TARX

NONAME057

Threat Actor Report

AUG 2024

XG3 UNIT

xMDR powered by Cipher

Noname: Detentions in Spain

In July, three Spanish pro-Russian cybercriminals operating from Huelva, Seville and Manacor (Balearic Islands) for their alleged involvement in denial-of-service cyber-attacks against public institutions and strategic sectors in Spain and other NATO countries.

The computer resources that the individuals had allegedly used to carry out the attacks were seized. These attacks had been organised by the hacktivist group NONAME057, one of the most active groups targeting Spain, among other European countries, as it is pro-Russian.

This group has dedicated itself to carrying out Distributed Denial of Service (DDoS) attacks against websites of public and private organisations in the governmental sectors, critical infrastructures and essential services in those countries that have positioned themselves in favour of Ukraine in the context of the war.

Subsequently, following the Guardia Civil's operation, the so-called Operation Grizzlie, in which three of its members have been arrested, they have retaliated. In a later message, they also appeal to other collaborators to help them in the operation: "*We declare revenge against the Spanish authorities, who arbitrarily detained our comrades. We call on all pro-Russian hacker groups to join us in unleashing all their power against Spain in support of the arrested*".

The Group

NoName057 is a pro-Russian hacktivist group that has been active since March 2022, in response to the tensions arising from Russia's invasion of Ukraine.

During 2022, new communication channels emerged for pro-Russian hacktivist groups such as **KillNet, NoName057, and Anonymous Sudan**. These groups use these platforms to coordinate their operations, disseminate comunications, and identify potential targets for their attacks. NoName057 actively uses **Telegram** channels to interact with its followers, set attack targets, distribute attack tools, and showcase evidence of their successes.

The use of publicly accessible communication platforms to broadcast their achievements and garner significant media attention, aiming to influence political and social opinion in the targeted countries, can be seen as a form of information campaign supporting the **pro-Russian cause**.

By 2024, both the **DDoSia Project** and the NoName057 group have become widely recognized. On November 11, 2023, the administrators of the DDoSia Project's Telegram channel shared a new version of their software. This update, released without prior announcement, includes support for more processor architectures, adding compatibility for 32-bit systems and FreeBSD, alongside the previously supported AMD64, ARM, and ARM64.

Throughout 2024, the Command and Control (C2) servers have been changed dozens of times, often several times a day. This high frequency of changes indicates significant organizational efforts to counter this threat.

Additionally, when an attack successfully targets a specified objective, NoName057 posts a screenshot on Telegram showing the target was unavailable at a given time as proof of success, along with a link to a report from the **Check-Host.net website**.

Moreover, the group has become **more aggressive and vengeful,** responding swiftly to any operations that might be conducted against them. This escalation in their tactics and behavior indicates an increased willingness to retaliate against perceived threats, thereby posing a greater challenge to those working to defend against their cyberattacks. This heightened aggressiveness underscores the need for vigilant monitoring and robust countermeasures to effectively combat their activities.

Hacktivism & Revenge

A distinctive feature of some hacktivist groups, such as NoName057(16), is their tendency to respond aggressively to any attempt to stop their activities. When the authorities succeed in identifying and dismantling part of their operations, these groups often escalate their attacks in retaliation. This escalation can take the form of more frequent, better coordinated and targeted attacks on more critical targets. The intention is clear: to demonstrate that they will not be easily silenced and that any attempt at repression will only strengthen their resolve and ability to cause damage.

This cycle of attack and retaliation creates a significant challenge for authorities and affected companies, who must be prepared for an immediate and escalating response from hacktivists. Revenge in hacktivism not only seeks to restore "balance" after a strike, but also serves as a warning to future attempts at intervention. By demonstrating their ability to strike back with greater force, hacktivist groups send an intimidating message to both their enemies and potential allies, consolidating their position in cyberspace as formidable and resilient actors.

Modus Operandi

Large-scale DDoS attacks: NoName057(16) is known for conducting distributed denial-of-service (DDoS) attacks through its DDoSia project. These attacks target entities in countries that support Ukraine, especially NATO members, including private companies, ministries and public institutions.

