01

War, Religion, and Politics: A Battleground For DDoS

NETSCOUT

DDoS attacks with sociopolitical roots have been a fact of life on the internet since the early 2000s. Disputes relating to politics, religion, and ideology often have been accompanied by—and increasingly are centered around—attack campaigns intended to disrupt the online operations and communications capabilities of governments, companies, communities of interest, and individuals.

This phenomenon has never been more apparent than during 1H 2022. Worldwide consequences and collateral damage resulted from DDoS attacks motivated by conflict that previously would have been considered local or regional in nature. This is especially true with increasing globalization and interconnectivity of the socioeconomic model.

Likewise, military capable nation-states now are openly embracing online aggression with the understanding that their behavior may result in kinetic responses that usher dangerous new levels of unpredictability into already-fraught situations.

THINK LOCALLY, ATTACK GLOBALLY

Most of the high-profile DDoS attack campaigns we've observed during 1H 2022 have corresponded with national or regional conflicts that have generated worldwide reactions. Indeed, most DDoS attacks are inherently transnational in both scope and scale, with skilled adversaries increasingly performing extensive pre-attack reconnaissance to identify key elements in the service delivery chains of their targets to ensure the success of adaptive DDoS attacks.

The result is that organizations and individuals with no obvious interest in a particular sociopolitical event are, nevertheless, negatively impacted by DDoS attacks that are based on those events.

FLASHPOINTS OF GEOPOLITICAL CONFLICT

Russia, Ukraine, and the Ripple Effect

As Russian ground troops prepared to enter Ukraine in late February, there was a significant uptick in DDoS attacks that targeted governmental departments, online media organizations, financial firms, hosting providers, and cryptocurrency-related firms.

Ukraine

The frequency and impact of these attacks escalated significantly after Russia invaded Ukraine on February 24. However, the effectiveness of these attacks largely depended on whether targeted organizations had organized DDoS defenses. This issue was quickly remedied for unprotected organizations as global DDoS defense companies stepped in to help Ukrainian organizations that needed it.

By April, the frequency of DDoS attacks directed toward networks located in Ukraine leveled off, followed by an additional rapid decrease. This likely is attributable to Ukrainian internet properties migrating to countries such as Ireland as instability in the intra-Ukraine internet forced many network segments to rely on connectivity in other countries.

