ZEROFOX Intelligence

Brief

Hacktivism: Tactics, Techniques, and Procedures

B-2025-09-04a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Hacktivism, Threat Actor, TTPs

September 4, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 9:00 AM (EDT) on September 4, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Brief | Hacktivism: Tactics, Techniques and Procedures

| Key Points

- Hacktivist collectives are motivated by an array of incentives ranging from perceived persecution to the pursuit of transparency, justice, or systemic reform. Hacktivists are typically politically, socially, or ideologically motivated.

- Although hacktivists are most often driven by political, social, or ideological motivations—matters that do not usually draw state entities into offensive cyber activity—state-affiliated collectives are aligned with national interests to some extent through a shared ideology, informal coordination, or direct sponsorship.

- Hacktivists use a variety of methods to achieve their desired end state, which are collectively referred to as their tactics, techniques, and procedures (TTPs). They employ a wide range of TTPs, which can be attributed to disparity in expertise, available resources, risk appetite, and technical knowledge, all of which vary significantly across collectives.

- In response to geopolitical events and growing tensions, hacktivist collectives often form alliances with other collectives that share perceived injustices underpinned by ideological, religious, political, or national beliefs.

Introduction

Hacktivism combines hacking and activism and is carried out by a diverse array of actors leveraging digital tools and offensive cyber TTPs to promote or achieve political, social, or ideological causes. Unlike other types of cybercrime—which are often financially motivated and centered around personal gain—hacktivists often conduct attacks against individuals, as well as public and private organizations that they perceive as unjust, corrupt, oppressive, or opposing a specific set of ideals and beliefs. For example, a financially motivated actor, such as a ransomware collective, would seek to breach a bank's network for financial gain, usually displaying indifference to the organization’s publicly stated social or political allegiances. Meanwhile, a hacktivist collective may target the same bank and seek only to expose perceived unethical practices or beliefs, with zero or minimal interest in obtaining funds.

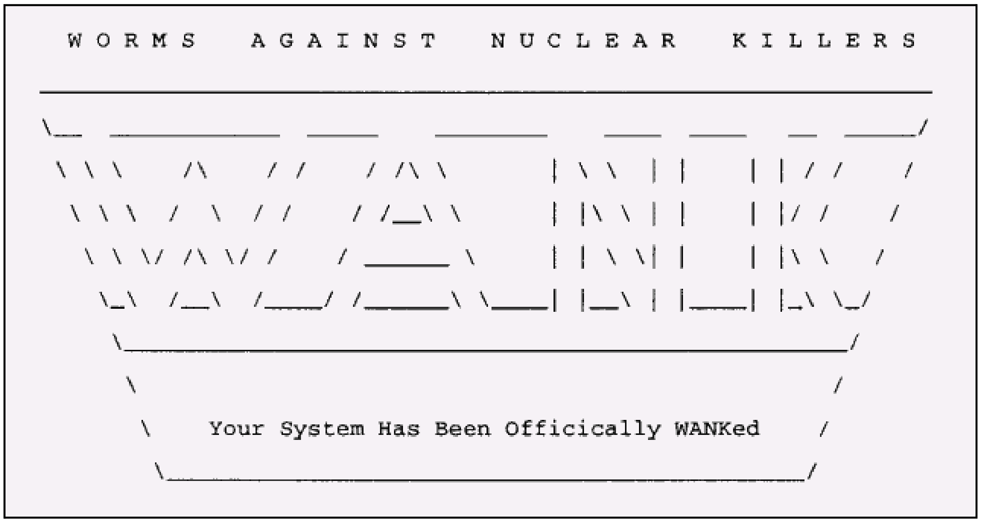
In pursuit of the incentives listed above, hacktivist collectives very often respond to geopolitical events, such as a rise in state tensions or the outbreak of conventional conflict. During these events, hacktivist collectives commonly pledge allegiance—through their messaging channels, such as Telegram or X (formerly, Twitter)—to one side of the conflict that they perceive to be politically, socially, or ideologically aligned.

As with many other types of cyberattack, hacktivism is difficult to track and the impact of hacktivists’ activities is difficult to establish, as proof of their claims is often very difficult to verify. Hacktivist collectives are often observed falsely claiming responsibility for attacks, particularly those against prominent targets such as multinational corporations or government entities. The complexity or impact of attack is also often exaggerated in a likely bid to garner publicity, accumulate media attention, and bolster notoriety.

Historical Overview

Hacktivism dates back to the late 1980s when it was widely viewed as a subculture of young and technically proficient individuals using their talents to protest political or social issues, focusing more on activism than hacking. Conversely, in modern hacktivism, there is heavier focus by collectives on malicious cyber attacks to disrupt and undermine their targets. As technology was less sophisticated, potential targets less numerous, and attack surfaces significantly smaller, early hacktivism was conducted on a much smaller scale than today.

- One of the most well-known hacktivist attacks of all time occurred in 1986, when National Aeronautics and Space Administration (NASA)'s research systems were targeted by a still unidentified actor who deployed a self-replicating malware strain known as the WANK worm.[1]
- Affected networks denied access to staff, causing a brief but notable operational disruption. Additionally, employees attempting to log in were met with a website defacement message that alluded to attacker motivations being anti-nuclear technology—very likely intended as an act of protest against NASA's involvement in developing nuclear capabilities.



```
  W O R M S    A G A I N S T    N U C L E A R    K I L L E R S
 _______________________________________________________________
 \__  ____________  _____    ________    ____  ____   __  _____/
  \ \ \    /\    / /    / /\ \       | \ \  | |    | | / /    /
   \ \ \  /  \  / /    / /__\ \      | |\ \ | |    | |/ /    /
    \ \ \/ /\ \/ /    / ______ \     | | \ \| |    | |\ \   /
     \_\  /__\  /____/ /______\ \____| |__\ | |____| |_\ \_/
      \___________________________________________________/
       \                                                 /
        \    Your System Has Been Officically WANKed    /
         \_____________________________________________/
```

Message displayed on NASA computers during WANK worm attack

Source: hXXps://www.oddee[.]com/item_99175.aspx

During the 80s and 90s, hacktivist collectives most often communicated with each other via bulletin board systems (BBS) and internet relay chat (IRC), which limited their public exposure. The 2000s saw the widespread uptake of the internet, which also led to the proliferation of social media networks and the use of messaging boards such as 4chan—which facilitated message amplification of hacktivist collectives to an ever-greater scale.