Use of Public Communication Channels: The group uses publicly accessible communication platforms, such as Telegram, to coordinate its operations. Through these channels, they interact with their followers, establish attack targets, distribute tools to carry out attacks, and show evidence of their successes, such as screenshots of inaccessible targets.

Frequent C2 Infrastructure Change: To evade detection and countermeasures, NoName057(16) frequently changes its Command and Control (C2) servers, sometimes several times a day. This strategy allows them to remain operational and respond quickly to attempts to dismantle their infrastructure.

Revenge and Escalation: In response to any operation against them, NoName057(16) tends to escalate its attacks. This retaliatory behaviour not only seeks to restore their operational capacity, but also to send a deterrent message to their adversaries and reinforce their aggressive posture.

Actions to be taken

- **Web Application Firewall (WAF)**: Implement a WAF to filter and monitor HTTP traffic between a web application and the Internet. A WAF can protect against common attacks, such as SQL injections and cross-site scripting (XSS). Configure custom rules in the WAF to identify and block specific attack patterns.

- **DDoS Protection Services**: Use services such as Cloudflare, Akamai Kona Site Defender or AWS Shield Advanced to protect against DDoS attacks. These services offer mitigation capabilities at the network and application level, absorbing and diverting malicious traffic.

- **Network segmentation**: Apply micro-segmentation using tools such as VMware NSX or Cisco ACI to create security zones within the network and limit lateral movement of attackers.

- **Threat Intelligence Sharing**: Integrate threat intelligence sharing platforms such as ThreatConnect, MISP (Malware Information Sharing Platform) or Anomali to receive and share information on attacker tactics, techniques and procedures (TTPs).

- **Continuous Monitoring**: Use continuous monitoring solutions such as ELK Stack (Elasticsearch, Logstash, Kibana), Prometheus and Grafana to gain real-time visibility into network traffic and application behaviour.

- **Endpoint Detection and Response (EDR)**: Implement EDR solutions such as CrowdStrike Falcon, Carbon Black or SentinelOne to proactively detect and respond to endpoint threats.

Conclusion

Key Points:

- **Hacktivism beyond?** At the moment it does not appear that the group intends to carry out attacks beyond those related to denial of service, but in the past they have carried out attacks involving the exfiltration of information.

- **Revenge:** This is a group that is characterised by taking actions based on political decisions made by other countries and sectors, so this could be a factor that makes attacks predictable.

Upcoming:

- With simple mechanisms, denial of service attacks can be easily stopped, so it will be necessary if you can be a target to put up these defences.
- With the use of cyber intelligence, these attacks could be prevented, therefore it is recommended to study the company's position.

Overall:

We expect Noname057 to continue attacking targets that are contrary to its political motivations, but it should also be noted that such hacktivist attacks can be easily contained. By studying their modus operandi and analysing their patterns of behaviour, we can take simple steps to help counter these actions.

Threat actor data available in xMDR Platform

TTP'S **13**

Top 3 Most Relevant

- Network Denial of Service
- System Network Configuration Discovery
- Develope Capabilities

3 **Tools Used**

Top 3 Most Used By Actor

- DDosia
- RedLine Stealer
- Bobik

xMDR

ADVERSARIALLY

Threat Actor Report

AUG 2024

cipher

a Prosegur company

LEGAL NOTICE: PROHIBITION OF DISTRIBUTION, USE OR SHARING WITHOUT AUTHORIZATION This document (hereinafter, “the Document”) is the exclusive property of Prosegur Ciberseguridad S.L. (hereinafter, “the Owner”). The Owner possesses all intellectual property rights associated with the Document, including, among others, copyright and property rights. Access to this Document is granted only to parties authorized by the Owner for the specific purpose of confidential evaluation.

Any distribution, reproduction, unauthorized use, disclosure or sharing of the Document, in whole or in part, with third parties without the prior and express written authorization of the Owner is strictly prohibited. Any unauthorized use of the Document will constitute a violation of the Owner’s intellectual property rights and may result in legal action. Access and use of this Document are subject to the terms and conditions established by the Owner. Any authorized party that receives the Document must comply with the restrictions and obligations established by the Owner.
Any questions or requests for authorization for distribution, reproduction or use of the Document should be directed to the Owner.

Failure to comply with these restrictions may have legal consequences. By accessing or using the Document, you accept and acknowledge the terms of this legal notice.