Data Insights from Russian Cyber Militants: NoName057

By L M

Published: 2024-11-20 · Archived: 2026-04-10 02:47:58 UTC

8 min read

Nov 20, 2024

Press enter or click to view image in full size

Introduction

Starting from February 2022, the Ukraine-Russia conflict changed the shape of the cyber threat landscape. Many new actors emerged and the phenomenon of the Cyber Militia raised in popularity on both sides. Starting since March 2022, the NoName057(16) has been one of the most active collective targeting western companies and institutions with DDoS attacks fostered by russian supporting cyber miliants: volunteers who donate their bandwidth, or bandwidth stone from hacked third parties, to the russian cause, hitting many high level organization especially in Italy, where they repeatedly targeted major private banks, institutions, military infrastructures and public administrations. Recent threat actor activities reported by SentinelOne researchers on Jan 23, have also targeted politically sensitive objectives such as the Czech presidential election candidates (link).

Technical analysis

NoName057(16) classified as a cyber collective motivated by pro-russian hacktivism. It actually represents a sort of modern cyber militia operating to mainly support state propaganda and, potentially, even other state sponsored operations.

Also known as also known as NoName05716, Nnm05716, or 05716nnm, the threat actor high level modus operandi resemble what the Killnet group is doing since the start of the Russian special-operation: abusing computational resources to direct bot-based denial of service attack against wester representative organizations, and also communicate and spread their achievement through social media and press.

The mediatic component of this modus operandi is even more important for NoName057(16) rather than Killnet due to a significative difference in the groups methodological approaches: NoName057(16) heavily rely on volunteers' contribution to fuel and empower its offensive operations. Even Killnet relies on volunteer cyber partisans, but its structure also includes dedicated sub-groups leveraging IoT botnet infrastructures such as Mirai.

Even NoName057(16) leveraged botnets, on Sept 22 Avast linked Bobik RAT infection to the Noname collective due to the inoculation of a second stage module designed to conduct DDoS attacks (link), but the collective's operations are much more focused on volunteers and it leverages a particular Distributed Denial of service platform named DDosia.

DDosia is a complex program designed to enable volunteers to conduct DDoS attacks against the target NoName057(16) choose: it is not just a bot. Obviously, DDosia also includes a software package, in this case a Go lang based stresser compiled for multiple operating systems and multiple architectures such as Linux x64, Linux ARM, Mac x64, Mac ARM64, Windows x64, and Windows ARM64, but it actually brings more to the table: DDosia includes also support channels, community, detailed instructions, and product communication. A whole ecosystem of services to enable even the involvement even of non technical personnel.

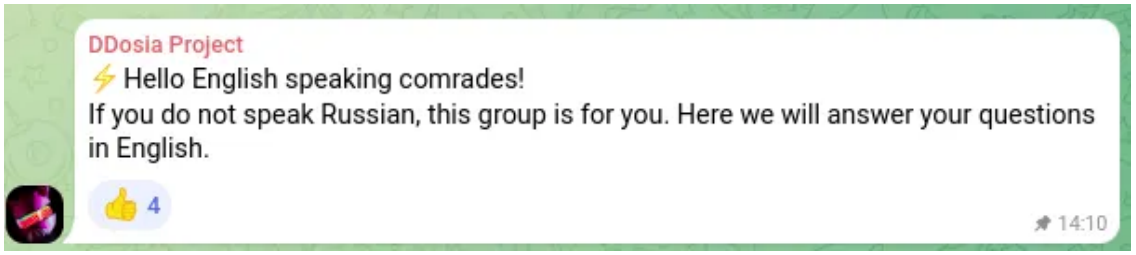


Figure. Example of support channel from DDosia community

This approach is not new at all in the revived threat landscape we are facing since the start of the Russian-Ukrainian kinetic operations. Similar approaches have been taken since day one by the Ukrainian government, which launched a state sponsored cyber militia named "The IT ARMY of Ukraine". In fact, this collective were, and still is, leveraging a similar application: the Liberator app, a fully automated DDoS bot project aimed to employ volunteers' computational resources to target Russian organizations with distributed denial of service attacks.