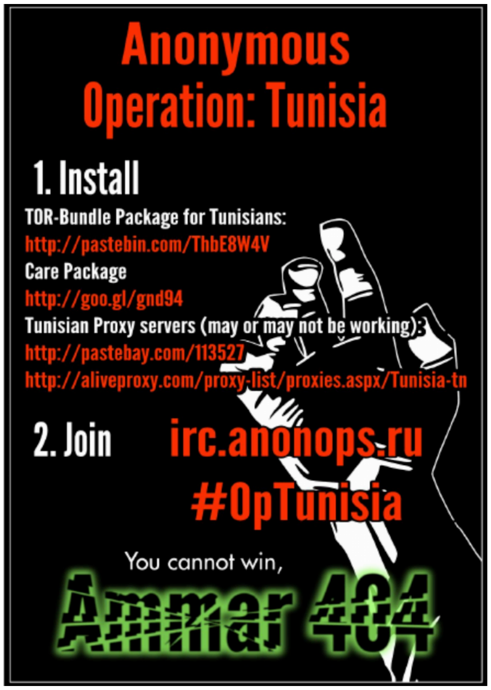
[1] hXXps://cyber.tap.purdue[.]edu/blog/articles/the-mystery-of-the-wank-worm/

One notable hacktivist collective that took advantage of this evolution was "Anonymous," a group that leveraged public internet-based communications to consolidate its reputation on the global scene. Throughout the late 2000s, Anonymous used social media campaigns to announce its intent and targets, almost certainly in a bid to amplify its messaging and increase its public profile, marking a significant change in the way hacktivist collectives project their messaging.

Anonymous quickly gained global attention for numerous well-known campaigns—such as 2010's Operation Payback, which targeted perceived opponents of internet freedom—as well as its role in movements such as Occupy Wall Street and the Arab Spring.[2] The success of these campaigns was largely due to hacktivists who began heavily leveraging social media platforms to organize campaigns, amplify messaging, and seek collaborators. Through these means, Anonymous successfully marketed and popularized hacktivism in a new way, increasing its appeal to people inclined to become involved in cybercrime. Consequently, the early 2010s saw an increase in hacktivist activities overlapping with geopolitical events as social media and online messaging played a more pivotal role in amplifying tensions and conflicts worldwide.

- During the early 2010s Arab Spring Protests in Tunisia, Anonymous launched “Operation Tunisia” in support of protestors, consisting of both distributed denial-of-service (DDoS) attacks against Tunisian government websites, as well as the provisioning of digital hygiene advice and secure online working practices advice. This operation was very likely done to protest perceived corruption of the Tunisian government and help to protect the protestors online by providing digital hygiene advice.

[2] hXXps://www.theguardian[.]com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court



Anonymous
Operation: Tunisia

1. Install

TOR-Bundle Package for Tunisians:
http://pastebin.com/ThbE8W4V
Care Package
http://goo.gl/gnd94
Tunisian Proxy servers (may or may not be working):
http://pastebay.com/113527
http://aliveproxy.com/proxy-list/proxies.aspx/Tunisia-tn

2. Join irc.anonops.ru
#OpTunisia

You cannot win,
Ammar 404

"Operation Tunisia" poster

Source: researchgate[.]net

The 2000s: Rise of Modern Hacktivism

Several hacktivist collectives played key roles in the evolution of hacktivism TTPs between 2000–2010, pivoting away from the norms of early hacktivism and increasingly leveraging modern means of communications to increase the breadth of potential victims and reshape the hacktivism threat landscape.

- **Cult of the Dead Cow (cDc)**: Founded in 1984, cDc is widely regarded as one of the most influential hacktivist collectives of all time, having reportedly coined the term hacktivist in 1996.[3] During the 2000s, cDc promoted hacktivism for human rights, privacy, and anti-censorship causes through speaking at public events and publications on its website.

- **Anonymous**: Known for its iconic Guy Fawkes mask, Anonymous has conducted multiple high-profile campaigns targeting both public and private institutions around the globe. Notably, and unlike many other hacktivist collectives, Anonymous has been observed targeting entities along opposing sides of a

[3] hXXps://cyber.tap.purdue[.]edu/blog/articles/hacktivism-the-cult-of-the-dead-cow/

political or ideological divide. Prominent targets have included the Russian, Australian, Chinese, and U.S. governments, during which messaging and TTPs reflected free speech advocacy and corruption exposure.

- **LulzSec**: LulzSec is a now-defunct hacktivist collective that sought to expose security flaws within the networks of well-known organizations. LulzSec claimed its primary motivation was to have "fun by causing mayhem," likely meaning that it sought to inflict operational disruption upon its targets. While Lulzsec occasionally accompanied its attacks with political messages, the majority were accompanied by "trolling" messages.[4]
- **Chaos Computer Club (CCC)**: CCC is an online self-proclaimed threat group that was one of the first hacktivist collectives to publicly expose a vital security flaw in a government system.[5] Today, CCC has moved away from traditional hacktivism and aims to provide information and advice on technical issues, data security, and privacy through its online publications and in-person events.
- **WikiLeaks**: While not a hacktivist collective, WikiLeaks engages in data leak and whistleblowing activity, whereby sensitive information—often obtained from volunteers—is released in order to expose perceived corruption, injustices, or human rights violations. WikiLeaks does not partake in other offensive hacktivist TTPs and instead opts to campaign for transparency and expose organizational wrongdoings.

Motivations

Hacktivist collectives are motivated by an array of different incentives, from perceived persecution to the pursuit of transparency, justice, or systemic reform. A commonly observed motivation is that of political affiliations—which are central to many hacktivist campaigns. During periods of heightened geopolitical or domestic national tensions, hacktivist collectives often declare their support for one side while targeting their opponents.

[4] hXXps://www.independent[.]co[.]uk/news/world/americas/who-are-the-group-behind-this-week-s-cia-hack-229843

[5] hXXps://www.heise[.]de/en/news/40-years-ago-the-Btx-hack-celebrates-a-happy-birthda

- In May 2025, ZeroFox observed multiple hacktivist collectives claiming responsibility for a variety of cyberattacks that were almost certainly in response to the increased hostilities between India and Pakistan. On May 8, 2025, pro-Pakistan hacktivist collective “AnonSec” claimed on its Telegram channel to have successfully conducted DDoS attacks targeting multiple Indian government websites and institutions and provided Check-Host[.]net links to verify its claims.

Social issues such as perceived human rights violations, environmental degradation, and inequality also prompt many hacktivist campaigns to take action. Like most other hacktivist activities, socially motivated campaigns tend to be reactive and are usually short-lived, typically responding to a particular event or escalating tensions.

