zerodayx1: Hacktivist groups turning to ransomware operations

⋮ 9/22/2025

Contents

Research & Threat Intel Last updated: 22 Sep 2025
Written By
KrakenLabs Threat Intelligence Team, Outpost24

In July 2025, pro-Palestinian hacktivist group *zerodayx1* launched its own Ransomware-as-a-Service (RaaS) operation, following the path of other hacktivist teams. They loudly announced the initiative on platforms commonly used for such purposes, including X (formerly Twitter) and Telegram. *Zerodayx1* exemplifies the ongoing evolution of these groups, underscoring the importance of studying and understanding their methods in order to better prepare for and respond to such threats.

Key takeaways

- **Financial gain integrated into hacktivist objectives**: Hacktivism is no longer confined to ideological messaging. Increasingly, groups are integrating financially motivated operations, signaling a shift toward hybrid models that combine activism with profit-seeking agendas.
- **Conflict-driven resurgence**: Geopolitical conflicts have catalyzed the revival of hacktivist movements. Pro-Russian actors are setting tactical and operational trends, ranging from alliance-building to communication strategies, that are being mirrored across other conflict-driven ecosystems.
- **Adoption of advanced tactics**: Profitable cybercriminal techniques such as data exfiltration and ransomware, previously reserved for financially motivated actors, are being assimilated into hacktivist toolkits, expanding their impact potential and monetization pathways.
- **Ambiguity of intent and impact**: The decentralized and chaotic nature of hacktivist groups makes it difficult to discern their true objectives or predict success rates for their projects.
- **Leveraging accessible platforms**: Mainstream channels such as X and Telegram remain critical for outreach and coordination. These platforms are not only used for propaganda and narrative shaping but also for fostering alliances among like-minded groups.
- **Concealed financial activities**: While public-facing narratives emphasize ideology, financially oriented operations are often obscured within harder-to-access ecosystems, such as underground forums and dedicated leak sites.

The threat of hacktivism evolving into ransomware and data exfiltration

By definition, hacktivism implies the use of hacking techniques to promote a political or ideological agenda. Its primary motivation would not be obtaining a financial profit but rather to protest. Furthermore, hacktivist movements have historically been independent and not backed up by states or private organizations.

However, the basic pillars that once defined these groups have begun to tremble. On the one hand, with the emergence of groups whose operational capabilities and messages strongly suggest state sponsorship (commonly referred to as "faketivist" groups). On the other hand, the use of attack methods indicates a dual objective: not only to disrupt operations but also to secure financial gain.

And to reap the greatest benefits, hacktivist groups appear to be trying to copy those groups that have been most successful in recent years, namely ransomware groups that use double extortion techniques and organize their products around the "as-a-service" business model.

The earliest examples of groups engaged in this type of activity were pro-Russian, and they laid the foundation for the groups that exist today. Although the reality is that most of these projects initiated have not been very successful or have not lasted long, this has not prevented pro-Palestinian groups from joining this line of activity.

zerodayx1: hacktivist launching its ransomware project

Zerodayx1 is a likely Lebanese hacktivist active since at least 2023, who positions themselves as a Muslim and pro-Palestinian threat actor.

Initially focused on DDoS and defacement attacks, they have recently evolved toward data exfiltration, publishing stolen information for free. In July 2025, they launched the BQTLock RaaS project; however, despite including ransom demands and cryptocurrency wallets for donations, their activity suggests ideological rather than financial motivations.

Zerodayx1 maintains strong visibility within the hacktivist sphere, being an active member of the *LulzSec* community, attempting to lead the Anonymous movement in Lebanon, and running a Telegram channel called Mohamed Brigade (Liwaa Mohamed) with over one thousand followers. Their messaging is consistently pro-Muslim and pro-Iranian, serving as both propaganda and community-building.

Unlike other hacktivist groups, their alliances with other groups remain relatively limited. However, this does not interfere with occasional collaborations in the execution of attacks. Furthermore, they have also been targeted by pro-Israeli groups like *R00TK1T ISC CyberTeam*, who doxed them as Karim Fayad, a Lebanese national born in 2002, though *Zerodayx1* has publicly denied the claim.

zerodayx1 attacks and services

We can only infer *zerodayx1's* modus operandi from the content they share on their social media accounts. So far, it seems clear their activities have been evolving since they began operating.

