Radware Cybersecurity Advisory

OpIsrael: A Decade in Review

March 29, 2023

Anonymous and several cornerstone operations like OpIsrael have faced a significant decline in support and backing for years. This was the result of the fragmentation of Anonymous, competition from other threat groups, and the general escalation of the threat landscape. But over the last year, the war in Ukraine and geo-political tensions around the world have resulted in a renewed growth in hacktivism that has revolutionized the way armed conflicts will be fought in the future.

Background

OpIsrael is an Anonymous operation that was launched in **November 2012** in response to an Israeli military operation, Pillar of Defense. Pillar of Defense was an eight-day operation launched by the Israel Defense Force on November 14th, 2012, in response to 100 rockets that were fired at Israel within 24 hours from the Hamas-governed Gaza Strip.

At the time, OpIsrael was not an official operation, but rather a battle tag the group of hacktivists associated with Anonymous chose to use for their response to the Israeli operation. During the Anonymous operation in 2012, hundreds of Israeli websites were targeted with data breaches, defacement, and denial-of-service attacks. This left many security professionals wondering if this was what the future of war would look like and if a hacktivist group such as Anonymous could be considered a legitimate army.

The following year, Anonymous moved to create an annual coordinated campaign against Israel under the battle tag, OpIsrael. The inaugural campaign was launched on **April 7, 2013**, parallel to Holocaust Remembrance Day, with the goal to "erase Israel from the internet." The operation targeted networks and applications in Israel for what Anonymous perceived as human rights violations against the people of Palestine in hopes the campaign would bring attention to the ongoing Israeli-Palestinian conflict.

Timeline

Over the last decade, OpIsrael has evolved both in its impact and relevance. In November 2012, OpIsrael was just a one-off response to an Israel military operation in the Gaza Strip. Still, OpIsrael gained widespread attention in April 2013 after Anonymous announced a dedicated yearly campaign. As the years passed, the operation continued to target Israeli institutions to raise awareness about the Israeli-Palestinian conflict. However, the collective's impact slowly declined in recent years due to the fragmentation within Anonymous, improved cybersecurity measures, shifting public opinion, and the rise of other hacktivist groups. As a result, OpIsrael's influence and effectiveness have diminished substantially, causing the campaign to lose much of its initial momentum and support.

2014 - During **OpIsrael 2014**, Anonymous and its affiliates continued their operations against Israel, hoping their attacks would raise awareness and support the people of Palestine. Attacks at that time mainly consisted of crowdsourced-based denial of service attacks, website defacements, and data breaches. In some cases, the hacktivist leaked personal information, including email addresses, passwords, and phone numbers. It is important to note that in 2014, several hacktivists were seen repackaging and publishing old data dumps and new leaks. This is a tactic that would be used heavily in the future as OpIsrael relevance declined. It was also important to note that a second operation, OpIsrael Reloaded, was launched in July 2014 by a pro-Muslim, Indian-based hacktivist.

2015 - During **OpIsrael 2015**, we began seeing Anonymous share knowledge with other members in IRC chats and on paste sites[1]. This is likely due to the group realizing the increased challenges they faced with maintaining a yearly operation with the same level of impact. Despite the hacktivist claims of widespread outages, the 2015 campaign was relatively limited due to Israeli authorities and organizations taking the appropriate measures to prepare for an attack.

2016 - During **OpIsrael 2016**, Anonymous began repeating many of its slogans and reposting content from the previous operations. At the time, the collective was distracted by the US presidential election. Before this year, Anonymous was mainly a voice for the powerless but had begun supporting political candidates as election-related cyberattacks started to take center stage. As a result, OpIsrael suffered and began to lose complete support for the operation.

2017 - During **OpIsrael 2017**, Anonymous once again attempted to leverage all the resources it could to combat the escalating defensive measures deployed by the government and organizations in Israel. In addition to repacking old data leaks, the group began searching for unprotected websites of small and medium-sized businesses in hopes of a more significate impact than the years prior. What was left of Anonymous—and its affiliates associated with OpIsrael—started focusing on maximizing effort by building groups and social channels to better organize those involved. Inside those channels, Anonymous began sharing more toolkits, loaded with denial-of-service scripts, but there was no large adoption of IoT botnets by the collective.