- In 2020, the threat collective “Distributed Denial of Secrets” (DDoSecrets) published data on its official website regarding policing procedures, including intelligence on the protests of over 200 police departments in the United States in response to the death of George Floyd.[6] This was almost certainly done to undermine U.S. police departments and expose policing procedures that were under heavy criticism at the time.

- In 2016, the collective “RedHack” leaked over 57,000 emails that reportedly originated from Berat Albayrak, son-in-law of Turkey’s President Recep Tayyip Erdoğan, revealing the details of a government campaign seeking to manipulate social media and smear prominent opposition figures.[7] RedHack almost certainly conducted this leak to expose perceived corruption and discredit Turkish government officials.

Some hacktivist collectives are driven by economic or social ideologies, such as anarchism or anti-capitalism or religious fundamentalism. These collectives view their malicious cyber activities as a means by which to pursue change in these areas, whether via the causing of disruption, reputation tarnishing, data theft, or by simply spreading a message across as wide a readership as possible. The targets of such attacks are

[6] hXXps://www.forbes[.]com/sites/thomasbrewster/2020/06/22/blueleaks-huge-leak-of-police-department-data-follows-george-floyd-protests/

[7] hXXps://www.refworld[.]org/reference/annualreport/freehou/2017/en/119773

usually either those perceived as opposed to or promulgating conflicting views or entities whose targeting is likely to assist in the conveying of a message.

- In April 2024, “SiegedSec” claimed to have conducted a hack-and-leak attack on the Westboro Baptist Church in protest of its criticism of the LGBTQ+ community, allegedly providing website source code and private files of members of the church.[8] SiegedSec, also known as the self-proclaimed “gay furry hackers,” often conducted attacks against targets that it perceived to be as critical of the LGBTQ+ community, almost certainly perceiving the Westboro Baptist Church as such.[9]
- Since 2020, “Cyber Partisans,” a Belarus-based hacktivist collective, has hacked government servers, leaked police data, and disrupted state-controlled railway systems.[10] Belarus President Alexander Lukashenko has been criticised for imposing a perceived authoritarian regime, so it is very likely that these malicious cyber attacks were conducted to undermine and discredit him, while disrupting national services as a form of protest.
- In 2019–20, while protests were taking place in Hong Kong to object against growing Chinese governance, hacktivists supporting the Hong Kong democracy movement attacked Chinese government websites and leaked police databases to expose excessive force against protesters.[11] It is very likely that these malicious cyber attacks were conducted to undermine and discredit Chinese government institutions in support of the people of Hong Kong.

State-Affiliated Hacktivism

Although the vast majority of hacktivist threat collectives operate with no or minimal affiliation to state entities, some opt to share resources, information, and combine resources during offensive operations. This collaboration is deemed optimal for many different reasons, most of which are underpinned by two primary reasons: shared interests and deniability. Cooperation has proven to benefit both the state and the threat collective; it also blurs the lines between illegal hacktivism and official state-directed

[8] hXXps://dailydarkweb[.]net/siegedsec-allegedly-hacks-westboro-baptist-church-leaks-data-and-source-code/

[9] hXXps://www.pcgamer[.]com/self-described-gay-furry-hackers-breach-one-of-the-biggest-nuclear-labs-in-the-us-and-demand-it-begin-researching-irl-catgirls/

[10] hXXps://cepa[.]org/article/belarus-cyber-partisans-prepare-for-uprising/

[11] hXXps://www.reuters[.]com/investigates/special-report/hongkong-protests-protesters/

operations, leading to an opaque and often unpredictable geopolitical and cyber landscape.

Though hacktivists are most often driven by political, social, or ideological motivations—matters that do not usually draw state entities into offensive cyber activity—state-affiliated collectives are aligned with national interests to some extent through a shared ideology, informal coordination, or direct sponsorship. No definitive metric exists for categorizing cyber threat collectives by their degree of affiliation with state entities, and deciphering the extent to which such activity is taking place is usually difficult—which is almost certainly itself a part of the appeal. However, based on observed alignments in motivations, TTPs, and intents, as well as public discourse, threat collectives can be placed roughly within one of three categories.

- **State-aligned** collectives would not necessarily receive significant direction or resources from a state entity, but the alignment of national, ideological, or political allegiances result in overlapping desired end states. During such cooperation, hacktivist collectives benefit from the ability to operate with some extent of domestic legal impunity, as well as the opportunity to partake in more impactful attacks against more prominent targets that the hacktivist collective alone may be too ill-resourced to conduct. Meanwhile, the state would benefit both from the acquisition of additional resources and expertise, as well as the ability to operate with additional deniability and conduct activities that fall outside the accepted norms of state conduct.

  These collectives most often conduct malicious activity in support of a nation in response to heightened geopolitical tensions or conflict. A prominent example is the Russian-aligned group "NoName057(16)", which has conducted malicious cyber activity against North Atlantic Treaty Organization (NATO) countries, Ukraine, and Western institutions.

- **State-sponsored collectives** typically receive varying degrees of support from a government entity while conducting operations outside government remit and often outside the law.

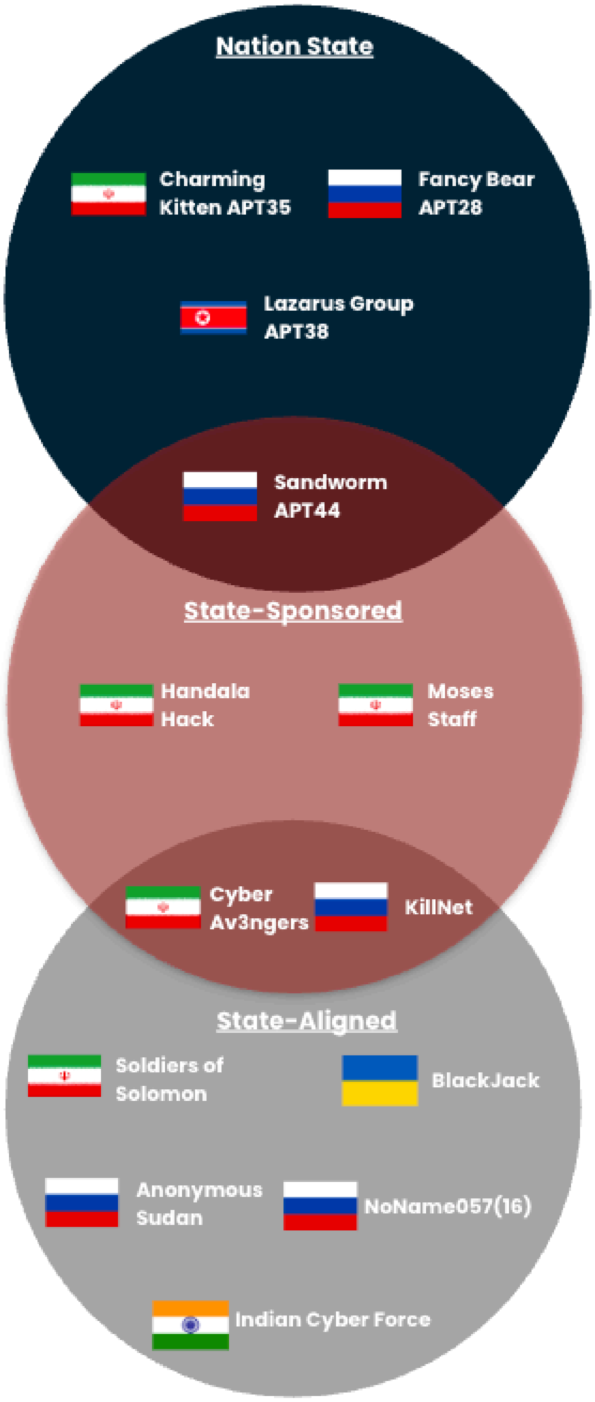
  State-sponsored hacktivist collectives are often aligned with state entities due to more than a shared desired end state and benefit from the procurement of tangible state support, such as financial support, personnel, specific expertise, or intelligence.

