



ThreatMon



# IN-DEPTH ANALYSIS ON THE ROLES OF THREAT ACTORS AND ATTACKS IN THE UKRAINE-RUSSIA WAR

---

KillNet



@threatmon



@MonThreat

<b>Summary</b>	<b>3</b>
<b>Cyber Wars in The Ukraine-Russia War</b>	<b>3</b>
<b>Threat Actor Review: KillNet</b>	<b>4</b>
Who is KillNet?	4
What are the Activities of KillNet?	5
Which Side They Supports?	5
What Types of Attacks Does KillNet Execute?	5
Which Industries Is KillNet Targeting?	5
<b>KillNet's Attacks</b>	<b>6</b>
Lockheed Martin:	6
Japan Government Websites and Systems:	7
NGA (National Geospatial Intelligence Agency):	8
Latvia, USA And Multi Country Attacks:	9
Starlink Attack:	9
DDoS Attack to German Federal Intelligence Agency:	12
Ignitis Attack:	13
Killnet Targeted Health Sector and Hospitals:	15
Indian Government Attack:	15
<b>KillNet's Attack TTPs</b>	<b>16</b>
<b>KillNet's Attack IOCs</b>	<b>17</b>

## Summary

The beginning of the Russia-Ukraine war dates back to Russia's annexation of Crimea in 2014. The political tension that erupted in 2021-2022 was the last straw and Russian forces took action on Putin's orders. Taking action on February 24, 2022, Russian forces launched a large-scale invasion of Ukraine. Russian President Vladimir Putin claims that this is not an invasion, but that Russia is protecting its geopolitical interests in the region, its citizens and its deployed soldiers.

## Cyber Wars in The Ukraine-Russia War

In 2014, Russia annexed Crimea, leading to conflict in the Donbass region and the start of a cyber war between Ukraine and Russia. Since then, Ukraine has been a frequent target of Russian cyber attacks, including ransomware, DDoS, and data manipulation. These attacks have targeted critical sectors such as energy, finance, and communication.

One of the most notable cyber attacks on Ukraine occurred in 2015 when parts of the country experienced power cuts. The attack was allegedly carried out by the pro-Russian group Sandworm, which targeted the country's electricity grid. This cyber attack caused a worldwide debate on cybersecurity and served as a wake-up call for Ukraine to take stronger measures on cybersecurity.

Following the attack, Ukraine implemented several measures to enhance its cybersecurity capabilities. The country established a National Coordination Center for Cybersecurity and developed a national cybersecurity strategy. Additionally, the government introduced legislation to strengthen cybersecurity regulations and established partnerships with international organizations to share best practices and expertise.

Despite these efforts, Ukraine remains a target for cyber attacks from Russia. In 2017, the country was hit by another cyber attack, the NotPetya ransomware attack, which caused widespread disruption in Ukraine and other countries. The attack is believed to have been carried out by Russian hackers and caused billions of dollars in damage.

Ukraine's experience highlights the growing threat of cyber attacks and the need for countries to take cybersecurity seriously. As technology continues to advance, the risk of cyber attacks is only going to increase. Therefore, countries must continue to invest in cybersecurity measures to protect themselves from these threats.

## Threat Actor Review: KillNet

### Who is KillNet?

KillNET is a hacker group that emerged directly out of the Russia-Ukraine war. With the merger of many different groups, the "KillNET Hacker Group" was created to defend Russia on the cyber front in the Ukraine war. Killnet announced that it has started a cyber war by launching DDOS attacks against many anti-Russian countries, including Ukraine, all countries that support Ukraine, NATO countries. In May 2022, Killnet hackers attacked the Romanian government, a NATO member state. The hackers targeted the Romanian government after its statements of support for Ukraine, causing Romanian government systems to experience days of outages.

In June 2022, they targeted Italy. The Italian attack started with a DDoS attack on several websites. The attacks continued with events such as the hacking of the Italian Senate website and the hacking of the Italian Automobile Club.

However, these attacks were not enough to satisfy KillNET because they did not make much noise and did not strengthen Russia's hand militarily and intelligence-wise. KillNET then issued a call for cyber mobilization.

It declared that other hacker groups should get involved and act in a much stronger way. KillNET openly called on all hacker groups that had declared cyber war against Ukraine to join its ranks.

Many famous hacker groups such as f-CkNet, Zarya, RaHDiT, DPR Joker, ZSecnet, XaKNET, Beregini, CyberArmyRussia, Anonymous Russia and many others responded positively to this call. KillNET was now one of the largest operational hacker armies in the world.

