Radware Cybersecurity Advisory

Unraveling Russian Multi-Sector DDoS Attacks Across Spain

August 2, 2023

After weeklong campaigns targeting websites in Ukraine, Poland and Lithuania, the pro-Russia patriotic hacktivist group NoName057(16) has put Spain in its crosshairs. The attacks started on July 19—just four days before the Spanish general election—and lasted until July 30. In almost two weeks, NoName057(16) claimed a total of 85 DDoS attacks targeting over 50 different government, finance, telecom, travel, public transport and news organizations across Spain.

On July 23, the Sunday of the elections, the group tried to disrupt the website of the Junta Electoral Central, the commission for elections in Spain responsible for monitoring and registering general elections and supervising the vote at polling stations. Also, the Instituto Nacional de Estadística (INE) official website, which collects and publishes statistics about demography, economy and Spanish society, appeared on the list of targets. That Sunday counted the most **distributed denial-of-service (DDoS)** attacks targeting multiple government websites and websites offering ticketing services for public transportation in different parts of the country.

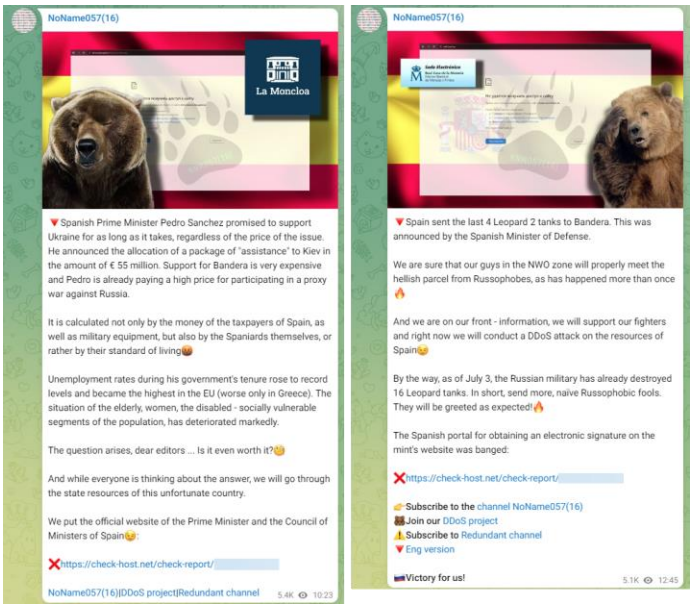

Figure 1: NoName057(16) claiming attacks against Spanish websites on Telegram (July 19, start of the campaign)

NoName057(16) was the only pro-Russia actor to target Spain during that period. The group is known to act independently and has stated in the past it does not want to be associated with **Killnet** or any of the Killnet cluster members. Operating as a lone bear, the group runs a crowd-sourced DDoS **botnet** named "**DDoSia**." Leveraging a community of over 10,000 members, it is the most active pro-Russian DDoS threat group, known to attack organizations in Western countries whose governments publicly support Ukraine in its war with Russia.

Attacked Websites

Travel websites were the most attacked category in this campaign against Spain. The key targets in this category encompassed platforms offering ticketing services for public transportation, the official web portals of hospitality establishments such as hotels and eateries, and various online ticket and reservation consolidators. Sites that offer public tourist information were not exempt from these attacks.

Beyond the travel industry, the online banking portals of numerous financial entities also fell victim to these cyber offensives. A variety of judicial and governmental platforms were similarly affected. The nation's primary internet and mobile service providers were not immune, as their digital touchpoints became targets. And cyberattacks also extended to media, targeting the web platforms of renowned newspapers such as Expansión and El Mundo.