2018 - During **OpIsrael 2018**, members of Anonymous continued to attempt to transfer knowledge to new hacktivists by sharing tools and recommendations for launching attacks. As a result, more defacements and simple denial-of-service attacks occurred compared to previous years. The collective started sharing detailed

[1] A website that allows users to store and share text-based information, such as code snippets, scripts, configuration files, or any other form of plain text (e.g., Pastebin, ControlC)

information about how to run reconnaissance operations, launch web application attacks and use Shodan[2] or Google Dorks[3] to increase their overall impact. One of the main concerns for many organizations during 2017 was the shift away from targeting well-protected assets to targeting small to medium-sized businesses and Israeli citizens who were indirectly involved with the conflict in Palestine.

2019/2020 - In 2019 and 2020, OpIsrael suffered a significant loss in support as Anonymous fell apart due to political infighting and a shifting of public opinion related to the Israeli-Palestinian conflict. The threat landscape evolved dramatically during these years as geo-political tensions flared up, making way for state-affiliated cyberattacks related to regional disputes. 2019 was also the year that the Israeli government targeted and killed a group of Hamas-linked hacktivists in Gaza with an air strike after the group launched a cyberattack against Israel, forcing many threat actors to think about the potential consequences of their attacks. The following year, a newly formed group called **Hackers of Savior** launched a one-off defacement campaign in May that targeted thousands of Israeli websites showing a video and a countdown related to Quds Day.

2021 - Following the downfall of Anonymous and the lack of support for OpIsrael, a group of pro-Muslim hacktivists from Southeast Asia launched a new campaign called **OpsBedil** to fill the void. In 2021, cyberattacks in general were mainly reactionary in the Middle East, with minor cases of hacktivism in the region typically following physical or political confrontation. Specifically, OpsBedil was a political response by **DragonForce Malaysia** to the Israeli ambassador to Singapore stating that Israel was ready to work towards establishing ties with Southeast Asia's Muslims-majority nations. As a result, the group and several affiliates launched a series of DDoS and defacement attacks against several organizations in Israel during June and July.

2022 - Following the success of OpsBedil the year before, DragonForce Malaysia launched **OpsBedil Reloaded** in response to tension in the Middle East during Ramadan. Over the year, the group grew to over 13,000 members who mainly communicated on their private forum. During this campaign, DragonForce Malaysia and other threat actors targeted several organizations in Israel with defacements, denial-of-service attacks, and data leaks. Hacktivist campaigns like OpsBedil, while nowhere close to as notorious as OpIsrael once was, present a renewed level of risk for the region. Unlike Anonymous, which had very little bandwidth remaining to target

[2] Search engine for internet-connected devices (shodan[.]io)
[3] A Google dork query, sometimes just referred to as a dork, is a search string or custom query that uses advanced search operators to find information. Multiple parameters can be used in a Google dork query to search for files or information on a website or domain (e.g., "radware report filetype:pdf").

Israel, DragonForce Malaysia and its affiliates had the time, the resources, and the motivation to present a new moderate level of risk for Israel and overshadowed anything that resembled OpIsrael in the month of April.

Attack Vectors

It is important to note that Anonymous is a decentralized group with diverse factions and individuals pursuing their own goals. As a result, the specific tactics and methods used in any cyberattack may vary depending on the threat actors involved.

DEFACEMENTS

Defacement attacks are a form of digital graffiti where an attacker gains unauthorized access to a website's web application to modify its appearance. Typically, attackers will replace the original content with their own text, images, and links to spread political messages, promote a cause, or cause disruption and embarrassment for the victim.

Defacement attacks usually exploit vulnerabilities in the target website or its underlying infrastructure, such as weak passwords, outdated software, or unpatched security vulnerabilities. While the immediate impact of a defacement attack is often reputational damage, it can also lead to loss of trust, revenue, and potentially legal consequences for the website owner.