DDoS Attacks in Ukraine 1H 2022

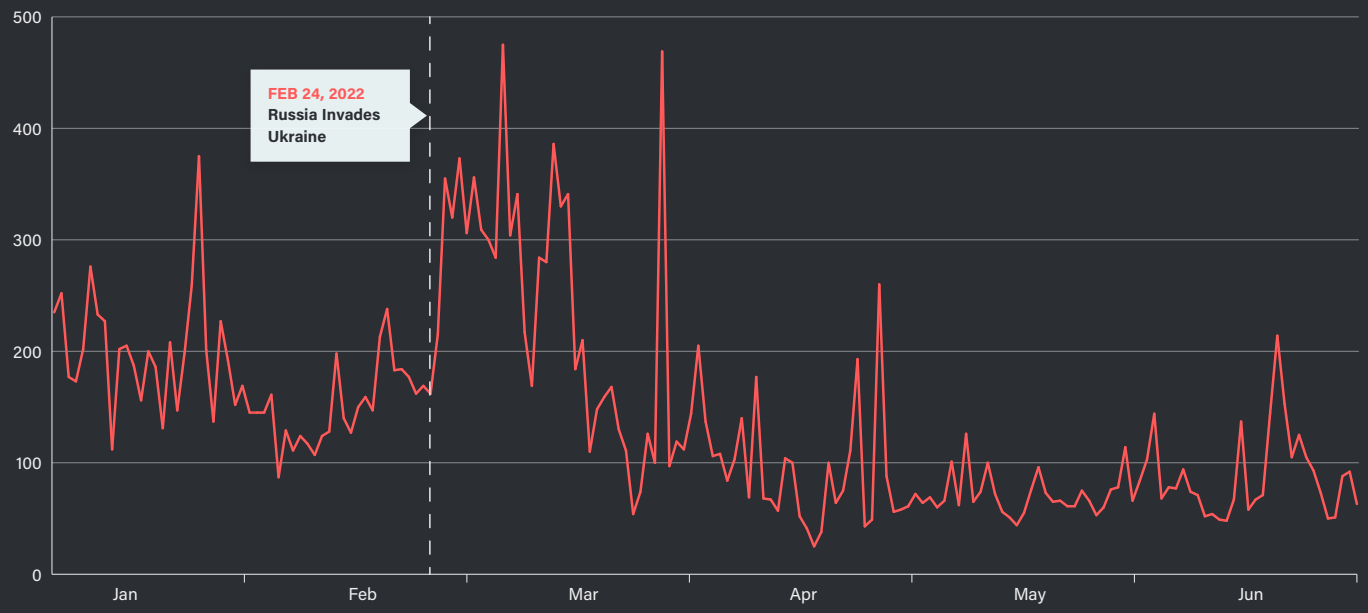


Figure 1: DDoS Attacks in Ukraine 1H 2022 (Data: ATLAS)

Ireland

As shown below, organizations in Ireland were pummeled by a huge surge in attacks after providing service to Ukrainian organizations.

DDoS Attacks in Ireland 1H 2022

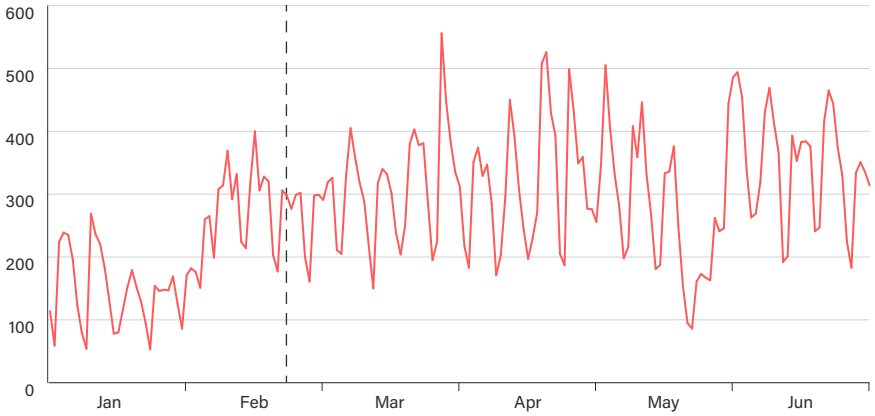


Figure 2: DDoS Attacks in Ireland 1H 2022 (Data: ATLAS)

India, Taiwan, and Belize

Echoes of this conflict continue to resonate across the global internet. India experienced a measurable increase of DDoS attacks following its abstentions from United Nations Security Council and General Assembly votes condemning Russian actions in Ukraine. The daylong attack on Taiwan coincided with public remarks at a policy seminar sponsored by Taiwan's representative to the United States; likewise with Belize (below).

Taiwan endured it's single highest number of DDoS attacks in a single day which coincided with public remarks at a policy seminar sponsored by Taiwan's representative to the United States.

DDoS Attacks in India, Belize and Taiwan 1H 2022

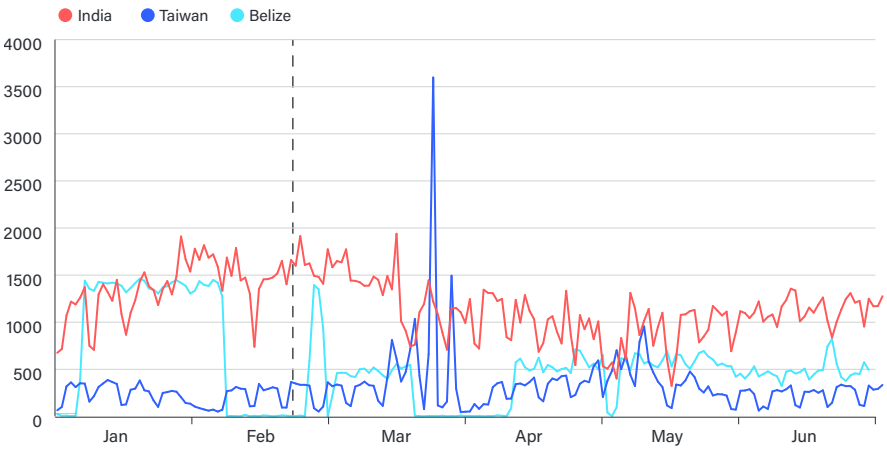


Figure 3: DDoS Attacks in India, Belize and Taiwan 1H 2022 (Data: ATLAS)

Finland

Finland experienced a 258 percent year-over-year increase in DDoS attacks that started with early discussions from the Prime Minister to join "without delay" in May 2022, a decision vehemently opposed by Russia, its physical neighbor (below)

+258%

increase in DDoS attacks on Finland which directly coincides with their announcement to apply for membership in NATO.