## What are the Activities of KillNet?

It carried out DDOS attacks on critical systems of many countries such as the USA, France and Italy. NATO countries, especially the US, did not take KillNet seriously because its first cyber attacks were DDoS attacks. There was no leakage of critical information. After all, these attacks only caused interruptions.

However, the hacker group made some strategic changes within itself, divided into sub-groups and this time joined the front line to carry out much more critical cyber attacks. KillNet united a number of hacker groups, all Russian nationalists (LEGION, Russia Anonymous, etc.), all of them closely allied with Russian intelligence, but also with units of the Russian military, and they began to carry out direct targeted attacks.

## Which Side They Supports?

It was created to defend Russia on the cyber front in the Ukrainian war.

## What Types of Attacks Does KillNet Execute?

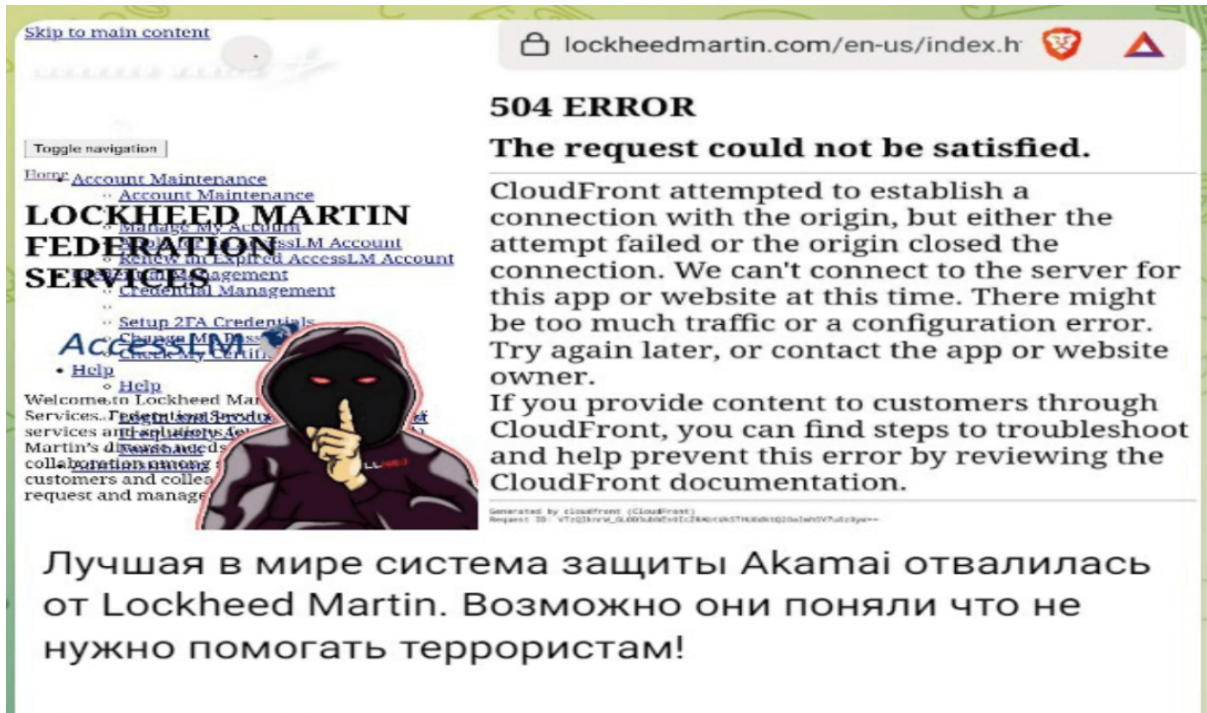
KillNET hackers do not perform technically complex attacks. In fact, they usually perform DDOS Attack attacks. Services known to conduct Brute-Force-Attacks attacks:  
21 FTP, 80 HTTP, 443 HTTPS, 22 SSH

## Which Industries Is KillNet Targeting?

KillNet attacked sectors such as government, health, defense and weapons, technology, airports and more.

## KillNet's Attacks

Lockheed Martin:



By August 2022, the KillNET hackers, now sufficiently powerful and strategically divided into many sub-groups, carried out the first high-profile attack, which frightened the countries that sided with Ukraine against Russia. Lockheed Martin, the largest defense and weapons technology developer in the US and the world, was targeted. And this time it was not just a DDoS attack. Many critical military technology information, Lockheed Martin employees' information, and many information and documents belonging to the US Army were leaked.