DATA LEAKS

A data leak is a cybersecurity incident that involves the **exfiltration** of sensitive, confidential, or proprietary information. That information can later be maliciously disclosed or otherwise made available by unauthorized individuals. Data leaks can occur through various compromises, including but not limited to misconfigurations, human error, insider threats, or vulnerabilities found within a targeted system.

Data leak campaigns usually have a devastating impact on targeted organizations and individuals. A successful attack can result in financial loss, reputational damage, and possible regulatory fines. Typically, leaked information from data breaches includes personally identifiable information, such as names, addresses, social security numbers, credit card numbers, banking details, or other sensitive data.

DENIAL OF SERVICE

A **network** or **endpoint** denial-of-service (DoS) attack is a technique used by hacktivists to disrupt or degrade a targeted system or service by overwhelming it with an excessive volume of traffic or requests. These types of cyberattacks, when successfully launched, can render targeted networks and applications inaccessible or unresponsive to legitimate users, resulting in possible financial losses and damage to an organization's reputation.

A variation of the denial-of-service attack is a distributed denial-of-service (DDoS) attack, which involves attackers leveraging multiple compromised or volunteered devices, often called a botnet, to generate distributed floods of malicious traffic. DDoS attacks are typically harder to mitigate because they involve numerous sources, rendering thresholds ineffective and making it harder to differentiate between legitimate and malicious traffic.

PHISHING

A **phishing** attack is a technique attackers use to gain access to a victim's system. The attack exploits human psychology to trick individuals into revealing sensitive information or performing specific actions that compromise their security. These attempts are either sent to everyone in the company or, in the case of spear phishing attacks, specifically designed to target important associates.

Phishing attacks often occur via email but can also occur through other communication channels, such as text messages or social media platforms. The attackers create fake messages or websites, called lures, to trick their victims into believing they are interacting with a legitimate source.

Manipulating Facts

It is important to note that, over the years, Anonymous has been found to exaggerate its accomplishments, manipulate facts, and claim responsibility for cyberattacks they may not have performed. In the past, these bits of misinformation have generated substantial amounts of media attention, bolstered the group's reputation, and created an atmosphere of uncertainty around Anonymous' true capabilities.

Critics over the years have argued that such actions undermine the group's credibility and undermines the legitimate issues they are attempting to address. Nevertheless, whether the claimed cyberattacks are authentic or not, Anonymous' actions have sparked discussions about cybersecurity's importance, hacktivism's role in modern society, and the need for increased transparency and accountability from organizations and governments alike.

OpIsrael 2023

It appears now that Anonymous still lacks the support and backing it used to have for OpIsrael. Adding to the group's limited resources is their competition for media attention with the war in Ukraine. The hacktivist groups associated with the war in Ukraine are either state-backed or organized in clusters and have become media savvy, with references to new operations in the daily news cycles.

Nevertheless, the growing geo-political tension in and around Israel, together with the revival of hacktivism spurred by the war, has set the stage for a potential return of mainstream operations against the country, with

several events to react to. Specifically, one of the more politically charged events outside the country revolves around the upcoming FIFA U-20 World Cup in Indonesia. After a protest to remove Israel from the global youth soccer tournament by Indonesians in the Muslim-majority nation, **FIFA has cancelled preparations for the event**, which should start on May 20, 2023. It is rumored that the U-20 World Cup could be moved last minute to Peru, and Indonesia could lose their chance to qualify for the 2026 World Cup due to the country's negative response to the Israel youth soccer team. If Indonesia loses its opportunity to host the soccer tournament and is banned from the 2026 World Cup, it can be expected that pro-Muslim hackers from the region will retaliate against Israel for years to come.

Figure 1: Source @cyberofgaruda

Inside the country, Israel has been faced with civil unrest resulting from judicial reform and has been targeted by several violent terrorist attacks due to escalating tensions in eastern Jerusalem. As a result, a handful of Anonymous hacktivists have begun leveraging images from the protest in Tel Aviv and east Jerusalem to fill the narrative that Israel is collapsing from within. Specifically, an Israeli citizen at the judicial reform protest in Tel Aviv was photographed carrying an anti-Israeli banner associated with OpIsrael—displaying the word "OpIsrahell"—which furthered the group's conspiracy theory.