Similar to state-aligned collectives, those that are state-sponsored often become more active during times of conventional conflict or interstate tensions, due both to a legally passive cyberspace as well as a desire to impact the situation's outcome. However, these collectives are significantly more likely to assist state activities, offensive activities outside of times of conflict, and enjoy increased immunity if identified or compromised.

- **Nation-state** hacktivists are usually embedded within national cyber units, often operating alongside intelligence, military, or internal security agencies. These collectives conduct malicious cyber activities under the guise of hacktivism to hide official involvement, targeting foreign governments and infrastructure, typically with a high level of sophistication and resource. Due to the nature of its establishment, it is very unlikely to definitively label a hacktivist collective as nation-state. However, some Advanced Persistent Threat (APT) groups have carried out some TTPs used by hacktivist collectives; for instance, the Russian linked group Fancy Bear (APT28) has previously conducted DDoS hack-and-leak attacks.[12][13]

[12] hXXps://www.politico[.]eu/article/macron-leaks-cyberattack-russia-gru-moscow-war/

[13] hXXps://www.akamai[.]com/site/en/documents/research-paper/the-evolution-of-ddos-return-of-the-hacktivists[.]pdf



Selected state-linked hacktivist collectives

Source: ZeroFox Intelligence

Tactics, Techniques and Procedures

Hacktivists use a variety of methods to achieve their desired end state, which are often collectively referred to as TTPs. A wide range of TTPs are employed, which can be attributed to disparity in expertise, available resources, risk appetite, and technical knowledge, all of which vary significantly across collectives. TTPs are continuously developing, adjusting in response to advancements in capabilities, evolving strategies, and the types of digital technology employed by potential targets.

The majority of commonly deployed hacktivist TTPS seek to have a malicious effect against their desired target by disrupting their services, the severity of which can vary significantly. Other attack methods are leveraged as a means by which to advance a political or ideological cause. For example, website defacement attacks can be conducted with the intent of vocalizing political messages, while sensitive information can be stolen and subsequently leaked in an effort to expose perceived corruption.

DDoS

DDoS attacks seek to overwhelm a target's server or network with excessive traffic—using tools like HTTP stressors or botnets—rendering it inaccessible to legitimate users and denying service. DDoS attacks are primarily used by hacktivist collectives to temporarily disrupt their target's operational output, often while drawing attention to a particular belief or cause. DDoS attacks are used by hacktivist collectives with a wide variety of technical expertise, ranging from newly established groups to well-established collectives and state-affiliated hacktivism.

- In 2022, Estonian authorities removed many Soviet-era memorials in what was largely perceived as distancing themselves from the country's Soviet history, as well as present-day Russia. In August 2022, more than 200 public and private Estonian institutions suffered multiple DDoS attacks. Killnet, a pro-Russia hacktivist collective that has claimed multiple DDoS attacks against Western targets, claimed responsibility for the attacks, which were very likely motivated by anti-Western sentiment.[14]

[14] hXXps://allaboutcookies[.]org/the-worst-ddos-attacks

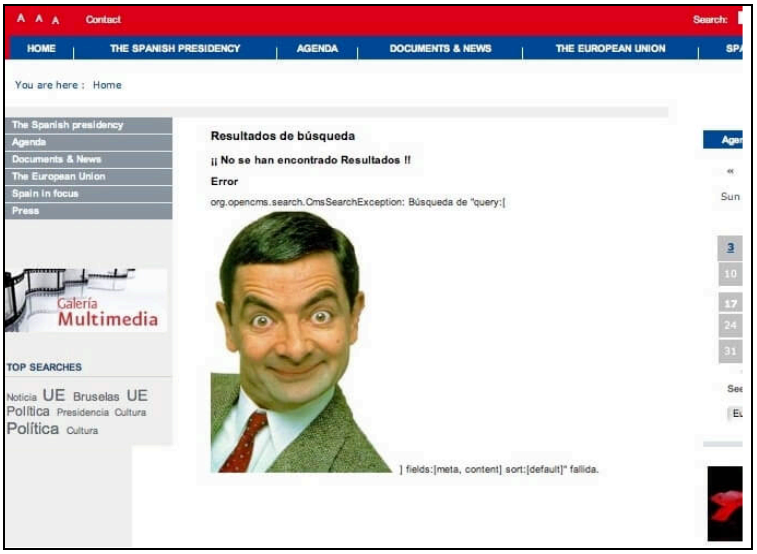
Since the 2000s, DDoS attacks have become one of the most popular TTPs used by hacktivist collectives globally because their implementation is relatively low-effort and low-cost. Successful DDoS attacks can enable hacktivists to quickly and effectively disrupt online platforms which can make strong symbolic statements against the intended victims. While DDoS attacks are effective in causing short-term disruption, their impact is often limited as servers can recover quickly once the attack subsides; additionally, the attack can also be halted or disrupted by the defender.

Website defacement

Website defacement occurs when an attacker gains illicit access to a target website, usually by the exploitation of a security vulnerability present in the domain's back-end. The attacker is then able to either replace existing content or add their own, before adding or replacing front-end content with protest messages, graphics, or claims of responsibility. Hacktivists often deface websites of victims that they recently compromised with a successful DDoS attack to cause further disruption and undermine the victim. Website defacement typically serves as a symbolic act of protest against the target and is commonly used to spread ideological messages or highlight grievances.