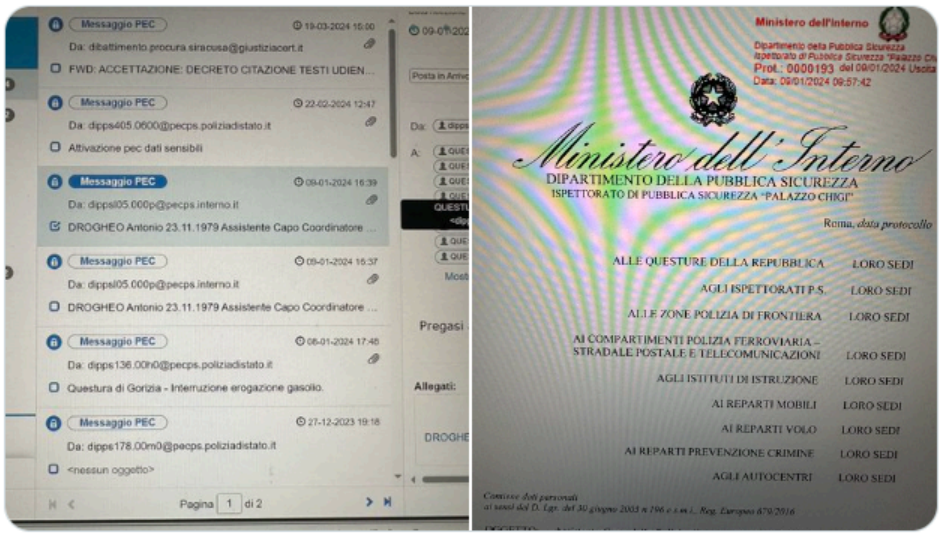
Email compromise

Among the first pieces of content shared on the social media platform X (formerly Twitter), we can see evidence of email compromises. Although not confirmed, it is most likely that they relied on compromised legitimate credentials to access these corporate emails.

Based on the chosen targets, including accounts from the Ministry of the Interior of Italy or the Lebanese Forces political party, it is likely that they carried out some sort of data exfiltration and disruptive activities afterwards.

لواء محمد
@zerodayx1

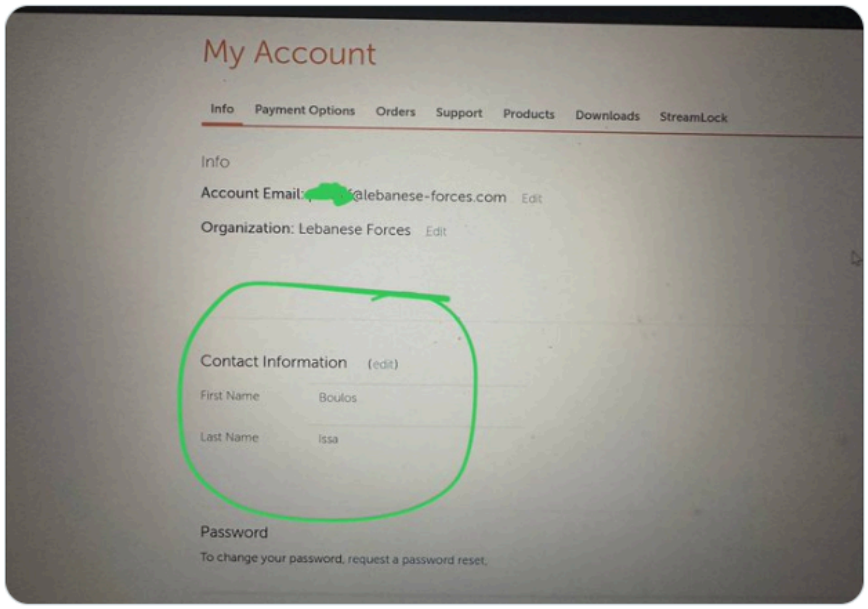
All italy police Secret mailing stored
#FreePalestine



