Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3 Analyst Note

April 5, 2023 TLP:CLEAR Report: 202304051200

KillNet's Targeting of the Health and Public Health Sector (December 2022 – March 2023)

Executive Summary

Pro-Russia hacktivist group, KillNet, has actively targeted the United States health and public health (HPH) sector since December 2022. Their signature distributed denial-of-service (DDoS) attacks on critical infrastructure sectors typically only cause service outages lasting several hours or even days. However, the range of consequences from these attacks on the HPH sector can be significant, threatening routine to critical day-to-day operations. An examination of the group's cyber offensive from December 2022 to March 2023 provides insight into how and why they target the healthcare industry, and recommendations for how HPH organizations can better protect themselves.

Overview

On January 28, 2023, KillNet and its affiliates conducted numerous coordinated DDoS attacks, targeting HPH organizations in the U.S. and several NATO countries, apparently, in retalition for the allocation of tanks to and in support of Ukraine. Active since at least January 2022, KillNet is known for conducting DDoS campaigns against multiple critical infrastructure sectors in countries that support Ukraine in the war between Russia and Ukraine or appear to be "anti-Russia." Although their primary type of cyber-attack method usually does not cause major damage, it can cause service outages to vulnerable systems lasting several hours or even days. Whereas many hactivist groups abstain from targeting HPH organizations, the group has dispassonately targeted hospitals and medical organizations across the sector.

Impact to HPH Sector

In the late January 2023 attack, over 90 known orchestrated DDoS attacks took place on healthcare systems (covering multiple hospitals), lone hospitals, and medical centers. Of these, 55% were healthcare systems with at least one hospital and lone hospitals with Level I trauma centers, which provide the most comprehensive and highest level of trauma care to critically ill or injured patients. As they are normally large establishments with considerable patient data to enter and exploit, these types of HPH organizations are ideal targets for KillNet and its affiliates.

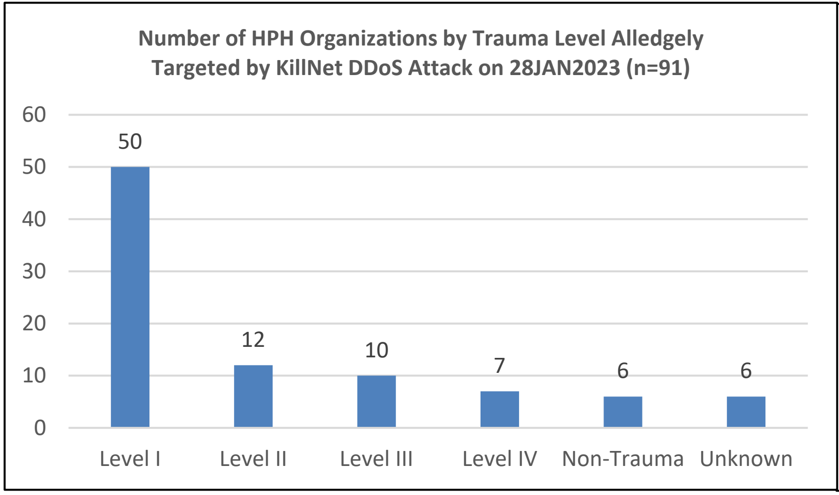


Figure 1: Graph of HPH Trauma and non-Trauma Organizations Alledgely Targeted by KillNet on January 28, 2023.

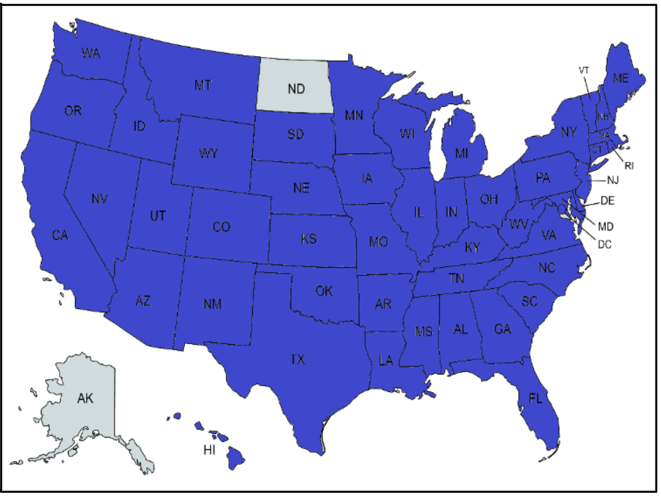
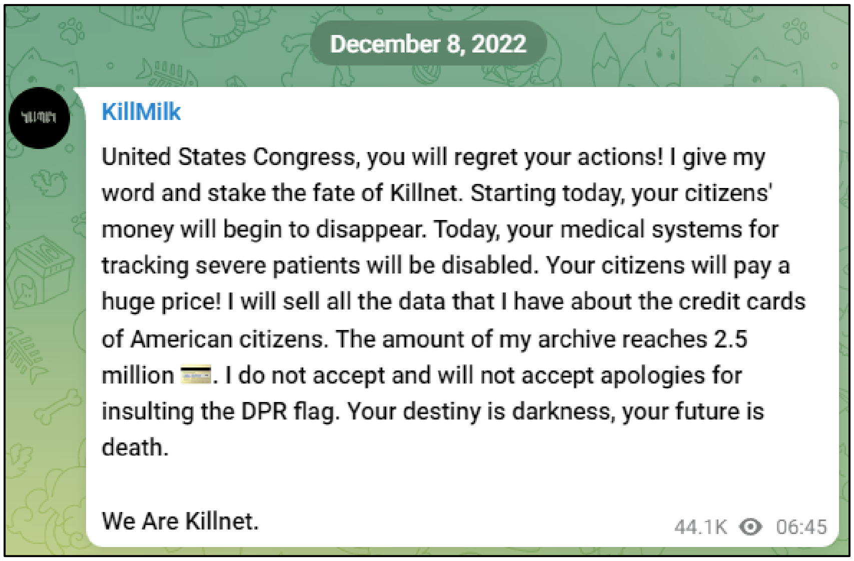


Figure 2: Map of 48 U.S. States Alledgely Targeted by KillNet on January 28, 2023.

Since the February 24, 2022 Russian invasion of Urkaine, KillNet continued its harassment of U.S. and NATO countries' critical infrastructure. By December 2022, their targeting of the HPH sector was apparent, with announcements of their coordinated attacks across multiple countries posted on the Telegram channel of its founder and leader, KillMilk. A timeline of the posts exclusively targeting the sector from both KillMilk and KillNet can be found below. For purposes of this case study, only threats to and attacks on the HPH sector will be examined.

December 2022



December 8, 2022

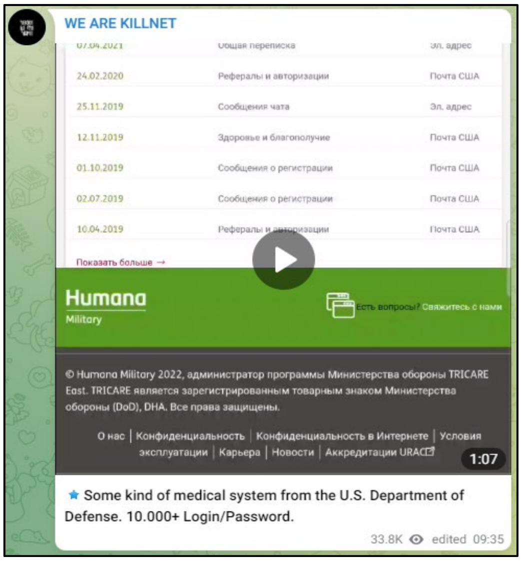
KillMilk

United States Congress, you will regret your actions! I give my word and stake the fate of Killnet. Starting today, your citizens' money will begin to disappear. Today, your medical systems for tracking severe patients will be disabled. Your citizens will pay a huge price! I will sell all the data that I have about the credit cards of American citizens. The amount of my archive reaches 2.5 million 💳. I do not accept and will not accept apologies for insulting the DPR flag. Your destiny is darkness, your future is death.

We Are Killnet.

44.1K 06:45

Figure 3: KillMilk threatens U.S. Congress with extortion of health and personal data of Americans because of U.S. military aid to Ukraine. (December 8, 2022)



WE ARE KILLNET

07.04.2021	Общая переписка	Эл. адрес
24.02.2020	Рефералы и авторизации	Почта США
25.11.2019	Сообщения чата	Эл. адрес
12.11.2019	Здоровье и благополучие	Почта США
01.10.2019	Сообщения о регистрации	Почта США
02.07.2019	Сообщения о регистрации	Почта США
10.04.2019	Рефералы и авторизации	Почта США

Показать больше →

© Humana Military 2022, администратор программы Министерства обороны TRICARE East. TRICARE является зарегистрированным товарным знаком Министерства обороны (DoD), DHA. Все права защищены.

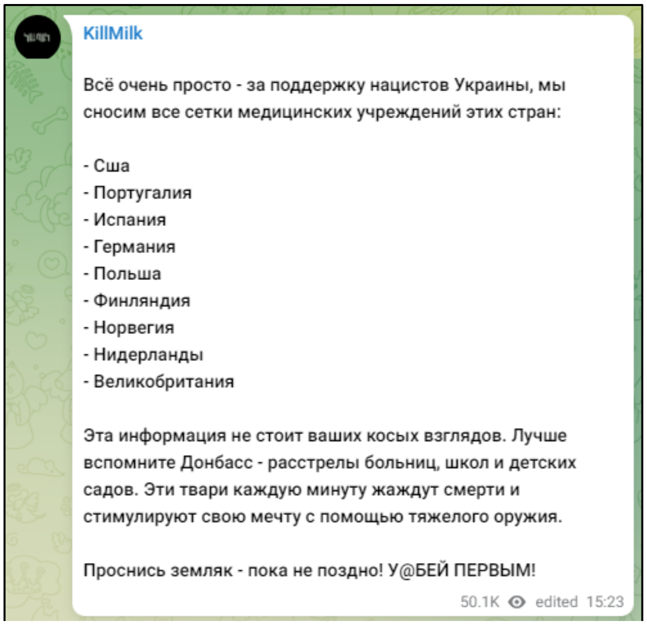
О нас | Конфиденциальность | Конфиденциальность в Интернете | Условия эксплуатации | Карьера | Новости | Аккредитации URAC
1:07

★ Some kind of medical system from the U.S. Department of Defense. 10.000+ Login/Password.