The impact of website defacement on the website, target, and potential customers is usually small. The attack does not require a high level of technical expertise and is often viewed as a low-effort and low-risk TTP by hacktivists. Operational disruption can ensue depending upon the post-incident usability of the website, though recovery periods are usually relatively short. However, even once remediation has taken place, significant reputational damage can occur, due both to the perception of insecure network interfaces and the questioning of data integrity. Further costs may be inflicted during any subsequent cybersecurity investigations or legally imposed financial penalties.

- In 2010, a website was created for the Spanish Presidency of the Council of the European Union (EU). However, within days of its creation, it was defaced by unidentified hacktivists and replaced with an image of the well-known fictional comedic persona Mr. Bean. While no message or statement was posted alluding to motivations, the attackers almost certainly sought to undermine José Luis Rodríguez Zapatero, the then-Prime Minister of Spain.



Resultados de búsqueda

¡¡ No se han encontrado Resultados !!

Error

org.opencms.search.CmsSearchException: Búsqueda de "query:[ ] fields:[meta, content] sort:[default]" fallida.

Spanish Presidency of the Council of EU website defacement

Source: hXXps://www[.]huffpost[.]com/entry/mr-bean-replaces-spanish

Hack-and-Leak

Hack-and-leak operations are composed of an attacker breaching a target network or server in order to acquire data, which is then leaked—often publicly through messaging platforms such as Signal or Telegram, file-sharing websites such as BitTorrent, or various deep and dark web (DDW) forums. The diverse potential outcomes of such attacks make them appealing to a host of different cyber threat actors with varying motivations. Hacktivists conducting hack-and-leak operations most often seek to cause reputational damage, expose alleged corruption, or condemn perceived human rights violations. Many of these attacks have been observed taking place amidst interstate conflict, in which collectives leak stolen personally identifiable information (PII) associated with government and military personnel. In these instances, the attacker often conveys their intention for the information to be leveraged either in the physical targeting of the personnel or in aid of warfighting efforts.

- In July 2023, hacktivist collective SiegedSec claimed responsibility for a hack-and-leak attack, whereby it allegedly obtained roughly 3,000 NATO documents (9 GB of data), while providing screenshot samples of the data in its Telegram channel. A link was subsequently shared in the collective's Telegram channel, which granted access to roughly 700 documents.[15] SiegedSec claimed that the attack was "a retaliation against the countries of NATO for their attacks on human rights."

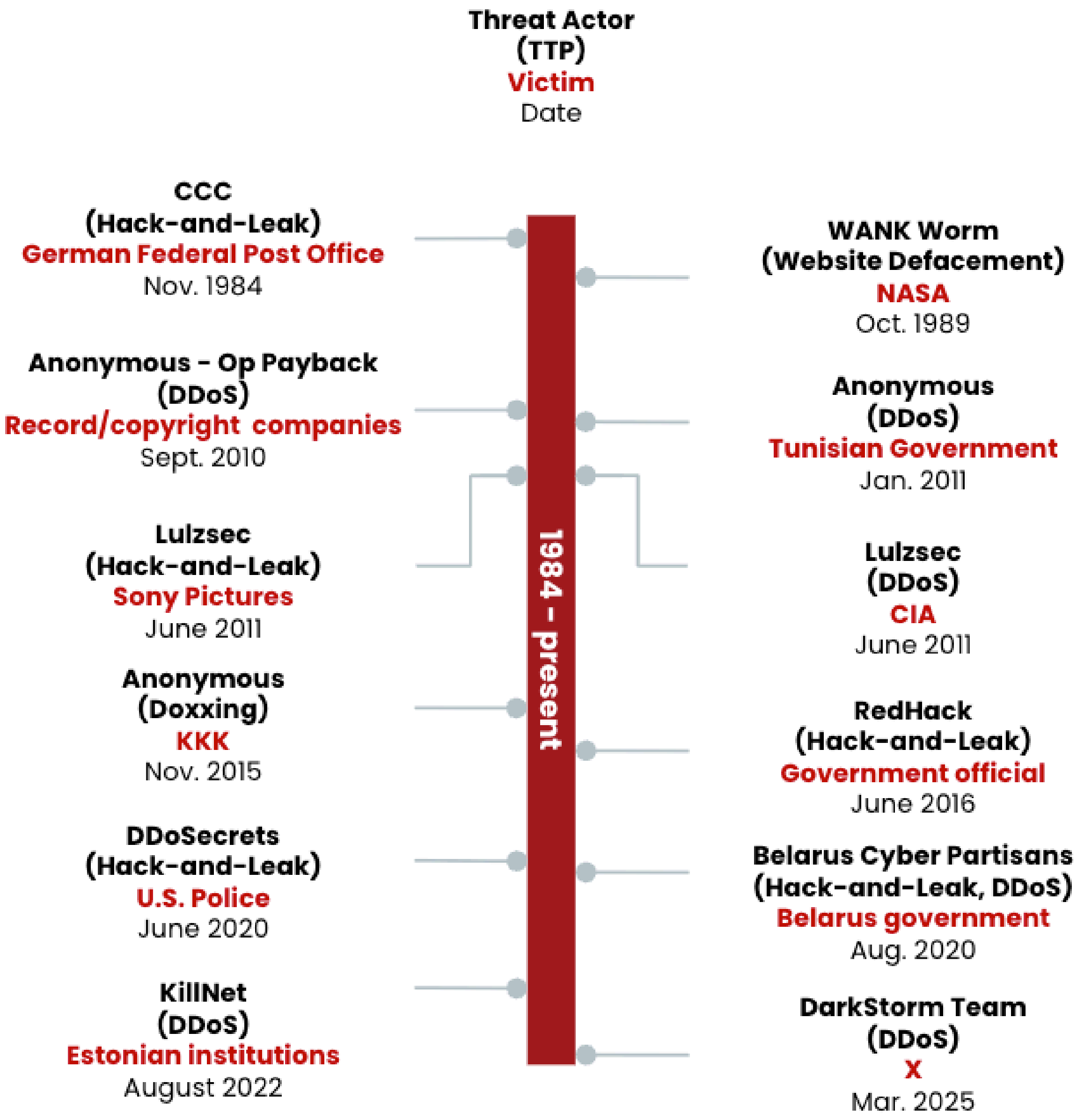
Doxxing

Doxxing refers to the act of publicly exposing information associated with individuals or organisations online without their consent—typically PII such as names, addresses, employment data, or phone numbers. Often, the types of information obtained during doxxing incidents can be acquired by low-skill hacktivists with minimal risk appetites, leveraging basic open-source intelligence (OSINT) techniques. Hacktivists will typically conduct doxxing to intimidate their intended victims, spread malinformation, or hold them accountable for a perceived wrongdoing.

