VEDERE LABS

Killnet

Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group

Contents

1. Executive Summary 3
2. Technical Analysis 4
   2.1. Data from our honeypot 4
   2.2. Telegram chat 7
   2.3. “Wawsquad” and Telegram copycats 12
3. IoCs 16
4. Mitigation Recommendations 20
5. References 20

1. Executive Summary

Killnet is one of many hacktivist groups that has taken a side in the ongoing Russian invasion of Ukraine. There have been more than 100 groups conducting cyberattacks since we published our initial analysis at the beginning of the war. Most of the attacks from these groups are distributed denials of service (DDoS), but they also include data breaches, data wipers and psychological operations (i.e., distributing propaganda).

These groups include hacktivists such as Killnet, state-sponsored entities such as Sandworm and ransomware gangs such as Conti. There are currently more than 70 active groups, located mainly in Russia or Ukraine, but also in Belarus (e.g., Belarusian Cyber Partisans), Turkey (e.g., Monarch Turkish Hacktivists), Romania (e.g., Anonymous Romania), Poland (e.g., Squad303), Portugal (e.g., Anon666) and Italy (e.g., Anonymous Italia). Their coordination and the communication of their actions usually happens via either Twitter or Telegram.

Killnet stands out as one of the most active groups in this conflict, having declared war on Anonymous, a group supporting Ukraine, since February 25, 2022. Killnet is located in Russia and supports its country in the war, alongside other groups such as Xaknet and, often in joint operations, Legion. Killnet has gained certain notoriety for DDoSing the websites of western critical infrastructure operators, such as airports, banks, energy providers and governmental agencies. Killnet also spreads propaganda to more than 70,000 members of its Telegram channel. Killnet hacktivists were part of a recent CISA alert and other reports shared by CERTs and ISACs.

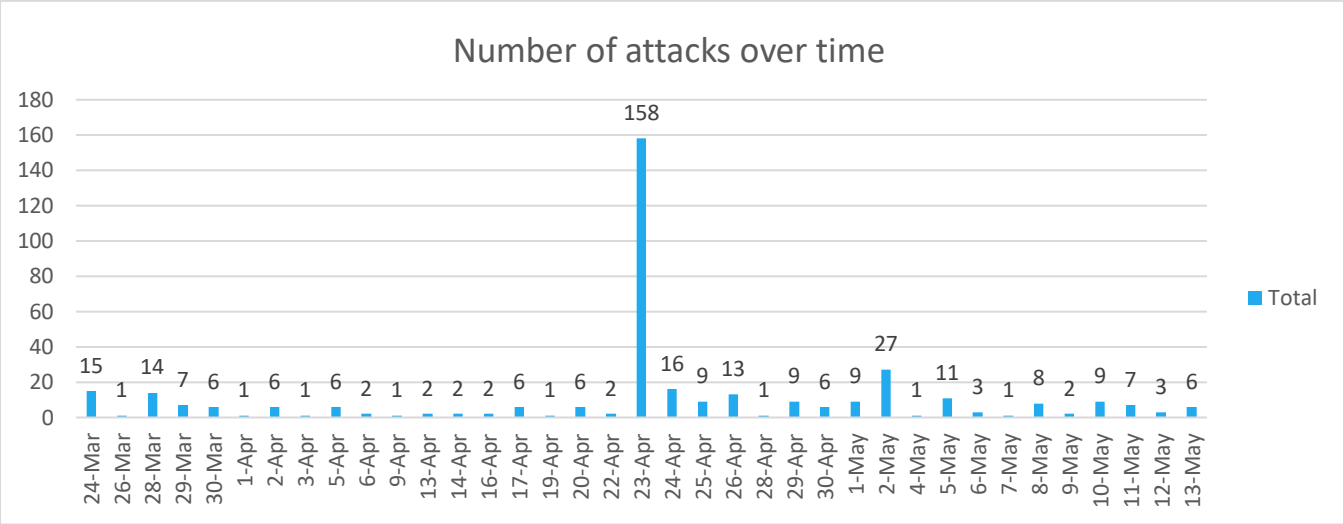
Although the group has been very active, appears to have effective communication, a semi-structured organization and managed some level of success in their campaigns, there is no evidence that Killnet uses or develops custom tools or even that it reuses very sophisticated tools in its attacks.