DDoS Attacks in Finland 1H 2022

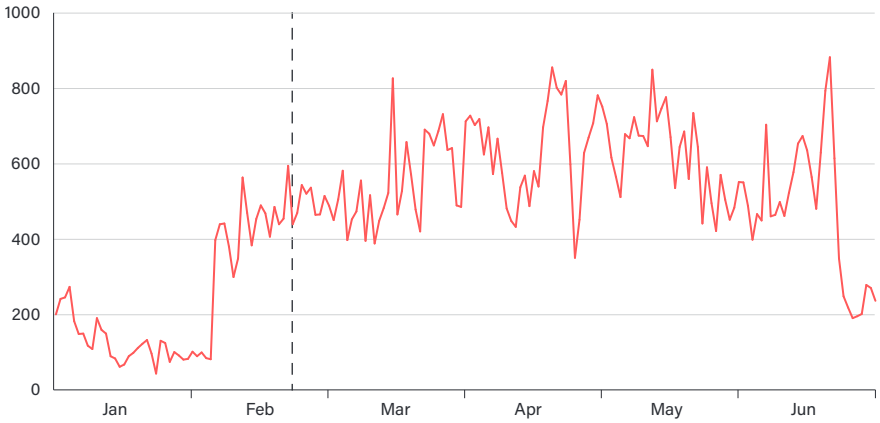


Figure 4: DDoS Attacks in Finland 1H 2022 (Data: ATLAS)

Satellite Telecommunications

And although the frequency and severity of DDoS attacks in North America was relatively consistent across the first half of the year, specific industry sectors did experience an increase in high-impact DDoS attacks. For example, satellite telecommunications providers were targeted more frequently after providing support for Ukraine's communications infrastructure (below).

Satellite telecommunications providers were targeted more frequently after providing support for Ukraine's communications infrastructure.

Attacks Against Satellite Telecommunications Providers 1H2022

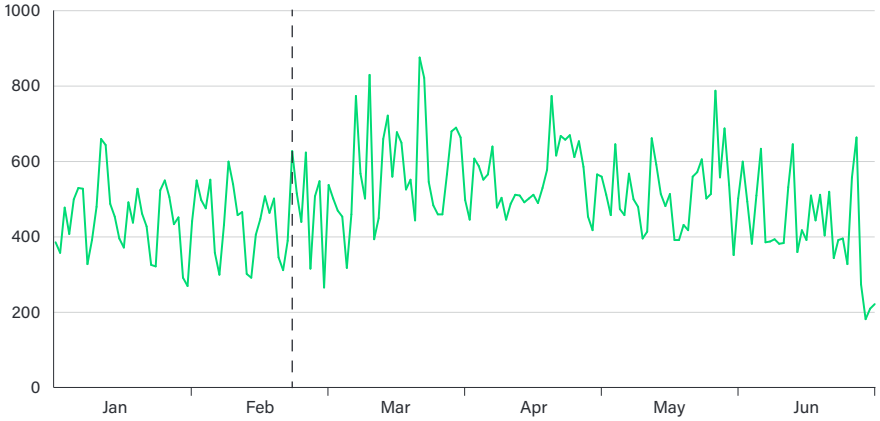


Figure 5: DDoS Attacks Against Satellite Telecommunications Providers (Data: ATLAS)

Poland, Romania, Lithuania and Norway

Poland, Romania, Lithuania, and Norway all were targeted with DDoS attacks by adversaries that linked to Killnet, a group of online attackers aligned with Russia (below).

