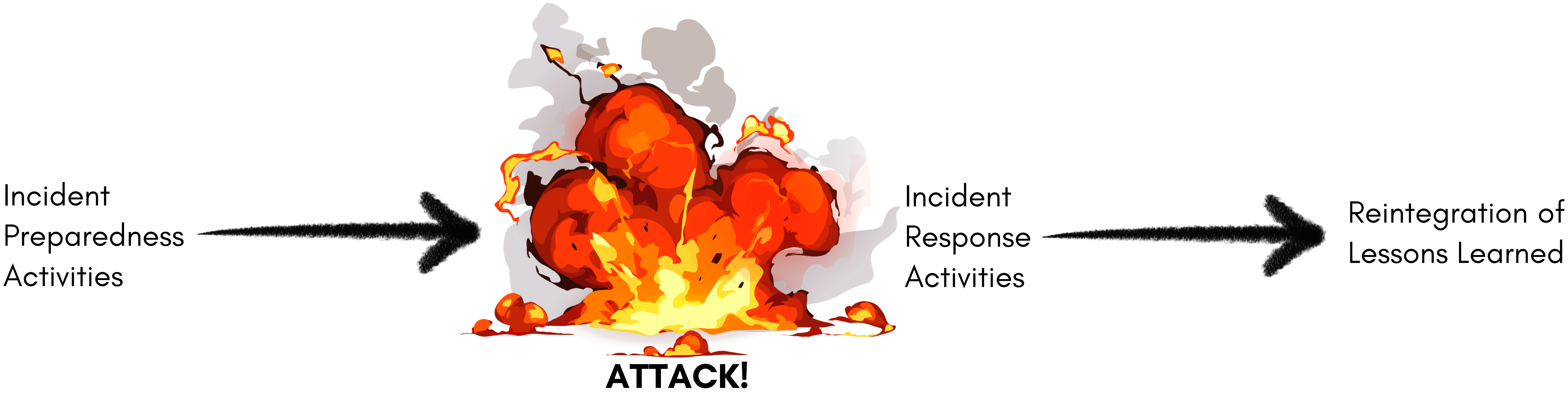
Transferring the risk is not feasible for individual victims as they have no control over the threat scenario and cannot simply choose to “pass it on” to another entity in such a context.

Risk Management Choice: Ignore?

Ignoring the risk is an approach ***already taken*** by entities higher up the chain.

Ignoring results in a detrimental "trickle down" effect onto the victims, exacerbating their vulnerabilities.

Left of “Boom” vs. Right of “Boom”



Incident Preparedness Activities

ATTACK!

Incident Response Activities

Reintegration of Lessons Learned

Risk management choices as mentioned all come before the BOOM, but ***what about during or after an incident?***

There is ***no support available for individuals*** (unless you’re rich or otherwise powerful!)

There are ***no effective mitigation for these types of attacks at scale***.

Natural Victimology

When we work on government or corporate infosec teams, we tend to have a natural understanding of our own ***victimology***, or understanding of ourselves as crime victims.

It's us! We are the victims! Our understanding of those risks is innate.

But: We infosec professionals tend to mostly focus on problems that pay a good salary.

So, we must learn empathy for victims affected by our company's tech, even if they don't fit inside our respective organizational boundaries.

Those problems are worth investigating, too.

Potential Solutions: Infosec Professionals

- **Shift Left!**—The earlier in the process that these personas are considered and integrated, the better equipped you will be to detect and prevent misuse.

- **Incorporate Psychologically-Motivated Threat Actors into Your Threat Models**—Recognizing these actors in earlier stages of development can lead to more comprehensive security measures.

- **Un-Silo Abuse Reports**—To ensure that reported abuse cases are taken seriously and analyzed for potential threats, it's essential to integrate abuse reporting with infosec teams for further integration of lessons learned and to ensure an accurate picture of incidents affecting the organization. Siloing these reports within other departments reduces their improvement value.

- **Deplatform**—Actively seek to identify and remove bad actors using harassment and disinformation tactics from your platforms. Deplatforming can act as a sharp deterrent for those using tech to spread hate or engage in harmful targeted activities, limiting your platform's use amongst the attacker's movement.

Potential Solutions: Tech Professionals

- **Pressure on Hosting Services**—Organizations like Cloudflare should be lobbied to actively deny services to websites that promote hate, extremism, and other illegal activities such as harassment and doxing. Their role in facilitating access is pivotal, and their policies can significantly impact the spread of harmful content.
- **Reevaluate Certain Free Speech Advocacy**—EFF recently dropped a policy piece promoting free speech and net neutrality using hate forum “Kiwi Farms” as the use case (an extremely bad look which caused chaos internally at the organization). While free speech is a cornerstone of democratic societies, civil service nonprofits need to find a balance to ensure that their advocacy of free speech doesn't inadvertently shield malicious actors. Promoting responsible speech while curbing harmful narratives is crucial.
- **Data Privacy Legislation Advocacy**—We need our governments to prioritize enacting strong data privacy laws to protect us from unwarranted surveillance and potential misuse of our data. Please complain about this to your elected officials!
- **Enhance Law Enforcement Cyber Units**—Agencies like the FBI should bolster their cyber capabilities to track and respond to cyber threats affecting individuals more proactively, and work to identify larger patterns. Local law enforcement agencies must become better equipped and trained to handle basic technology-driven crimes.

Acknowledgements

- My partner Jason for supporting me emotionally & putting up with extra targeting 😅
- Patrick and Niki Tomlinson
- OWASP ❤️
- Lora Kolodny/NBC
- Michael Nuccitelli, Psy.D/iPredator.co
- @pagvac/GNUCITIZEN
- Southern Poverty Law Center

OWASP 2023 GLOBAL AppSec

WASHINGTON DC

OCT 30•NOV 3

THANK YOU