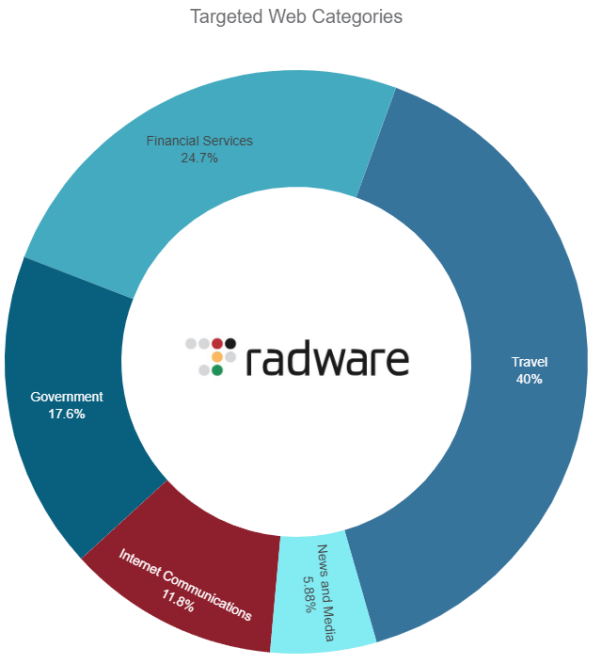

Figure 2: Claimed attacks by website category

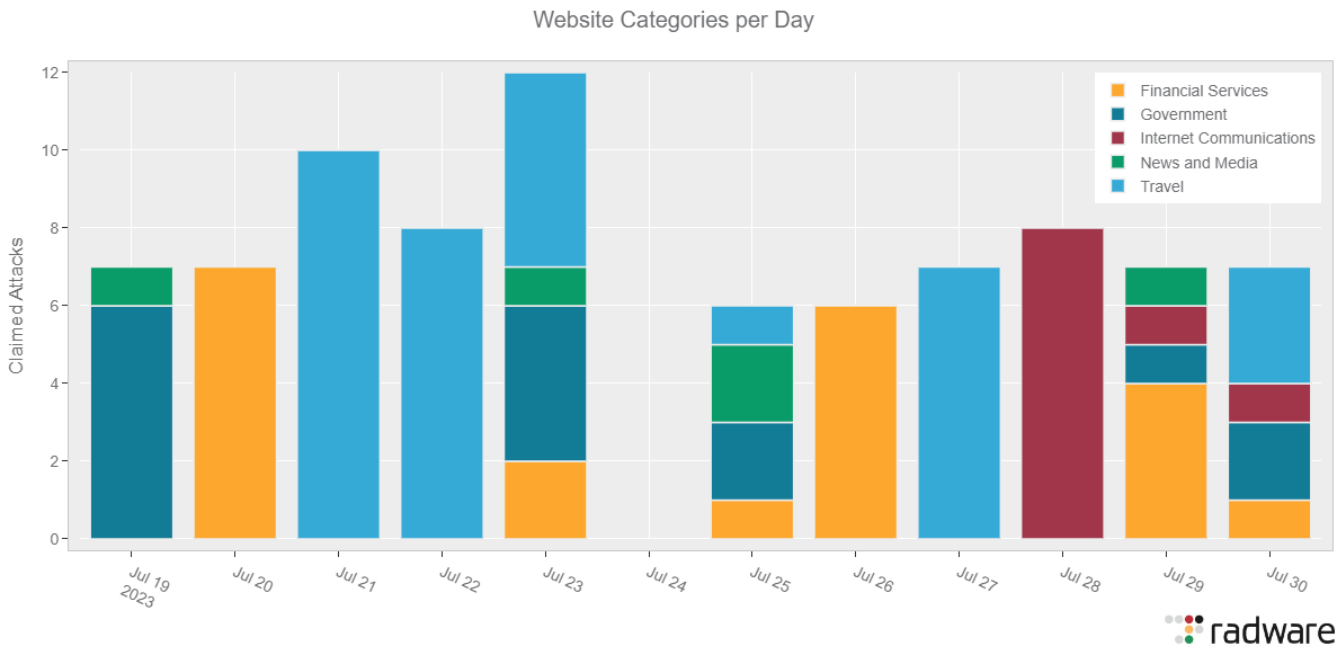

Figure 3: Attacks claimed per day

Who is NoName057(16)

NoName057(16) is a pro-Russian threat group known for launching DDoS attacks against Ukraine and those that directly or indirectly support Ukraine. The hacktivist group formed in March of 2022 on Telegram and became a notable threat group. While less media savvy than Killnet, it is considered one of the most active groups and the most prominent threat to Western organizations. The group operates solitarily and explicitly noted that they don't want to be associated with their fellow pro-Russian hacktivist group Killnet or its affiliates. After an article published on Hacker.ru by Maria Nefyodova, a respected Russian journalist, NoName057(16) reacted in a Telegram message, noting, "[We] operate independently and have nothing to do with the KillNet hack group. We choose our own targets for DDOS attacks," demanding to edit the publication or it might turn ugly.