However, DDosia represents a step ahead in this approach due to the inclusion of payment systems to reward the cyber partisans with cryptocurrency, mixing and reinforcing the ideological motivation with the economical gain to expand their user base, and their consequent impact.

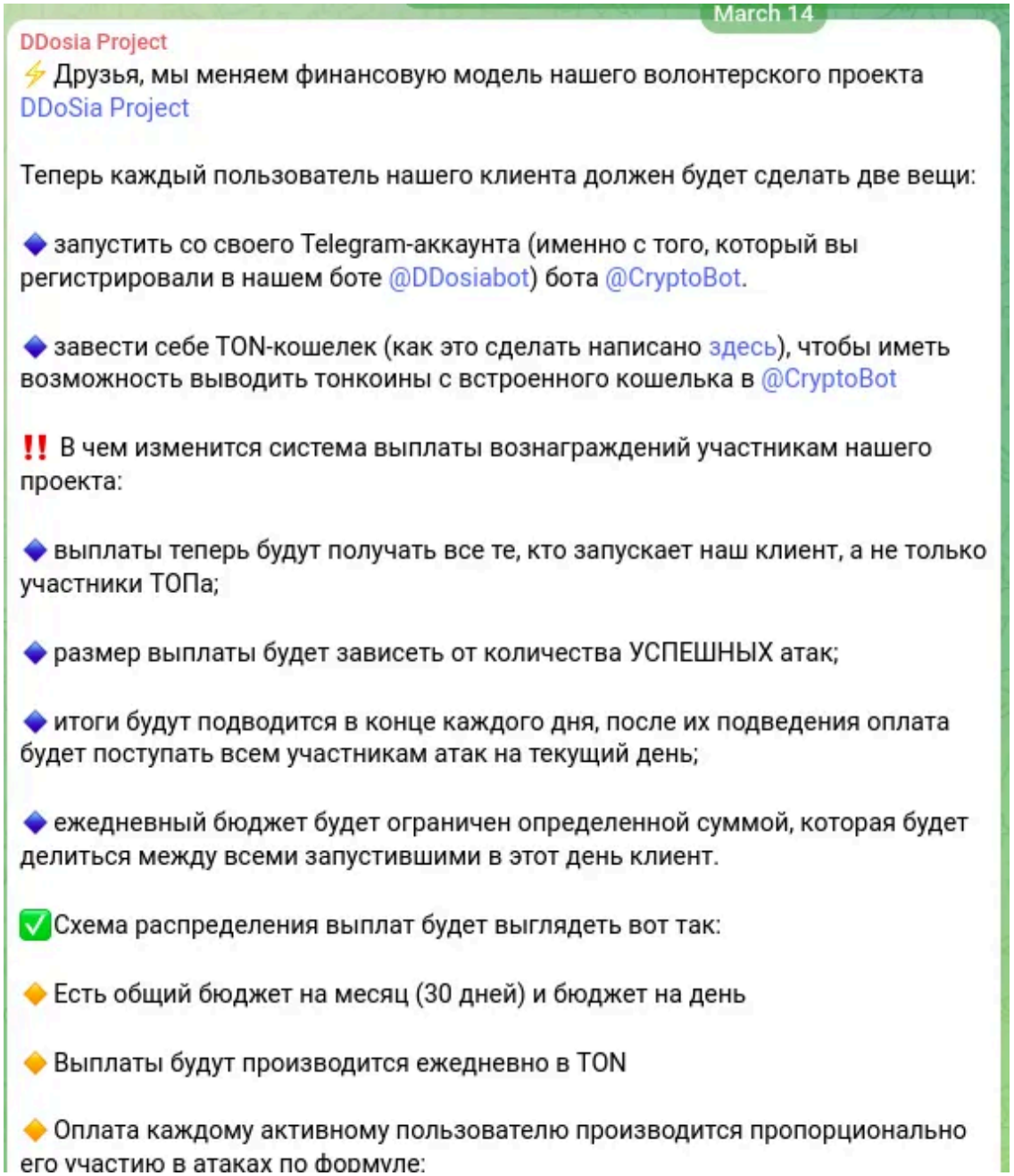


Figure. DDosia improvement in reward/payment system (March 23)