33.8K edited 09:35

Figure 4: KillNet targets U.S. DoD healthcare subsidiary, Humana Military. (December 16, 2022)

January 2023



KillMilk

Всё очень просто - за поддержку нацистов Украины, мы сносим все сетки медицинских учреждений этих стран:

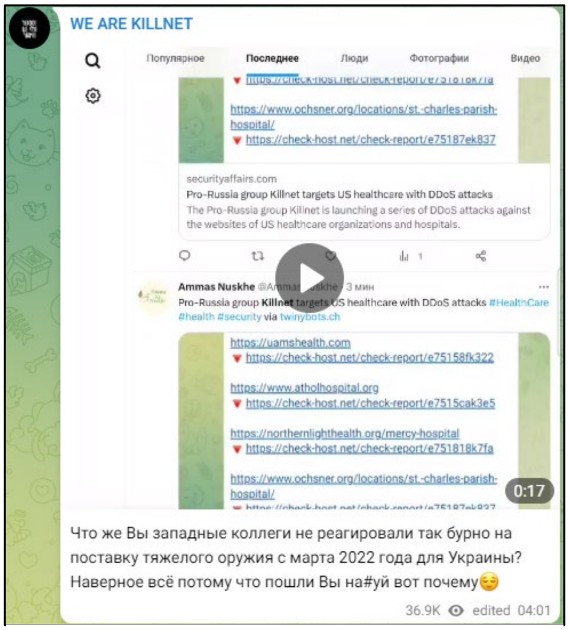
- Сша
- Португалия
- Испания
- Германия
- Польша
- Финляндия
- Норвегия
- Нидерланды
- Великобритания

Эта информация не стоит ваших косых взглядов. Лучше вспомните Донбасс - расстрелы больниц, школ и детских садов. Эти твари каждую минуту жаждут смерти и стимулируют свою мечту с помощью тяжелого оружия.

Проснись земляк - пока не поздно! У@БЕЙ ПЕРВЫМ!

50.1K edited 15:23

Figure 5: KillMilk announces targeting of U.S. and European HPH Sector in response to support for Ukraine. (January 27, 2023)



WE ARE KILLNET

https://www.ochsner.org/locations/st.-charles-parish-hospital/
▼ https://check-host.net/check-report/e75187ek837

securityaffairs.com
Pro-Russia group Killnet targets US healthcare with DDoS attacks
The Pro-Russia group Killnet is launching a series of DDoS attacks against the websites of US healthcare organizations and hospitals.

Ammas Nuskhe @Ammas Nuskhe · 3 мин
Pro-Russia group **Killnet** targets US healthcare with DDoS attacks #HealthCare #health #security via twinybots.ch

https://uamshealth.com
▼ https://check-host.net/check-report/e75158fk322

https://www.atholhospital.org
▼ https://check-host.net/check-report/e7515cak3e5

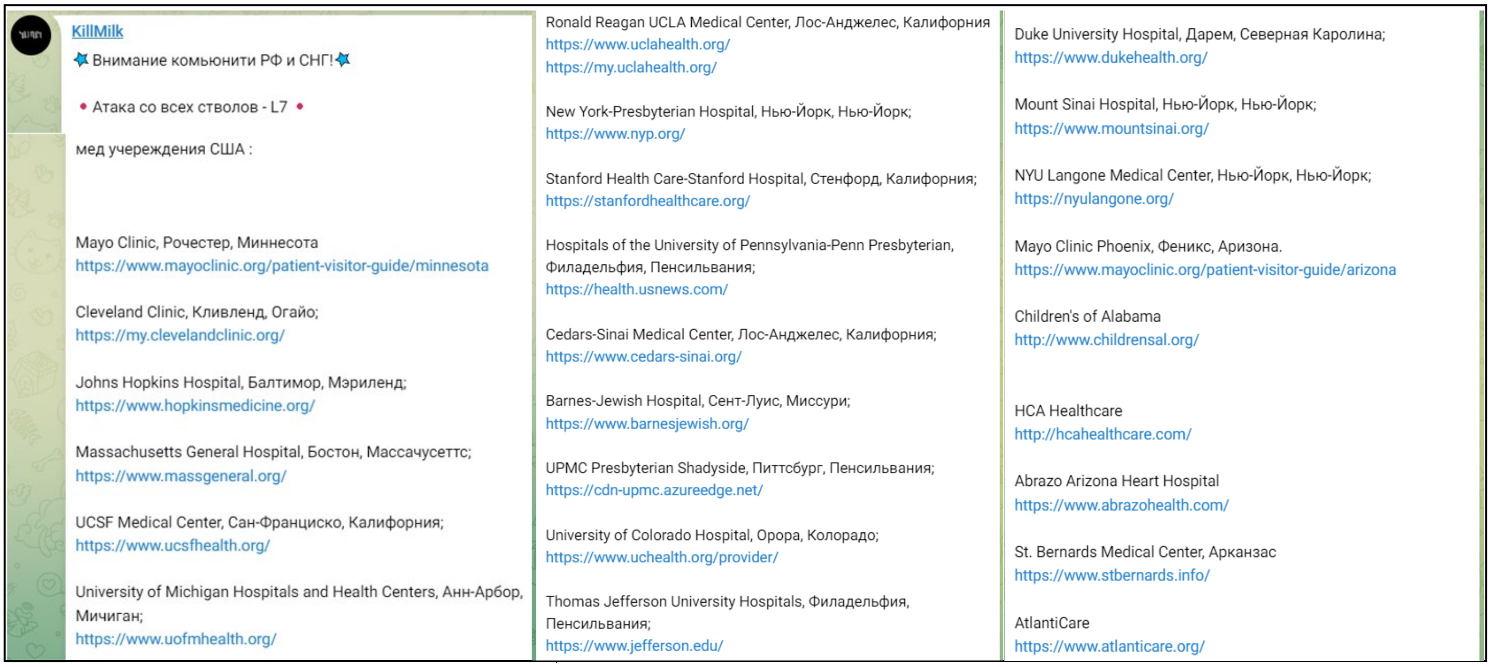
https://northernlighthealth.org/mercy-hospital
▼ https://check-host.net/check-report/e751818k7fa

https://www.ochsner.org/locations/st.-charles-parish-hospital/

Что же Вы западные коллеги не реагировали так бурно на поставку тяжелого оружия с марта 2022 года для Украины? Наверное всё потому что пошли Вы на#уй вот почему😌

36.9K edited 04:01

Figure 6: KillNet re-posts article on their targeting of HPH sector. (January 31, 2023)



KillMilk

✪ Внимание комьюнити РФ и СНГ!✪

• Атака со всех стволов - L7 •

мед учереждения США :

Mayo Clinic, Рочестер, Миннесота
https://www.mayoclinic.org/patient-visitor-guide/minnesota

Cleveland Clinic, Кливленд, Огайо;
https://my.clevelandclinic.org/

Johns Hopkins Hospital, Балтимор, Мэриленд;
https://www.hopkinsmedicine.org/

Massachusetts General Hospital, Бостон, Массачусеттс;
https://www.massgeneral.org/

UCSF Medical Center, Сан-Франциско, Калифорния;
https://www.ucsfhealth.org/

University of Michigan Hospitals and Health Centers, Анн-Арбор, Мичиган;
https://www.uofmhealth.org/

Ronald Reagan UCLA Medical Center, Лос-Анджелес, Калифорния
https://www.uclahealth.org/
https://my.uclahealth.org/

New York-Presbyterian Hospital, Нью-Йорк, Нью-Йорк;
https://www.nyp.org/

Stanford Health Care-Stanford Hospital, Стенфорд, Калифорния;
https://stanfordhealthcare.org/

Hospitals of the University of Pennsylvania-Penn Presbyterian, Филадельфия, Пенсильвания;
https://health.usnews.com/

Cedars-Sinai Medical Center, Лос-Анджелес, Калифорния;
https://www.cedars-sinai.org/

Barnes-Jewish Hospital, Сент-Луис, Миссури;
https://www.barnesjewish.org/

UPMC Presbyterian Shadyside, Питтсбург, Пенсильвания;
https://cdn-upmc.azureedge.net/

University of Colorado Hospital, Орора, Колорадо;
https://www.uchealth.org/provider/

Thomas Jefferson University Hospitals, Филадельфия, Пенсильвания;
https://www.jefferson.edu/

Duke University Hospital, Дарем, Северная Каролина;
https://www.dukehealth.org/

Mount Sinai Hospital, Нью-Йорк, Нью-Йорк;
https://www.mountsinai.org/

NYU Langone Medical Center, Нью-Йорк, Нью-Йорк;
https://nyulangone.org/

Mayo Clinic Phoenix, Феникс, Аризона.
https://www.mayoclinic.org/patient-visitor-guide/arizona

Children's of Alabama
http://www.childrensal.org/

HCA Healthcare
http://hcahealthcare.com/

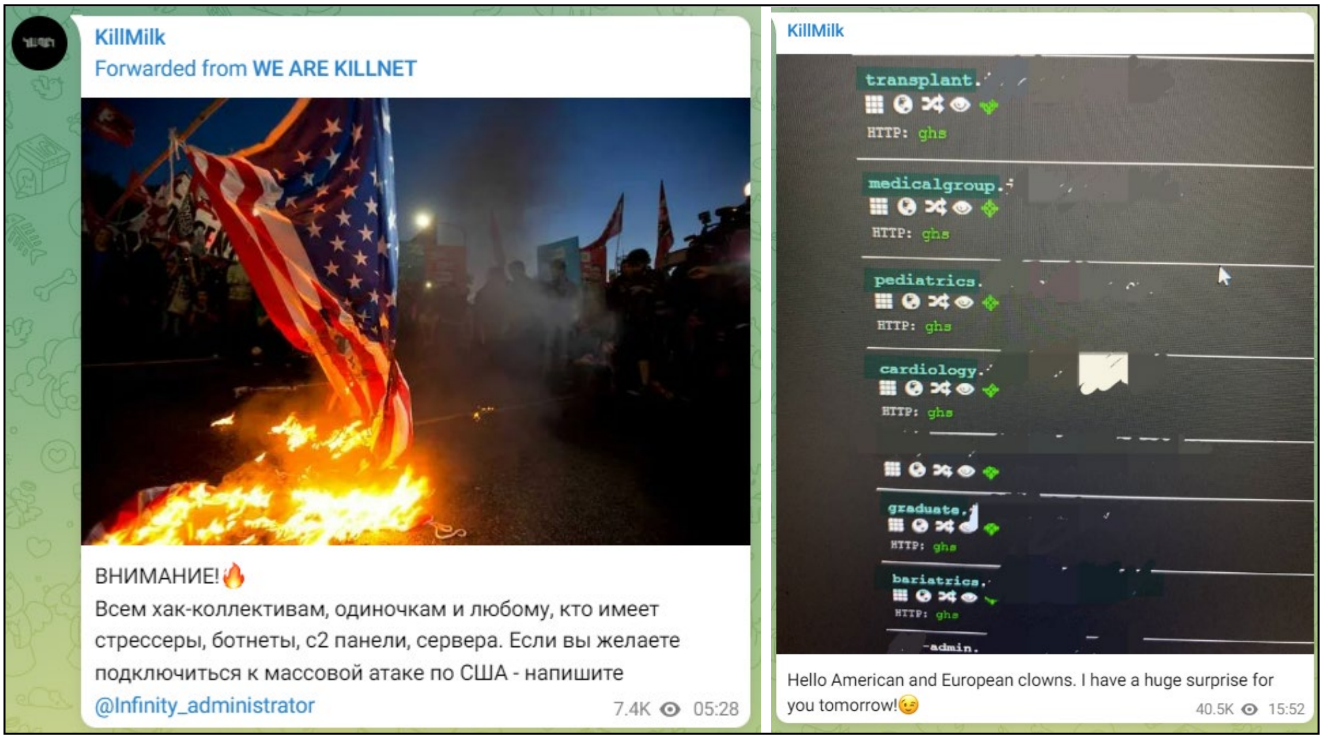
Abrazo Arizona Heart Hospital
https://www.abrazohealth.com/