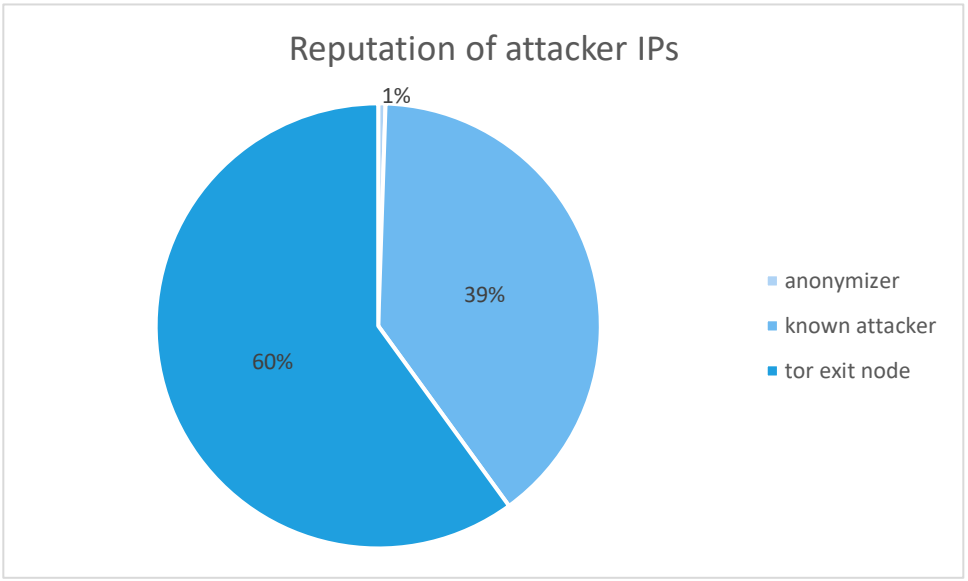
In this report, we leverage a list of IP addresses known to be used by Killnet during past attacks to study the group's TTPs when attacking a series of honeypots we control (Section 2.1), which reveals the hacktivist's preference for brute-forcing credentials on TCP ports 21 (FTP), 80 (HTTP), 443 (HTTPS) and 22 (SSH), and its use of SSH tunneling. We analyze the Telegram channels associated with the group (Section 2.2) to confirm Killnet's use of mostly L4/L7 DDoS (e.g., SYN flood or resource exhaustion via massive amounts of POST/GET requests) and show its point of view on the attacks the group has conducted. We discuss the emergence of several copycat groups on Telegram and analyze an example one named Wawsquad (Section 2.3). We also provide a list of IoCs (3) and mitigation recommendations (Section 4).

2. Technical Analysis

2.1. Data from our honeypot

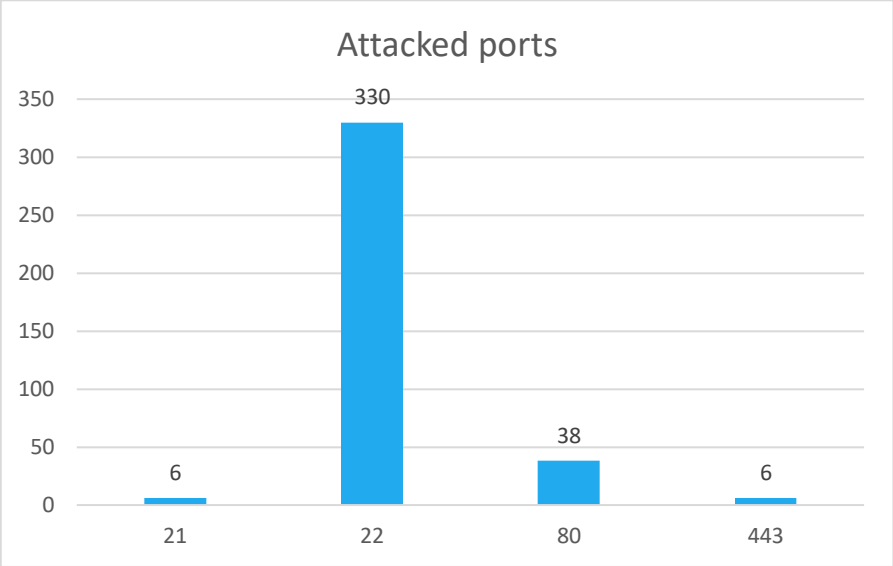
Our sensors started to observe attacks from IP addresses associated with Killnet from 24 March, peaking around April 23 and still ongoing up to May 13, 2022. According to our analysis of the official Telegram chat of the threat actor (see the next Section), most of the major DDoS attacks happened within that timeline. The attackers' IP addresses consisted mainly of TOR exit nodes and known malicious clearnet or proxied addresses.