In July 2022, the group quietly launched DDoSia, a crowdsourced botnet project. Similar to the pro-Ukrainian Liberator by disBalancer and the fully automated DDoS bot project by the IT ARMY of Ukraine, this project leverages politically-driven hacktivists willing to download and install a bot on their computers to launch denial-of-service attacks. Project DDoSia, however, raises the stakes by providing financial incentives for the top contributors to successful denial-of-service (DoS) attacks. By July 2023, the member count of the DDoSia Project Telegram group was over 11,300.

The DDoSia project allows the group to continuously attack government and private organization websites, mainly targeting Western nations that support Ukraine during the ongoing invasion of Russia. NoName057(16) claims the most DDoS attacks on Telegram by far, and Poland is the most targeted of Western countries with over 200 attacks. Lithuania, Czechia, Ukraine and Italy were also countries heavily targeted by NoName057(16) during the first half of 2023. After the recent attack campaign, Spain ranks sixth on the list of most attacked countries by NoName057(16).

NoName057(16) is the only actor that has claimed at least one attack per day since they started their DDoSia Project, which has included up to 15 DDoS attacks on some days. This feat was only possible by leveraging automation, in this case using a volunteer-based, crowdsourced DDoS botnet that performs Web DDoS attacks around the clock on a curated list of websites updated daily by the NoName057(16) leadership team.