St. Bernards Medical Center, Арканзас
https://www.stbernards.info/

AtlantiCare
https://www.atlanticare.org/

Figure 7: KillMilk threatens specific U.S. medical organizations. Not pictured: other countries' medical organizations also threatened include Finland, Germany, the Netherlands, Norway, Poland, Spain, and the United Kingdom. (January 28, 2023)

February 2023



KillMilk
Forwarded from WE ARE KILLNET

ВНИМАНИЕ!🔥
Всем хак-коллективам, одиночкам и любому, кто имеет стрессеры, ботнеты, с2 панели, сервера. Если вы желаете подключиться к массовой атаке по США - напишите @Infinity_administrator

7.4K 05:28

KillMilk

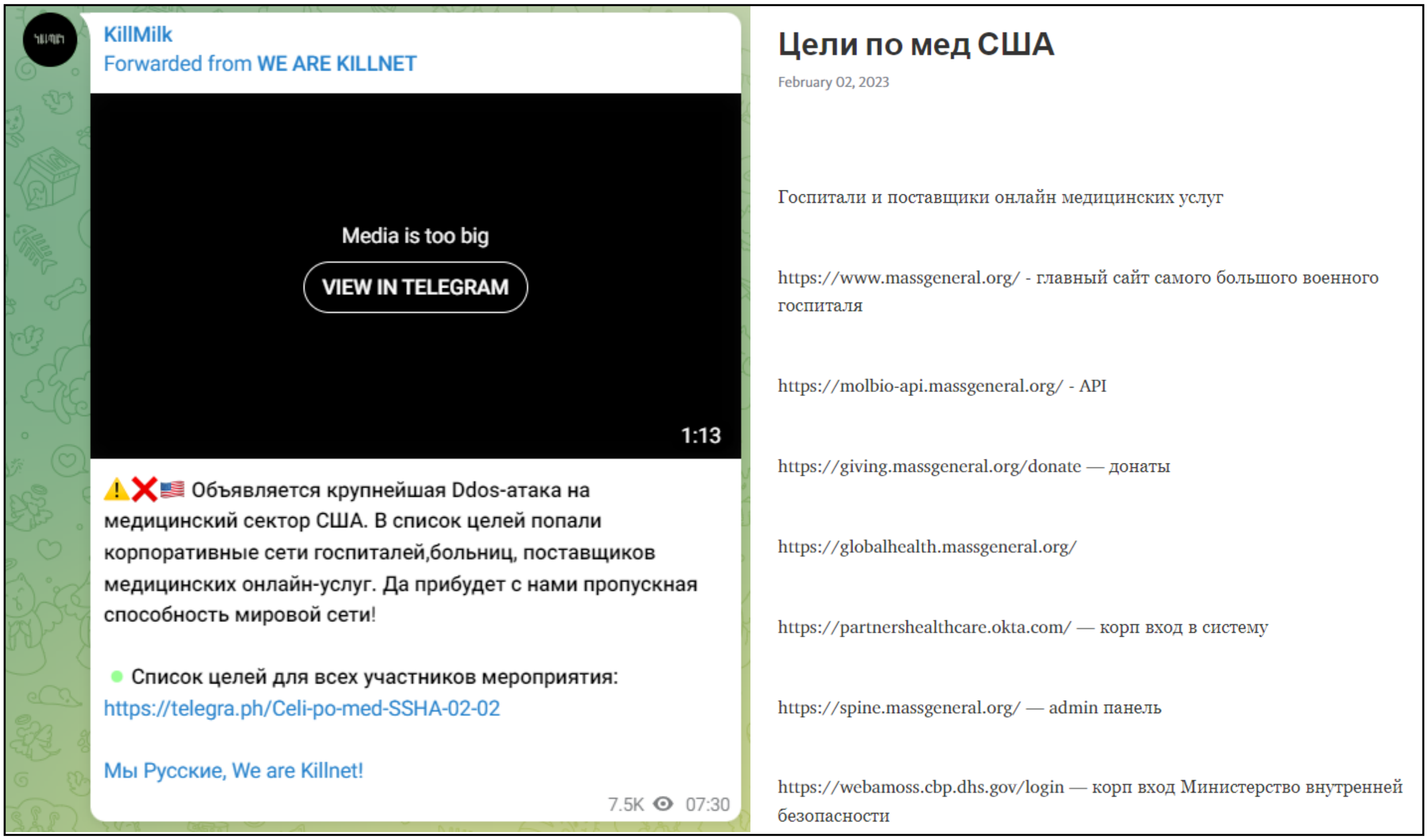
```
transplant.
HTTP: ghs
medicalgroup.
HTTP: ghs
pediatrics.
HTTP: ghs
cardiology.
HTTP: ghs

graduate.
HTTP: ghs
bariatrics.
HTTP: ghs
-admin.
```

Hello American and European clowns. I have a huge surprise for you tomorrow!😉

40.5K 15:52

Figure 8: KillNet posts open invitation to its affiliates to join mass attack on United States and includes medical-related screenshot announcement of a "huge surprise" for American and European audiences. (February 1, 2023)



KillMilk
Forwarded from WE ARE KILLNET

⚠️❌🇺🇸 Объявляется крупнейшая Ddos-атака на медицинский сектор США. В список целей попали корпоративные сети госпиталей,больниц, поставщиков медицинских онлайн-услуг. Да прибудет с нами пропускная способность мировой сети!

🟢 Список целей для всех участников мероприятия:
https://telegra.ph/Celi-po-med-SSHA-02-02

Мы Русские, We are Killnet!

7.5K 👁 07:30

Цели по мед США

February 02, 2023

Госпитали и поставщики онлайн медицинских услуг

https://www.massgeneral.org/ - главный сайт самого большого военного госпиталя

https://molbio-api.massgeneral.org/ - API

https://giving.massgeneral.org/donate — донаты

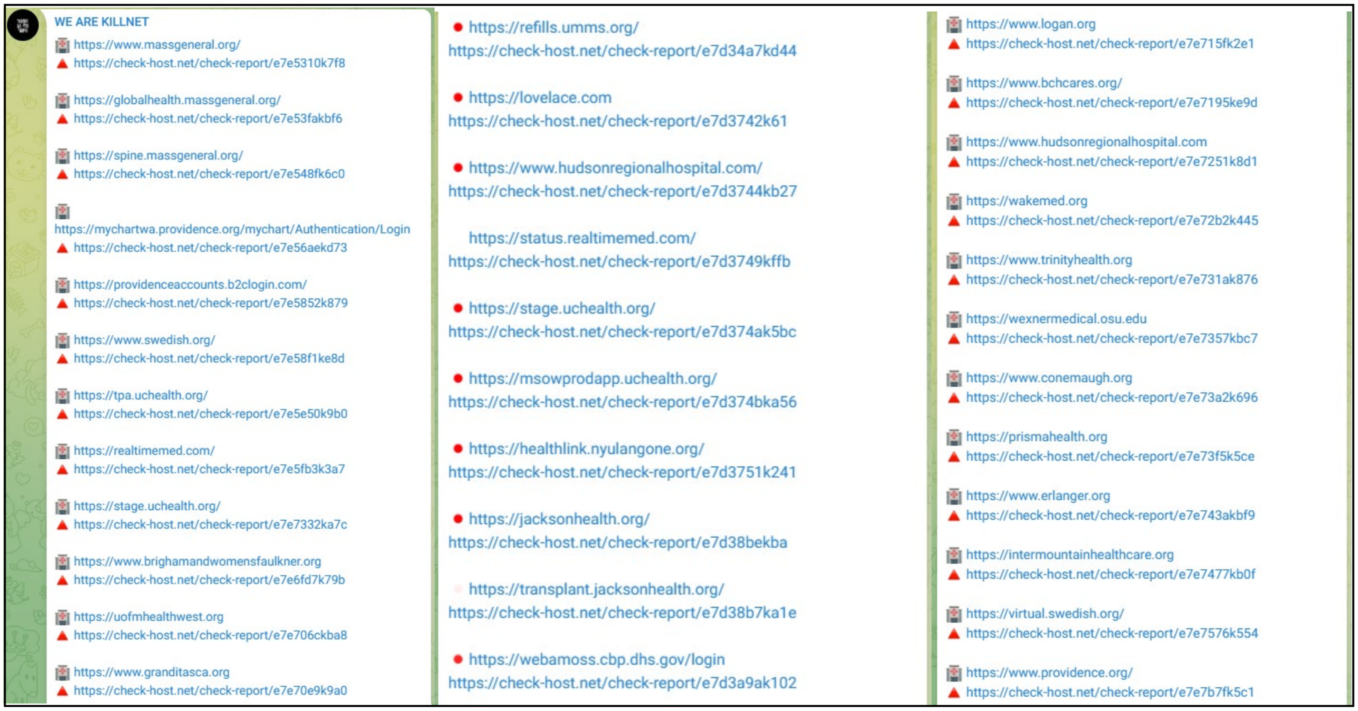
https://globalhealth.massgeneral.org/

https://partnershealthcare.okta.com/ — корп вход в систему

https://spine.massgeneral.org/ — admin панель

https://webamoss.cbp.dhs.gov/login — корп вход Министерство внутренней безопасности

Figure 9: KillMilk announces DDoS attack on specific U.S. HPH sector organizations. (February 2, 2023)



WE ARE KILLNET

🏥 https://www.massgeneral.org/
▲ https://check-host.net/check-report/e7e5310k7f8

🏥 https://globalhealth.massgeneral.org/
▲ https://check-host.net/check-report/e7e53fakbf6

🏥 https://spine.massgeneral.org/
▲ https://check-host.net/check-report/e7e548fk6c0

🏥
https://mychartwa.providence.org/mychart/Authentication/Login
▲ https://check-host.net/check-report/e7e56aekd73

🏥 https://providenceaccounts.b2clogin.com/
▲ https://check-host.net/check-report/e7e5852k879