DDosia program has been well described by Radware back in October 22 (link), along with estimation of pps generated by the single bots, but here we decided to focus on peculiarities we directly noticed through the analysis of the bot and the monitoring of their operations

People Go Stresser 2.0

The current version of the DDosia bot is named “People Go Stresser 2.0” an it is compiled with Go 1.19.2 within a Windows machine using the local user “ron”. Like the previous python version, even this bot version supports both L7 and L4 attack techniques.

```
mov     rax, [rsp+70h+var_50]
movups  [rsp+70h+var_18], xmm15
call    runtime_convT64
lea     rcx, asc_6D3420 ; "\b"
mov     qword ptr [rsp+70h+var_18], rcx
mov     qword ptr [rsp+70h+var_18+8], rax
mov     rbx, cs:qword_98F328
lea     rax, off_7BB700
lea     rcx, aGoStresser ; "Go-Stresser "
mov     edi, 26h ; '&'
lea     rsi, [rsp+70h+var_18]
mov     r8d, 1
mov     r9, r8
call    fmt_Fprintf
movups  [rsp+70h+var_28], xmm15
lea     rax, unk_6D3CE0
mov     qword ptr [rsp+70h+var_28], rax
lea     rcx, off_7BA110 ; "© NoName057(16)\n"
mov     qword ptr [rsp+70h+var_28+8], rcx
mov     rbx, cs:qword_98F328
lea     rcx, [rsp+70h+var_28]
mov     edi, 1
```

Figure. DDosia bot “SayHello” snippet (Linux64)

The main modules of the bot are divided in service and management functions (e.g. “UserInfo”, “GetRealIp”, “StartJobs”), command and control functions (e.g. “Login”, “SetStatToBot”, “GetTargets”, “ReloadTargets”) helper functions (e.g. “GetHashFromFile”, “SayHallo”, “GetRealIp”, “GetMyLocation”), and request generation (e.g. “HttpJob”, “FastRequest”, “GenNumber”).

Get L M’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

In general DDosia bots currently support four types of DDoS techniques.

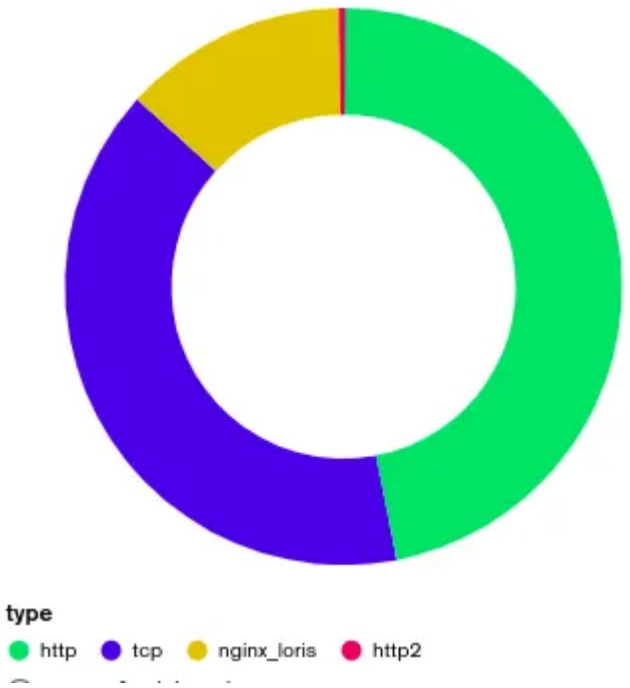
```
+-------------+------+-------------------------------------------------------------------------------
| Mode        | Type | Description
+-------------+------+-------------------------------------------------------------------------------
| http        | L7   | Classical HTTP GET/POST request generation, but with advanced customization a
|             |      | Bots receive precise HTTP request patterns to customize with host-based rando
+-------------+------+-------------------------------------------------------------------------------
| nginx_loris | L7   | Nginx Loris targets web servers running Nginx software using slow-rate attack
|             |      | This attack exploits how Nginx handles incomplete HTTP requests, tying up res
+-------------+------+-------------------------------------------------------------------------------
| tcp         | L4   | Classic TCP-SYN flooding. Bots forge TCP segments with the SYN flag set and s
+-------------+------+-------------------------------------------------------------------------------
| http2       | L7   | Similar to the HTTP module but utilizes the modern HTTP/2 protocol for enhanc
+-------------+------+-------------------------------------------------------------------------------
```