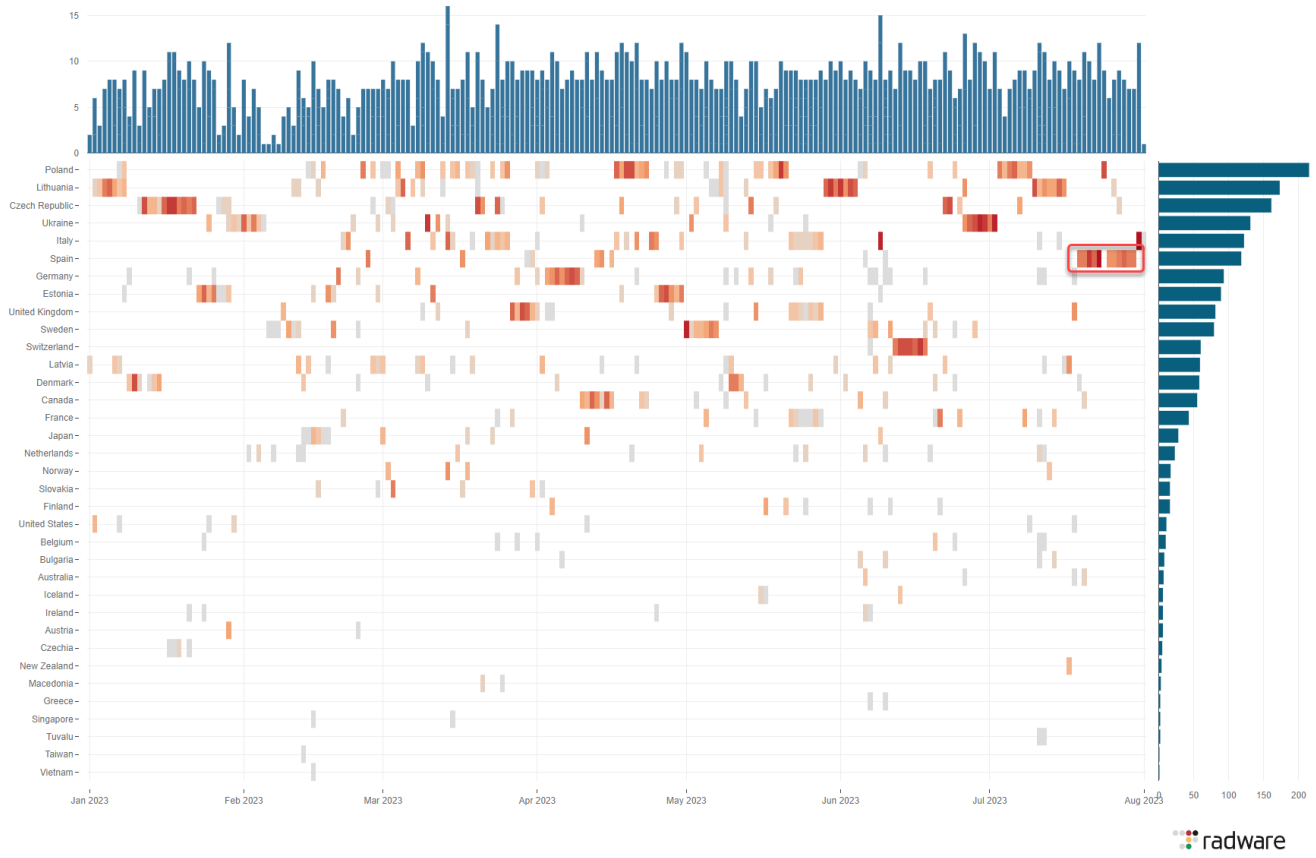

Figure 4: DDoS attacks claimed by NoName057(16) per country over time

NoName057(16) Tactics and Techniques

NoName057(16) operates a crowd-sourced botnet called Project DDoSia. The group provides client software (a bot) to volunteers who download and run the software on their PC or cloud-rented hosts. The client software communicates with a command and control (C2) server. This is very aligned with IoT DDoS botnets. The difference? Instead of being installed on compromised IoT devices, it is installed on home PCs, mobile phones and cloud servers by volunteers. To make it more interesting, NoName057(16) provides financial incentives for those performing the most attacks.

The group's admins update the list of targets daily and distribute them through a C2 server. The bots download the list of new targets and start executing attacks until the bot is stopped or a new list of targets is provided. So far, this suggests nothing unusual about the attack technique.

However, what is new about NoName057(16)'s DDoSia attacks is that the group admins perform reconnaissance before staging their attack vectors. They investigate the target website and identify the most resource-intensive parts of the site. Pages with a search function or a form to fill in are typical candidates. NoName057(16) records all the variables used by GET and POST requests for those pages, including any cookies and potential captcha keys, and then crafts specific web requests with placeholders for random data to be leveraged as attack vectors.

http-GET	port:443	ssl:True	ratio:1	path: /sok?q=$_1
http-GET	port:443	ssl:True	ratio:1	path: ?search_api_fulltext=$_1
http-POST	port:443	ssl:True	ratio:1	path: / /
	[str] intressen%5B215%5D=215&fornamn=$_1&efternamn=$_1&foretag=$_1&e_post=$_1%40gmail.com&jag_godkanner=1&captcha_sid=11367359&captcha_token=4rAH0 ys&captcha_response=Google+no+captcha&g-recaptcha-response=03AFY zlPo2x0YY_UEel QxRlM9doaBZ3n nRLN_obmefrcC q32JZfQ&captcha_cacheable=1&utm_source=&utm_medium=&utm_campaign=&utm_term=&utm_content=&op=%D0%9E%I 82%D1%8C&form_build_id=form-lo &form_id=webform_ _add_form			
http-GET	port:443	ssl:True	ratio:1	path:/full-search?q=$_1
http-POST	port:443	ssl:True	ratio:1	path: /views/ajax?_wrapper_format=drupal_ajax
	[str] view_name=press_releases&view_display_id=block_1&view_args=&view_path=%2Fnode%2F3346&view_base_path=&view_dom_id=137 43d9&pager_element=0&page=$_2&_drupal_ajax=1&ajax_page_state%5Btheme%5D=rise&ajax_page_state%5Btheme_token%5D=&ajax_page_state%5Blibraries%5D=better_exposed_filters%2Fgeneral%2Cdatalayer%2Fbehaviors%2Feu_cookie_compliance%2Feu_cookie_compliance_bare%2Crise%2Fglobal%2Crise%2Fmmenu%2Crise%2Fsanitize%2Crise_core%2Fsearch%2Crise_core%2Fvisitor-ip%2Cshare_everywhere%2Fshare_everywhere.css%2Csystem%2Fbase%2Cviews%2Fviews.module%2Cviews_infinite_scroll%2Fviews-infinite-scroll			
http-POST	port:443	ssl:True	ratio:1	path: /views/ajax?_wrapper_format=drupal_ajax