🏥 https://www.swedish.org/
▲ https://check-host.net/check-report/e7e58f1ke8d

🏥 https://tpa.uchealth.org/
▲ https://check-host.net/check-report/e7e5e50k9b0

🏥 https://realtimemed.com/
▲ https://check-host.net/check-report/e7e5fb3k3a7

🏥 https://stage.uchealth.org/
▲ https://check-host.net/check-report/e7e7332ka7c

🏥 https://www.brighamandwomensfaulkner.org
▲ https://check-host.net/check-report/e7e6fd7k79b

🏥 https://uofmhealthwest.org
▲ https://check-host.net/check-report/e7e706ckba8

🏥 https://www.granditasca.org
▲ https://check-host.net/check-report/e7e70e9k9a0

● https://refills.umms.org/
https://check-host.net/check-report/e7d34a7kd44

● https://lovelace.com
https://check-host.net/check-report/e7d3742k61

● https://www.hudsonregionalhospital.com/
https://check-host.net/check-report/e7d3744kb27

https://status.realtimemed.com/
https://check-host.net/check-report/e7d3749kffb

● https://stage.uchealth.org/
https://check-host.net/check-report/e7d374ak5bc

● https://msowprodapp.uchealth.org/
https://check-host.net/check-report/e7d374bka56

● https://healthlink.nyulangone.org/
https://check-host.net/check-report/e7d3751k241

● https://jacksonhealth.org/
https://check-host.net/check-report/e7d38bekba

https://transplant.jacksonhealth.org/
https://check-host.net/check-report/e7d38b7ka1e

● https://webamoss.cbp.dhs.gov/login
https://check-host.net/check-report/e7d3a9ak102

🏥 https://www.logan.org
▲ https://check-host.net/check-report/e7e715fk2e1

🏥 https://www.bchcares.org/
▲ https://check-host.net/check-report/e7e7195ke9d

🏥 https://www.hudsonregionalhospital.com
▲ https://check-host.net/check-report/e7e7251k8d1

🏥 https://wakemed.org
▲ https://check-host.net/check-report/e7e72b2k445

🏥 https://www.trinityhealth.org
▲ https://check-host.net/check-report/e7e731ak876

🏥 https://wexnermedical.osu.edu
▲ https://check-host.net/check-report/e7e7357kbc7

🏥 https://www.conemaugh.org
▲ https://check-host.net/check-report/e7e73a2k696

🏥 https://prismahealth.org
▲ https://check-host.net/check-report/e7e73f5k5ce

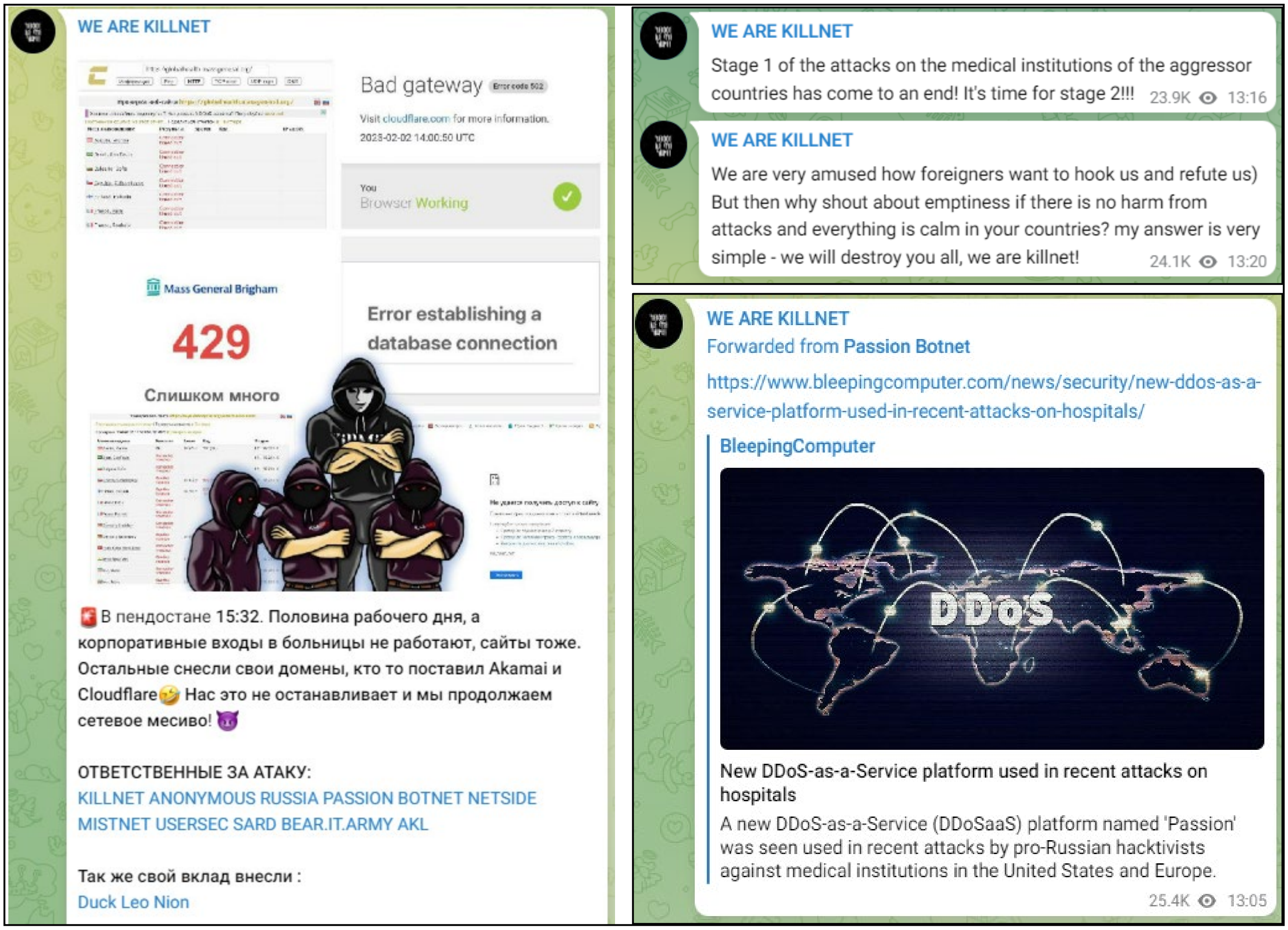
🏥 https://www.erlanger.org
▲ https://check-host.net/check-report/e7e743akbf9

🏥 https://intermountainhealthcare.org
▲ https://check-host.net/check-report/e7e7477kb0f

🏥 https://virtual.swedish.org/
▲ https://check-host.net/check-report/e7e7576k554

🏥 https://www.providence.org/
▲ https://check-host.net/check-report/e7e7b7fk5c1

Figure 10: KillNet announces more intended targets in disruption to HPH sector. (February 2, 2023)



WE ARE KILLNET

🚨В пендостане 15:32. Половина рабочего дня, а корпоративные входы в больницы не работают, сайты тоже. Остальные снесли свои домены, кто то поставил Akamai и Cloudflare🤣 Нас это не останавливает и мы продолжаем сетевое месиво! 😈

ОТВЕТСТВЕННЫЕ ЗА АТАКУ:
KILLNET ANONYMOUS RUSSIA PASSION BOTNET NETSIDE MISTNET USERSEC SARD BEAR.IT.ARMY AKL

Так же свой вклад внесли :
Duck Leo Nion

WE ARE KILLNET

Stage 1 of the attacks on the medical institutions of the aggressor countries has come to an end! It's time for stage 2!!! 23.9K 13:16

WE ARE KILLNET

We are very amused how foreigners want to hook us and refute us) But then why shout about emptiness if there is no harm from attacks and everything is calm in your countries? my answer is very simple - we will destroy you all, we are killnet! 24.1K 13:20

WE ARE KILLNET
Forwarded from Passion Botnet

https://www.bleepingcomputer.com/news/security/new-ddos-as-a-service-platform-used-in-recent-attacks-on-hospitals/

BleepingComputer

New DDoS-as-a-Service platform used in recent attacks on hospitals

A new DDoS-as-a-Service (DDoSaaS) platform named 'Passion' was seen used in recent attacks by pro-Russian hacktivists against medical institutions in the United States and Europe.

25.4K 13:05

Figure 11: KillNet posts announcing disruption to HPH sector, the end of Stage 1 of their DDoS attacks on the medical institutions of "aggressor countries," and shares a Bleeping Computer article on their recent DDoS campaign. (February 2, 2023)

March 2023

Few incidents in the HPH sector have been attributed to KillNet this month, with the exception of a DDoS attack on a laboratory, blood, and pharmaceutical sub-industry organization. While little to no content on their Telegram channel could be found that indicated a targeting of the sector, one information security publication unveiled a campaign that had gone previously unnoticed. On March 17, 2023, Microsoft Security published its observations that KillNet had been targeting healthcare applications using the Microsoft Azure infrastructure for over three months.

The findings illuminated new trends on KillNet and other hacktivist organizations' characteristic DDoS campaigns in Azure from November 18, 2022 to February 17, 2023. Of those, Microsoft observed:

- An increase from 10-20 attacks in November to 40-60 attacks daily in February.
- The types of HPH organizations attacked included pharma and life sciences with 31% of all attacks, hospitals with 26%, healthcare insurance with 16%, and health services and care also with 16%.
- In contrast to overall DDoS attack trends for 2022, in which Transmission Control Protocol (TCP) was the most common attack vector, 53% of the attacks on healthcare were User Datagram

Protocol (UDP) floods, and TCP accounted for 44%, reflecting a different mixture of attack patterns used by adversaries.