Data Insights

Data collected from recent attack operations shows the NoName057(16) collective strongly rely on L7 attacks the most of the time, around 46.9% of the attacks have been conducted using the above mentioned “http” mode. Despite that, almost the other half of their attack operations involves L4 DDoS techniques, in fact, the classical TCP-SYN technique has been abused 39.7% of the time. Less frequently, but consistently, NoName057(16) also leveraged the slowloris mode of attack “nginx_loris”, in about 13.0% of the attempts. The usage of HTTPS2 protocol is still marginal at the moment: the data we collected shows a negligible usage of the “http2” module in about 0.04% of the attacks.

Analyzing the distribution of target services we noticed that encrypted web services are among the favorite targets with over 69.4% of the attacks directed to the tls/443 network port, followed by unencrypted ones with 14.6% for both http/80 and http/8080.

Surprisingly, http based services are not the only target of the NoName057(16) attack operations, they also target SSH administration services on port tcp/22 (1.6%), file transfer services on port ftp/21 (1.6%), and encrypted email services on port imaps/993 and pop3s/995 (2.5%). Such kinds of services are typically less protected from malicious bot traffic and attacks rather than the web counterpart.



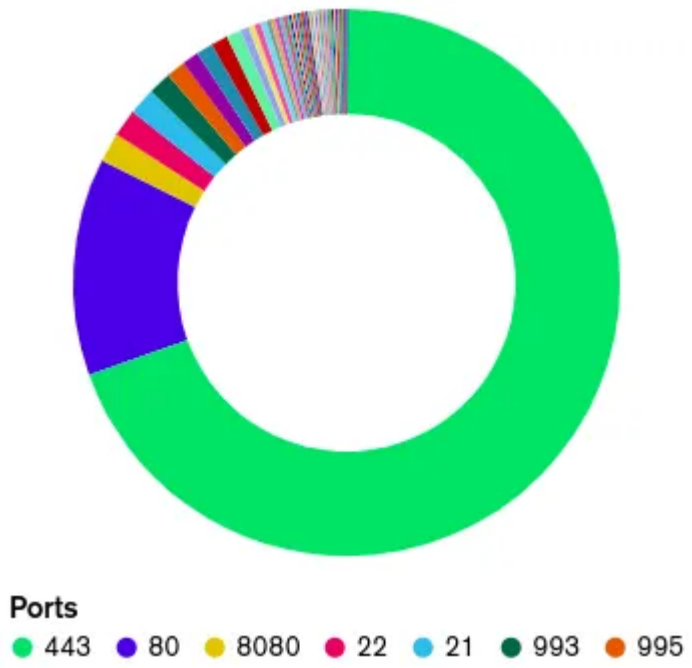


Figure. Distribution of attack modules (left) and targeted services (right)

Conclusion

Cyber partisan — or cyber militia — operations became a huge threat to our organizations and institutions. Groups like NoName057(16) are thriving in the cybercriminal underground and getting more sophisticated and inclusive.

As we noticed tracking the NoName057(16), they evolved their presence in the underground collecting support for thousands of hacktivists actively supporting the Russian regime, and mixing both ideology with economic incentives and reward programs.

Also, such threats are not only dangerous for public administration and government entities: as we observed in the past month, NoName057(16) heavily targeted even private companies and banking groups in Italy, blurring the lines between hacktivism and financial motivated intents.

Prompt intelligence on these criminal operations could help the CISOs of the targeted companies in the difficult task of mitigating the hacktivists attack waves in the first hours, avoiding service disruption and damages.