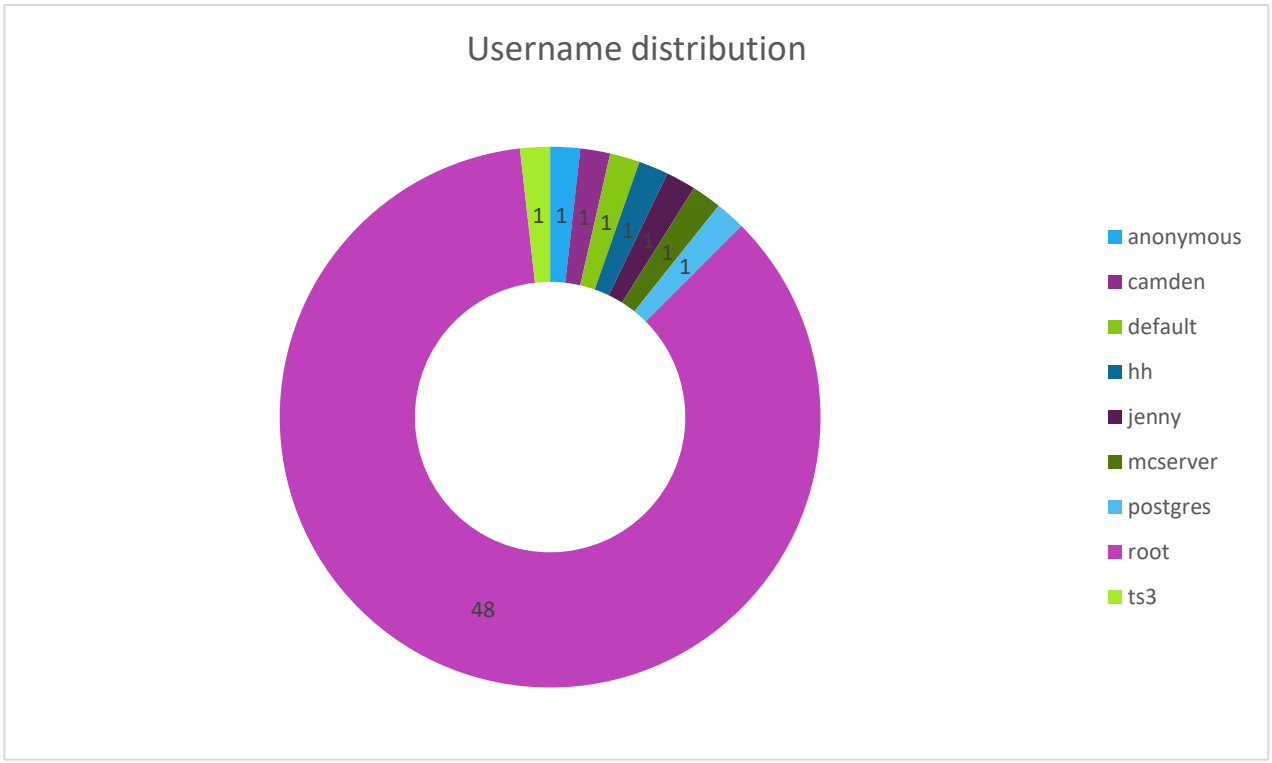


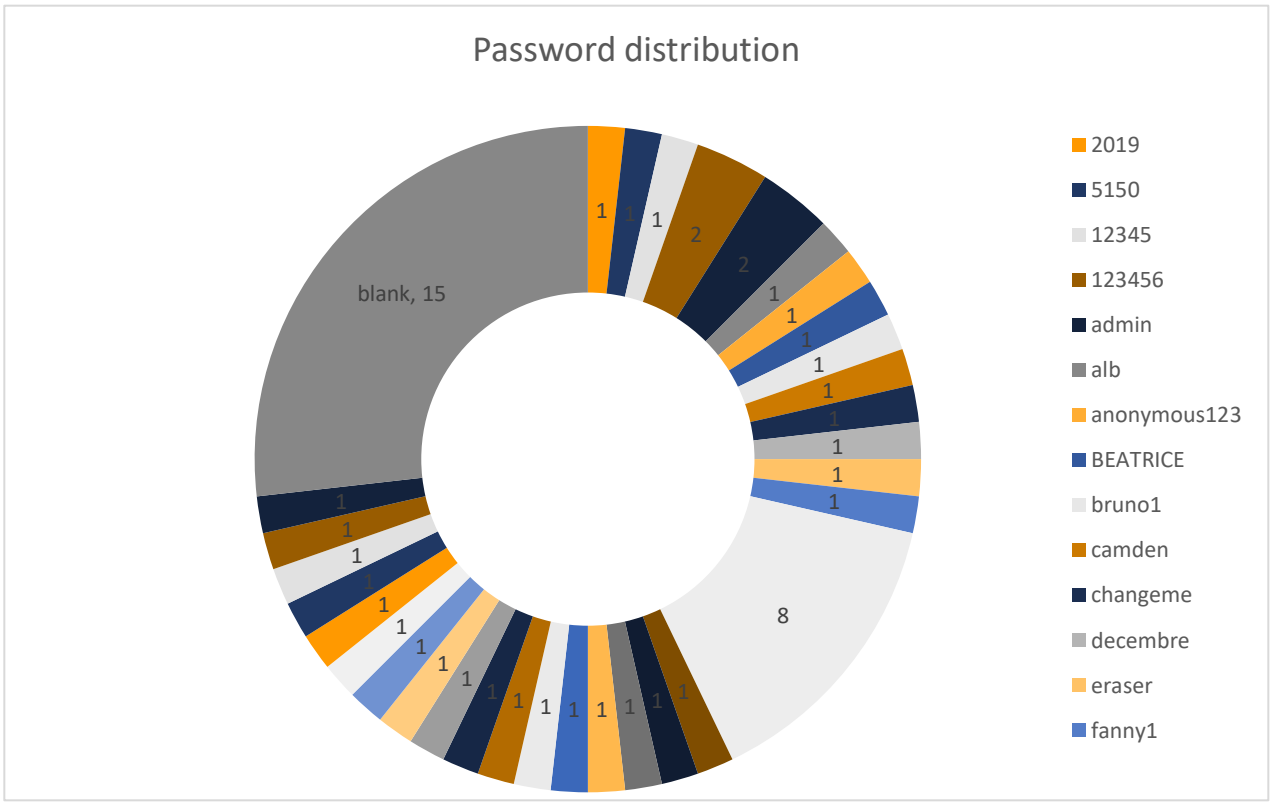
In total, we observed 381 attacks coming from 58 unique IP addresses, out of which 56 were dictionary attacks, using well-known default credentials in hopes that a victim did not change them, coming from 10 different IP addresses. The attacks consisted primarily of querying TCP

ports 21 (FTP), 80 (HTTP), 443 (HTTPS) and 22 (SSH), which is in line with the attack methods we have observed discussed in the Telegram chat.



