Radware Cybersecurity Alert

Cyber Aggression Rises Following the October 2023 Israel-Hamas Conflict

October 11, 2023

Background: 2023 Israel-Hamas War

The 2023 Israel-Hamas war is an ongoing conflict between Israel and Palestinian militant groups led by Hamas. Part of the broader Gaza-Israel conflict, the war began on October 7 with a militant Hamas invasion into Israel from the Gaza Strip. Israel Defense Forces (IDF) responded with a counteroffensive named Operation Iron Swords.

In parallel to the Hamas invasion of Israel, we have observed a significant increase in cyber aggression against Israeli targets. This advisory covers the activity and provides insights into the first few days of the conflict.

DDoS Attacks on Israeli Websites Reach New Heights

Looking at a snapshot of claimed attacks on Telegram between Monday, October 2, and Tuesday, October 10, Israel, by far, is the top attacked state. Israeli websites were targeted 143 times, mostly by pro-Palestinian hacktivists and in a few cases by pro-Russian hacktivists.

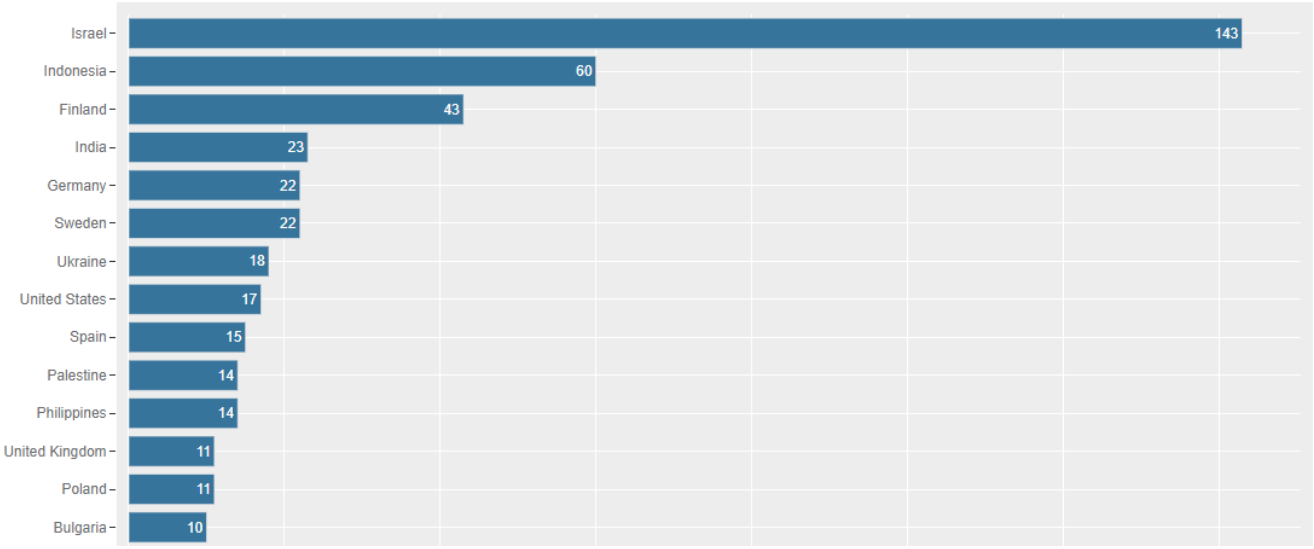

Figure 1: Number of DDoS attacks claimed on Telegram per country

Looking at the attack chronology over the past seven days, the activity started on Saturday, October 7, with almost 30 attacks claimed. Monday and Tuesday, October 9 and 10, were the most active days with over 40 claimed attacks per day.