4:01 AM · Mar 22, 2024 · **202** Views

لواء محمد
@zerodayx1

Boulos issa
Target Lebanese-forces
#opLebaneseMossad
@LFPartyOfficial



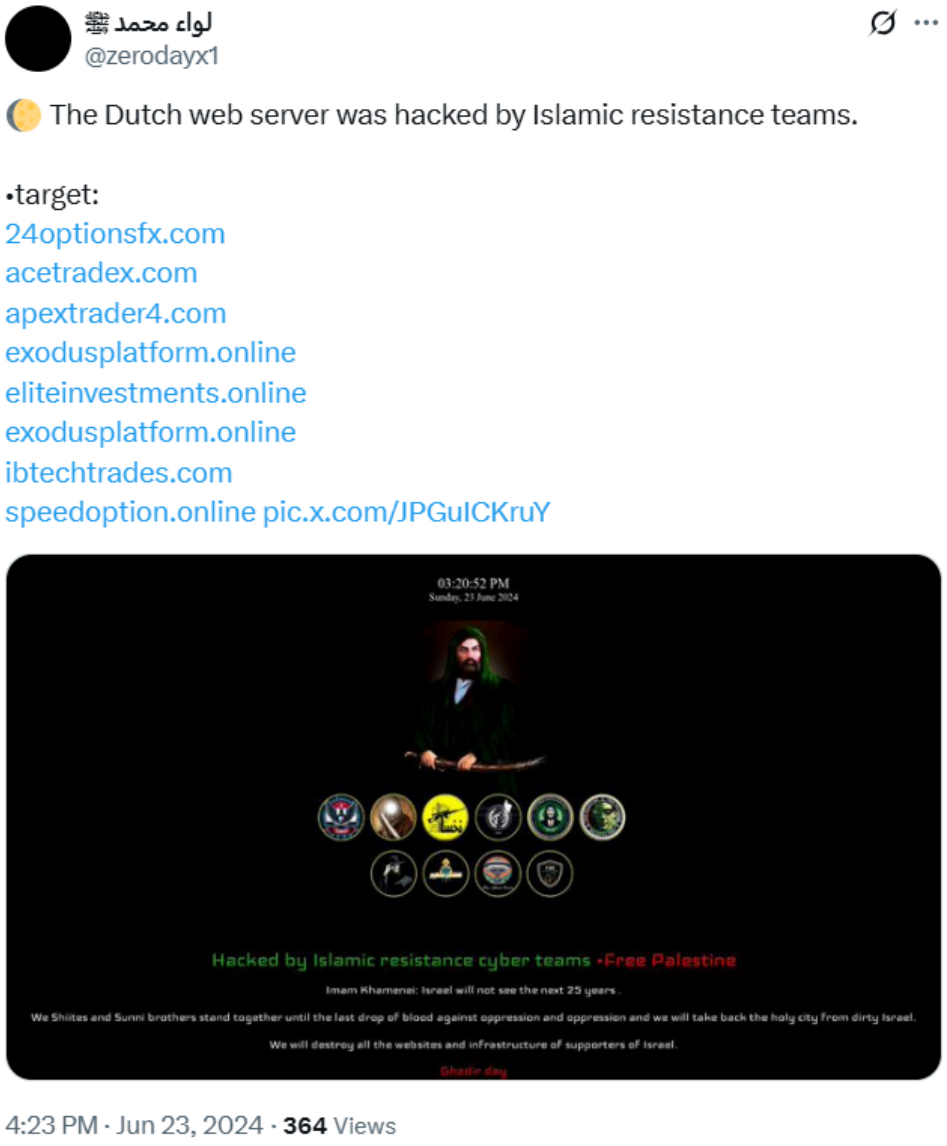
9:12 PM · Apr 9, 2024 · **169** Views

Figures 1 and 2. Email compromises reported through zerodayx1's X account.

Distributed Denial-of-Service (DDoS) and defacement attacks

Since their origins, they have been sharing proofs of Distributed Denial-of-Service (DDoS) and defacement attacks. Although there is a clear intention to attack certain regions or countries, the final chosen organizations or companies attacked seem opportunistic. They have reported victims in diverse regions like Europe (Belgium or Germany), Middle East (Lebanon, Israel, Kuwait, or Jordan), or North America (US or Canada).

They seem to operate both independently, since they alone have claimed responsibility for certain attacks, and in collaboration with other hacktivist groups. These are sometimes referred to as “Islamic resistance teams” and likely coordinate through Telegram.

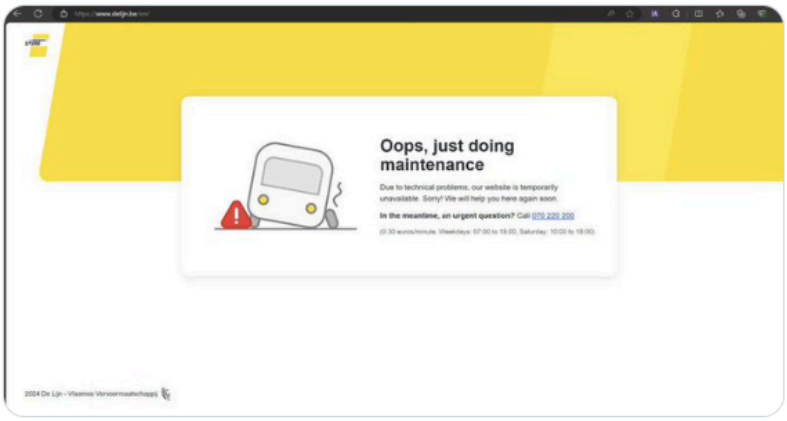


لواء محمد ﷺ
@zerodayx1

Target 🎯 delijn.be Top 1 transport
App in belgium 🇧🇪
Down 👍

Nimand is illegal Zwanger Guy
#Belgium
#LulzSec
#ZeroDayX

check-host.net/check-report/1...