Figure 2: Source @muhammadshehad2

Apart from internal and external geo-political tension related to Israel, a few pro-Muslim-based hacktivists have been targeting the country steadily for the past few weeks with minimal impact. Groups like AnonGhost team, not to be confused with the original AnonGhost, Mysterious Team, Anon Cyber Vietnam, WSHPCZ3, Cyber Army of Vietnam, Muslim Cyber Army, Cyber KEX, and Ghost Clan have all been seen launching defacement and denial-of-service attacks at targets in Israel.

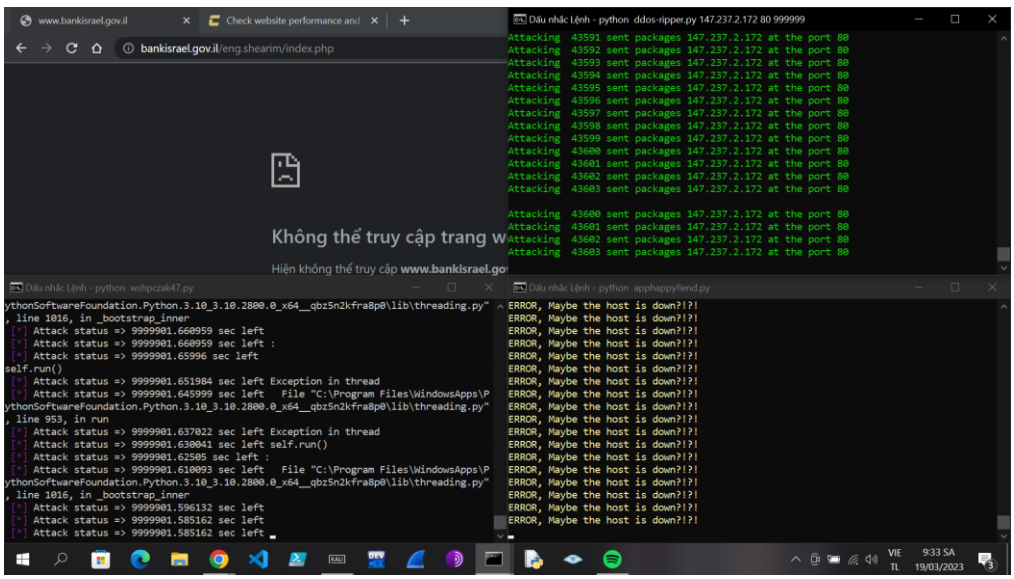

Figure 3: Source @wshpczakm12

Reasons for Concern

Over the last year, the continued war in Ukraine has resulted in a significant escalation in the threat landscape and a substantial increase in cyberattacks. Hacktivist groups like Anonymous have reemerged as tensions rise worldwide, launching renewed operations and cyberattacks that align with their political or social agendas once again. Hacktivists associated with OpIsrael often target a wide range of entities, including government agencies, critical infrastructure, and private organizations, aiming to make a statement or disrupt the operations of those they perceive to be acting unjustly.

With the re-emergence of hacktivist groups last year, there is also a growing concern that previous operations like OpIsrael may pose renewed threats to organizations across various sectors inside the country. Organizations should pay attention to the resurgence of Anonymous and similar hacktivist groups for several reasons. Hacktivist operations rapidly change and are unpredictable, preventing organizations from preparing for possible risks and establishing a suitable defensive strategy for a given situation. Secondly, associations between hacktivist collectives and other cybercriminals or state-sponsored agents can result in more significant cyberattacks. Moreover, major hacktivist operations often receive a considerable amount of media attention, leading to heightened public scrutiny.

Considering these factors, organizations in Israel must remain alert, monitor the changes in the threat landscape, and adopt comprehensive cybersecurity measures to safeguard their resources and reduce the likelihood of being targeted by hacktivists.