DDoS Attacks in Lithuania, Norway, Poland and Romania 1H2022

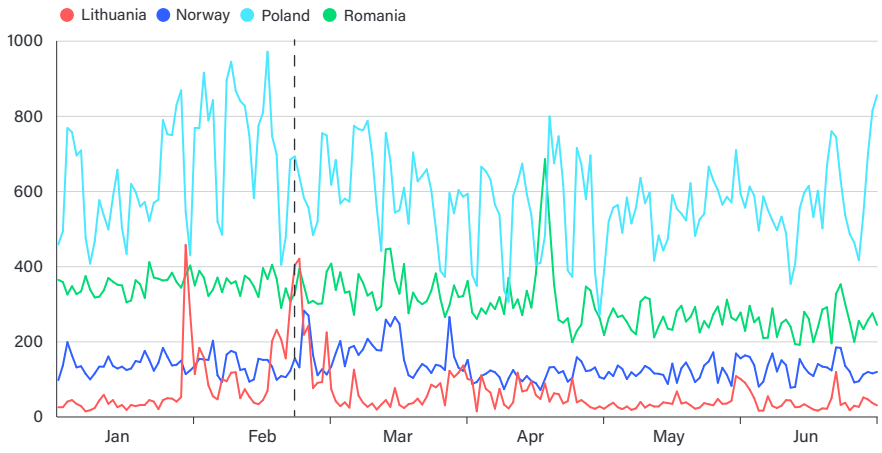


Figure 6: DDoS Attacks in Lithuania, Norway, Poland, Romania (Data: ATLAS)

DDoS Attack Vectors

All the DDoS attacks that appear to be related to the Ukraine/Russia conflict utilize well-known DDoS attack vectors. In terms of attack characteristics and impact, most can be attributed to standard DDoS-for-hire services, well-known botnets such as Meris and Dvinis, and manually driven DDoS attack tools such as Low Orbit Ion Canon (LOIC) and Killnet Vera.

Some high-volume reflection/amplification attacks were initiated via bespoke attack infrastructure. Likewise, we observed an instance of targeted spoofing that attempted to induce defenders into denying valid traffic from legitimate correspondents. Despite the variance in attack harness, it's clear that TCP-related attacks dominated globally. The same is true for all the aforementioned countries, as evidenced by the high-level split between vector types seen in the following chart.

In terms of attack characteristics and impact, most can be attributed to standard DDoS-for-hire services, well-known botnets like Meris and Dvinis, and manually driven DDoS attack tools like LOIC and Killnet Vera.

Attack Vector Breakdown

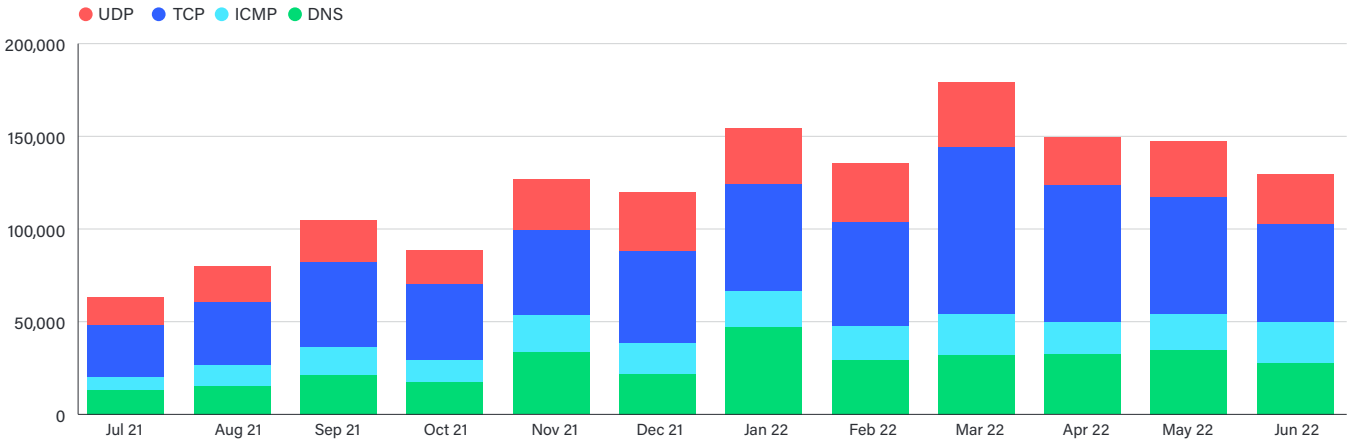
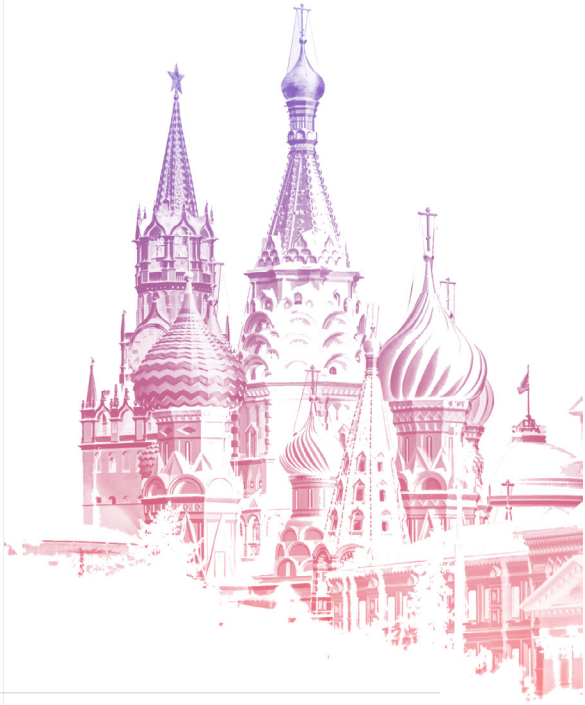