Radware Cybersecurity Alert

Cyber Aggression Rises Following the October 2023 Israel-Hamas Conflict

October 11, 2023

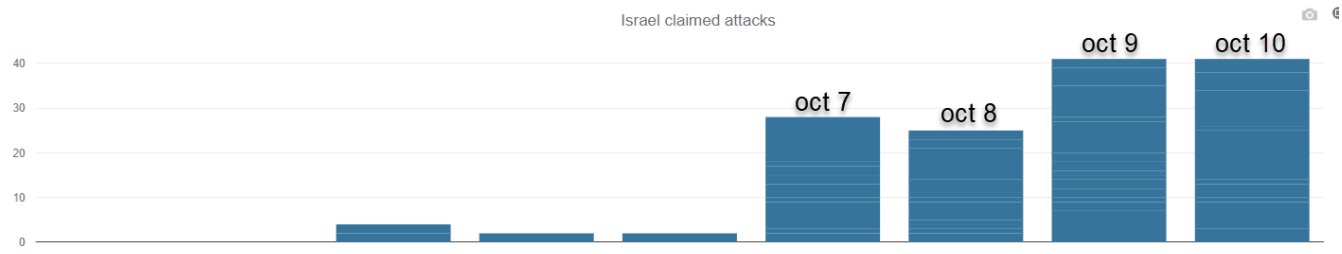

Figure 2: Number of DDoS attacks claimed on Telegram targeting Israeli websites, per day, from October 2 to October 10

Victims

Government was the most attacked website category with approximately 36% of all claimed attacks targeting Israeli websites, followed by News and Media (10%) and Travel (9%). Financial Services websites accounted for 5.6% of all claimed attacks, followed by Education (4.2%) and Healthcare (3.5%).

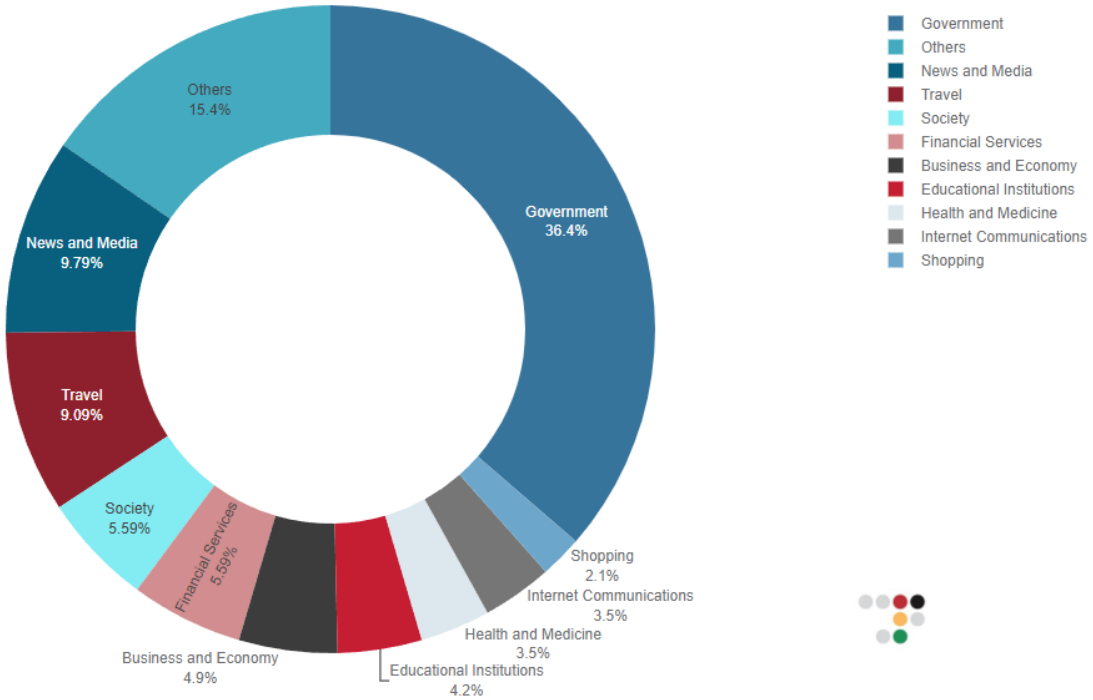

Figure 3: Top targeted website categories during attacks on Israel

Actors and Motivation

TOP CLAIMING ACTORS

The top claiming hacktivist groups that targeted Israeli websites include Indonesian threat actor Garnesia_Team, Moroccan Black Cyber Army, Indonesian threat actor Ganosec Team, Mysterious Team Bangladesh, and Indian group Team Herox. Among the threat actors we also observe Anonymous Sudan, whose attack vectors are usually very destructive.

The attacks are politically and ideologically motivated. Religious (Muslim) threat actors are conducting attacks in support of their brothers in the Gaza strip.