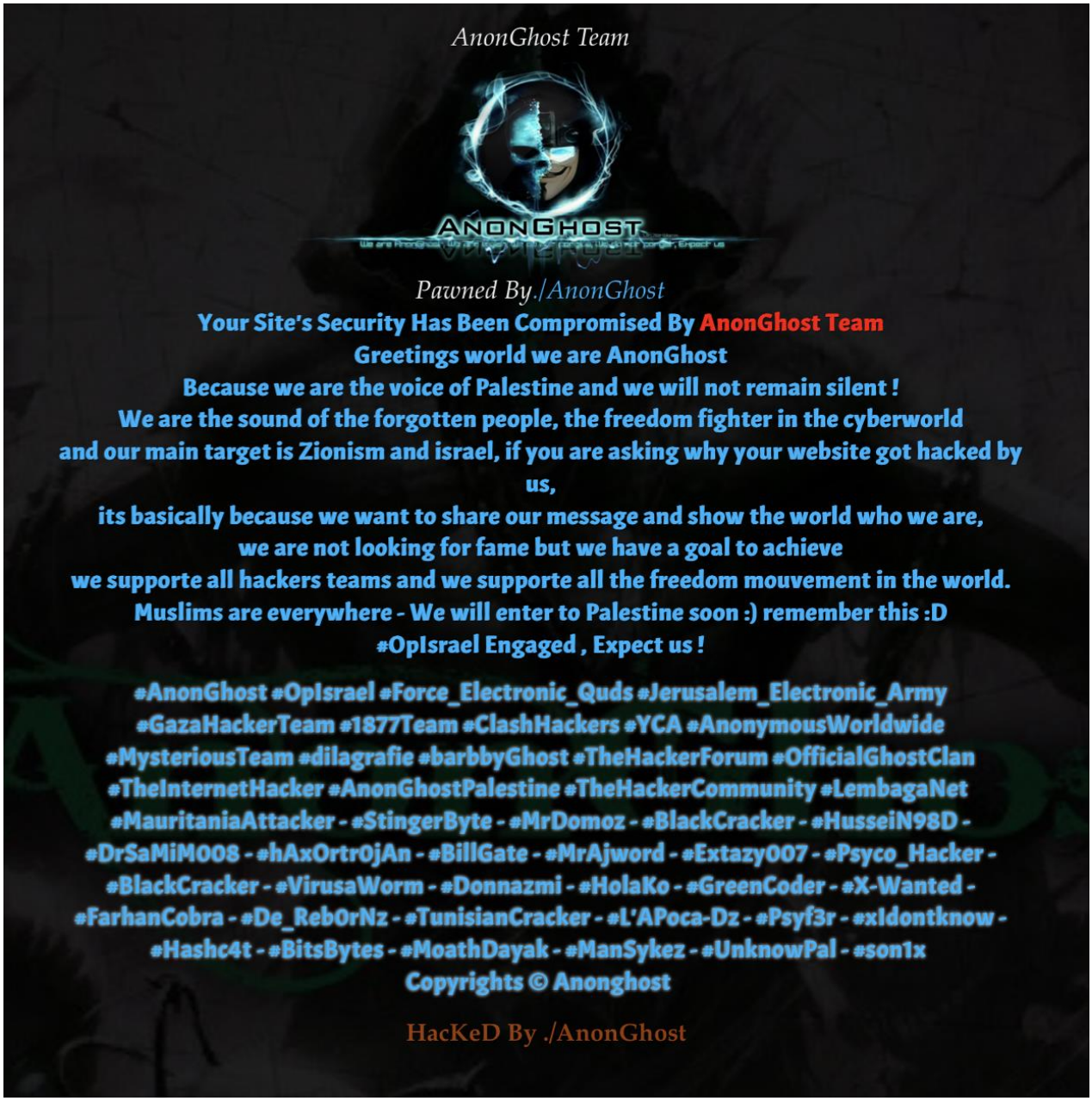

Figure 4: Source AnonGhost Team

Figure 5: Source alconanonymous

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation - Promptly protect against unknown threats and zero-day attacks

A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.