Radware Cybersecurity Alert

Project DDOSIA
Russia's answer to disBalancer

October 12, 2022

In July, threat group NoName057(16) quietly launched a crowdsourced botnet project named 'DDOSIA.' The project, similar to the pro-Ukrainian **Liberator** by **disBalancer** and the fully automated **DDoS bot project** by the **IT ARMY** of Ukraine, 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 attacks.

Background

NoName057(16) is a pro-Russian threat group known for launching defacement and DDoS attacks against Ukraine and those that directly or indirectly support Ukraine. The group formed in March of 2022 on Telegram and became a notable threat group by June. Since then, the group has gathered a following of nearly 13,000 subscribers.

Over the last few months, Noname057(16) has been operating in support of Killnet operations. Most recently, the group worked in parallel with Killnet during their campaign against civilian network infrastructure in the United States. During the operation, threat group NoName057(16) posted an invite link to a Telegram channel named **'DDOSIA Project**' and also reposted the Killnet target list for U.S. airports in the same channel.

Figure 1: NoName057(16) Manifesto Image

NONAME057(16) MANIFESTO

Inspired by Newton's third law of physics, NoName057(16) published a **Manifesto** in July denouncing the West for waging an open information war against Russia. They consider their cyberattacks to be the reaction to western "Russophobia" and western actions against Russia.

PROJECT BOBIK

On September 6, Avast published a **report** linking Bobik, a Remote Access Trojan (RAT) first discovered in 2020, infections to the threat group NoName057(16). Bobik, often dropped via information stealers such as RedLine Stealer, downloads a second-stage DDoS module that the threat group leveraged in DDoS attacks.

Avast was able to correlate the attacks performed by the newly discovered Bobik campaign to attacks claimed by NoName057(16). After monitoring attack activity between June and September, Avast concluded that successful attacks claimed by NoName057(16) make up only about 40% of their attempted attacks. The success of the group's attacks seemed to depend on the quality of protection of the targeted organization. Avast's evidence suggested that well-secured networks and applications could withstand attacks from the group's Bobik-based botnet.

Project DDOSIA

Mid-August, while publishing their manifesto, NoName057(16) simultaneously **disclosed** their 'special software' that will assist them in conducting DDoS attacks. Over the following days, the group provided more information about their 'special software' named DDOSIA and instructions on using it to contribute to the fight against Western Russophobes.

Instructions, publicly available at **dddosia.github.io**, explain how potential contributors can register through Telegram to receive a ZIP archive containing a Windows bot binary named 'dosia.exe' and a unique identifier file with the name 'client_id.txt.' The unique identifier allows the contributor to create a bragging alias while registration of a cryptocurrency wallet is required to receive potential financial rewards at a later phase in the project.

After the bot agent 'dosia.exe' is executed on a contributor's Windows machine, the bot registers itself with the command-and-control (C2) infrastructure of the authors. Subsequently, the C2 servers feed the bot with a list of targets, after which the malicious software begins attacking the provided targets with TLS encrypted Layer 7 and TCP-SYN denial-of-service attacks. Users who experience issues with the bot are invited to write a message to the authors at 05716nnm@proton[.]me with 'Bot does not work' as subject.