We have also observed that the brute-force attempts were exclusively against port 22, hinting that the threat actor aimed at having persistence/proxying capabilities or that it may be simply doing reconnaissance or credential harvesting for later use. The top username used in the dictionary attacks was ‘root,’ followed by far fewer attempts on ‘postgres’, ‘mcserver’ (minecraft servers), ‘ts3’ (teamspeak servers) and others. The passwords attempts did not strike any significant pattern except for being generally weak. Below is a distribution of top usernames and passwords used in the dictionary attacks.





The attacking IP addresses that did not execute dictionary attacks tended to repeat attacks over a maximum of three days, while the ones that did perform such attacks did not repeat the attack again, hinting at different goals of attack scripts associated to each IP. In some

instances, when the attacker was tricked into an SSH session, it tried to use our attacker engagement environment as a proxy toward **google.com** by attempting to create SSH tunnels.

Known Killnet IPs using SSH forwarding	Target
171.25.193.78	https://google.com
185.220.102.242	https://google.com

We found other attacking IPs, which were not among those initially attributed to Killnet. These IPs used the same SSH forwarding technique to the same target within the same time range (March 27 to May 15, 2022).

Attacking IPs using similar techniques not in the original Killnet list	Target
5.2.69.50	https://google.com
92.255.85.237	https://google.com
92.255.85.135	https://google.com

The attacks on FTP ports mainly executed the SYST command, which returns the system type, hinting at reconnaissance only.

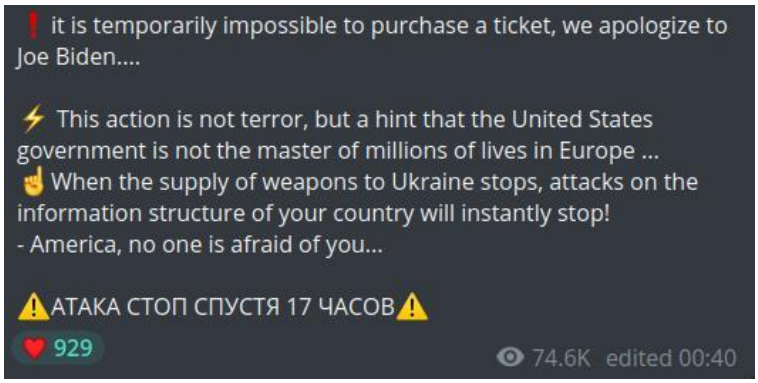
2.2. Telegram chat

Killnet often makes announcements about planned or successful attacks on its official Telegram channel at https://t.me/killnet_channel. The content on this channel is heavy with Russian propaganda and hate speech toward countries and individuals who do not support Russian aggression against Ukraine. As such, viewer discretion is strongly advised.

The channel was created in January 2022, and the first messages were about attacking the Anonymous group (which is allegedly at war with Killnet). The chronology of announced attacks began on March 3 with the takedown of a Ukrainian news service – https://korrespondent.net – and the Ukrainian branch of Vodafone –https://vodafone.ua. These actions are justified by the group as “a strike against propaganda.” After allegedly attacking the Ministry of Interior Affairs of Ukraine and several other Ukrainian resources related to higher education, the group proceeded with an attack on the Ministry of the Interior of Latvia on March 22.

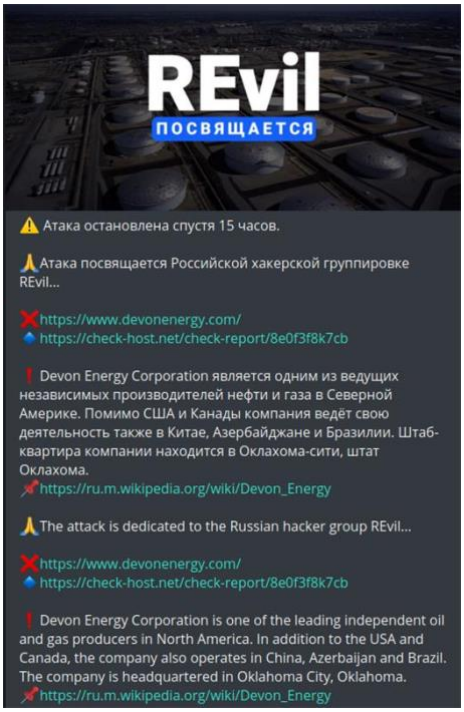
On March 23, the attackers shifted their focus to Poland, starting with the website of the Supreme Court in the Republic of Poland. On the next day, they reported an attack against Narodowy Bank Polski
(National Bank of Poland). As the message below shows, the attackers justify their actions by saying that “*any kind of aggression from the Polish authorities towards Russia will immediately result in massive DDoS attacks against critical network resources of Poland.*” Shortly after this announcement, the Killnet chat reported a successful attack against the Polish Investment and Trading Agency (https://www.paih.gov.pl/en), allegedly resulting in a 20Gb data leak.