2:17 PM · Jul 4, 2024 · **298** Views

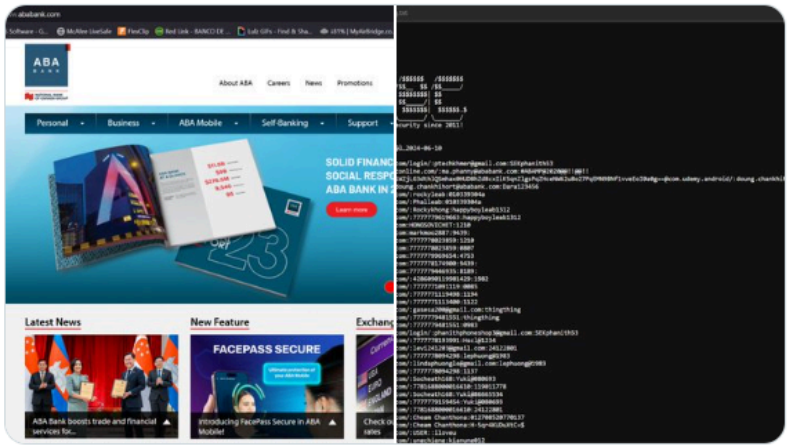
Figures 3 and 4. DDoS and Defacements reported through zerodayx1's X account.

Data leakage

zerodayx1 has also been leaking sensitive data from their victims, including users, login credentials, and complete databases of exfiltrated information. On some occasions they have just shared the data through temporary storage platforms links on X or Telegram channels while on others, they rely on underground forums. More recently, they have even created a Telegram channel dedicated exclusively to sharing these leaks.

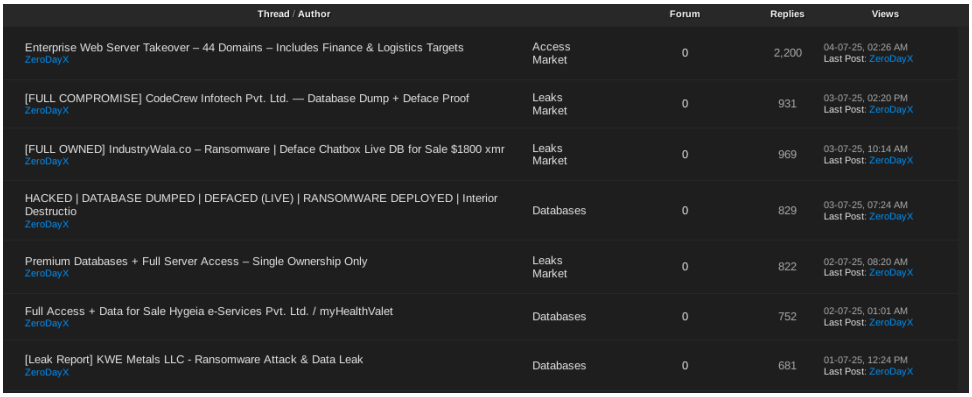
لواء محمد ﷺ
@zerodayx1

files.catbox.moe/4hh1dq.txt 💵🗂️
Bank login ababank./com
#ForMohammad عليه الصلاة و السلام
#FreePalestine



5:02 PM · Jun 30, 2024 · **230** Views

Figure 5. Data leak published on zerodayx1's X account.



Thread / Author		Forum	Replies	Views
Enterprise Web Server Takeover – 44 Domains – Includes Finance & Logistics Targets ZeroDayX	Access Market	0	2,200	04-07-25, 02:26 AM Last Post: ZeroDayX
[FULL COMPROMISE] CodeCrew Infotech Pvt. Ltd. — Database Dump + Deface Proof ZeroDayX	Leaks Market	0	931	03-07-25, 02:20 PM Last Post: ZeroDayX
[FULL OWNED] IndustryWala.co – Ransomware | Deface Chatbox Live DB for Sale $1800 xmr ZeroDayX	Leaks Market	0	969	03-07-25, 10:14 AM Last Post: ZeroDayX
HACKED | DATABASE DUMPED | DEFACED (LIVE) | RANSOMWARE DEPLOYED | Interior Destructio ZeroDayX	Databases	0	829	03-07-25, 07:24 AM Last Post: ZeroDayX
Premium Databases + Full Server Access – Single Ownership Only ZeroDayX	Leaks Market	0	822	02-07-25, 08:20 AM Last Post: ZeroDayX
Full Access + Data for Sale Hygeia e-Services Pvt. Ltd. / myHealthValet ZeroDayX	Databases	0	752	02-07-25, 01:01 AM Last Post: ZeroDayX
[Leak Report] KWE Metals LLC - Ransomware Attack & Data Leak ZeroDayX	Databases	0	681	01-07-25, 12:24 PM Last Post: ZeroDayX

Figure 6. Databases leaked in underground forums.