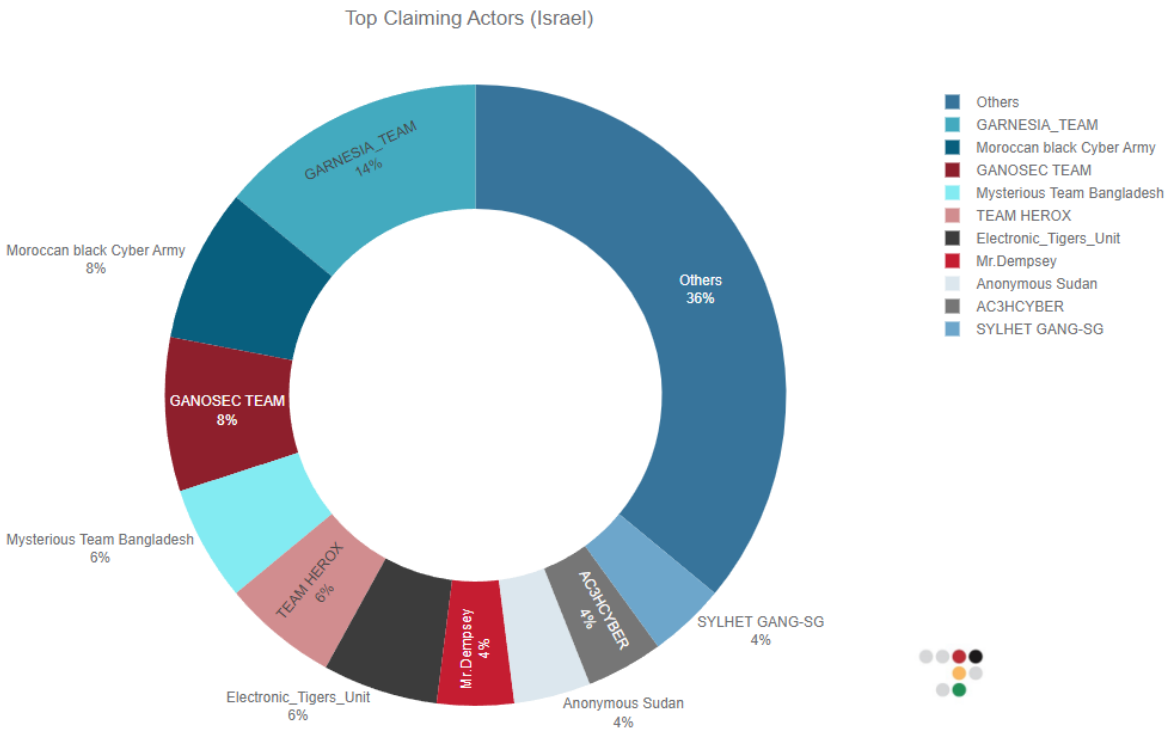

Figure 4: Top DDoS claiming actors for attacks on Israeli websites from October 7 to October 10

Some of the threat actors are coordinating their attacks on Israeli sites. In Figure 5, for example, Ganosec Team thanked Team Insane Pakistan and Mysterious Team Bangladesh for their cooperation. The Moroccan Black Cyber Army coordinated with the Indonesian actor Garnesia, while Team Herox attributed attacks in their messages to Ganosec Team and others.