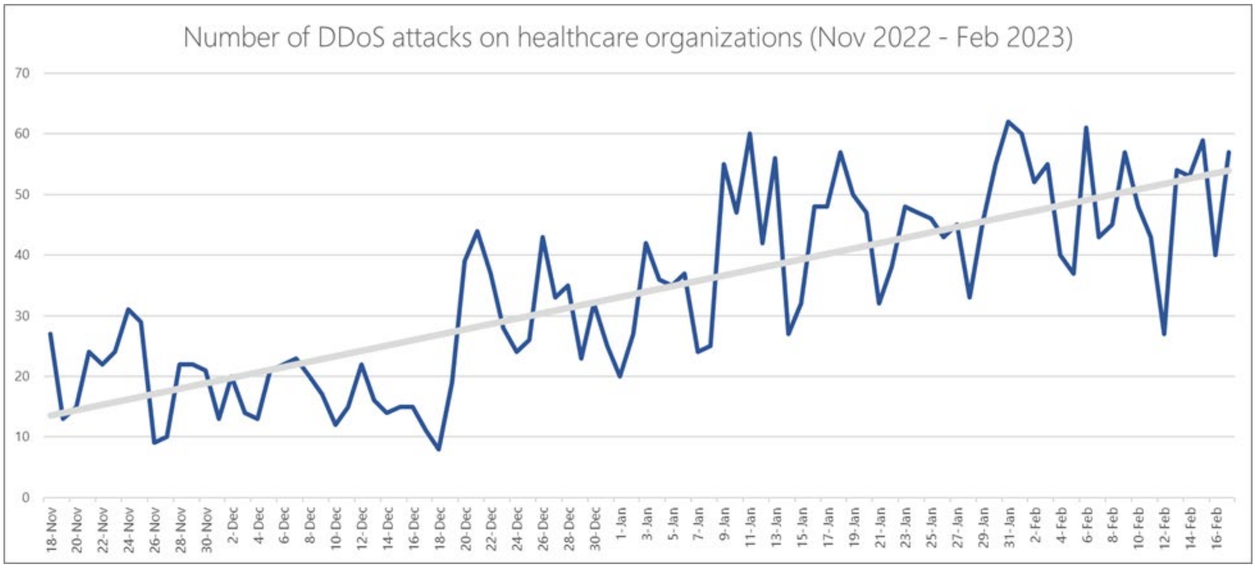


Figure 12: Microsoft Security graph of DDoS attacks on healthcare applications in Azure. (March 17, 2023)

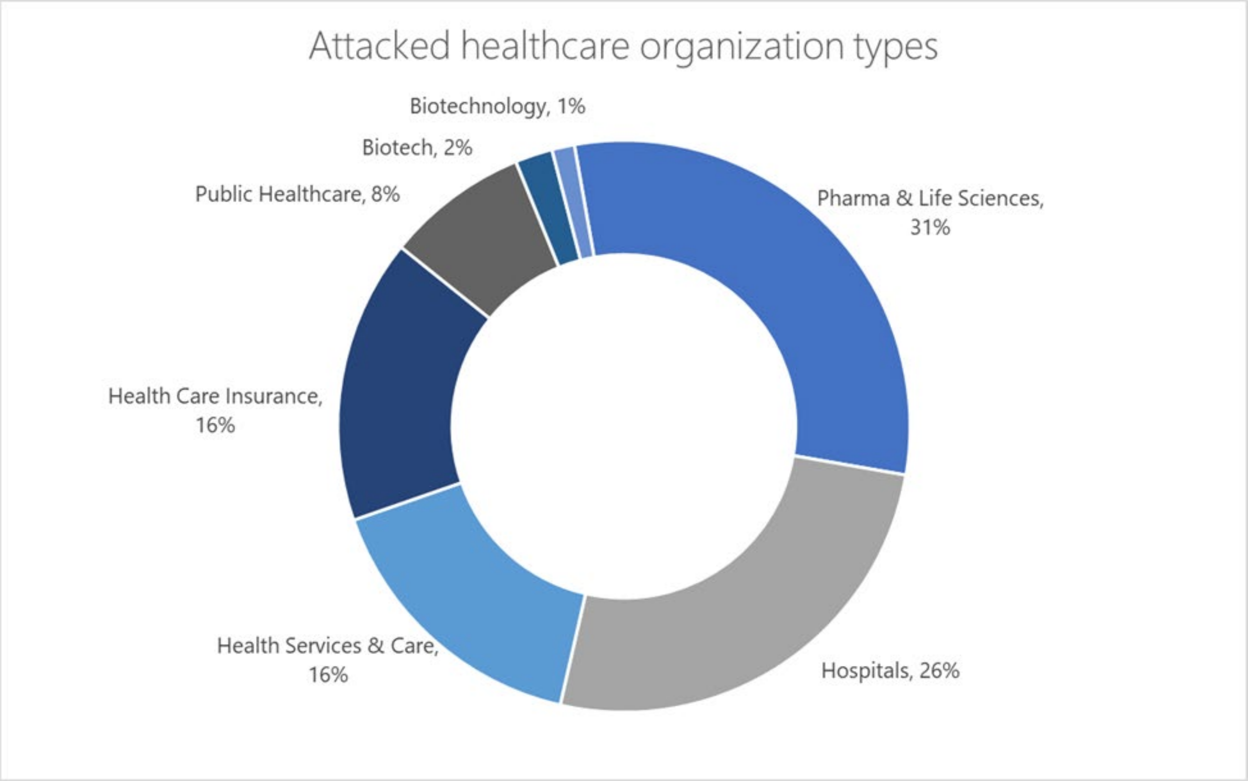
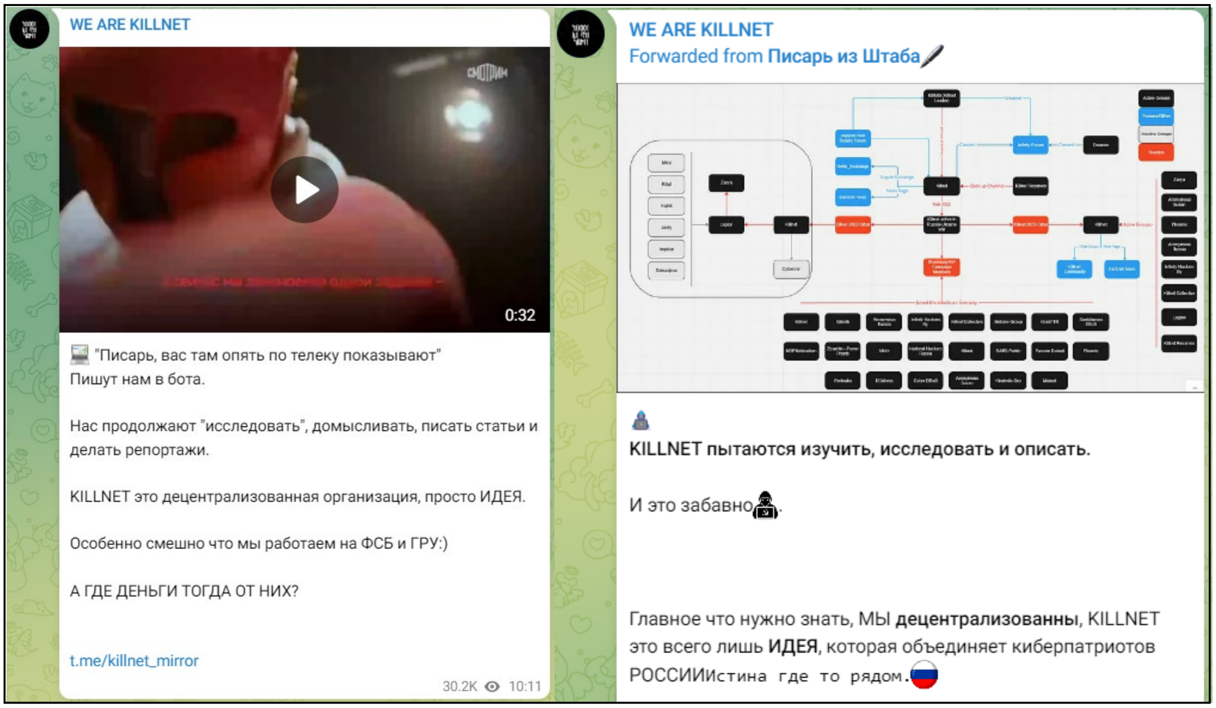


Figure 13: Microsoft Security graph of types of healthcare organizations targeted by DDoS attacks. (March 17, 2023)

Leadership and Key Individuals

On January 24, 2022, the Telegram channel "We are KillNet" was created, offering a DDoS/Stressor tool on various URLs. Ostensibly, KillNet appears to have a semi-formal organization, founded by KillMilk, with over 90,000 followers on their Telegram channel. The group collaborates with and recruits affiliates with similar ideologies or goals that align with Russian interests. Demonstrating that the group is acutely aware of their online image, KillNet recently rebuked one online analysis of their organizatonal structure, or lack thereof. In a March 21, 2023 post, the group emphasized that they are decentralized, that KillNet is just an “idea” that unites the cyber patriots of Russia, and that they are not supported by the [Russian] state.



WE ARE KILLNET

💻 "Писарь, вас там опять по телеку показывают"
Пишут нам в бота.

Нас продолжают "исследовать", домысливать, писать статьи и делать репортажи.

KILLNET это децентрализованная организация, просто ИДЕЯ.

Особенно смешно что мы работаем на ФСБ и ГРУ:)

А ГДЕ ДЕНЬГИ ТОГДА ОТ НИХ?

t.me/killnet_mirror

30.2K 👁 10:11

WE ARE KILLNET
Forwarded from **Писарь из Штаба**

KILLNET пытаются изучить, исследовать и описать.

И это забавно.

Главное что нужно знать, МЫ **децентрализованны**, KILLNET это всего лишь **ИДЕЯ**, которая объединяет киберпатриотов РОССИИИстина где то рядом.

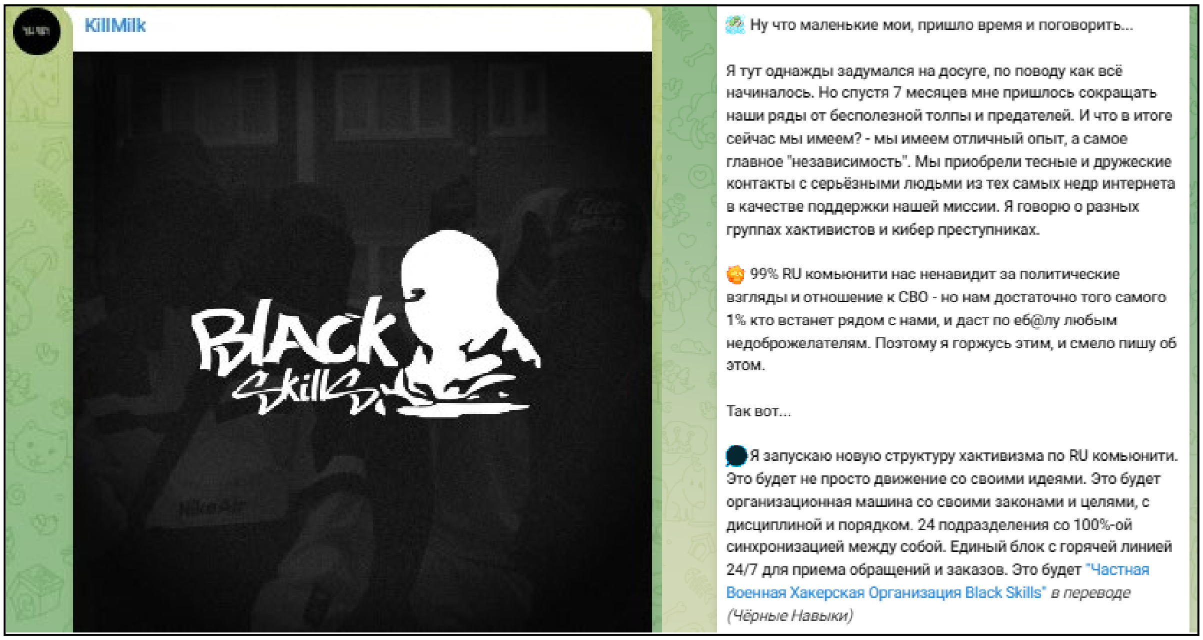
Figure 14: KillNet rebukes Medium user, CyberKnow’s claim that they have an organizational structure. (February 25, 2023 and March 21, 2023)

Ironically, this comes just one week after another KillMilk post detailing his creation of a new private military hacking company, Black Skills. The new group appears to be highly organized and structured with 24 “departments” in charge of various distinct functions such as intelligence, public relations, investments, accounting, and general staff. Adding more formality to the initiative, KillMilk even requires every applicant to list their skills whether they have served in the military or as public servants in a formal questionnaire. It remains unknown whether this is a rebranding of KillNet or an organizational initiative to better separate more skilled members from the rest of the community. Undeniably, however, is the fact that since the February 2022 Russian invasion of Ukraine, KillNet and its leader, KillMilk have garnered support from other hacktivist organizations, making them leaders in the cybercriminal underworld.