Indicator of Compromise

Hashes:

- d8631b2830af376932be65a5a7785df3bda93798 d_linux_arm
- 21f9cfdf4f6e85cf8834e1a4718395fe586d3b49 d_linux_x64
- 9b387e0ca5489f81b095f6719337d1fe13ebf60f d_mac_arm64
- dfae1df231ba8e8abfba4886df35a64c1d61d53d d_mac_x64
- 8e544c6b237da88467028d315012bd4c71e03c71 d_win_arm64.exe
- 9ab710153ddfa8fe87a9b13b653f37869247347d d_win_x64.exe

Yara Rules

```
rule go_stresser_20_x64 {
    meta:
        author = "@luc4m"
        date = "2023-04-13"
        hash_md5 = "c344f584881e90d426235553fedacff3"
        tlp = "CLEAR"
        yarahub_license = "CC0 1.0"
        yarahub_reference_md5 = "c344f584881e90d426235553fedacff3"
        yarahub_rule_matching_tlp = "CLEAR"
        yarahub_rule_sharing_tlp = "CLEAR"
        yarahub_uuid = "873ebbf5-9f83-4cf5-9670-b159211dd3c2"
    strings:
        $x64_0 = {f7 d8 49 c1 f8 3f 4d 21 e8 49 01 c0 4c 39 de 74 04}
        $x64_1 = {18 b9 ?? ?? ?? ?? e8 e2 0b 00 00 48 8b 6c 24 ?? 48 83 c4 20 c3}
        $x64_2 = {18 b9 ?? ?? ?? ?? e8 e2 0b 00 00 48 8b 6c 24 ?? 48 83 c4 20 c3}
        $x64_3 = {f7 da 49 c1 fa 3f 4d 21 e2 49 01 c2 ?? ?? 48 39 f7 74 04}
        $x64_4 = {6c 24 40 48 89 44 24 ?? 48 89 7c 24 ?? 31 d2 45 31 c0 eb 17}
        $x64_5 = {8d 5e ?? 45 69 e1 93 01 00 01 44 0f b6 2c 30 47 8d 0c 2c 4c 89 de 49 39 f0 7e 0b}
        $x64_6 = {48 89 4c 24 ?? 48 89 7c 24 ?? 44 89 54 24 ?? 89 54 24 ?? 41 39 d1 75 44}
        $x64_7 = {08 48 ?? 5c 24 10 e8 c9 08 06 00 48 8b 44 24 ?? 48 8b 5c 24 ?? eb bd}
        $x64_8 = {48 f7 c7 01 00 00 00 45 0f 45 d1 48 d1 ff 45 0f af c0 45 89 d1 48 85 ff 7f df}
        $x64_9 = {0f b6 14 31 43 8d 14 11 4c 89 c6 ?? 48 39 f7 7f e3}

 $s_0 = "HttpJob" wide ascii
 $s_1 = "SayHallo" wide ascii
 $s_2 = "StartJob" wide ascii
 $s_3 = "FastRequest" wide ascii
 $s_4 = "SetStatToBot" wide ascii
 $s_5 = "GetTargets" wide ascii

    condition:

        filesize < 10MB  and (5 of ($x64_*)) and (3 of ($s_*))
}
rule go_stresser_20_generic {
    meta:
        author = "@luc4m"
        date = "2023-04-13"
        hash_md5 = "ac0d5e1ec2664ad36db8877078bcf6c3"
        tlp = "CLEAR"
        yarahub_license = "CC0 1.0"
        yarahub_reference_md5 = "ac0d5e1ec2664ad36db8877078bcf6c3"
        yarahub_rule_matching_tlp = "CLEAR"
        yarahub_rule_sharing_tlp = "CLEAR"
```

```
        yarahub_uuid = "873ebbf5-9f83-4cf5-9670-b159211dd3c2"
    strings:

 $s_0 = "HttpJob" wide ascii
 $s_1 = "SayHallo" wide ascii
 $s_2 = "StartJob" wide ascii
 $s_3 = "FastRequest" wide ascii
 $s_4 = "SetStatToBot" wide ascii
 $s_5 = "GetTargets" wide ascii

    condition:

        filesize < 10MB  and (5 of ($s_*))
}
```

Source: https://medium.com/@lcam/data-insights-from-russian-cyber-militants-noname057-c9b7431f8352