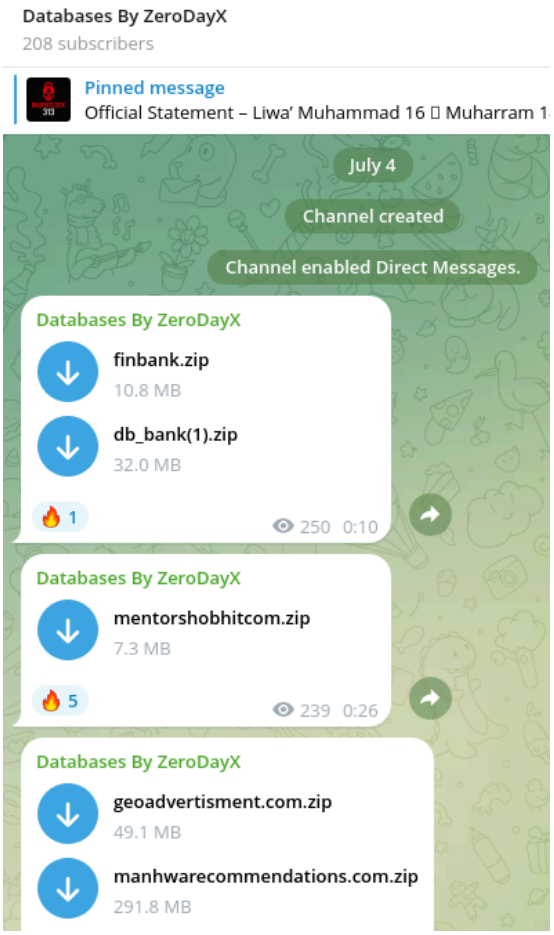


Figure 7. Telegram channel created for leaking databases.

In most cases, *zerodayx1* doesn't sell the data or ask the victim for money in exchange for not leaking it. In other words, they seem to limit their activities to data exfiltration and leaks. This isn't the case with databases advertised on underground forums, where they do put them for sale. The price of the sale is not publicly shared, as they ask potential customers to contact them via Telegram for more information.

Ransomware deployment – BQTLock Ransomware-as-a-Service (RaaS)

Although the first mentions to the use of ransomware date back to August 2024, when they referenced DoubleFace (a ransomware attributed to pro-Palestinian group *AzzaSec*), it was not until April 2025 that they claimed to have started their own ransomware attacks. According to their own words, for this first ransomware attack they would have leveraged a compromised email account belonging to a company based in Tel Aviv. The ransomware variant used in this attack was not specified.

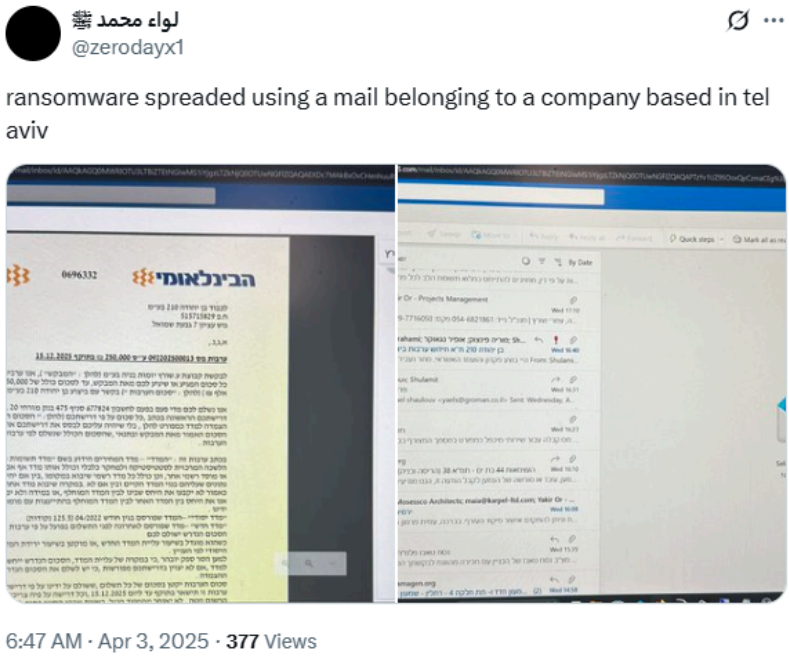


Figure 8. Announcement of the ransomware attack method on zerodayx1's X account.

Some months later, in July 2025, they officially launched the *BQTLock* (aka *Baqiyatlock*) Ransomware-as-a-Service (RaaS) project. They advertised it as a fully customizable project available through different subscription tiers.