## Japan Government Websites and Systems:

OFFLINE

Электронное правительство Японии (Госуслуги)  
◆ <https://www.e-gov.go.jp>  
<https://check-host.net/check-report/c48100bk9b9й>

Электронное приложение электронного правительства Японии.  
◆ <https://shinsei.e-gov.go.jp/>  
<https://check-host.net/check-report/c480f31k1fb>

Главный налоговый портал Японии (рабочий стол)  
◆ <https://www.portal.eltax.lta.go.jp/>  
<https://check-host.net/check-report/c480bc7keb0>

In September 2022, this time they targeted Japan, which had declared support for Ukraine. They hacked many Japanese government websites and systems.

## NGA (National Geospatial Intelligence Agency):

Имя пользователя

Представлять на рассмотрение

Забыл пароль

Вы получаете доступ к информационной системе правительства США, которая включает этот компьютер, эту компьютерную сеть, все компьютеры, подключенные к этой сети, и все устройства и/или носители данных, подключенные к этой сети или к компьютеру в этой сети. Эта информационная система предоставляется только для использования с разрешения правительства США. Несанкционированное или ненадлежащее использование этой системы может привести к дисциплинарным взысканиям, а также гражданским и уголовным санкциям. Используя эту информационную систему, вы понимаете и соглашаетесь со следующим: у вас нет разумных ожиданий конфиденциальности в отношении любых сообщений, передаваемых через эту информационную систему, или данных, хранящихся в этой информационной системе. В любое время правительство может отслеживать, перехватывать, искать и/или конфисковывать данные, передаваемые или хранящиеся в этой информационной системе.

Подать заявку на учетную запись

ПРЕДУПРЕЖДЕНИЕ! Использование общедоступных компьютеров (например, библиотек, аэропортов, кафе, отелей и т. д.) для доступа к этой информационной системе не допускается. Такой тип использования может привести к непреднамеренному распространению информации неуполномоченным лицам. Данные могут остаться на этом компьютере, в результате чего следующий человек, использующий этот компьютер, сможет просматривать ваши данные.

RISSNET www.riss.net

By clicking the Sign in button, you agree to the RISSNET Terms of Use

proverka@example.com

Пароль

Вход forgot password?

Nashua PD

DIS

LEEP

RDCIC

JOT VALOR - Azure

KBI

Intelink

🐱 Атака на электронную инфраструктуру Разведывательного Агентства США.

! "National Geospatial-Intelligence Agency, NGA)" — правительственное агентство США, в задачи которого входит обеспечение военных, государственных и гражданских пользователей данными видовой разведки и картографической информацией. Входит в разведывательное сообщество США.

In October 2022, they listed a number of targets against their main enemy, the United States. They particularly wanted the attacks to have a "humanitarian dimension". On their Telegram channel, they posted a video of the Statue of Liberty in the US being hit by a nuclear bomb and shared a complete list of US states they said they were targeting. The list was quite long. KillNET attacked airports in 23 US states, including Florida and Colorado. These attacks disrupted airline traffic, delayed flights for days, and canceled many flights.