Soon after on March 29, Killnet reported a successful attack against a target in the United States: the Bradley International Airport (https://www.nbcconnecticut.com/news/local/bradley-airport-website-suffers-cyber-attack/2750473/). The attackers' main point was to prevent any kind of military aid to Ukraine:

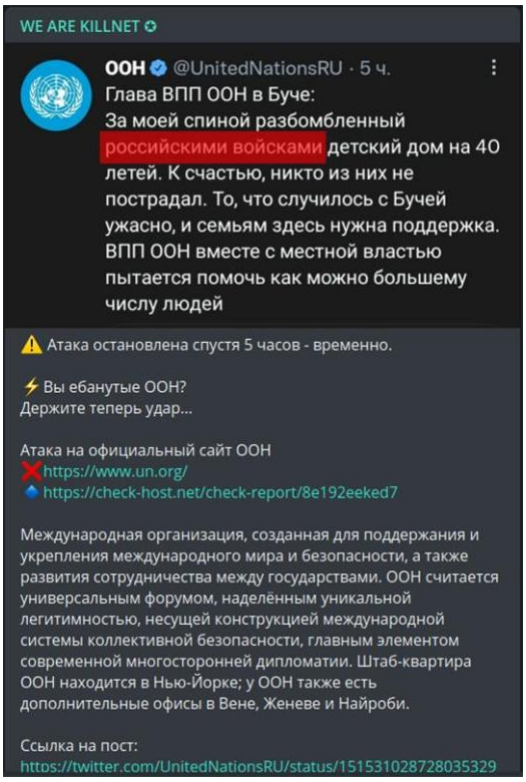


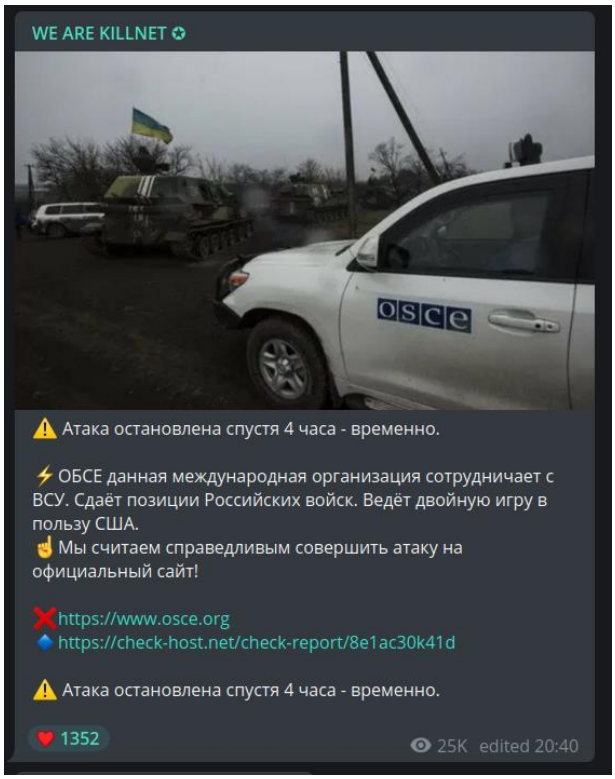
A couple of days later, Killnet claimed a successful DDoS attack on the website of CYBERPOL (https://www.cyberpol.info/), after which there has been a short gap until April 15 when Killnet reported a successful attack against the Federal Ministry of Defence of Germany (https://www.bmvg.de/de), claiming they targeted not Germany but "fascism":

This was immediately followed by several attacks on German airports (Koeln-Bonn, Bremen and Hamburg), the Gatwick airport in the UK and eight airports in Poland. Several German financial organizations (Commerzbank and KWF among them) were also under attack. During this time, Killnet announced a “special attack” which served as a homage to the REvil hacking group: They DDoSed the website of the Devon Energy Corporation in the U.S. (https://devonenergy.com). It is unclear at this stage if any critical infrastructure was damaged or if it was just an attack against the web-facing resources of the company.



Albeit targeting organizations in government, transportation and financial sectors, in one of the Telegram announcements, the attackers explicitly state that they are not going against healthcare targets. At the same time, the attackers choose several “political” targets (such as the UN and OSCE), justifying the attackers’ actions by the fact that these organizations spread “lies” about the war crimes committed by Russian troops and work with the Ukrainian military against Russia.