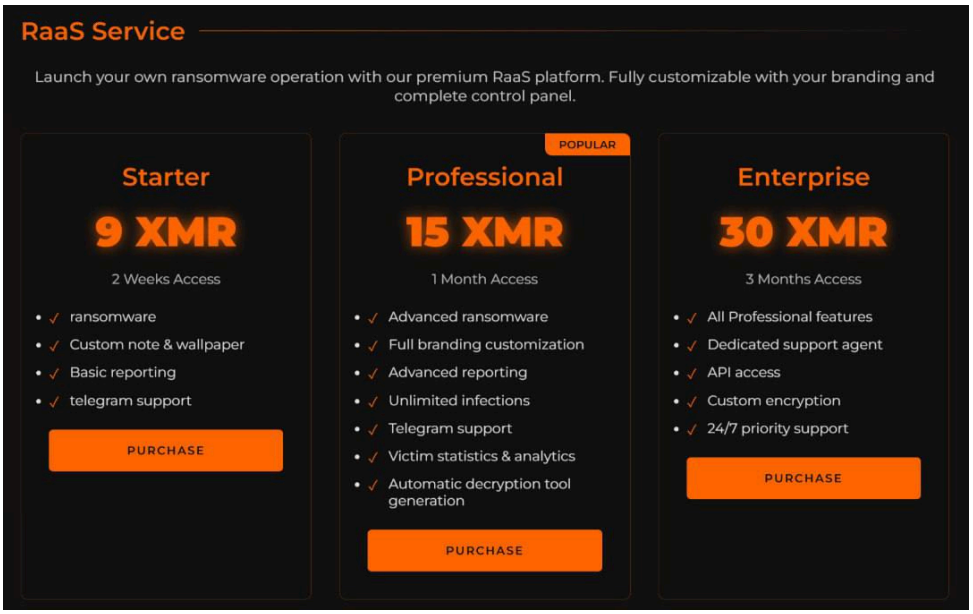


Figure 9. BQTLock subscription tiers.

This project is not only aimed at encrypting the victim's data but also at exfiltrating and leaking it on a dedicated Data Leak Site (DLS) if the ransom is not paid.

Researchers from K7 Security Labs, who analyzed the encryptor, observed various variants used in a short period of time, probing *zerodayx1* would be actively updating the ransomware to improve it and include newer functionalities such as credential-stealing capabilities. Furthermore, at the beginning of September, they announced the release of a Linux variant.

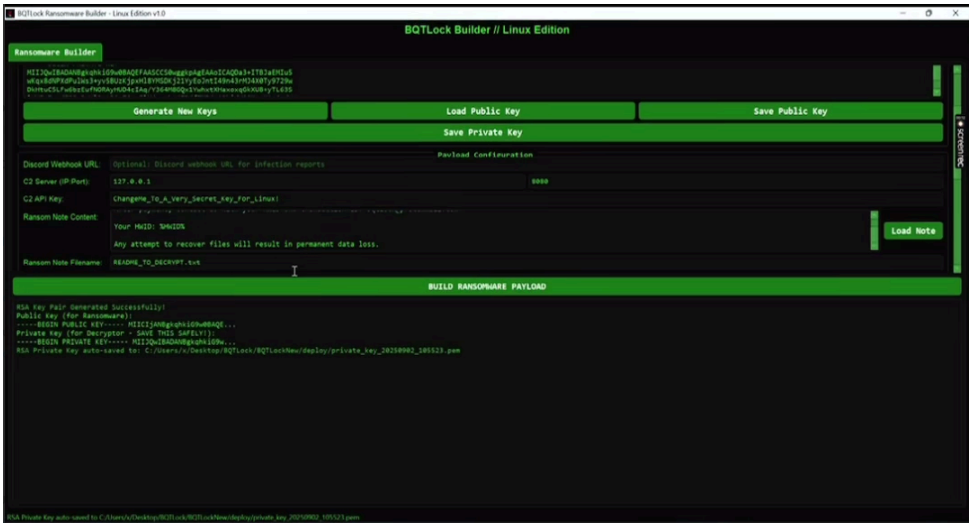


Figure 10. Linux builder shown in a promotional video on their Telegram channel.

The promotion of this project has been limited to Telegram and X, with no mentions in specialized forums. At the time of writing, the DLS was no longer available, but before it went down, it listed at least three victims from the US and Europe. Samples shared in malware sharing platforms might indicate that the number of victims could however be higher.

Who are zerodayx1 targeting?

zerodayx1 position themselves as a Muslim and pro-Palestinian threat actor and chooses their targets amongst countries that support Israel.

They have been launching attacks mainly but not exclusively against Israeli and US organizations and institutions, as well as against certain Egyptian, Jordan and Lebanese targets. Furthermore, they have also related themselves with activities against other countries like Kuwait, Bangladesh, or Syria because of religious motives.

Relationships with other hacking groups

LulzSec

LulzSec was born as a hacktivist movement in 2011, and during a short period of time they carried out some high-tier attacks. Despite their ties to the Anonymous collective, their name was chosen as a reference to the expression “for the lulz”, suggesting they launched their attacks for fun rather than to make a political statement. Although the original group disbanded, other hacktivist groups have since adopted the *LulzSec* name and their iconography.