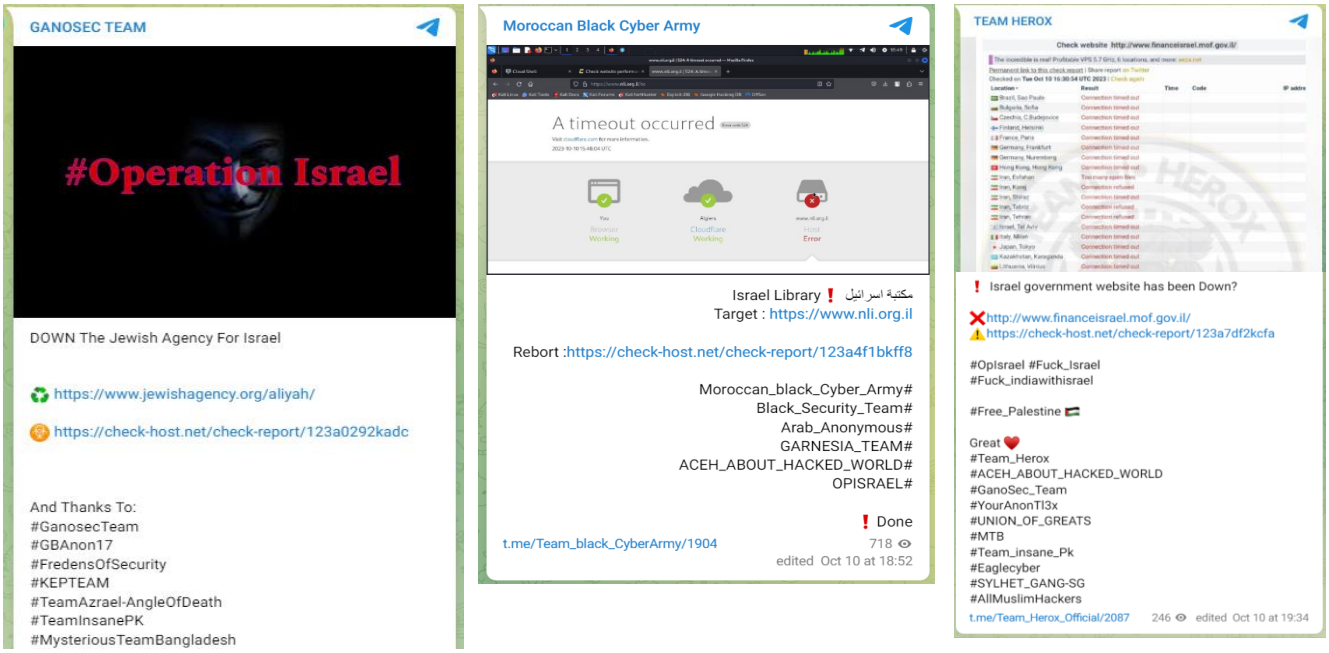

Figure 5: Telegram messages announcing attacks on Israeli sites

ANONYMOUS SUDAN

Anonymous Sudan is a group of religiously and politically motivated hacktivists from Sudan who have been conducting religiously motivated denial-of-service attacks against several Western countries since January 2023. Anonymous Sudan is one of the most active and persistent threat actors in today's cyber world. During the attacks on Israel, Anonymous Sudan was focused mostly on the Jerusalem Post newspaper and kept attacking them with DoS attacks for most of October 8-9.