KillMilk, left the group on July 27, 2022, seemingly, to recruit a new group, but both continue to share the others’ posts on Telegram, indicating some level of support still exists. KillMilk’s next day post, “*What I would do for my country now would be dangerous enough for my team. So I made the decision to withdraw from KillNet for their own safety*[.]” signals a possible departure due to threat from law enforcement. A similar trend can be seen across other pro-Russian hacktivist groups like Evil Corp and Conti, which splintered into smaller groups and rebranded to evade law enforcement. A Mandiant report also reinforced this trend of loosely connected Russia-linked ransomware groups splintering into smaller cells to obscure their identities and evade crackdowns. Though not much is known about the threat actor, the group’s new leader is a hacker using the name Blackside, and specializes in ransomware, phishing, and crypto theft.

Nomenclature and Associations

A post of KillNet's January 24, 2023 DDoS campaign against Germany highlighted many of their current affiliates, among them, Infinity Hackers, ANONYMOUS RUSSIA, Killnet Collective, NETSIDE GROUP, National Hackers Russia, KILLMIR, Passion Botnet, and PHOENIX. This campaign, while not against the HPH sector, revealed that KillNet has a huge influence over over pro-Russian groups. However, in a March 12, 2023 posting on his Telegram channel, former KillNet leader, KillMilk, stated that he had to "shrink [their] ranks from useless mobs and traitors" in preparation for the new Black Skills organization. On March 26, 2023, KillMilk subsequently announced that KillNet had undergone a reform of personnel. It is still unknown how KillNet's proposed reorganization will pan out, but owing to their successful attack record and the current admiration they have online and across several Russian media outlets, it is likely they will continue to grow in size and support.



Ну что маленькие мои, пришло время и поговорить...

Я тут однажды задумался на досуге, по поводу как всё начиналось. Но спустя 7 месяцев мне пришлось сокращать наши ряды от бесполезной толпы и предателей. И что в итоге сейчас мы имеем? - мы имеем отличный опыт, а самое главное "независимость". Мы приобрели тесные и дружеские контакты с серьёзными людьми из тех самых недр интернета в качестве поддержки нашей миссии. Я говорю о разных группах хактивистов и кибер преступниках.

99% RU комьюнити нас ненавидит за политические взгляды и отношение к СВО - но нам достаточно того самого 1% кто встанет рядом с нами, и даст по еб@лу любым недоброжелателям. Поэтому я горжусь этим, и смело пишу об этом.

Так вот...

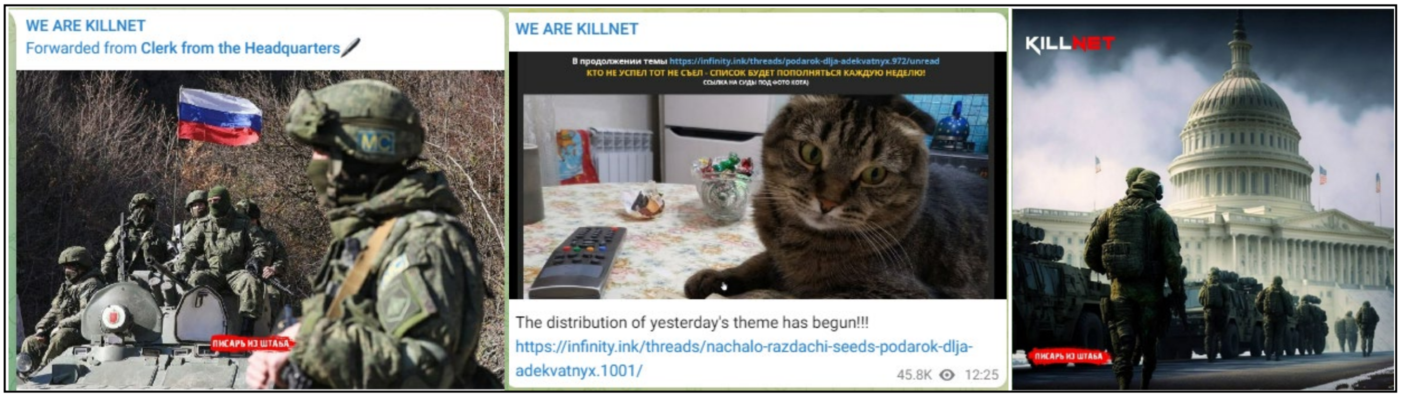
Я запускаю новую структуру хактивизма по RU комьюнити. Это будет не просто движение со своими идеями. Это будет организационная машина со своими законами и целями, с дисциплиной и порядком. 24 подразделения со 100%-ой синхронизацией между собой. Единый блок с горячей линией 24/7 для приема обращений и заказов. Это будет "Частная Военная Хакерская Организация Black Skills" *в переводе (Чёрные Навыки)*

Figure 15: KillMilk announces creation of private military hacking company, Black Skills, a 24/7 single unit made up of 24 divisions with its own laws and goals. (March 12, 2023)

Unlike the skilled hackers working for Russia's security services' groups like Fancy Bear and Sandworm, KillNet is radically different. Behaving in a more reactionary manner, the group of hactivists oftentimes appear to work in an emotional way, seeking revenge and retaliation against anything perceived as anti-Russia or pro-Ukraine, given the current conflict between the two powers. While KillNet has been criticized on some forums for perceiving to be seeking cooperation from Russian security services, any ties to official Russian government organizations such as the Federal Security Service (FSB) or the Foreign Intelligence Service (SVR) remain unconfirmed.

Motivations

KillNet is hardly subtle in its political agenda. Since the group's inception, they have always exhibited a pro-Russia or pro-Slavic state stance. This has garnered the support and coalescence of Russian and other Slavic hacktivist groups like the Belarusian Infinity Hackers. The promotion of a pro-Slavic sentiment, however, began to waver with the Russian invasion of Ukraine this past year, creating a new anti-Ukraine theme and strenghtening their pro-Russian military theme. This, in turn, spurned a political antagonism toward any country or group that displayed or provided support to Ukraine during the conflict. While not exclusively their main target, the United States has historically been the “Main Enemy” to Russia during the Cold War. This anti-American posture breeds over into modern times, and especially in the cyberspace.



WE ARE KILLNET
Forwarded from Clerk from the Headquarters

WE ARE KILLNET

В продолжении темы https://infinity.ink/threads/podarok-dlja-adekvatnyx.972/unread
КТО НЕ УСПЕЛ ТОТ НЕ СЪЕЛ - СПИСОК БУДЕТ ПОПОЛНЯТЬСЯ КАЖДУЮ НЕДЕЛЮ!
ССЫЛКА НА СИДЫ ПОД ФОТО КОТА)

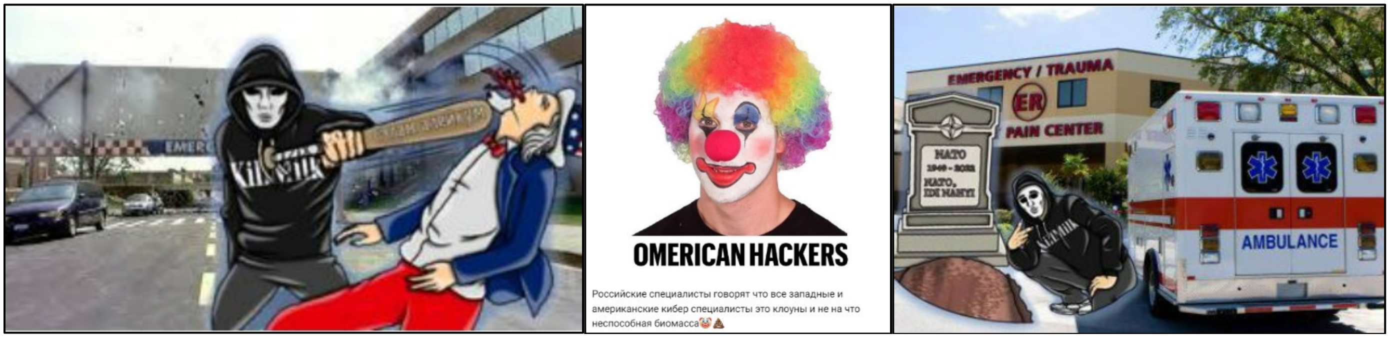
The distribution of yesterday's theme has begun!!!
https://infinity.ink/threads/nachalo-razdachi-seeds-podarok-dlja-adekvatnyx.1001/
45.8K 12:25

Figure 16: Sample postings from KillNet's Telegram channel displaying pro-Russia/Russian military, feline, and anti-American themes.

Interestingly, amongst the repository of boastful threats and attacks that KillNet and KillMilk both post on their separate Telegram channels, are numerous photo postings of cats or kittens that seemingly have no added strategic value, other than the fact that they like them. One such posting on January 23, 2023 even doxxes a Russian national and his parents for allegedly killing a cat. KillNet’s doxxing of a Russian national provides validation that they are more aligned with statecraft-level Russian support, but will make exceptions for low-level incidents that provoke offense.

In their assessment, SOCRadar reports that KillNet does not seem to be interested in financial gain. This is supported by donation links on and a review of their Telegram channel, where several posts ask for donations to support their network of hacktivists. However, like nearly all hacktivist groups, they aim to disrupt and harm organizations and critical infrastructure to procure a ransom.