- Geopolitical conflict and tensions often trigger a heightened risk of doxxing. On February 8, 2024, 600 members of the "J.E.W.I.S.H creatives and academics" Whatsapp group were subjected to doxxing, resulting in their contact details, photographs, and social media details being published online.[16] This incident was allegedly conducted by pro-Palestinian hacktivists, following the group's vocal criticism of a prominent Australian journalist,[17] almost certainly to highlight perceived wrongdoings of Israel in the conflict with Hamas.

Doxxing is legal in most countries—including most U.S. states—although it can be construed as stalking, malicious communications, or harassment crimes under specific circumstances.[18]

[15] hXXps://cyberscoop[.]com/nato-siegedsec-breac/
[16] hXXps://www.tortoisemedia[.]com/2024/08/23/academics-threaten-nyt-lawsuit-after-whatsapp-leak
[17] hXXps://www.thejc[.]com/news/world/australian-anti-israel-campaigners-publish-jew-list-mjtanvxp
[18] hXXps://hls.harvard[.]edu/clinic-stories/legal-policy-work/should-doxing-be-illegal/



Timeline of significant hacktivist operations

Source: ZeroFox Intelligence

Hacktivist Alliances

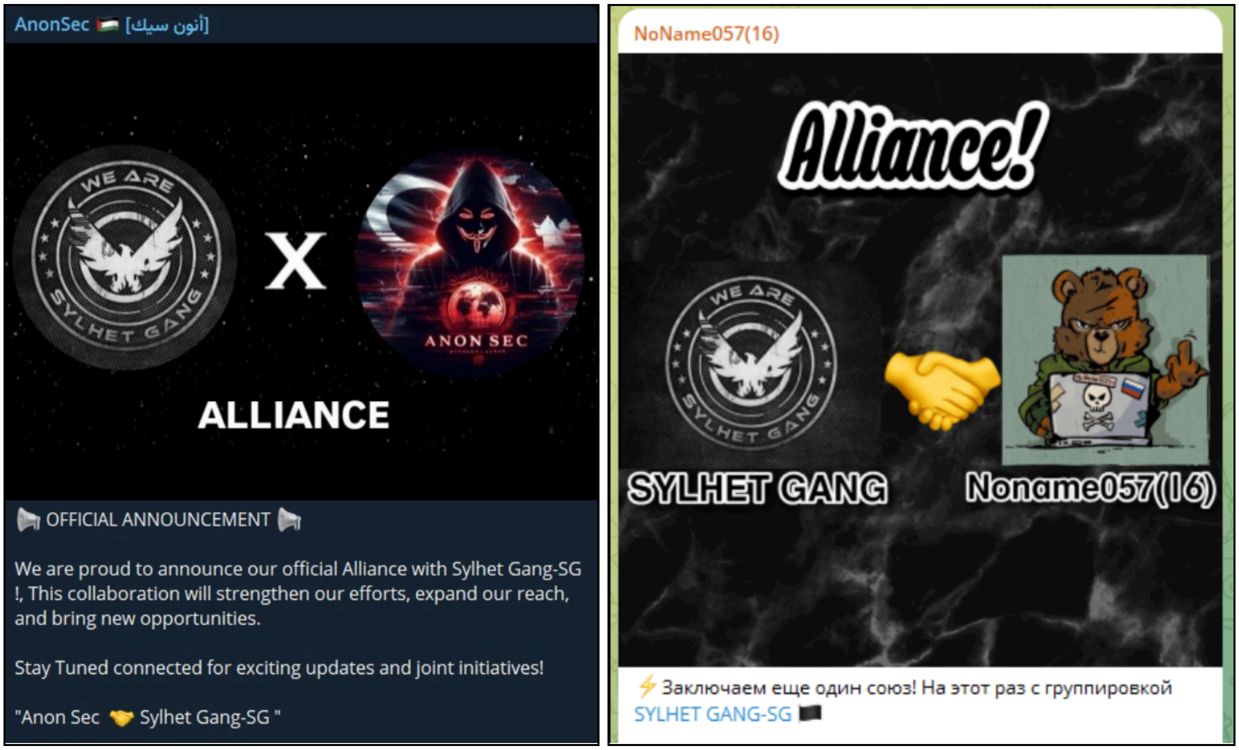
In response to geopolitical events and growing tensions, hacktivist collectives often form alliances with other collectives that share perceived injustices underpinned by ideological, religious, political, or national beliefs. Newly founded hacktivist collectives often seek to form alliances with established collectives in order to receive exposure to more advanced technical skills and knowledge, as well as to gain credibility for their own collective. Collaboration between hacktivist groups is commonly observed and is usually announced via social media platforms such as X or messaging channels such as Telegram. Below are some prominent examples of hacktivist collectives forming alliances with other collectives.

Sylhet Gang

"Sylhet Gang" is a prominent hacktivist collective whose motivations are very likely linked to Middle Eastern geopolitics, having been described as a "pro-Palestinian, anti-India, Bengali-speaking hacktivist group active since 2023."[19] Sylhet Gang has targeted entities it very likely perceives as aligned with or supportive of Israel, typically leveraging website defacement and DDoS to disrupt and undermine its targets. In recent months, Sylhet Gang has formed various alliances with other hacktivist collectives such as AnonSec, Killnet, and Noname057(16).[20][21][22]

- AnonSec, Killnet, and NoName057(16) have all expressed a pro-Palestinian stance in the past. On April 5, 2025, AnonSec announced on its Telegram channel that it had formed an alliance with Sylhet Gang, stating that "this collaboration will strengthen our efforts, expand our reach, and bring new opportunities." On May 9, 2025, AnonSec announced an alliance with "Dark Storm Team," another pro-Palestinian hacktivist collective. These alliances were almost certainly formed to collaborate on future attacks against enemies that they perceive as anti-Palestinian or pro-Western.

[19] hXXps://cyberpress[.]org/openai-targeted-by-sylhet-gang-sg/
[20] hXXps://x[.]com/FalconFeedsio/status/1908481237007638914
[21] hXXps://x[.]com/DailyDarkWeb/status/1753070700901077477
[22] hXXps://x[.]com/FalconFeedsio/status/1844527349762519457



AnonSec 🇵🇸 [أنون سيك]

📣 OFFICIAL ANNOUNCEMENT 📣

We are proud to announce our official Alliance with Sylhet Gang-SG !, This collaboration will strengthen our efforts, expand our reach, and bring new opportunities.