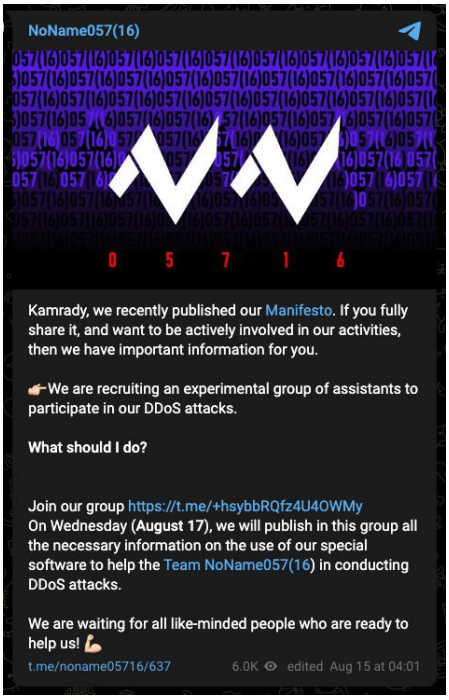

Figure 2: NoName057(16) announcing project DDOSIA

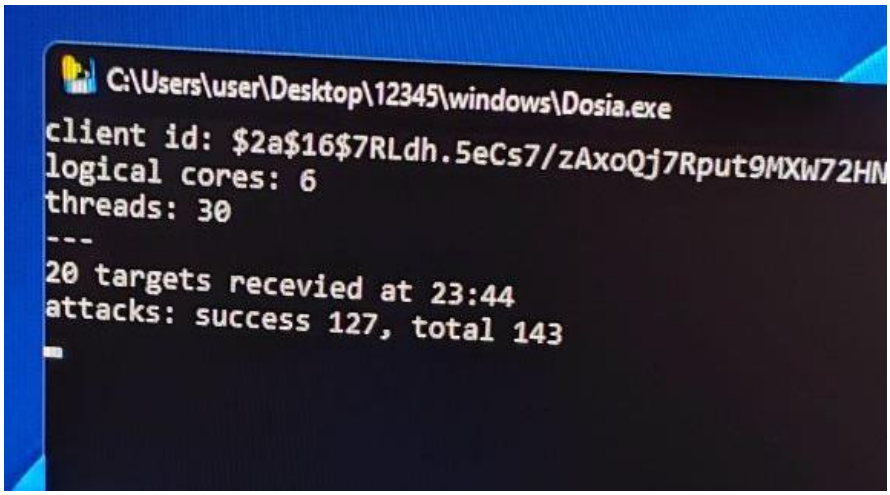

Figure 3: Ddosia agent screenshot posted by a contributor

FINANCIAL INCENTIVES

A month after the launch of the DDOSIA Project, the administrator posted an **update** on financial incentives for the top contributing attackers. It was announced that the top attacker would receive 80,000 rubles, about $1,240, in cryptocurrency equivalents, 2nd place would receive 50,000 rubles or $775, and 3rd place 20,000 rubles or $310. On top of that, a total of 50,000 rubles would be awarded to the attackers in 4th to 10th place, proportionally equal to their relative number of successful attacks. By September 8, the project would do its first incentive payout.