Common Tactics, Techniques, and Procedures (TTPs)



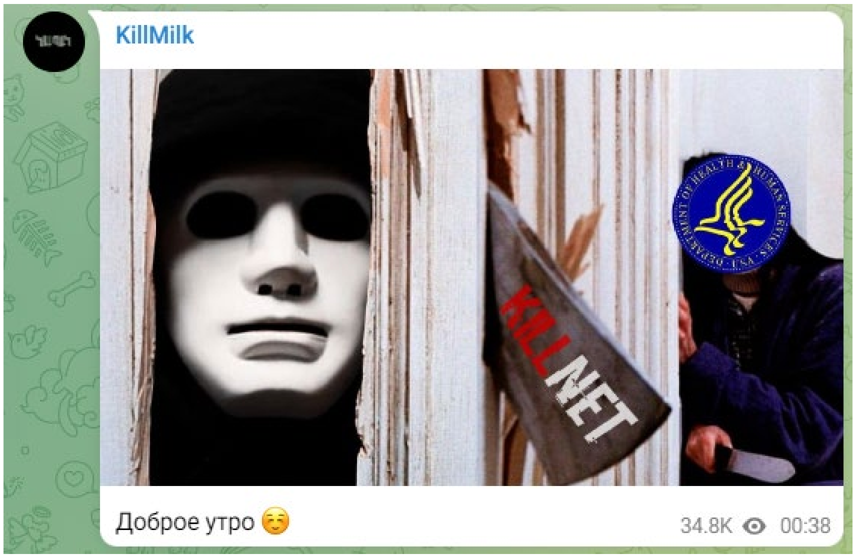
Российские специалисты говорят что все западные и американские кибер специалисты это клоуны и не на что неспособная биомасса🤡💩

Figure 17: Sample Anti-American and threatening healthcare memes from KillNet Telegram Channel.

In their March 2023 analysis, Microsoft Security highlighted that while KillNet uses DDoS as its main tool, they noted that that kind of attack method is a relatively easy, low-cost, and anonymous method of disrupting online services and websites. More so, KillNet and other similar hacktivist groups utilize them to draw attention than to do any major damage. Typically lasting less than 12 hours, attack vectors included TCP SYN, TCP ACK, and packet anomalies. KillNet and its affiliates likely launch attacks using DDoS scripts and stressors, recruiting botnets, and utilizing spoofed attack sources.

Like Russian security services, KillNet adopts similar active measure techniques in the form of propaganda, misinformation, and disinformation. In one Russian media interview on October 9, 2022, KillMilk continued his anti-American claims, stating in a media interview that his group had evidence that the United States created [the] COVID-19 [virus].

On their Telegram channels, both KillMilk and KillNet show that they are adroit in graphic design and have a penchant for using novel or "millenial" ways of announcing boastful threats or attacks, to include memes, gifs, emojis, and short edited videos. Demonstrating their hostility to the U.S. HPH sector, on February 4, 2023, five days after the release of HC3's most recent Analyst Note on KillNet, former leader, KillMilk, posted a meme that seemingly threatened the U.S. Department of Health and Human Services (HHS). Whether signaling a future warning to HHS writ large or coincidentally in response to the Analyst Note, it has already been shown that the hacktivist group remains aware of open source articles or publications about their group (namely, from Medium user, CyberKnow, and online publicaton, SOCRadar).

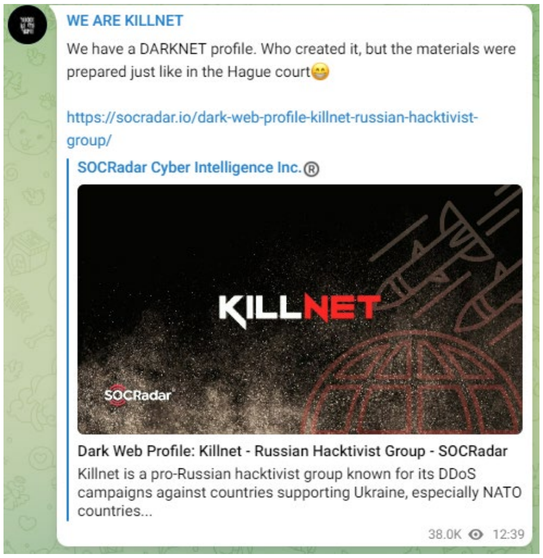


KillMilk

Доброе утро ☺️

34.8K 00:38

Figure 18: KillMilk meme threatening HHS. (February 4, 2023)



WE ARE KILLNET

We have a DARKNET profile. Who created it, but the materials were prepared just like in the Hague court😁

https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

SOCRadar Cyber Intelligence Inc.®

Dark Web Profile: Killnet - Russian Hacktivist Group - SOCRadar

Killnet is a pro-Russian hacktivist group known for its DDoS campaigns against countries supporting Ukraine, especially NATO countries...

38.0K 12:39

Figure 19: KillNet acknowledges SOCRadar's analysis product of threat group. (December 17, 2022)

As of March 30, 2023, a simple Google search for "KillNet" in English reveals that HC3's previous Analyst Note on the group is the top third result. KillNet, KillMilk, and their affiliates' proficiency in English on their Telegram channel demonstrate that their members have some degree of open source situational awareness. This was reinforced when they acknowledged postings of SOCRadar's analysis of the threat group on December 17, 2022 and Medium user, CyberKnow's, analysis of the group on March 21, 2023.

In their analysis, SOCRadar defined several of their prominent characteristics and TTPs of the group:

- Due to its motivation and determination to defend Russia, the group chose its targets among NATO-linked countries. It is also a potential threat to countries whose political interests contradict Russia.
- They prefer DDoS attacks against their targets. Victims can recover their systems from attacks, which usually take 1-3 days, with appropriate measures in a matter of hours.
- They target websites of governments or public institutions. This way, they think that they signal to the victims that the victims chose the "wrong side."
- They announce their attacks and targets on Telegram channels.

- They are associated with other hacker groups that have common goals or act in Russian interests.

Defense and Mitigations

There is no single action that can protect an organization from cyber threat groups, such as KillNet. Nevertheless, healthcare organizations need to take proactive measures to mitigate against a wide variety of attacks like DDoS. This Analyst Note presents a sample of mitigations, countermeasures, indicators of compromise, and other courses of action from various cybersecurity organizations and governmental publications as a guide to better prepare themselves against threats.

CISA Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

Health-ISAC – Distributed Denial of Service (DDoS) Attacks
https://h-isac.org/distributed-denial-of-service-ddos-attacks/

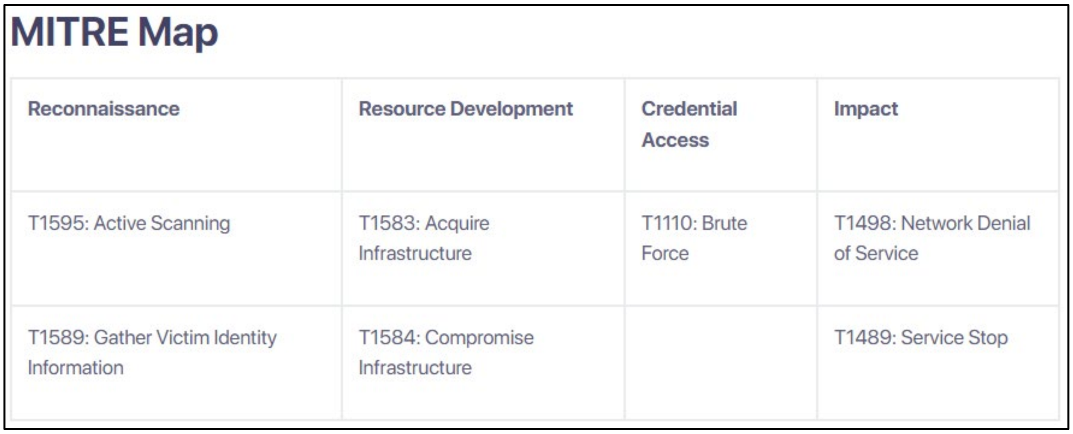
Microsoft Security
https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

Palo Alto Network – Unit 42
https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/#how-you-should-prepare-for-cyber-impact

SOCRadar
https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

MITRE ATT&CK

SOCRadar lists two reconnaissance techniques for KillNet from MITRE ATT&CK's map: Active Scanning and Gather Victim Identity Information.



MITRE Map

Reconnaissance	Resource Development	Credential Access	Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1110: Brute Force	T1498: Network Denial of Service
T1589: Gather Victim Identity Information	T1584: Compromise Infrastructure		T1489: Service Stop

Figure 20: MITRE Map of KillNet. (SOCRadar)

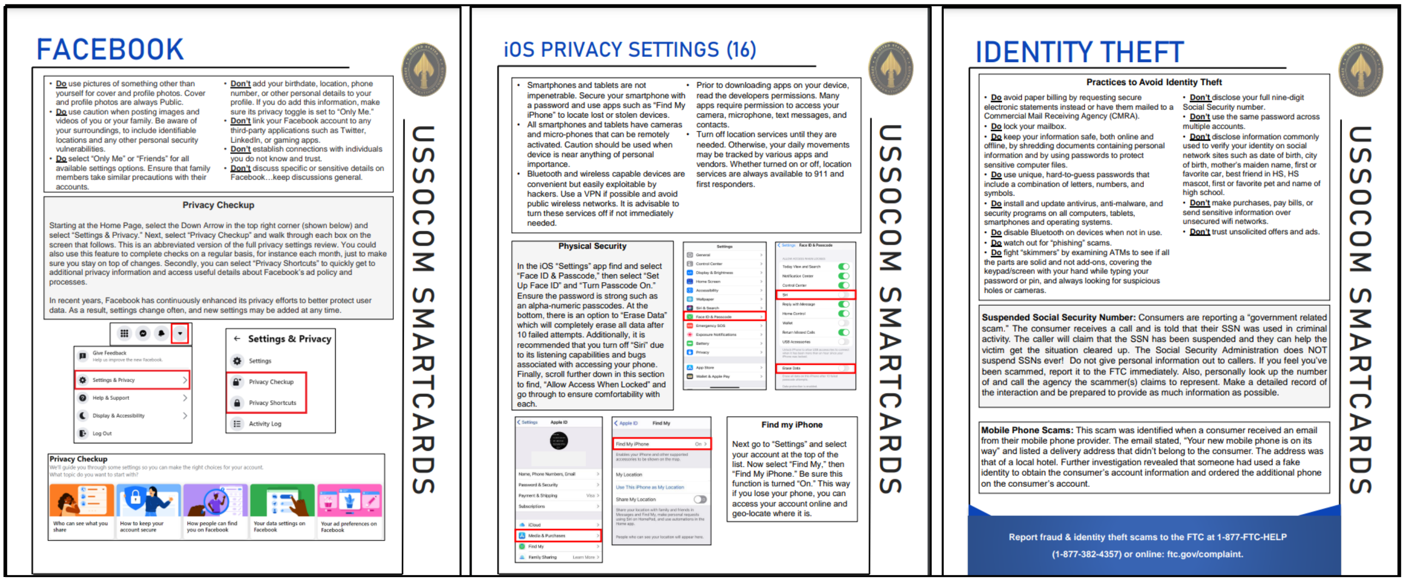
Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction. This technique can easily be mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Adversaries may also gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via phishing for information. Information about users could also be enumerated via other active means such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. Information about victims may also be exposed to adversaries via online or other accessible data sets. This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the among and sensitivity of data available to external parties.