Figure 7: Vector Attack Breakdown 2H 2021 vs. 1H 2022 (Data: ATLAS)



Russia

It's also important to note that Russia became a prime target for DDoS attacks immediately following the start of ground operations in Ukraine. There's little doubt that the genesis of this behavior was hacktivists and others opposed to the invasion, especially considering that many of the targets of those DDoS attacks were aimed at governmental, media, and financial organizations (below).

DDoS Attacks in Russia 1H2022

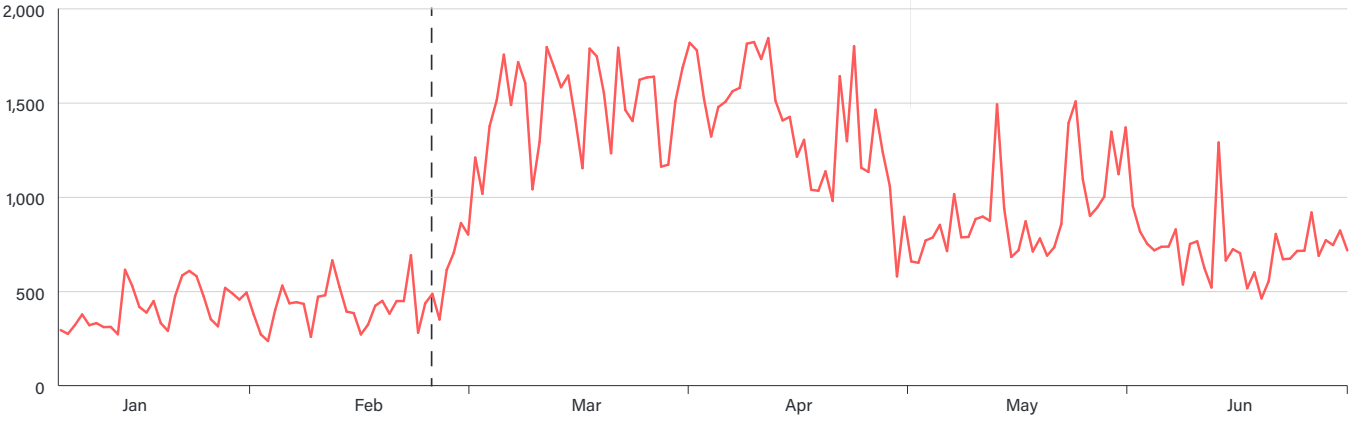
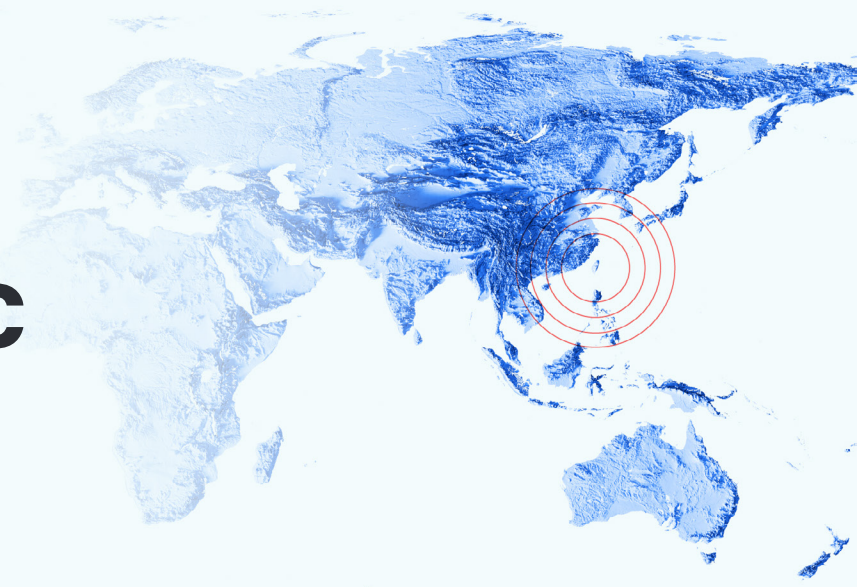


Figure 8: DDoS Attacks in Russia 1H2022 (Data: ATLAS)

It's important to note here the historical implications of DDoS attacks previously related to Russia and Ukraine. Since the early 2000s, Russia has almost certainly worked with cyber criminal groups who shared goals of launching attacks against their opponents, including DDoS attacks. In many cases, these are homegrown online criminal enterprises provided operational leeway and designated targets for attack by Russian security organizations—a tactic employed to provide the Russian state with plausible deniability for online aggression.

It is likewise important to note that Ukraine has also utilized this tactic. In underground forums frequented by European internet adversaries, the Ukrainian language is nearly as prevalent to that of Russian. However, in the conflict with Russia, Ukraine has placed a far greater emphasis on recruiting ideologically motivated volunteers to launch DDoS attacks against Russia and perceived Russian allies. Ukraine also has benefited from DDoS attack campaigns launched by Western-affiliated online activist groups, providing it with plausible deniability for those attacks.

We anticipate these trends will continue for the duration of hostilities between Russia and Ukraine, with shifts in scope, targets, and impact as the conflict evolves.



Asia-Pacific

As tensions between Taiwan and China and Hong Kong and China escalated during 1H 2022, DDoS attack campaigns routinely targeted involved parties (below).

In particular, DDoS attacks directed against Taiwan regularly occurred in concert with related public events. As with Russia and Ukraine, China utilizes arm's-length online groups to launch attack campaigns against perceived opponents, whereas other disputants tend to rely more heavily on ideologically motivated volunteers and online activist groups unofficially sponsored by various countries (below).

DDoS Attacks in China, Hong Kong, and Taiwan 1H2022

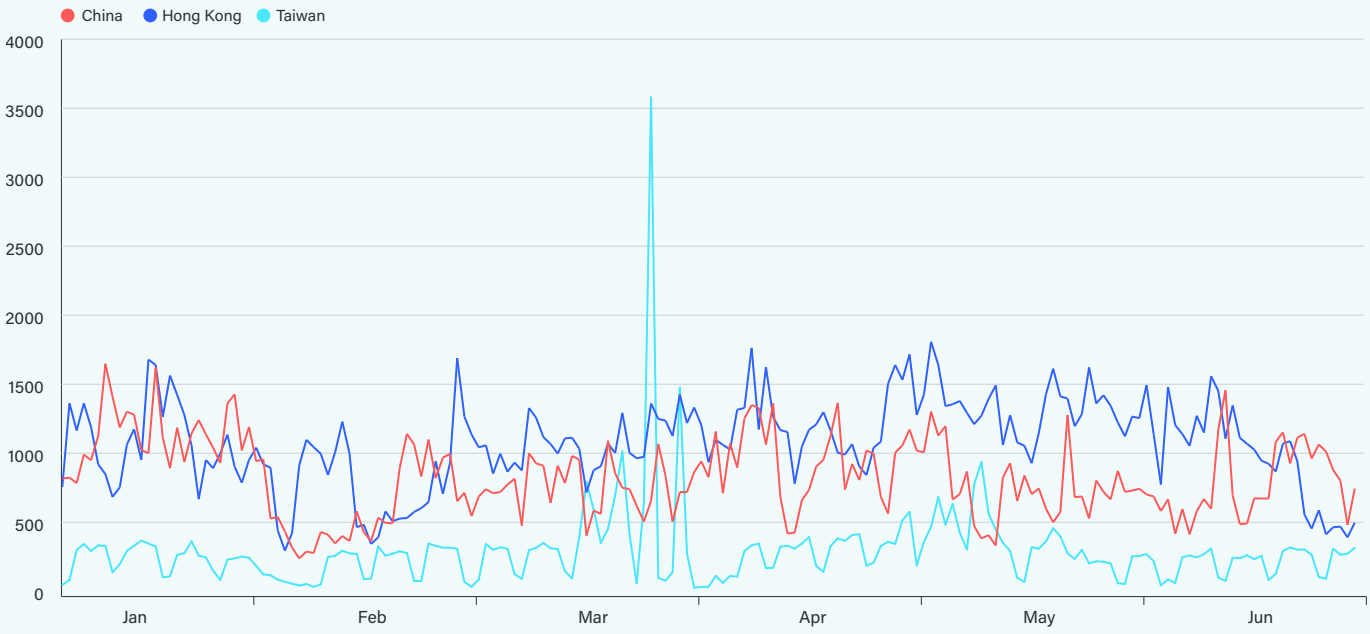
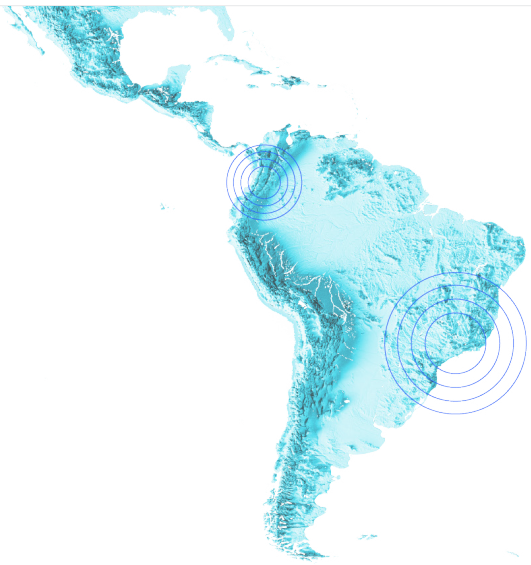


Figure 9: DDoS Attacks in China, Hong Kong and Taiwan 1H2022 (Data: ATLAS)



The Americas

Colombia

An unusually contentious presidential election cycle in Colombia was accompanied by successive waves of DDoS attacks both during the initial vote and in concert with the contested runoff election between the top candidates (Figure 10).

DDoS Attacks in Colombia 1H2022

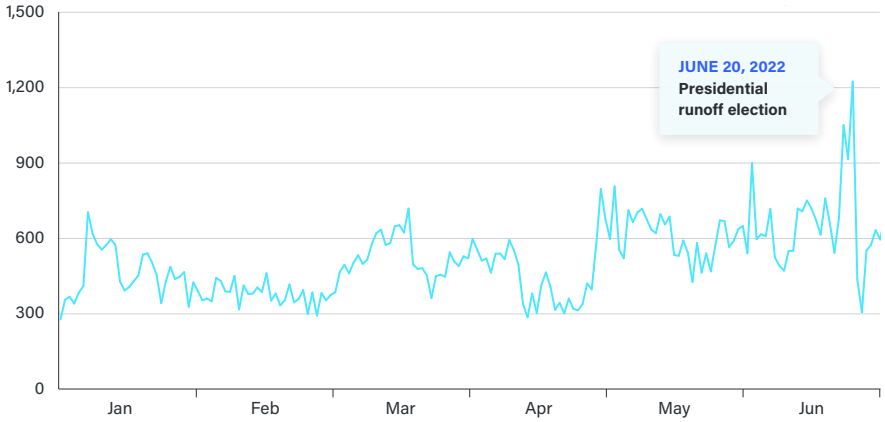


Figure 10: DDoS Attacks in Colombia 1H2022 (Data: ATLAS)

Brazil

Although politics play a key role in the DDoS world, other major events can also draw adversaries. The largest spike seen over the six-month window of 1H 2022 took place just as the Rio Carnival kicked off—a much-delayed event due to COVID-19. Several major business summits also took place around the same period, increasing the amount of activity in the country (Figure 11).

DDoS Attacks in Brazil 1H2022

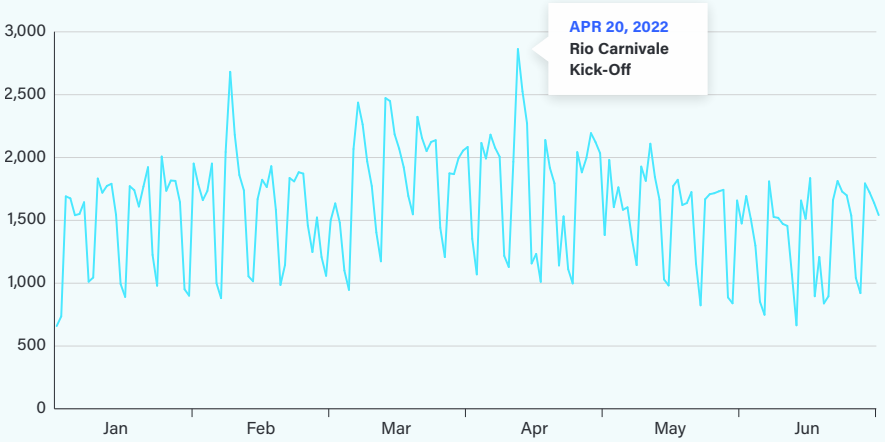


Figure 11: DDoS Attacks in Brazil 1H2022 (Data: ATLAS)

Religious Organizations

DDoS attacks against governmental and religious institutions in Brazil appeared to coincide with contentious public debate over a series of court decisions in the United States with religious leaders in Brazil landing on one side of the issues in one country often spur attacks in seemingly unrelated areas of the world (below).

DDoS Attacks on Religious Organizations 2H2021–1H2022

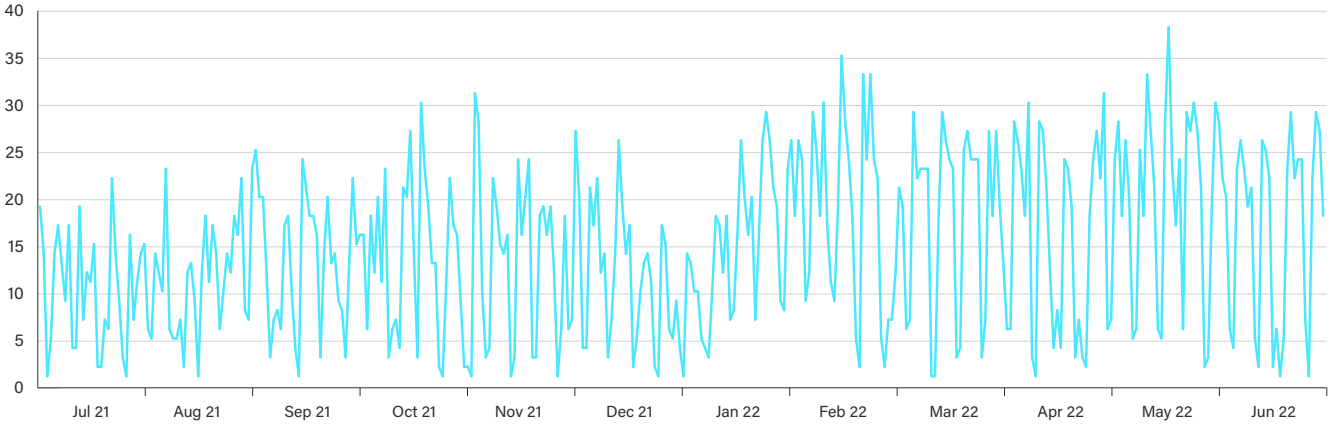


Figure 12: DDoS Attacks on Reglious Organizations (Data: ATLAS)

Conclusion

DDoS trends from 1H 2022 show that militarily capable nation-states are discarding strategic ambiguity in favor of open hybrid warfare, and as unpleasant as that is, it is important to use caution and restraint when attributing those attacks, because many challenges remain when it comes to positively identifying online perpetrators.

DDoS is an effective tool for disrupting networks and degrading morale for countries embroiled in sociopolitical upheaval. But adversaries don't need a particular reason to launch an attack; they're happy to do so under the guise of activism, religion, nihilism, military conquest, and more.

Organizations must consider both local and international conflicts when assessing DDoS risk factors, especially as they relate to direct service delivery elements, supply-chain partners, and other dependencies. Global situational awareness and continuous risk assessment are key to survival in this era of deliberate online disruption driven by sociopolitical events.

EXPLORE MORE OF THE 1H2022 DDoS THREAT INTELLIGENCE REPORT

For more expert insight in DDoS global and regional attack statistics, botnet activity, attack vectors and DDoS is used in geopolitical conflicts, revisit the NETSCOUT 1H 2022 DDoS Threat Intelligence Report landing page.

VISIT THE SITE

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against security, availability, and performance disruptions. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our Omnis™ cybersecurity advanced threat detection and response platform offers comprehensive network visibility, threat detection, highly contextual investigation, and automated mitigation at the network edge. NETSCOUT nGenius™ service assurance solutions provide real-time, contextual analysis of service, network, and application performance. And Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

To learn more about improving service, network, and application performance in physical or virtual data centers or in the cloud, and how NETSCOUT's security and performance solutions can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

CONTRIBUTORS

Richard Hummel
AUTHOR

Roland Dobbins
AUTHOR

NETSCOUT

SECR_042_EN-2201 09/2022