Stay Tuned connected for exciting updates and joint initiatives!

"Anon Sec 🤝 Sylhet Gang-SG "

NoName057(16)

⚡ Заключаем еще один союз! На этот раз с группировкой SYLHET GANG-SG 🏴

Sylhet Gang alliance announcements

Source: Telegram

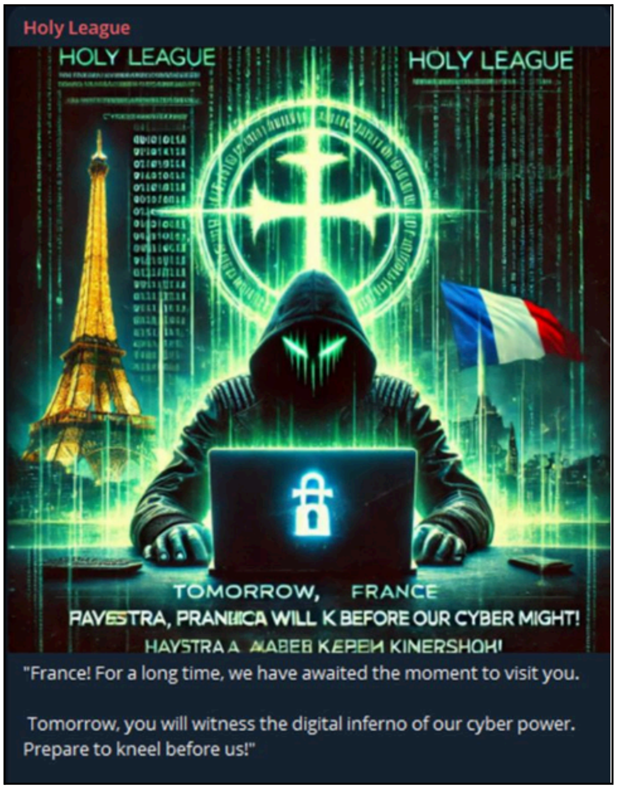
Holy League

"Holy League" was formed in July 2024 and is composed of pro-Russian and pro-Palestinian hacktivist collectives overtly opposed to Western values, as well as those supportive of Ukraine and Israel. Holy League has been responsible for an array of coordinated cyberattacks targeting Western military and government agencies, with the intent to disrupt services and instill societal unease, primarily conducted by DDoS and website defacement attacks.[23]

- On December 6, 2024, Holy League announced plans to attack the government of France in protest of its continued support for Ukraine and Israel. This was echoed by other members of the alliance, including NoName057(16), pro-Islamic group "Mr. Hamza," and pro-Palestinian collective "Anonymous Guys."[24] Holy League subsequently conducted multiple DDoS and website defacement attacks on

[23] hXXps://hide[.]me/en/blog/uk-infrastructure-under-siege/
[24] hXXps://thecyberexpress[.]com/holy-league-hacktivists-uniting-against-france/

French government websites and institutions, almost certainly to disrupt and undermine services.



Holy League

"France! For a long time, we have awaited the moment to visit you.

Tomorrow, you will witness the digital inferno of our cyber power. Prepare to kneel before us!"

HOLY LEAGUE
HOLY LEAGUE
TOMORROW, FRANCE
FAVESTRA, PRANЦICA WILL K BEFORE OUR CYBER MIGHT!
HAYSTRA A AABEB KEPEИ KINERSHOH!

Holy League announcement

Source: Telegram

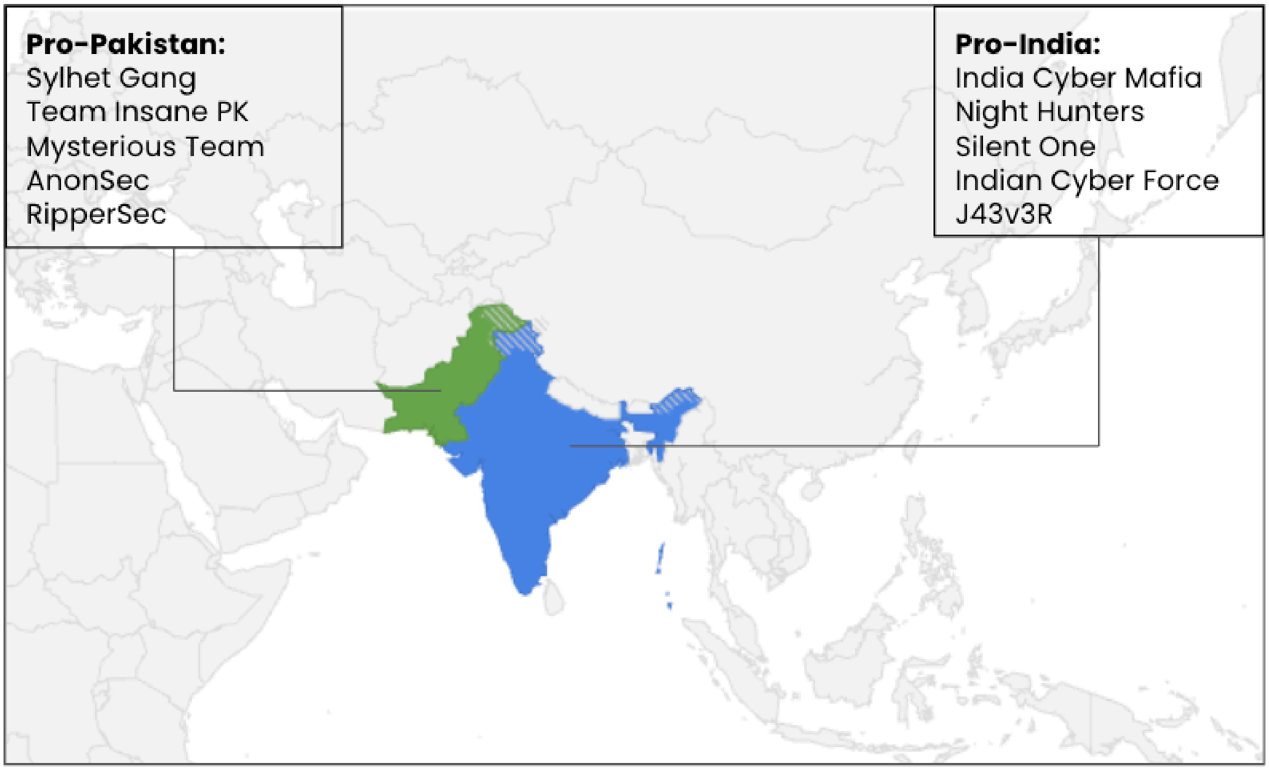
India-Pakistan 2025 Conflict

Following the escalation of hostilities between India and Pakistan in April–May 2025, ZeroFox observed an increase in hacktivist incidents targeting entities on both sides of the border. Since the onset of these hostilities, various hacktivist collectives have proclaimed their allegiance toward either Pakistan or India, while also forming new alliances in support of shared causes. According to announcements from malicious collectives, leveraged TTPs include DDoS, website defacement, and data breaches.