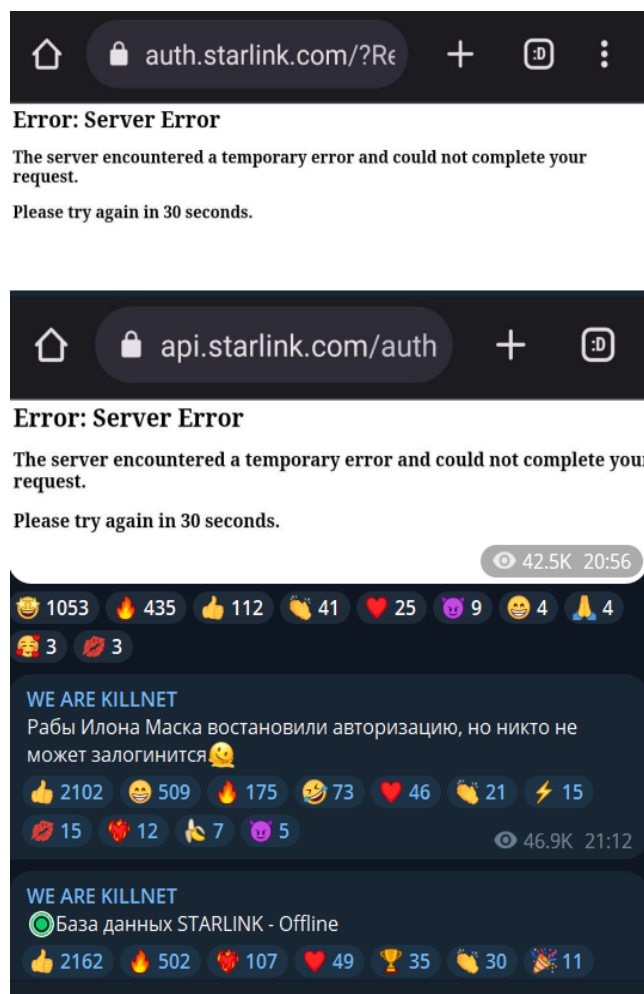


## Latvia, USA And Multi Country Attacks:

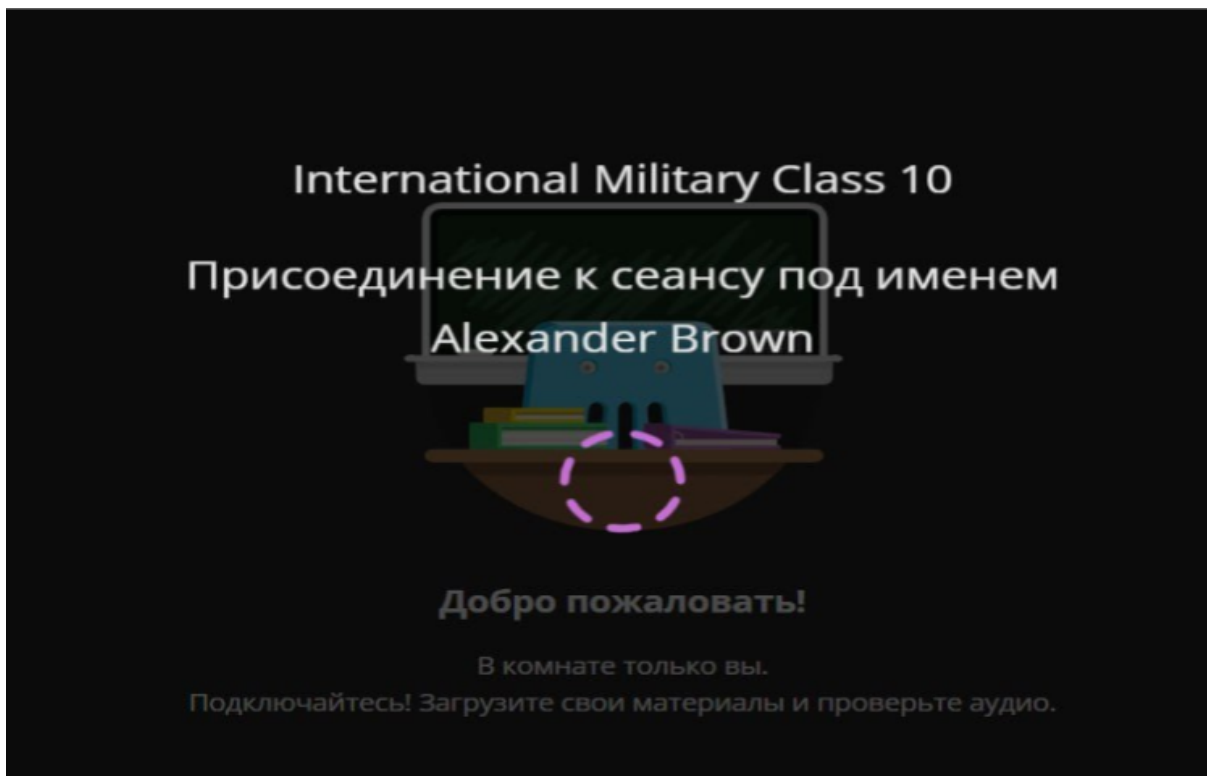
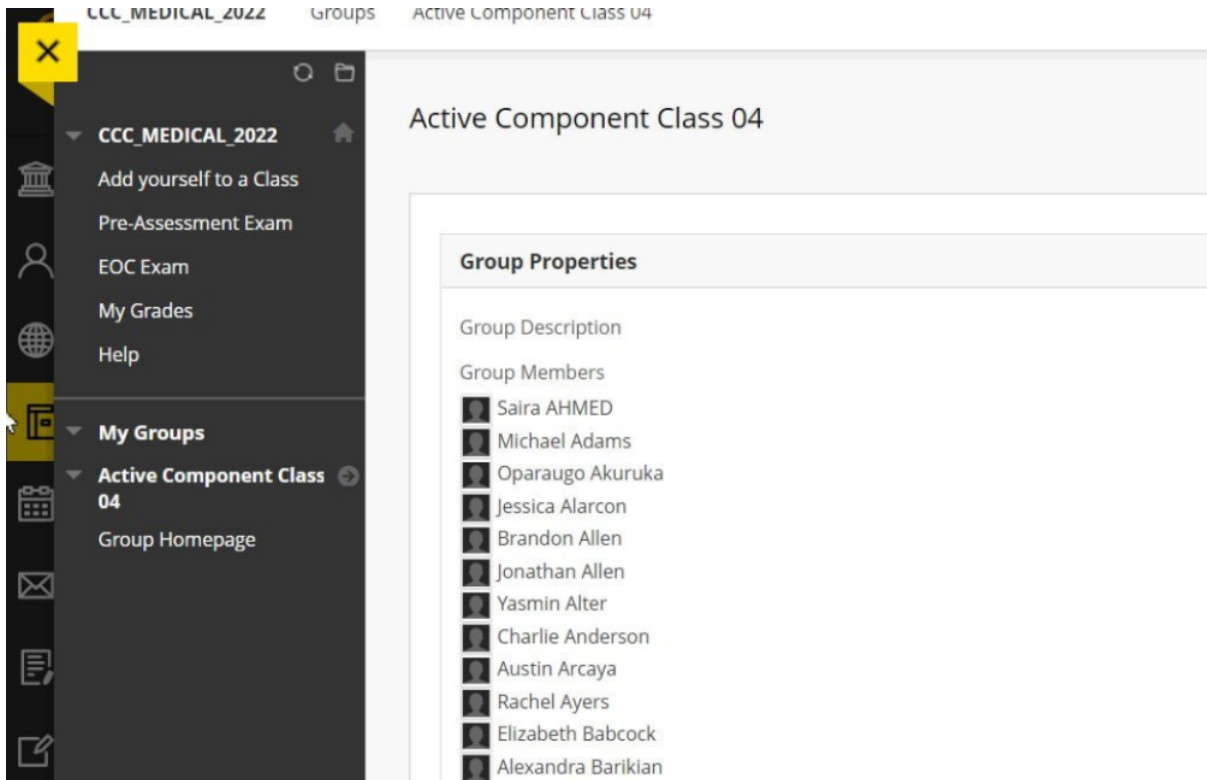
In November 2022, KillNET targeted not just one country, but several. Latvia and the United States were at the top of the list. The hacker group intercepted and published many secret documents of the Latvian government. Immediately afterwards, it launched a series of attacks on the White House. It carried out prolonged DDoS attacks on the White House website.

## Starlink Attack:

With the famous businessman Elon Musk's redirection of Starlink Satellite Systems over Ukraine, StarLink also got its share from KillNET. The hacker group announced that they took over the Starlink API system and redirected the satellites. The Ukrainian military stopped using Starlink satellites after this attack.



And they claim to have infiltrated closed US military systems.



## In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

Killmilk has put up for sale 150 million passwords belonging to residents of Europe, America, Ukraine and other unfriendly countries.

The data includes :

- Bank account passwords
- Credit and debit card information
- Crypto diaries
- Desktop access systems from 6,000 different organizations worldwide.
- Government portals

And thousands of other accesses.

**Killmilk**  
INFINITY TEAM



10 мин. назад

13687_US,72,28,219,121,24-11-22	17415_US,174,39,70,215,25-11-22	21090_US,199,38,247,130,26-11-22	23527_US,75,164,174,9,27-11-22	30719_US,174,199,230,200,27-11-22	32547_US,174,134,6,132,20-11-22
13813_US,66,31,59,11,34-11-22	17535_US,154,6,61,143,25-11-22	21295_US,24,255,219,110,26-11-22	25615_US,60,109,68,67,27-11-22	30837_US,47,22,6,228,64,20-11-22	33204_US,73,22,19,152,20-11-22
13930_US,72,107,23,188,24-11-22	17562_US,99,98,194,102,25-11-22	21336_US,73,66,72,214,26-11-22	25808_US,24,17,121,94,27-11-22	30873_US,174,235,83,102,28-11-22	33289_US,23,248,172,94,20-11-22
14052_US,98,200,2,30,24-11-22	17689_US,174,198,136,122,25-11-22	22077_US,67,232,196,110,26-11-22	25817_US,107,77,76,94,27-11-22	30884_US,24,228,239,154,28-11-22	33315_US,171,105,15,107,20-11-22
14107_US,172,74,20,64,24-11-22	17940_US,108,190,227,222,25-11-22	22740_US,172,58,45,215,26-11-22	25957_US,24,130,54,91,27-11-22	30945_US,142,129,204,173,28-11-22	33790_US,47,27,230,215,20-11-22
14241_US,75,249,166,229,25-11-22	18140_US,154,47,26,227,25-11-22	22910_US,47,187,190,196,26-11-22	26421_US,166,137,125,16,27-11-22	30974_US,67,230,126,18,20-11-22	34141_US,162,255,46,189,20-11-22
14252_US,24,43,124,33,25-11-22	18386_US,108,81,23,234,25-11-22	23059_US,73,7,50,51,26-11-22	26385_US,148,72,164,48,27-11-22	30978_US,76,153,204,6,20-11-22	34146_US,94,140,8,122,20-11-22
14314_US,71,133,205,237,25-11-22	18596_US,162,255,45,120,25-11-22	23682_US,198,255,74,221,20-11-22	26386_US,162,251,174,23,27-11-22	31029_US,209,142,101,20,28-11-22	34513_US,88,61,91,217,20-11-22
14419_US,72,47,168,41,25-11-22	18661_US,166,137,90,113,25-11-22	23949_US,98,159,224,224,26-11-22	27172_US,92,119,17,249,27-11-22	31154_US,99,195,77,97,20-11-22	34542_US,47,5,226,112,20-11-22
14446_US,96,27,127,204,25-11-22	18665_US,60,94,124,78,25-11-22	24047_US,98,255,26,221,26-11-22	27599_US,204,14,73,202,27-11-22	31156_US,94,85,31,102,20-11-22	34661_US,63,116,4,110,20-11-22
14715_US,24,251,2,152,25-11-22	18716_US,24,153,120,7,25-11-22	24286_US,74,142,151,174,26-11-22	27716_US,97,98,99,80,27-11-22	31254_US,24,99,205,70,20-11-22	34673_US,71,81,236,97,20-11-22
14739_US,172,56,51,28,25-11-22	18994_US,104,15,118,167,25-11-22	24423_US,60,88,80,12,26-11-22	28273_US,172,58,30,175,27-11-22	31272_US,104,181,245,196,20-11-22	34846_US,65,68,240,162,20-11-22
14777_US,98,223,80,130,25-11-22	19010_US,45,29,54,185,25-11-22	24424_US,100,40,191,138,26-11-22	28375_US,172,58,184,248,27-11-22	31299_US,104,220,483,20-11-22	35467_US,213,59,118,15,20-11-22
14781_US,98,242,246,44,25-11-22	19067_US,172,90,43,157,26-11-22	24495_US,107,127,42,55,26-11-22	28401_US,173,175,10,15,27-11-22	31323_US,107,72,164,98,20-11-22	35489_US,47,6,197,219,20-11-22
14872_US,73,232,63,106,25-11-22	19204_US,73,42,82,180,26-11-22	24527_US,173,239,204,206,27-11-22	28837_US,174,100,238,157,27-11-22	31489_US,173,77,235,235,20-11-22	35627_US,173,66,249,32,20-11-22
14911_US,73,208,142,155,25-11-22	19291_US,45,131,195,85,26-11-22	24554_US,199,244,86,234,27-11-22	28884_US,172,56,153,41,27-11-22	31491_US,75,82,192,216,20-11-22	35811_US,148,72,171,3,20-11-22
15109_US,47,105,169,168,25-11-22	19346_US,74,90,203,26,11-22	24642_US,172,112,46,107,27-11-22	29385_US,73,141,88,242,27-11-22	31537_US,68,42,196,70,20-11-22	35905_US,64,25,196,29,20-11-22
15339_US,76,201,73,223,25-11-22	19449_US,172,221,198,33,26-11-22	24815_US,71,238,77,105,27-11-22	29546_US,195,181,163,29,27-11-22	31585_US,40,138,182,45,20-11-22	35924_US,174,58,223,132,20-11-22
15349_US,174,78,12,154,25-11-22	19538_US,104,6,150,153,26-11-22	24925_US,107,146,242,144,27-11-22	29587_US,35,144,13,129,27-11-22	31942_US,135,26,73,251,20-11-22	35946_US,172,58,223,134,20-11-22
15487_US,67,140,176,89,25-11-22	19544_US,172,182,230,161,26-11-22	24938_US,98,118,140,27-11-22	29610_US,198,167,1188,27-11-22	31989_US,80,48,206,244,20-11-22	36018_US,104,243,213,196,20-11-22
15585_US,69,248,2,139,25-11-22	19677_US,67,185,144,107,26-11-22	24979_US,184,58,237,232,27-11-22	29795_US,73,2,224,27-11-22	31755_US,23,25,12,128,20-11-22	36392_US,143,244,151,20,20-11-22
15637_US,73,241,108,189,25-11-22	19819_US,72,217,223,70,26-11-22	25040_US,98,219,64,234,27-11-22	29754_US,172,58,83,187,27-11-22	31919_US,47,210,72,230,20-11-22	36399_US,208,83,63,31,20-11-22
15908_US,174,255,1,146,25-11-22	19887_US,172,56,130,62,26-11-22	25092_US,73,76,165,246,27-11-22	29859_US,75,12,131,88,27-11-22	31936_US,216,106,119,216,20-11-22	36523_US,97,71,88,187,20-11-22
16054_US,23,249,172,144,25-11-22	19980_US,216,245,122,200,26-11-22	25180_US,108,89,110,109,27-11-22	30042_US,199,46,164,172,27-11-22	31967_US,173,169,119,216,20-11-22	36649_US,192,145,117,189,20-11-22
16528_US,209,142,101,71-11-22	20061_US,162,236,248,115,26-11-22	25272_US,68,50,301,120,27-11-22	30423_US,99,162,187,80,27-11-22	31988_US,174,213,160,56,20-11-22	37010_US,108,75,189,202,20-11-22
16548_US,47,108,110,3,25-11-22	20110_US,108,52,119,226,26-11-22	25323_US,98,221,115,24,27-11-22	30544_US,173,63,84,27-11-22	32119_US,172,58,103,204,20-11-22	37249_US,198,45,183,230,20-11-22
16948_US,137,119,62,86,25-11-22	20762_US,24,25,237,86,26-11-22	25338_US,108,228,180,95,27-11-22	30647_US,73,255,99,189,27-11-22	32439_US,47,42,217,122,20-11-22	37285_US,75,215,203,172,20-11-22
17122_US,75,184,9,183,25-11-22	20957_US,185,238,200,51,26-11-22	25357_US,67,68,136,94,27-11-22	30687_US,67,182,212,62,27-11-22	32476_US,45,15,144,190,20-11-22	37299_US,47,284,106,171,20-11-22

**Привет мой друг!**  
**Европа, Америка, Украина и другие НЕДОСтраны рады**  
**Вам предложить свои логи в размере 150 млн**  
**паролей и других вкусных данных!**











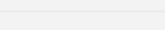

## In-Depth Analysis on The Roles of Threat Actors and Attacks In The Ukraine-Russia War

### DDoS Attack to German Federal Intelligence Agency:

Check website <https://www.bnd.bund.de/>  

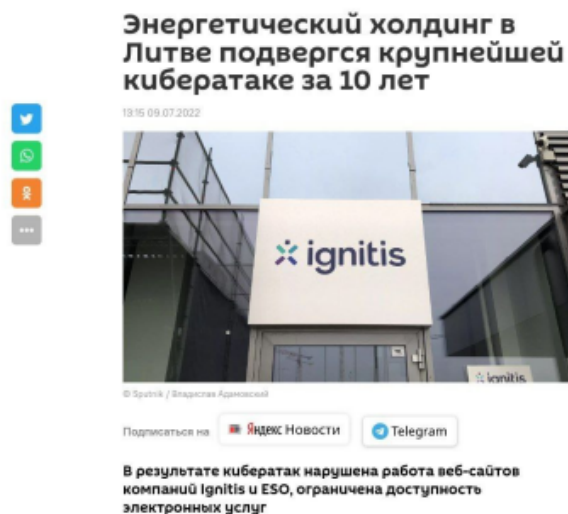
[Permanent link to this check report](#) | [Share report on Twitter](#)

Checked on **Thu Feb 16 08:36:44 UTC 2023** | [Check again](#)

Location ▾	Result	Time	Code	IP address
 <a href="#">Austria, Vienna</a>	Connection timed out			
 <a href="#">Brazil, Sao Paulo</a>	Connection timed out			
 <a href="#">Bulgaria, Sofia</a>	Server error	5.312 s	403 (Forbidden)	
 <a href="#">Czechia, C.Budejovice</a>	Server error	7.170 s	403 (Forbidden)	
 <a href="#">Finland, Helsinki</a>	Connection timed out			
 <a href="#">France, Paris</a>	Connection timed out			
 <a href="#">France, Roubaix</a>	Connection timed out			
 <a href="#">Germany, Frankfurt</a>	Server error	5.242 s	403 (Forbidden)	
 <a href="#">Hong Kong, Hong Kong</a>	Connection timed out			

The German Federal Intelligence Agency was attacked by DDoS on February 16 and the main domain could not be accessed for a certain period of time.

## Ignitis Attack:



⚡ Комментарии от Службы безопасности "ЕСО"  
"В настоящее время проводится работа с Национальным центром кибербезопасности и предпринимаются все возможные шаги для восстановления систем", — говорится в сообщении компании.

👊 Таким образом я буду продолжать бить и бить в самые больные места наших врагов. Сносить десятки сайтов больше не интересно. Меня больше интересует когда бьёшь один а падают все. Для этого необходим анализ и исследования уязвимых мест у наших коллег. Такие точечный удары в @бало гораздо эффективнее и наносят в 100 крат больше урона чем работа наших подражателей.

VILNIUS, 9 July - Sputnik. Lithuanian state-owned energy company Ignitis groupé is facing the biggest cyberattack of the decade by Killnet. Killnet stated that the attacks will continue.

## Killnet Targeted Health Sector and Hospitals:

KillNet launched its attacks on companies focusing on the health sector, targeting western companies on March 17, 2023. DHHS released an analyst note on KillNet's threats to the healthcare industry, and the group talked about the hijacking of a US medical ship sent by US army troops.

## Indian Government Attack:

Phoenix did not approve of the actions of the Indian government. They were able to access the hospital, its staff and chief physicians on March 17, 2023.

"We have nothing against you and your people. But any action you take will have irreversible and devastating consequences for the situation you're in. Don't mess with Phoenix and the KillNet fraternity guys." The explanation has come.



## KillNet's Attack TTPs

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

## KillNet's Attack IOCs

IOC Type	IOC	IOC Type	IOC
IPv4	91[.]132[.]147[.]168	IPv4	195[.]206[.]105[.]217
IPv4	81[.]17[.]18[.]62	IPv4	185[.]83[.]214[.]69
IPv4	81[.]17[.]18[.]58	IPv4	185[.]67[.]82[.]114
IPv4	72[.]167[.]47[.]69	IPv4	185[.]56[.]80[.]65
IPv4	5[.]2[.]69[.]50	IPv4	185[.]220[.]102[.]253
IPv4	45[.]154[.]255[.]139	IPv4	185[.]220[.]102[.]243
IPv4	45[.]154[.]255[.]138	IPv4	185[.]220[.]102[.]242
IPv4	45[.]153[.]160[.]139	IPv4	185[.]220[.]101[.]35
IPv4	45[.]153[.]160[.]132	IPv4	185[.]220[.]101[.]15
IPv4	23[.]129[.]64[.]219	IPv4	185[.]220[.]100[.]252
IPv4	23[.]129[.]64[.]218	IPv4	185[.]220[.]100[.]250
IPv4	23[.]129[.]64[.]217	IPv4	185[.]220[.]100[.]248
IPv4	23[.]129[.]64[.]216	IPv4	185[.]220[.]100[.]243
IPv4	23[.]129[.]64[.]213	IPv4	185[.]220[.]100[.]242
IPv4	23[.]129[.]64[.]212	IPv4	185[.]220[.]100[.]241
IPv4	23[.]129[.]64[.]210	IPv4	185[.]129[.]61[.]9
IPv4	23[.]129[.]64[.]149	IPv4	185[.]100[.]87[.]202
IPv4	23[.]129[.]64[.]148	IPv4	185[.]100[.]87[.]133
IPv4	23[.]129[.]64[.]147	IPv4	171[.]25[.]193[.]78
IPv4	23[.]129[.]64[.]142	IPv4	171[.]25[.]193[.]25
IPv4	23[.]129[.]64[.]139	IPv4	164[.]92[.]218[.]139
IPv4	23[.]129[.]64[.]137	IPv4	162[.]247[.]74[.]200
IPv4	23[.]129[.]64[.]134	IPv4	156[.]146[.]34[.]193
IPv4	23[.]129[.]64[.]133	IPv4	144[.]217[.]86[.]109
IPv4	23[.]129[.]64[.]132	IPv4	173[.]212[.]250[.]114
IPv4	23[.]129[.]64[.]131	IPv4	92[.]255[.]85[.]135
IPv4	23[.]129[.]64[.]130	IPv4	92[.]255[.]85[.]237
IPv4	209[.]141[.]58[.]146	IPv4	209[.]141[.]57[.]148
IPv4	205[.]185[.]115[.]33	IPv4	45[.]227[.]72[.]50
IPv4	199[.]249[.]230[.]87	IPv4	185[.]220[.]100[.]255





ThreatMon

010100011010000110100101110011010000000110100101  
10010000001110110110111011011010110010100100100  
01100110000101101110011001000110111101101101010  
110100011001010111100001110100000100000000  
1011010010110111001100111001000000001101  
1000110100001100101011100100110010  
0110111101110010001000000011001111  
100110100101101110011001110010

45305 Catalina cs St 150, Sterling VA 20166