Figure 5: Example of attack vectors targeting a single website captured from DDoSia C2 servers

When a bot receives the attack vectors, it will craft the GET or POST requests containing legitimate parameters, arguments and cookies, and randomize the data passed through the arguments for each request. The randomization of the data takes into account the type of data the application expects. For example, for a phone number field the bot will generate a 7- to 12-digit random number. For email fields the bot will generate a random 10-15 alphanumeric sequence and append "@gmail.com" to it. The resulting request from the bot will look like a legitimate web page request or form post. Neither a **web application firewall (WAF)** nor the application itself will be able to detect any anomalies because the variable names will correspond to the names used by the web application and the contents of the variable will be within the bounds set by the application.

The only difference between this and real requests is that the data will be completely random and would be recognized by a human operator as garbage.

All the volunteers that run a bot submit these legitimate looking requests as fast as their resources allow. This creates a lot of stress on the back end of the application, such as the database used for search queries and for storing the data of form posts. Also, after the attack, the person processing posted forms will have a nice surprise consisting of millions of new information requests of which only a small fraction will be legitimate requests. NoName057(16) is growing its following, and as of today their active volunteers is estimated in the range of several thousands. The botnet does not generate millions of RPS, but because of the reconnaissance step, the attacks can still target the most critical parts of a web application or API. In many cases, mere hundreds of requests per second (RPS) are enough to create issues in the back-end infrastructure of the application.

The botnet could be better. Instead of using anonymizing proxies, it relies on the volunteers to create a VPN tunnel to conceal their origins. This means that most requests from a single bot will originate from the same source IP and isolating the IP addresses performing several hundreds of requests per second will, in most cases, mitigate at least part of the attack. If the bot had leveraged per-request anonymous HTTPS proxies, the requests would originate from multiple tens of thousands of IPs, and it would become much harder to correlate the hundreds of requests per second to a single source IP. Also, the bot is written in Go and leverages the net/http Go package, which is directly reflected in the user-agent header of the requests.

Disruptive Web DDoS Attacks

As Radware has observed in recent attack campaigns, attackers leverage multiple types and vectors as part of a single attack campaign. They combine both network- and application-layer attack vectors by leveraging improved and new publicly available tools. They create sophisticated attacks that hit harder and sometimes are impossible to detect and mitigate with traditional methods.

Attackers generate new types of HTTPS Flood attacks—also called Web DDoS attacks—that are more sophisticated and aggressive. They bypass traditional application protections using sophisticated methodologies, such as randomizing HTTP methods, headers and cookies, impersonating popular embedded third-party services, proxying IPs, HTTP pipelining and more. Among the application-level attack methods seen in these recent campaigns were HTTPS GET, PUSH and POST request attacks with changing parameters and arguments. These were orchestrated from cloud-hosted virtual private servers and hidden behind several thousands of daily rotating proxies.

The move towards encrypted attacks and the increase in the scale and sophistication of these attacks raises the bar needed for detection. It renders network-based DDoS mitigation tools and traditional on-prem and cloud-based WAF solutions ineffective against these attacks.

NEW ADVANCED PROTECTION FOR WEB DDOS ATTACKS

As part of its Cloud Application Protection Service, Radware's new Cloud Web DDoS Protection solution is uniquely designed to protect against high-scale, newly emerging Web DDoS Tsunami attacks. It provides customers with advanced protection at the scale needed to combat these threats.

Radware Cybersecurity Advisory

Unraveling Russian Multi-Sector DDoS Attacks Across Spain

August 2, 2023