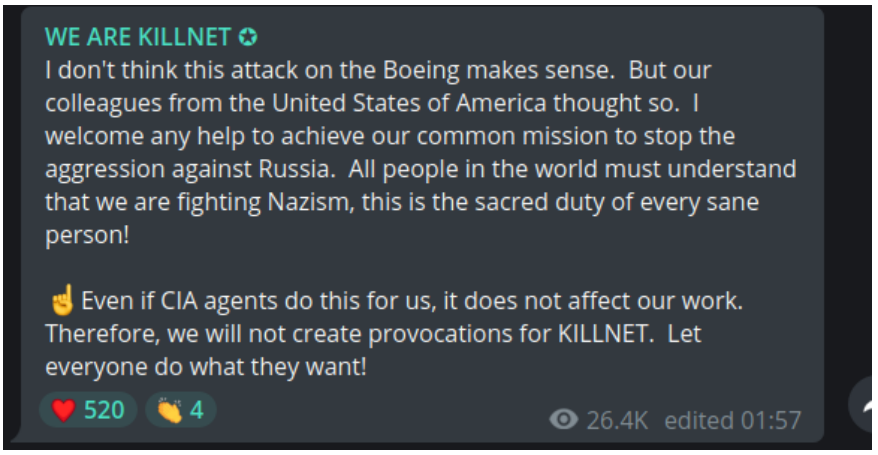




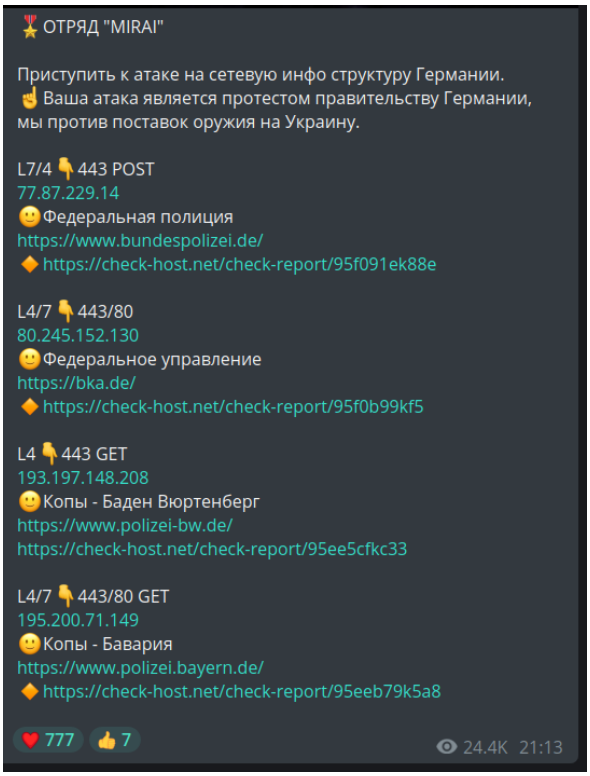
The time between April 19 and the beginning of May contains a lot of announcements/reports about successful attacks against many targets in Europe – Czech Republic, Lithuania, Latvia, Estonia, Poland, Romania, UK, France and Italy are among the targeted countries – as well as the United States. The rhetoric around these attacks suggests that these countries must drop their support of Ukraine and stop “their aggression against Russia.” Some messages contain obscenity and “trolling.” However, it is peculiar that the messages are mostly in Russian; therefore, it is difficult to say whether the witticisms have reached the intended audience in the end. The messages and the corresponding attacks, however, are clearly aimed at wreaking havoc among Western countries and shift the opinion of people within these countries about the Russian war. The latter clearly suggests there is no financial motivation behind the attacks – the motives are purely political.

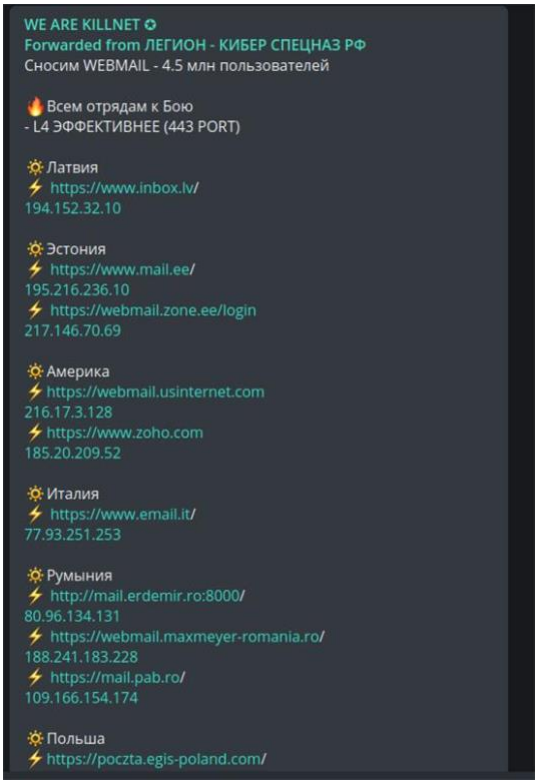
From the chat messages, it also becomes clear that Killnet is not a well-defined group, rather a conglomerate of smaller hacking groups and individuals that have united in their common goal of “making Russia great again” by “fighting fascism” (as supported by other investigation). We observed mentions of various squads such as “Mirai squad”, “Sakurajima”, “JACKY”, “Заря”

and “DDOSGUNG”. Some messages even mention a recently established U.S. branch of Killnet:



Several messages in the chat suggest that the main type of attack is L4/L7 DDoS (e.g., SYN flood or resource exhaustion via massive amounts of POST/GET requests). Several “groups” within Killnet seem to get attack orders from the chat (or other chats) directly:

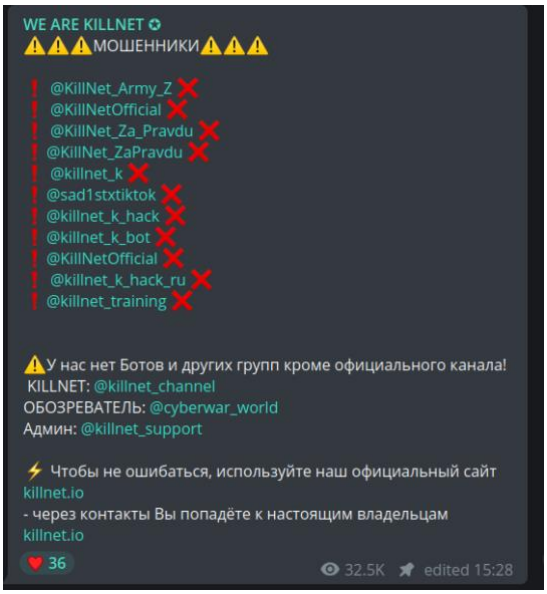




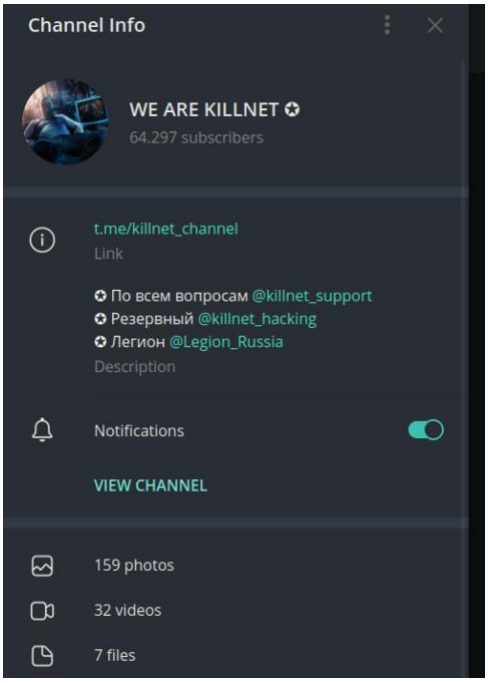
The attack methods and the networking ports involved seem to correspond to the evidence of the Killnet attack traffic that reached our Honeypot (see the previous Section).

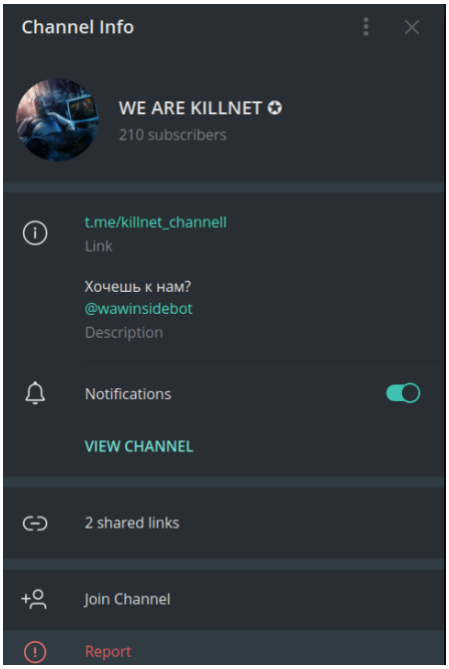
2.3. “Wawsquad” and Telegram copycats

The official Telegram chat often contains messages about various “copycats” that either pretend to be Killnet or refer to themselves as their associates:



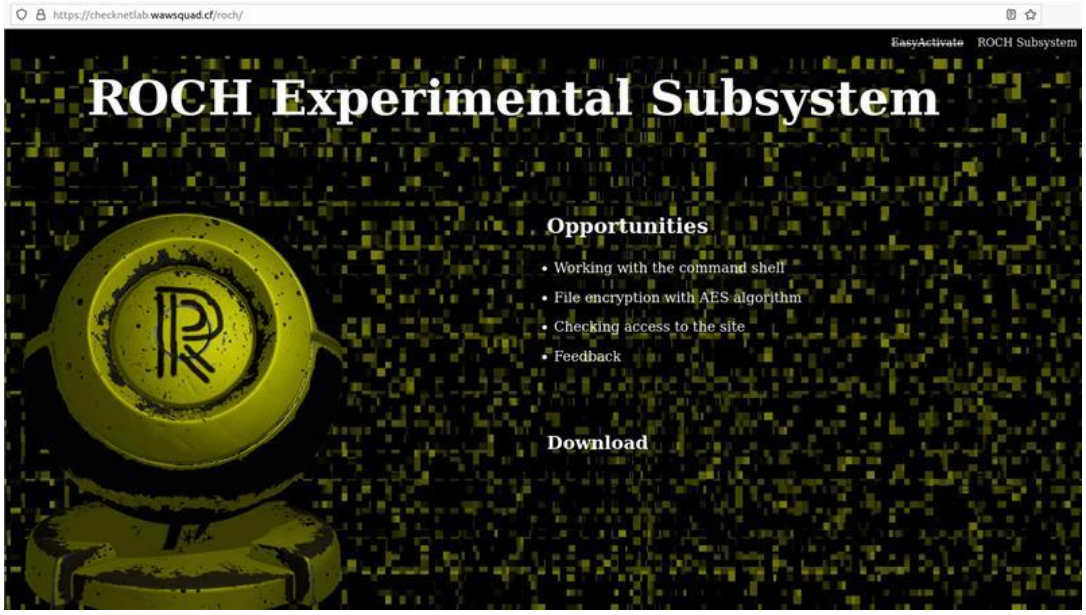
We have also found several chats that attempt to mimic the original one. It seems that while some intend to commit scams by offering bespoke “DDoS-as-a-Service” piggybacking on all the news behind Killnet, others do it out of pure desire of someone else’s “glory.” For example, there is another chat in Telegram that attempts to “typosquat” the name of the original one. The original one is shown on the left, and the fake one is shown on the right:





This particular “copycat” leads to another channel called “WAWHACKERS,” and the participants in the chat seem to share similar political views of the original Killnet. The WAWHACKERS have several web resources: an official website (“wawsquad[.]cf”) and software archive (“checknetlab[].wawsquad[.]cf) where they advertise free and non-free hacking software “coming from their lab.”