- Pro-Palestinian hacktivist groups have reportedly announced collaboration with pro-Pakistani hacktivists in the targeting of India-based infrastructure.[25]

[25] hXXps://www.darkreading[.]com/cyberattacks-data-breaches/pahalgam-attack-hacktivists-unite-opindia

- Hacktivist collectives such as “Vulture” (an Iran-based collective), “RipperSec” (likely a Malaysia-based collective), and “Mysterious Team Bangladesh” all announced within their respective messaging channels that they intend to support Pakistan in any ongoing conflict.



Examples of hacktivist allegiances as of May 14, 2025

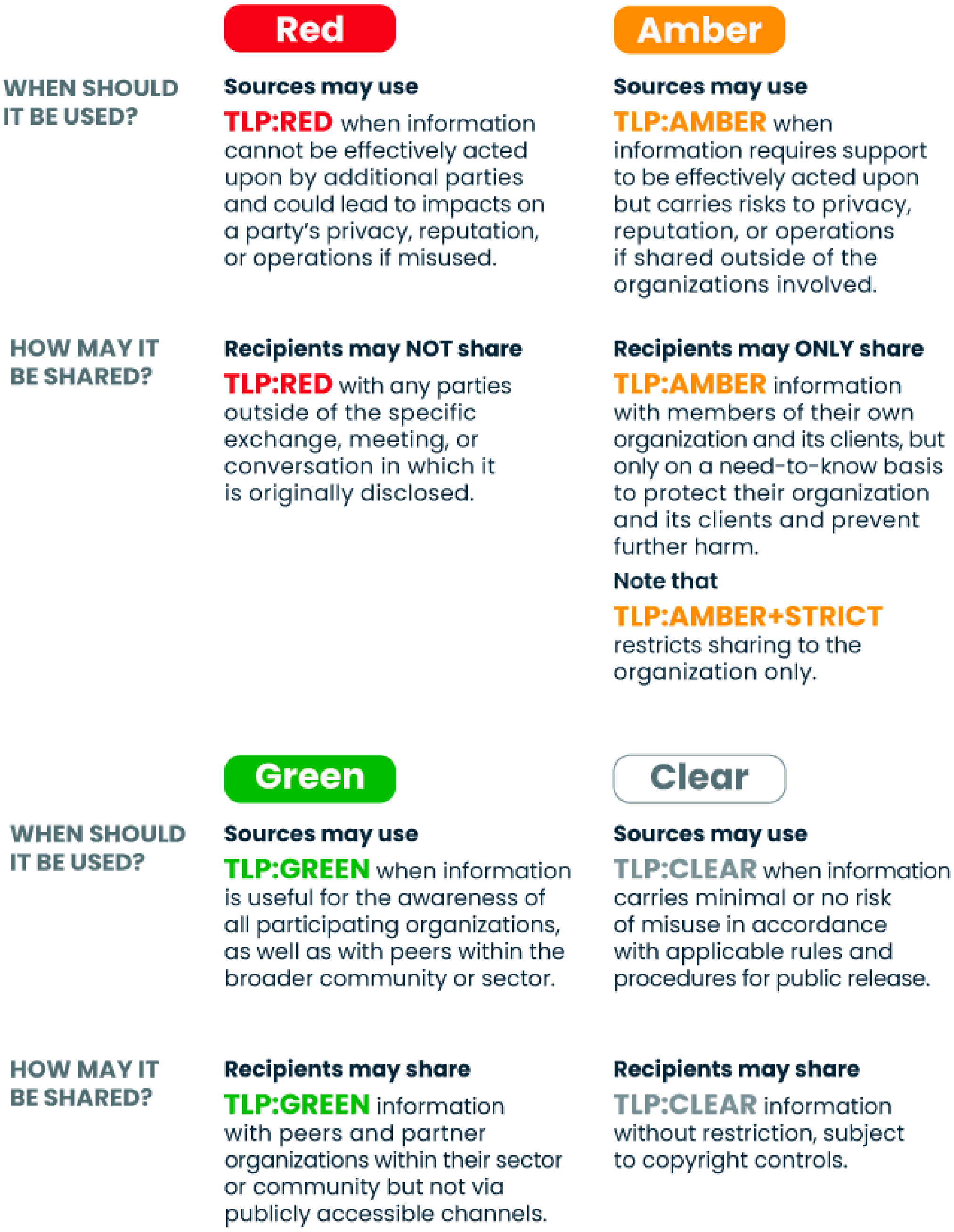
Source: ZeroFox Intelligence

As observed during the April–May 2025 India-Pakistan conflict, regional conflict can lead to an increase in hacktivist activity, and several new alliances can be formed as a response. ZeroFox has observed this reaction in several conflicts, including Ukraine-Russia, Israel-Hamas, and most recently, Israel-Iran. Future conflicts will almost certainly cause a similar response from the hacktivist community and lead to malicious cyber attacks—largely in the form of DDoS and website defacement—as well as the formation of new alliances between hacktivist collectives who share perceived injustices underpinned by ideological, religious, political, or national beliefs.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

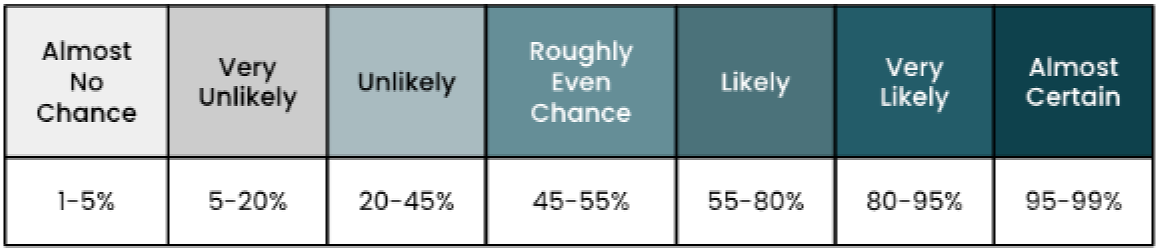


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%