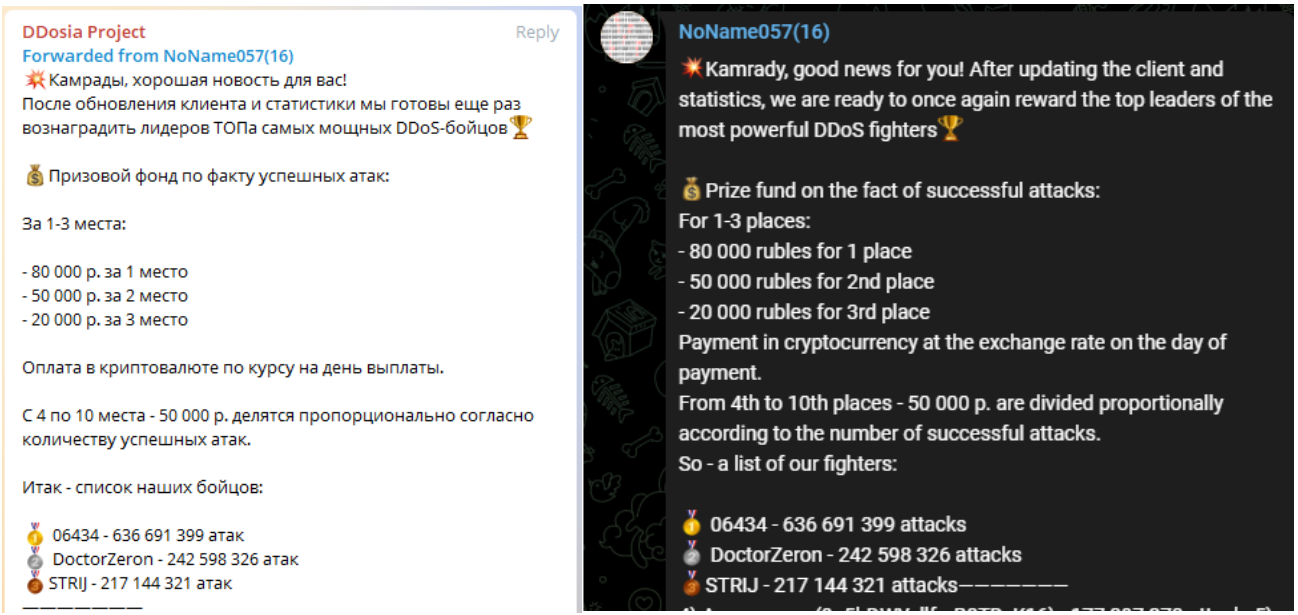

*Figure 4: Incentive payout on October 11th (**source**, **source**)*

On October 11, about 24 hours after the **DDoS attacks on US airports** ceased, the DDosia Project announced its second incentive payout for its top contributors. The message was posted in the DDosia Project Telegram channel and reshared in the NoName057(16) channel. The top ten contributors were attributed the promised incentives.

Figure 5: Measuring aggregate attack capacity by targeting a DStat service

By the end of the second month, the aggregate attack capacity of the crowdsourced botnet DDOSIA amounted to almost 2 million TLS requests per second as measured through a Layer 7 DStat service.

DDOSIA VS THE UNITED STATES

The owners of the DDOSIA Project, NoName057(16), reshared the targets listed by Killnet during the attacks on U.S. airports on October 10th. Anonymous Russia's list of origin server IP addresses and ports was also reshared on the channel while US government websites were attacked between October 5th and 6th. More information on these attacks are available in the Radware alert "**US Civilian Network Infrastructure Targeted by pro-Russian Hacktivists**."

CURRENT DDOSIA TARGETS

At the time of publication, the target list fed by the DDOSIA servers contains more than 60 targets in Ukraine, mostly military targets but also over a dozen education organizations. Attack vectors include HTTP GET and POST using SSL as well as TCP-SYN. More information about cyberattacks directed at the educational vertical is available in the Radware alert "**Education: A Rough Start to the School Yeah.**"

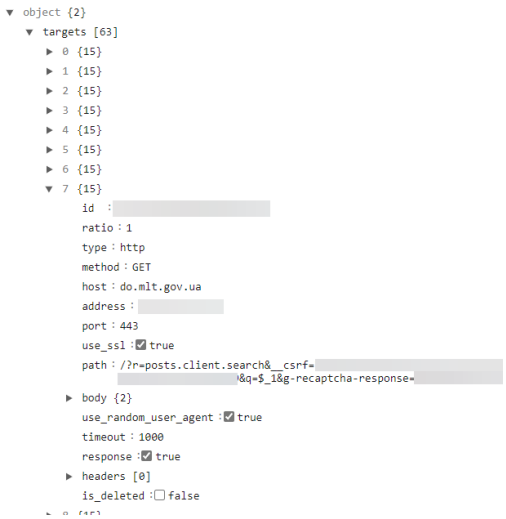

Figure 6: DDOSIA JSON formatted target feed

Reasons for concern

Currently, the DDOSIA Project is an invite-only group comprised of over 400 members. If this project gains popularity and incentives keep being paid, this crowdsourced cyberweapon might become a threat to many organizations that are either directly or indirectly involved in the Russo-Ukrainian war.

The project also shows the desire of Russian hacktivists to emulate the successes that Ukrainian hacktivists have had this year with their DDoS campaigns. While NoName057(16) lacks a mass following, the community between Killnet, Anonymous Russia, and themselves is large enough to present a moderate risk to public and private infrastructure.

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - 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 from unknown threats and zero-day attacks
- **A 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 date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order 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 achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.