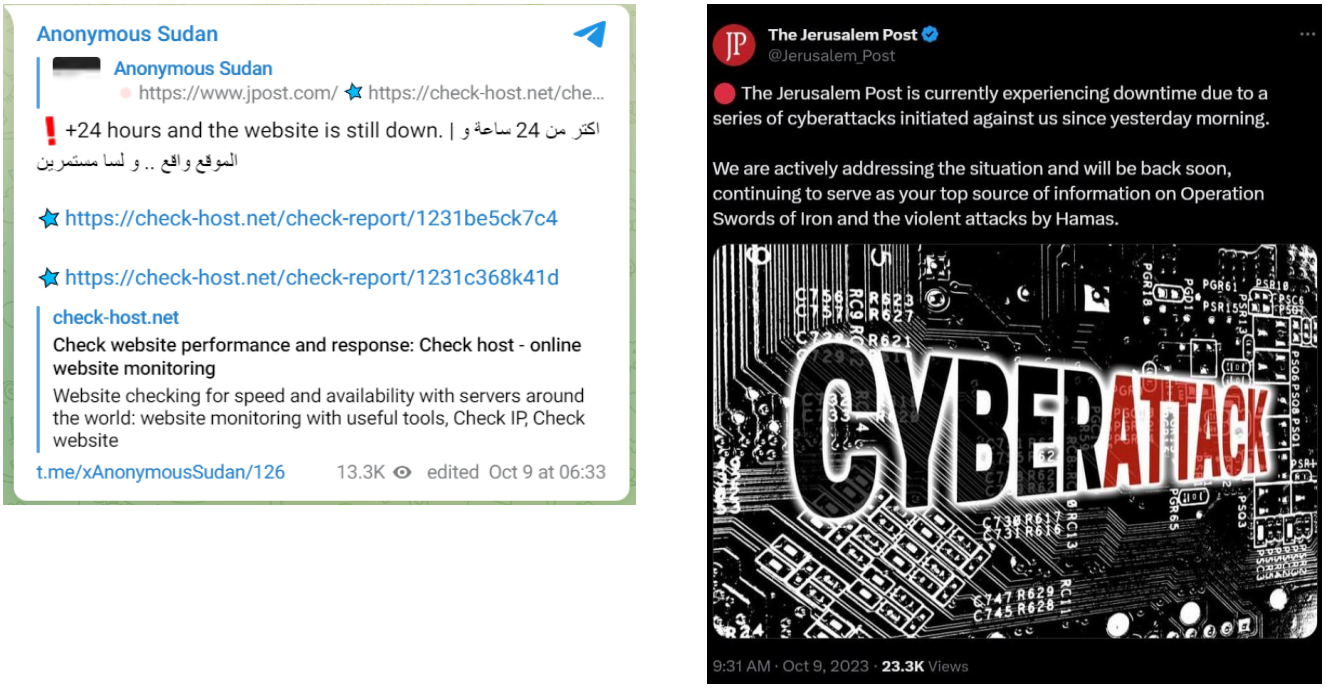

Figure 6: Anonymous Sudan continues to attack the Jerusalem Post newspaper

KILLNET GETTING INTO THE MIX

Killnet is a pro-Russia hacker group known for its denial-of-service attacks targeting government and private company websites in countries that supported Ukraine during the 2022 Russian invasion of Ukraine.

Killnet, led by Killmilk, also claimed several attacks on Israel government sites and banks including Shabak.gov.il, which they specifically mention: “Shin Bet [Shabak] belongs to the Israeli intelligence system and is engaged in counterintelligence activities and ensuring internal security. Its function is comparable to the FBI and FSB.”

Given that Killnet is the most media-savvy of all pro-Russia hacktivist groups, the decision by Killmilk to join the cyberattacks targeting Israel could be interpreted as a need for recognition in the media, regardless of the type of conflict or event.

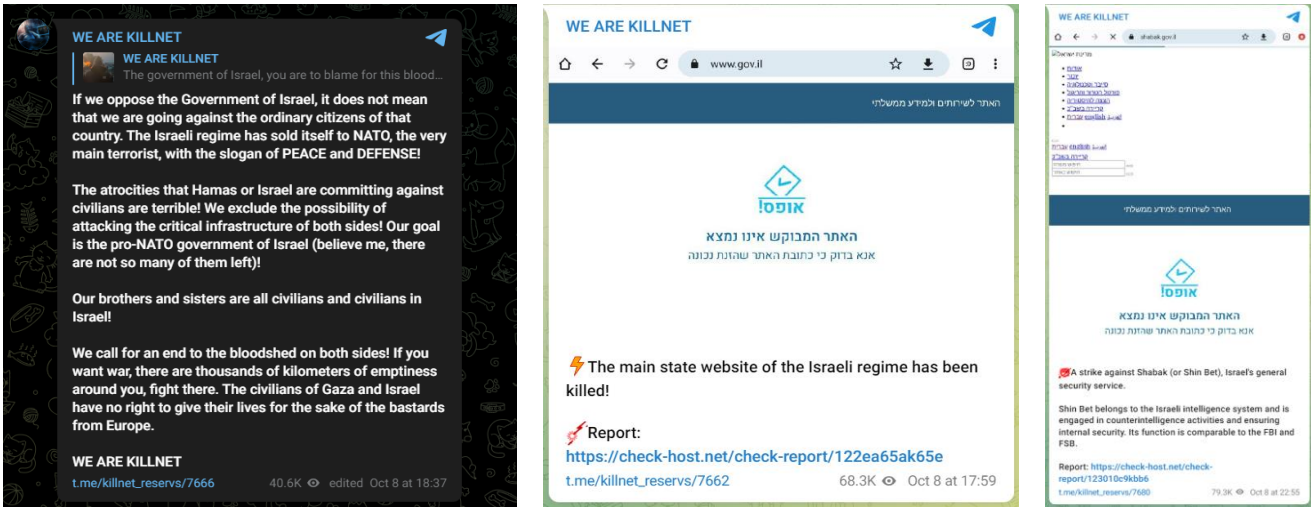

Figure 7: Killnet joins the attacks on Israel

FAKE ATTACKS AND KEEPING UP YOUR REPUTATION

The message that claimed a **DDoS** attack on the Palestine's Safa Bank was followed by an announcement by Team Insane Pakistan, published on their Telegram, calling the attackers "clowns" (see figure below). To support their claim, and probably to strengthen their reputation, they added a link to the Check Host site, demonstrating that at the time of attack Safa Bank was accessible from all over the globe.