One of these would have been *zerodayx1*. Shortly after creating their X and Telegram accounts, they created others identifying themselves as *LulzSec*. Furthermore, *Zerodayx1* has been a very active member in some *LulzSec* chat groups in Telegram, even claiming to be the “leader” of the group.

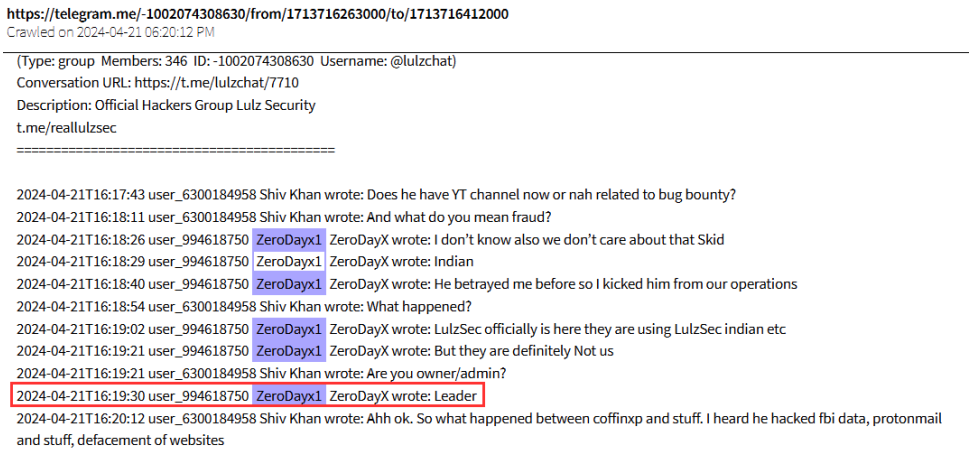


Figure 11. Messages where zerodayx1 claims to be the leader of LulzSec.

Despite their implication in the *LulzSec* community, creating their own *LulzSec*'s accounts on X and Telegram seemed more like a strategy to boost their own activity's audience. Reinforcing this idea is the fact that they did not claim authorship of any attacks as *LulzSec* and only leveraged these accounts to republish activity previously reported in their parallel accounts.

On July 24, 2024, *zerodayx1* published a statement in Telegram claiming they would abandon the use of the *LulzSec* name and change it to *Mohamed Brigade* (*Liwaa Mohammed*). This change was only effective in Telegram while the activity on the *LulzSec* account created on X remained after this announcement.

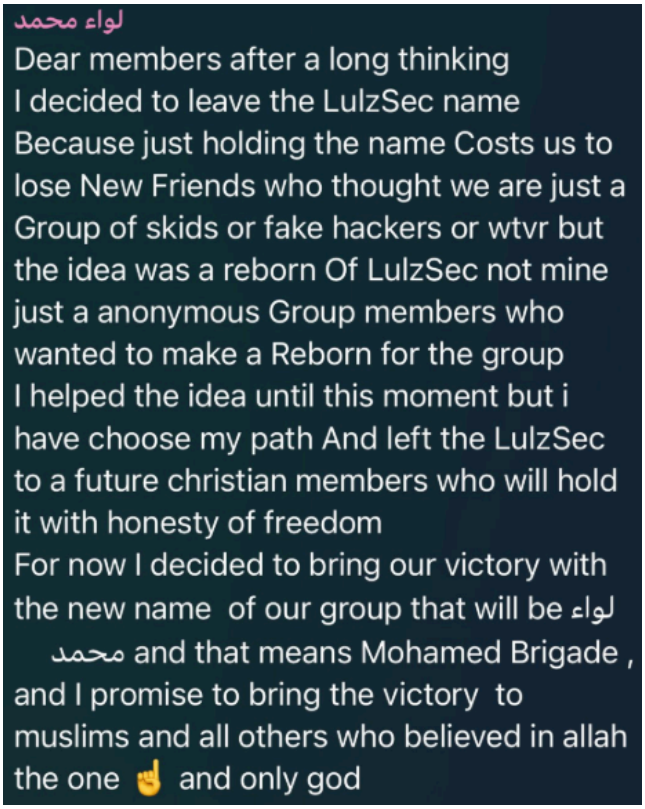


Figure 12. Statement announcing their intention to abandon the LulzSec name.

With the alias *Mohamed Brigade* (aka *Liwaa Mohamed*), they have managed to create a Telegram community of over one thousand users. In the channel, they share mostly religious content and promote their services, as well as the results of cyberattacks carried out by themselves or related groups.

Anonymous Lebanon

In June 2024, they created a Telegram channel intended to serve as a communication channel for the Anonymous faction in Lebanon. A few months later, in February 2025, they did the same, but on X.

zerodayx1 has made little effort to conceal its management of these accounts, openly referencing their name directly in the account's biography or by reposting on them almost exclusive content from their other accounts.

zerodayx1 commercialization and communication

X and Telegram

Their main communication platforms are X and Telegram, where they have created accounts tied to all their projects. They are quite active and constantly publish content on most accounts, mainly reposting content between their accounts.

Like other hacktivist groups, their activity in Telegram is suffering the consequences of the newer policies implemented, and some of their accounts have been banned for violating its terms of service.

Alias and identified contact details

Zerodayx1

- X: x[.]com/zerodayx1 – Created in March 2023
- Instagram: instagram[.]com/zerodayx_
- GitHub: github[.]com/zerodayx
- Telegram:
  - Account: t[.]me/ZeroDayX1
  - Channel:
    - t[.]me/liwaamohammad – Created on May 1, 2025
    - t[.]me/database0dx – Created on July 4, 2025
- Monero address: 8Ab1SXRmgWyGdLhULAHDwUEWuiuDniLP4YZkpCjwKaEP8LdsWXrKh49BsErV4oXmV2PqYN3fQ2QT4hEDpq5CprNXHc6F8rw

LulzSec

- X:
  - x[.]com/theelulzsec – Created in April 2023
  - x[.]com/LULZSEC_FR
- Telegram channel: t[.]me/realLulzSec
- Bitcoin address: 16pkGQEQxEmfszi5R4bY93BSGgZQ9BTTN3

Anonymous Lenanon

- X: x[.]com/anonlb_ – Created in February 2025
- Telegram channel: t[.]me/anonlb

BQTLock

- Data Leak Site (DLS): yywhylvqeqynzik6ibocb53o2nat7lmzn5ynjpar3stndzcgmy6dkgid[.]onion
- Email: BQTlock@tutamail[.]com
- Telegram:
  - Account:
    - t[.]me/BQTlock
    - t[.]me/Fuch0u
  - Channels:
    - t[.]me/BQTnet
    - t[.]me/BQTosint – Created on August 15, 2025
    - t[.]me/BQTscanner – Created on July 21, 2025
    - t[.]me/BQTlock_raas – Created on July 19, 2025
- Monero address: 89RQN2EUmiX6vL7nTv3viqUAgbDpN4ab329zPCEgbceQJuS233uye4eXtYk3MXAtVoKNMmzgVrxXphLZbJPtearY7QVuApr

Alleged personal accounts

- X: x[.]com/Karimf01164593 – Created in February 2024
- VK: vk[.]com/id656161617

Underground forums

zerodayx1's activity in forums seems to have been limited to BreachForums and DarkForums, where they have been putting leaks for sale. Activity in forums has been limited to announcing the leaks, while asking potential customers to contact them through Telegram to formalize the sale.

Forum	Username	Registration date
BreachForums	ZeroDayX	December 20, 2023
DarkForums	ZeroDayX	June 12, 2025

What's the real risk associated with these threat actors?

Unlike traditional financially motivated threat groups, these hacktivist groups tend to be surrounded by a degree of uncertainty. Ransom or leak activity may be presented as financially motivated, but such indicators should be treated with caution, as they may conceal broader strategic intentions.

Has the victim been chosen opportunistically, or is it aligned with their ideology? Do they want to create additional damage to the company's reputation by listing them on the data leak site? Have they leaked the information to others prior to selling it? This inability to ascertain their true motives renders them a more challenging threat to confront.

Furthermore, hacktivist groups' capabilities are becoming more difficult to assess, and it is important to choose the correct methods to face them or to evaluate the type of threat they do really pose. When confronting such threats, we could be facing a single individual, an unorganized group, a coordinated community, and even a coordinated group with resources (that is participants, infrastructure, knowledge, etc.) traditionally tied to state sponsored activity.

Consequently, the expansion of these groups' goals and capabilities and a major diversification in their type of attack methods and fundings turns them into a more complex and unpredictable threat. Knowing as much about them as possible, simply by analyzing the content they publicly share and their behavior in underground platforms, seems like one of the only ways to correctly evaluate them and choose the correct methods to confront them.

Moreover, it is crucial to recognize that ideology remains the core driver of the hacktivist movement. Growing social unrest and escalating violence in conflict zones further fuel their momentum, increasing the risk of sustained or even intensified operations, and paving the way for the rise of new groups.

Asset discovery + threat intelligence powered DRP.

Stay ahead of emerging threats

About the Author

KrakenLabs Threat Intelligence Team, Outpost24

KrakenLabs is Outpost24's Cyber Threat Intelligence team. Our team helps businesses stay ahead of malicious actors in the ever-evolving threat landscape, helping you keep your assets and brand reputation safe. With a comprehensive threat hunting infrastructure, our Threat Intelligence solution covers a broad range of threats on the market to help your business detect and deter external threats.