However, after a few minutes of browsing it becomes clear that the group is not affiliated with Killnet. For example, a piece of software listed as “ROCH Experimental Subsystem” is nothing but a simple python script packed as a Windows executable:



The script contains basic functionality for checking whether a website is available (that is, returns HTTP code 200), local shell functionality, basic local file encryption and “feedback” that allows to send questions and bug reports to the authors. This last feature uses a pair of hardcoded Google mail addresses so that the bug reports created within the tool are sent as email messages from one hardcoded account to another. It also helps to reveal the identity of the author. The screenshots below show the python disassembly fragments related to this functionality:

```
 82  LOAD_FAST                'smtp'
 84  LOAD_METHOD              login
 86  LOAD_STR                 'nikanat500@gmail.com'
 88  LOAD_STR                 'Rapid7Rapid8'
 90  CALL_METHOD_2         2  ''
 92  POP_TOP
```

```
152  LOAD_GLOBAL              input
154  LOAD_STR                 'Enter your name: '
156  CALL_FUNCTION_1       1  ''
158  STORE_FAST               'name'

160  LOAD_GLOBAL              input
162  LOAD_STR                 'Enter your problem: '
164  CALL_FUNCTION_1       1  ''
166  STORE_FAST               'mistake'

168  LOAD_GLOBAL              print
170  LOAD_GLOBAL              Fore
172  LOAD_ATTR                BLUE
174  CALL_FUNCTION_1       1  ''
176  POP_TOP

178  LOAD_GLOBAL              print
180  LOAD_STR                 '[~]Sending log...'
182  CALL_FUNCTION_1       1  ''
184  POP_TOP

186  SETUP_FINALLY       258  'to 258'

188  LOAD_FAST                'smtp'
190  LOAD_METHOD              sendmail
192  LOAD_STR                 'nikanat500@gmail.com'
194  LOAD_STR                 'alekmalekov500@gmail.com'
196  LOAD_STR                 'Здравствуйте, я '          # Hello, my name is
198  LOAD_FAST                'name'
200  BINARY_ADD
202  LOAD_STR                 '. Моя проблема: '          # My problem is:
204  BINARY_ADD
206  LOAD_FAST                'mistake'
208  BINARY_ADD
210  CALL_METHOD_3         3  ''
```

It seems that both email accounts belong to someone called “**Alek**sey” or “**Alex**andr” “**Malekov**”. The hardcoded password “Rapid7Rapid8” was recently changed on the first email address, but not on the second one.

After looking a bit more at the chat messages and other resources provided by this particular “copycat” and several others, it has become clear that they are not part of the “official” Killnet and are likely being run by minors who are learning their way around programming and cybersecurity. However, these minors share and spread the political beliefs of the original Killnet, which shows the adverse effect of cyber propaganda.

3. IoCs

IoC	Type	Description
5.2.69.50	IPv4 address	IP address using TTPs similar to Killnet
92.255.85.237	IPv4 address	IP address using TTPs similar to Killnet
92.255.85.135	IPv4 address	IP address using TTPs similar to Killnet
173.212.250.114	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
144.217.86.109	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
156.146.34.193	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
162.247.74.200	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
164.92.218.139	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
171.25.193.25	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
171.25.193.78	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.100.87.133	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.100.87.202	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.129.61.9	IPv4 address	IP address used in Killnet attacks and observed on our honeypots

185.220.100.241	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.242	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.243	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.248	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.250	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.252	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.100.255	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.101.15	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.101.35	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.102.242	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.102.243	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.220.102.253	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.56.80.65	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.67.82.114	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
185.83.214.69	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
195.206.105.217	IPv4 address	IP address used in Killnet attacks and observed on our honeypots

199.249.230.87	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
205.185.115.33	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
209.141.57.178	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
209.141.58.146	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.130	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.131	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.132	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.133	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.134	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.137	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.139	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.142	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.147	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.148	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.149	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.210	IPv4 address	IP address used in Killnet attacks and observed on our honeypots

23.129.64.212	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.213	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.216	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.217	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.218	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
23.129.64.219	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
45.153.160.132	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
45.153.160.139	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
45.154.255.138	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
45.154.255.139	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
45.227.72.50	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
72.167.47.69	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
81.17.18.58	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
81.17.18.62	IPv4 address	IP address used in Killnet attacks and observed on our honeypots
91.132.147.168	IPv4 address	IP address used in Killnet attacks and observed on our honeypots

4. Mitigation Recommendations

- Follow the NCSC-UK's guide on Denial of Service attacks, which includes a preparation phase of understanding weak points in your service, ensuring that service providers can handle resource exhaustion, scaling the service to handle concurrent sessions, preparing a response plan and stress testing systems regularly.
- Monitor the activity of hacktivist groups on Telegram, Twitter and other sources where attacks are planned and coordinated.
- Identify and patch vulnerable IoT devices to prevent them from being used as SSH tunnels or part of DDoS botnets.
- Change defaults or easily guessable passwords of IoT devices.
- Monitor the traffic of IoT devices to identify those being used as part of distributed attacks.

5. References

- https://us-cert.cisa.gov/ncas/alerts/aa22-110a
- https://cyberknow.medium.com/update-14-2022-russia-ukraine-war-cyber-group-tracker-may-22-b00ed4d899bf
- https://cyberknow.medium.com/killnet-pro-russian-hacktivists-e916ac7201a3
- https://malpedia.caad.fkie.fraunhofer.de/actor/killnet
- https://dnsc.ro/vezi/document/situatie-site-uri-cu-activitate-in-contextul-crizei-ucraina-rusia-plus-adrese-ip-specifice-utilizate-in-atacuri-malware