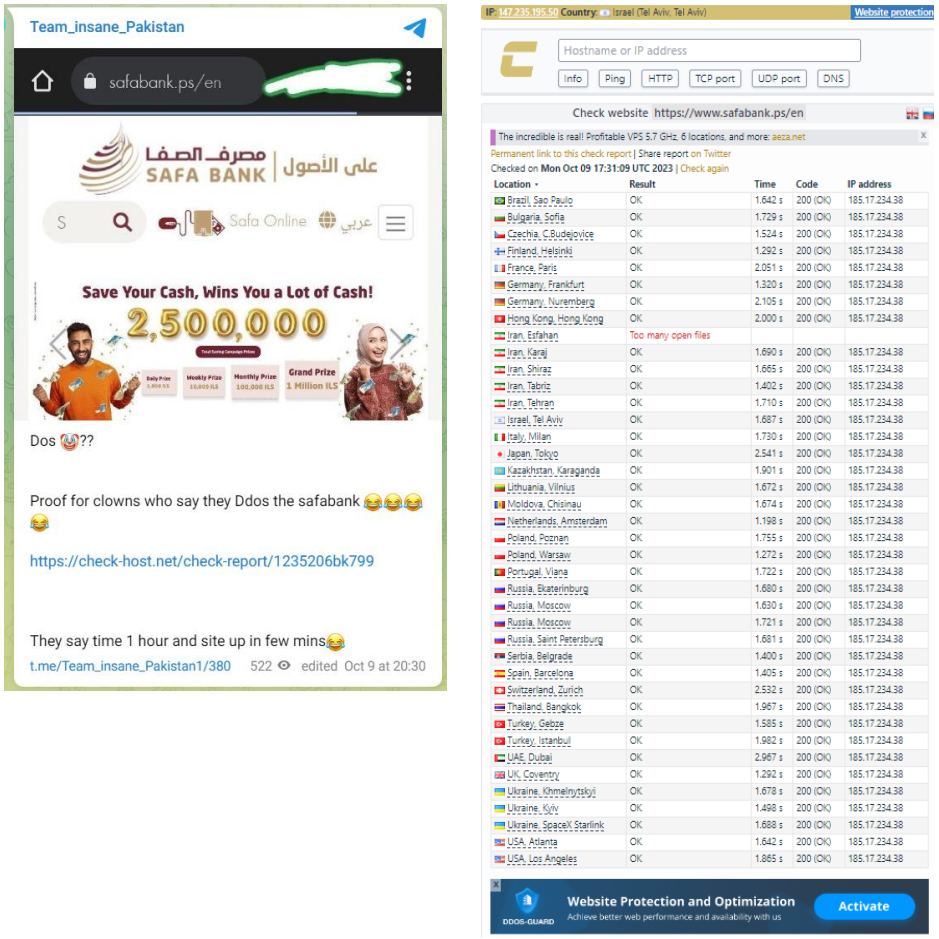

Figure 8: Team Insane Pakistan publishes proof that Safa Bank website was operational during a claimed DDoS attack by an opposing threat actor

Attack Characteristics

ATTACK VECTORS

Many of the attacks targeting Israeli web sites observed by Radware's DDoS Cloud Protection service were multi-vector attacks, consisting of application layer and network level DDoS attacks running concurrently.

The most common attack vectors observed during this campaign include:

- HTTPS Floods

- IPv4 UDP Floods
- IPv4 UDP-FRAG Floods
- IPv4 ICMP Floods
- HTTP SYN Floods
- ARMS floods
- Chargen Floods
- UDP Flood Port 80
- TCP FIN-ACK Flood
- DNS Amplification flood

ATTACK SIZE

Attack sizes of the observed volumetric, network level, DDoS attacks were in the range of 1.2Gbps up to 135Gbps. Application Web DDoS attacks ranged between 9K HTTPS Requests per Second (RPS) and up to 2M RPS.

DURATION OF DDOS ATTACKS

Although some of the DDoS attacks lasted only a few minutes, most of the observed attacks lasted several hours, with some cases up to 24 hours. During the longer assaults, the attackers morphed their attacks by regularly switching between different attack vectors because their targets are able to catch up and mitigate their vectors.

Staying Protected

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

Cybersecurity 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.