Identity Management

One of the easiest ways for hacktivists to get information about you is through your online presence. Anyone can research you with just a few clicks of the mouse and a quick Internet search. It is important to know what is publicly available about yourself, and then decide what to do about unwanted information. One such way is through Identity Management (IdM), a program that could be utilized by HPH sector employees to proactively protect themselves against KillNet's and other hacktivists' Gather Victim Identity Information reconnaissance technique.

IdM consists of the discovery, analysis, and management of an individual or organization's identity elements, characteristics, and/or other attributes in public and non-public records, social media, and other unstructured data sources. IdM programs seek to improve an organization's ability to mitigate current threats to its mission, capabilities, and personnel from adversarial and/or criminal entities seeking to exploit identity data, as well as identify emerging threats to organizational assets.



FACEBOOK

- **Do** use pictures of something other than yourself for cover and profile photos. Cover and profile photos are always Public.
- **Do** use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- **Do** select "Only Me" or "Friends" for all available settings options. Ensure that family members take similar precautions with their accounts.
- **Don't** add your birthdate, location, phone number, or other personal details to your profile. If you do add this information, make sure its privacy toggle is set to "Only Me."
- **Don't** link your Facebook account to any third-party applications such as Twitter, LinkedIn, or gaming apps.
- **Don't** establish connections with individuals you do not know and trust.
- **Don't** discuss specific or sensitive details on Facebook…keep discussions general.

Privacy Checkup

Starting at the Home Page, select the Down Arrow in the top right corner (shown below) and select "Settings & Privacy." Next, select "Privacy Checkup" and walk through each box on the screen that follows. This is an abbreviated version of the full privacy settings review. You could also use this feature to complete checks on a regular basis, for instance each month, just to make sure you stay on top of changes. Secondly, you can select "Privacy Shortcuts" to quickly get to additional privacy information and access useful details about Facebook's ad policy and processes.

In recent years, Facebook has continuously enhanced its privacy efforts to better protect user data. As a result, settings change often, and new settings may be added at any time.

Give Feedback
Help us improve the new Facebook.
Settings & Privacy
Help & Support
Display & Accessibility
Log Out
Settings & Privacy
Settings
Privacy Checkup
Privacy Shortcuts
Activity Log
Privacy Checkup
We'll guide you through some settings so you can make the right choices for your account.
What topic do you want to start with?
Who can see what you share
How to keep your account secure
How people can find you on Facebook
Your data settings on Facebook
Your ad preferences on Facebook

USSOCOM SMARTCARDS

iOS PRIVACY SETTINGS (16)

- Smartphones and tablets are not impenetrable. Secure your smartphone with a password and use apps such as "Find My iPhone" to locate lost or stolen devices.
- All smartphones and tablets have cameras and micro-phones that can be remotely activated. Caution should be used when device is near anything of personal importance.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks. It is advisable to turn these services off if not immediately needed.
- Prior to downloading apps on your device, read the developers permissions. Many apps require permission to access your camera, microphone, text messages, and contacts.
- Turn off location services until they are needed. Otherwise, your daily movements may be tracked by various apps and vendors. Whether turned on or off, location services are always available to 911 and first responders.

Physical Security

In the iOS "Settings" app find and select "Face ID & Passcode," then select "Set Up Face ID" and "Turn Passcode On." Ensure the password is strong such as an alpha-numeric passcodes. At the bottom, there is an option to "Erase Data" which will completely erase all data after 10 failed attempts. Additionally, it is recommended that you turn off "Siri" due to its listening capabilities and bugs associated with accessing your phone. Finally, scroll further down in this section to find, "Allow Access When Locked" and go through to ensure comfortability with each.

Find my iPhone

Next go to "Settings" and select your account at the top of the list. Now select "Find My," then "Find My iPhone." Be sure this function is turned "On." This way if you lose your phone, you can access your account online and geo-locate where it is.

USSOCOM SMARTCARDS

IDENTITY THEFT

Practices to Avoid Identity Theft

- **Do** avoid paper billing by requesting secure electronic statements instead or have them mailed to a Commercial Mail Receiving Agency (CMRA).
- **Do** lock your mailbox.
- **Do** keep your information safe, both online and offline, by shredding documents containing personal information and by using passwords to protect sensitive computer files.
- **Do** use unique, hard-to-guess passwords that include a combination of letters, numbers, and symbols.
- **Do** install and update antivirus, anti-malware, and security programs on all computers, tablets, smartphones and operating systems.
- **Do** disable Bluetooth on devices when not in use.
- **Do** watch out for "phishing" scams.
- **Do** fight "skimmers" by examining ATMs to see if all the parts are solid and not add-ons, covering the keypad/screen with your hand while typing your password or pin, and always looking for suspicious holes or cameras.
- **Don't** disclose your full nine-digit Social Security number.
- **Don't** use the same password across multiple accounts.
- **Don't** disclose information commonly used to verify your identity on social network sites such as date of birth, city of birth, mother's maiden name, first or favorite car, best friend in HS, HS mascot, first or favorite pet and name of high school.
- **Don't** make purchases, pay bills, or send sensitive information over unsecured wifi networks.
- **Don't** trust unsolicited offers and ads.

Suspended Social Security Number: Consumers are reporting a "government related scam." The consumer receives a call and is told that their SSN was used in criminal activity. The caller will claim that the SSN has been suspended and they can help the victim get the situation cleared up. The Social Security Administration does NOT suspend SSNs ever! Do not give personal information out to callers. If you feel you've been scammed, report it to the FTC immediately. Also, personally look up the number of and call the agency the scammer(s) claims to represent. Make a detailed record of the interaction and be prepared to provide as much information as possible.

Mobile Phone Scams: This scam was identified when a consumer received an email from their mobile phone provider. The email stated, "Your new mobile phone is on its way" and listed a delivery address that didn't belong to the consumer. The address was that of a local hotel. Further investigation revealed that someone had used a fake identity to obtain the consumer's account information and ordered the additional phone on the consumer's account.

Report fraud & identity theft scams to the FTC at 1-877-FTC-HELP (1-877-382-4357) or online: ftc.gov/complaint.

USSOCOM SMARTCARDS

Figure 21: Sample IdM mitigation recommendation pages from DoD Social Media Smartcard booklet.

One sample toolset is the Department of Defense's (DoD) Social Media Smartcard booklet. This comprehensive and regularly updated publication covers how to effectively manage one's Social Networking Services (i.e., Facebook, dating apps, message-to-message apps, etc.), Digital Ecosystems (i.e., Amazon, Coinbase, YouTube, etc.), Devices (i.e., Android, iOS, gaming systems, etc.), and General Best Practices of recommendations and tips of online use for both adults and children. A link to the full booklet can be found here.

Relevant HHS Reports

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (May 9, 2022)

HC3: Alert - Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 1, 2022)

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector (January 30, 2023)

HC3: Analyst Note – Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector (December 22, 2022)

HC3: Analyst Note – The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector (March 1, 2022)

References

Azure Network Security Team. "KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks." Microsoft Security. March 17, 2023. https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

"'Black Skills' Is Killnet's Attempt to Form a 'Private Military Hacking Company.'" Flashpoint Team. March 14, 2023. https://flashpoint.io/blog/killnet-killmilk-private-military-hacking-company/

CISA – Stop Ransomware. "Ransomware Guide." CISA. Accessed March 24, 2023. https://www.cisa.gov/stopransomware/ransomware-guide

Davis, Jessica. "Passion botnet cyberattacks hit healthcare, as actors offer threat as DDoS-as-a-service." SC Media. February 2, 2023. https://www.scmagazine.com/analysis/cybercrime/passion-botnet-cyberattacks-hit-healthcare-as-actors-offer-threat-as-ddos-as-a-service

"KillNet Founder Leaves Hacktivist Group." GroupSense. July 29, 2022. https://www.groupsense.io/resources/killnet-founder-leaves-hactivist-group

"KillNet Group." BlackBerry Limited. Accessed March 21, 2023. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet#:~:text=In%20July%202022%2C%20KillNet%20leader,new%20head%20of%20the%20group.

Lee, Matthew and Lolita C. Baldor. "US sending $275 million in military aid to Ukraine. *The Associated Press*. December 8, 2022. https://apnews.com/article/russia-ukraine-jens-stoltenberg-government-united-states-and-politics-70d14a614b847b37038535e3251f92e6

Medium Account: Cyberknow. "Killnet 2023 [Order of Battle] ORBAT." Medium. March 8, 2023. https://cyberknow.medium.com/killnet-2023-orbat-a9584d5c6e66

Medium Account: Cyberknow. "KillNet: Pro-Russian Hacktivists." Medium. May 19, 2022. https://cyberknow.medium.com/killnet-pro-russian-hacktivists-e916ac7201a3

"Passion: A Russian Botnet." Radware. January 31, 2023. https://www.radware.com/security/ddos-threats-attacks/passion-russian-botnet/

Reshetnikova, Ksenia. "Основатель группы Killmilk заявил, что хакеры имеют на руках пакет доказательств о причастности США к мировой пандемии" [The founder of the group Killmilk said that hackers have in their hands a package of evidence about the involvement of the United States in the global pandemic]. *Social Media News*. October 9, 2022. https://sm.news/osnovatel-rossijskoj-gruppy-xakerov-killnet-zayavil-chto-ssha-prichastny-k-sozdaniyu-covid-19-71516-u3t5/

Roussi, Antoaneta. "Meet Killnet, Russia's hacking patriots plaguing Europe." Politico. September 9, 2022. https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

SOCRadar Research. "Dark Web Profile: Killnet – Russian Hacktivist Group." SOCRadar. December 16, 2022. https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/

Telegram Account: KillMilk. *Telegram*. Accessed March 2023. https://t.me/s/killmilk_rus

Telegram Account: WE ARE KILLNET. *Telegram*. Accessed March 2023. https://t.me/s/killnet_reservs

Unit 42. "Russia-Ukraine Cyberattacks (Updated): How to Protect Against Related Cyberthreats Including DDoS, HermeticWiper, Gamaredon, Website Defacement, Phishing and Scams." Palo Alto Networks. February 22, 2022. https://unit42.paloaltonetworks.com/preparing-for-cyber-impact-russia-ukraine-crisis/#how-you-should-prepare-for-cyber-impact

Vijayan, Jai. "Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows." DARKReading. February 1, 2023. https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback