

# What You Need to Know About Russian Cyber Escalation in Ukraine

---

 [socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/](https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/)

**UPDATE February 26, 2022, 04.40 AM (EST):** *This blog has been updated with details of posts of the Conti ransomware group and Anonymous.*

**UPDATE February 27, 2022, 05.50 AM (EST):** *This blog has been updated with details of new IoCs, a list of IoC sources, and claimed Nvidia breach.*

**UPDATE February 28, 2022, 06.50 AM (EST):** *This blog has been updated with details of threat actors taking sides.*

The Russian invasion of Ukraine has caused a substantial increase in cyberattacks. What's happening in cyberspace related to the Russia-Ukraine war? How does it affect the countries and organizations all around the world? How can a company detect cyber attacks associated with this war? What are the IoCs that need to be monitored? The SOCRadar Research Team did a thorough analysis to find the answers that you can find all below.

Skip to [how SOCRadar provide related threat intelligence feeds, including IoCs, for free](#) and see [how to protect your company from the potential impacts of Russia-Ukraina cyber crisis](#).

## Executive Summary

---

The Russian invasion of Ukraine has caused a substantial increase in cyberattacks. The public and private organizations can be impacted even before they are not located in the region. Therefore, the SOCRadar analyst team, monitoring the situation from its early hours, has gathered initial findings in this blog post.

Here is what you should know about the cyber repercussions of the Russian-Ukraine war:

- Beginning from January 13, 2022, various companies in Ukraine were infected with harmful malware designed to render targeted machines useless. The malware deleted victims' machines before passing itself off as a ransomware attack without offering a ransom payment and recovery mechanism.
- The first wave of cyberattacks on February 15th, mostly potent DDoS, targeted Ukrainian government organizations. Several agencies, including the Ministry of Foreign Affairs and the Security and Defense Council, were impacted.

- Following the Russian troops' invasion, the second wave of DDoS attacks started on February 23. The target included government agencies and two of the largest state-owned banks. Attacks were paired with some disinformation attempts in which SMS were sent to customers falsely claiming the ATMs were out of order.
- In addition to DDoS attacks, two malware equipped with significant destructive capabilities has been found in the attacks. HermeticWiper is utilized to delete the data in a digital device that cannot be recovered. Recently discovered Cyclops Blink is employed to exfiltrate data from the network.
- Underground groups such as Anonymous and Conti ransomware groups have picked their sides in the cyber conflict. The largest hacktivist initiative, Anonymous, launched a virtual war against Russia. Conti, the notorious ransomware gang, decided to stand with Russia threatening to attack any rivals' critical infrastructure.
- Dark web forums have become a show-off platform for warring factions. Detected by SOCRadar, several posts have been published alleging that sensitive information from the government organizations was leaked.
- You can also find lists of IoCs, TTPs, and Yara rules in this article.

## What Happened So Far?

---

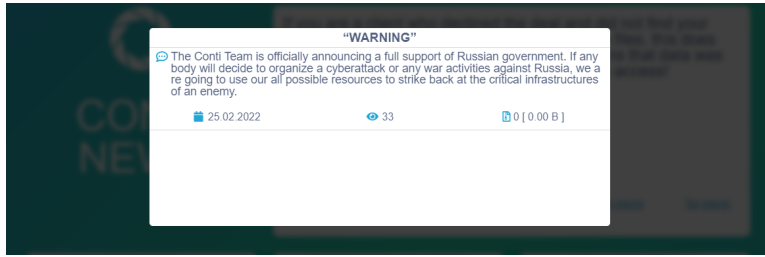
During the 2021–2022 **Russian – Ukrainian crisis**, a series of cyberattacks took down more than a dozen of Ukraine's government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council.

After recognizing territorial claims of self-declared separatist republics in eastern Ukraine, Russian force deployments in these regions coincided with two massive DDoS attacks (Distributed Denial-of-Service) with destructive malware implications targeting Ukraine.

The first wave of **cyber-attacks on Ukraine** started on February 15th, and the second one on February 23rd, made many Ukrainian governments, military, and bank websites inaccessible.

Russian cyberattacks against Ukraine have led hackers, ransomware gangs, and companies to pick upsides. Underground groups publicly expressed their side in the military conflict.

In the underground world, the actors have diverse decisions. Conti, the notorious ransomware group and claimed to be a state-sponsored threat actor, announced that they will strike back if cyber-attacks are conducted against Russia. In two different posts, the group states that they would target the opposite countries' critical infrastructure on its official website.



---

## Which Cyber Threat Actor Takes Which Side in the Ukraine-Russia War?

Many different cyber threat actors who continue their operations on the dark web have actively participated in the

Russia-Ukraine war in cyberspace

. During the conflict that has lasted for nearly a week, many threat actors have declared their sides or switched sides. Many threats, from hacktivist groups to ransomware gangs, announced their support for one of the warring parties.




First, the Anonymous group announced that it had declared its support for Ukraine. After this announcement, some websites belonging to Russia's state and private sector became unavailable.

In another tweet, Anonymous TV, an account close to Anonymous, claimed that Anonymous leaked the database of the Russian Ministry of Defense website. The group also claimed to breach Tetradr, a Belarusian weapon manufacturer and leaked about 200GB of emails.

**RELEASE**

**Tetraedr**



**ANONYMOUS LIBERLAND  
AND THE PWN-BÄR HACK TEAM**

**About us**

Greetings citizens of the world. Let us introduce ourselves. We are the Pwn-Bär International Hack Team. We stand for moral superiority, power and unrestricted access to information. Our Russian and friends were kinda out of shape, so we (secretly) took a little break. We thought maybe they needed a little reminder of what real hacking is like, so we stopped off "Russia" to have a little break and we were shocked with what we saw. They have the most secure Cyber, in entire world and we could not hack them. Nobody, just kidding.

We announce the start of #CyberBullshit. We are going to show you how prepared for cyberwar Russia and EU countries really are. We are Anonymous, we are a legion, we do not forgive, we do not forget, expect us.

**Info**

The Military Enterprise "Tetraedr"

Country: Belarus, category: Military industrial complex

The TETRAEDR LLC is a scientific and industrial private military enterprise specializing in development and manufacture of advanced radio electronic weapon systems, development and manufacture of hardware and software used in radar and radio electronic control assets, operating of air defense radars systems.

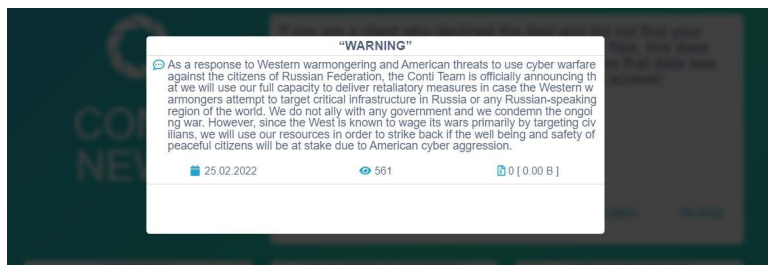
The TETRAEDR LLC was founded on 26 April 2001, state registration No 19820044. The TETRAEDR LLC is a full member of the Belarusian Chamber of Commerce and Industry.

The TETRAEDR LLC does not catch ransomware in year 2022. The Pwn-Bär Hack Team and copied their ransomware.

If you see pictures from Russian state tv of missiles being fired or military training in Belarus, included are the addresses for some of those links, and email addresses that might be of interest to researchers of Belarusian government or the international press team.

## Conti ransomware group

, which has made a name for itself with its organized ransomware attacks, announced that it sided with Russia. It was noted that the group exhibited a slightly softer attitude in the second statement made later. In this statement, Conti claimed that they did not support the war. Some insiders not happy with Conti's support for Russia leaked inside jabber chats of the group.



The CoomingProject group, which has been selling/sharing the data it has obtained from critical institutions since 2021 on Russian-speaking hacker forums, was also among the hacker groups that sided with

## **Russia**

. The Cooming Project has announced that they will respond if the Russian

government targets a cyberattack

.

LockBit

announced that it was not a party to the war. Noting that there are hackers from different nationalities within the group, the group stated that people from many countries, not only from

### **Ukraine and Russia**

but also from China to the USA, are working for them. "Business is important to us, and we all take an apolitical stance. We are only concerned with money."

Along with Anonymous, another hactivist group targeting **Russia**

is AgainstTheWest. In the statement made by the group, it was stated that the systems of various Russian government institutions were infected with ransomware, attacked with data-destroying malware, and all the data were seized.

The Red Bandits, known for their data breach attacks, CyberGhost, and Sandworm groups, known for their hacking and

### DDoS attacks

, were shared on the hacker channels that they were Russian supporters. It is known that the Raidforum Admins group, which came to the fore with cyber sanctions against

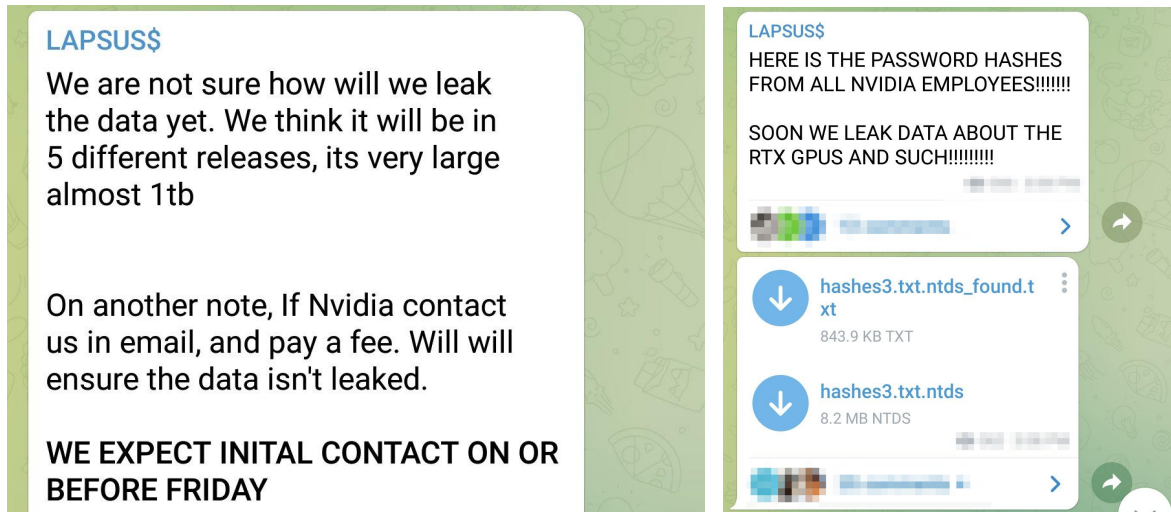
**Russia**, is in the ranks of Ukraine.

Some groups that carried out DDoS attacks on behalf of Ukraine are as follows as of February 27: "IT Army of

### **Ukraine**

, BlackHawk, and Anonymous Liberland & PWN Bar hack team." It is understood that the ransomware group called Belarussian Cyber Partisans is a supporter of "free Ukraine," as far as it is followed on Twitter channels.

On the other side, the Lapsu\$ extortion group claimed to breach Nvidia, one of the largest technology manufacturers in the world. The US and western sanctions in retaliation for Russia's invasion of Ukraine shut off the supply from leading US groups such as Intel, AMD, and Nvidia at Russia's military and its tech industry. After the sanction decision, Russian origin hacker groups allegedly shared data about hashes of Nvidia's employees on a Telegram Channel monitored by SOCRadar.



### **Hacker groups supporting Ukraine:**

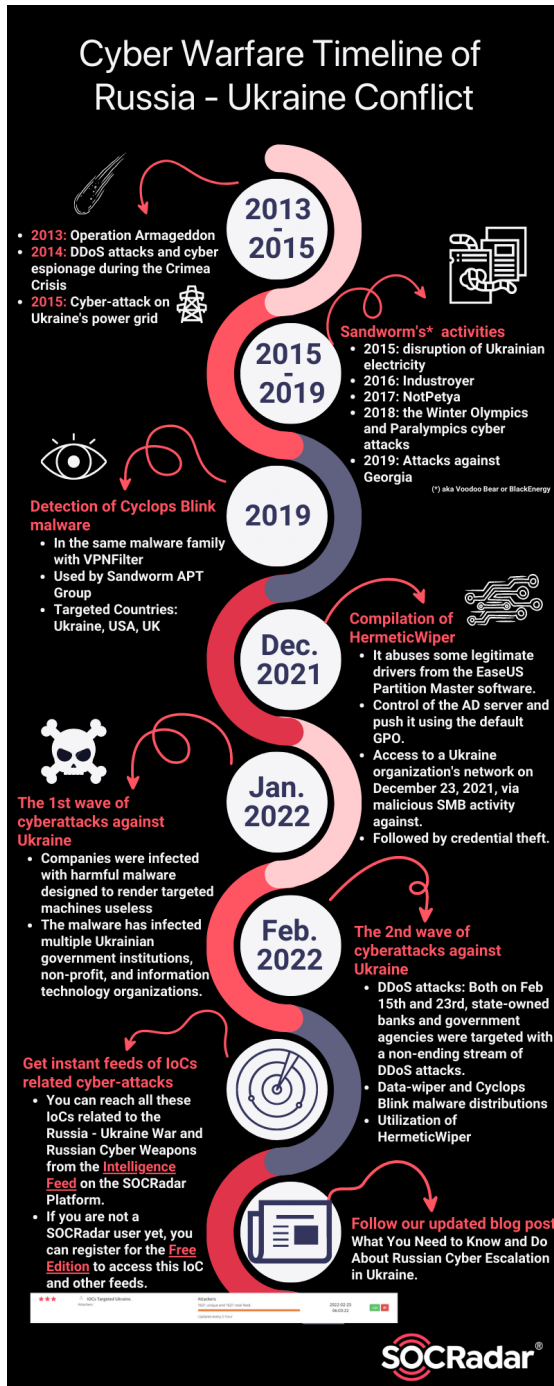
Anonymous, AgainstTheWest (AWT), Belarusian Cyber Partisans, GhostSec, IT Army of Ukraine, KelvinSecurity Hacking Team, BlackHawk, Anonymous Liberland & the PWN-BAR Hack Team, Raidforum Admins, GNG, NB65, ECO, Raidforums2, ContiLeaks, SHDWSec, GhostClan, Eye of the Storm, and Netsec.

### **Hacker groups supporting Russia:**

Sandworm, Conti, CoomingProject, The Red Bandits, and CyberGhost.

## **2022 Russian-Ukrainian Crisis: The FirstWave of Cyberattacks**

---



Beginning from January 13, 2022, various companies in Ukraine were infected with harmful malware designed to render targeted machines useless.

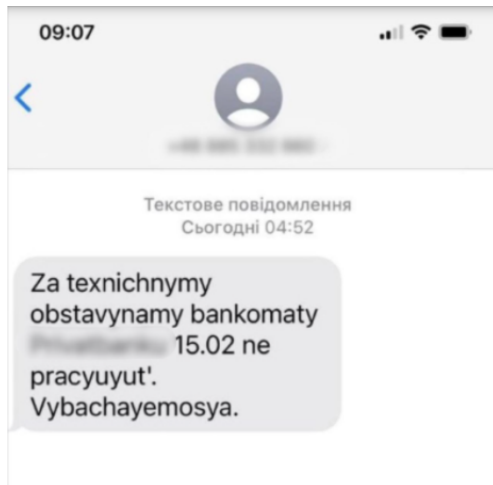
The malware deleted victims' machines before passing itself off as a ransomware attack without offering a ransom payment and recovery mechanism.

The malware has infected multiple **Ukrainian** government institutions, non-profit, and information technology organizations.

On February 15th, **Ukraine** became the victim of numerous powerful DDoS attacks again, resulting in the disruption of services in government agencies and state-owned banks.

The affected enterprises were two of the largest state-owned banks, namely Privatbank and Oschadbank, and several other government agencies, including the Ministry of Defense and the Armed Forces of **Ukraine**.

The attacks were carried out by flooding the web servers with high traffic volumes the server could not handle. As a result, the servers were inaccessible for several hours. Many Ukrainians could not use mobile banking apps and log into their accounts on the above-mentioned banks' websites, even though they were up and running.



Fake SMS messages customers of Privatbank received

on February 15th

On the same day, customers of Privatbank has received fake SMS messages claiming that the ATMs of the bank were down, according to the cyberpolice of Ukraine. The cyberpolice stated that these SMS messages did not reflect reality and were just mere parts of an “information attack.”

In addition to the state-owned banks, the Ministry of Defense and the Armed Forces of **Ukraine** were also attacked on the 15th of February. The website of the Ministry of Defense was taken down, unable to operate for several hours.

Ukraine’s online news agency Ukrainska Pravda states that these attacks are potent DDoS attacks on government agencies and have never happened before on this scale.



Сайт знаходиться на технічному обслуговуванні.

A Snapshot shows that the Ministry of Defense was inaccessible on February 15th. Translation of the sentence: “The site is under maintenance” (Source: Wayback Machine)

## The Second Wave of Cyber Attacks on Ukraine: Deadlier than the First Wave



On the 23rd of February, Ukraine woke up to a new series of cyber-attacks threatening to disrupt the services of enterprises and several government agencies of Ukraine.

These cyber-attacks were in parallel with **Ukraine's invasion** by the Russian military. As the Russian army crossed Ukraine's border, numerous malicious cyber-attacks believed to be coming from Russia were launched.

Two of the largest state-owned banks (Privatbank and Oschadbank) were targeted once again, along with several government agencies with a non-ending stream of DDoS attacks. The websites of government agencies, including the Ministry of Defense, the Ministry of Foreign Affairs, and the Ministry of Internal Affairs, and the targeted banks became inaccessible due to the attacks.

The State Service of Special Communication and Information Protection of **Ukraine** said on the 23rd of February, acknowledging the attacks and the aftermath:

“Today, websites of a number of government and banking institutions have undergone a massive DDoS attack again. Some of the attacked information systems are not available or work intermittently. It is due to switching traffic to another provider to minimize damage.”

Along with DDoS attacks targeting Ukrainian organizations, two important cybersecurity firms, namely ESET and Broadcom's Symantec, revealed that a new data-wiper malware had targeted Ukrainian organizations' computer networks.


The new data-wiper is a malware that deletes data on a device for the data to be unrecoverable and the operating system to stop working correctly.

Besides the new data-wiper, a new malware known as Cyclops Blink, which targets the **Ukrainian organizations** in the second wave of cyberattacks, has been identified by a joint UK – US advisory and might be used remotely to access networks.

The malware is believed to be utilized by Sandworm, an APT group. In the past, the group has been linked to the Russian GRU.

Moreover, Cyclops Blink looks to be a replacement for the VPNFilter malware that was discovered in 2018, and its deployment could allow Sandworm to access networks remotely.

Western Allies of Ukraine declare their readiness to support **Ukraine** in cyberspace. The European Defence Agency (EDA) tweeted on 24 February that Cyber Rapid Response Team (CRRT) was activated following a request from Ukraine. EDA website states that CRRT will support Ukraine in monitoring the threat landscape and detecting and mitigating cyber attacks.

@Lithuanian\_MoD coordinated   
Cyber Rapid Response Team activated following a request from #Ukraine

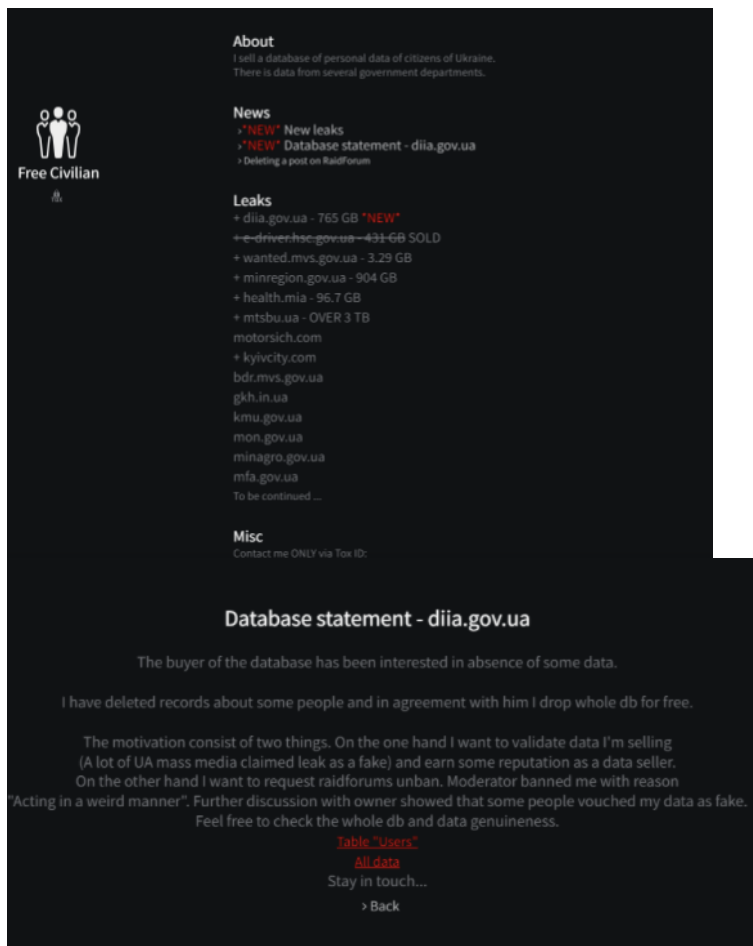
First #PESCO capability activated in an operational context.

CRRTs are equipped with commonly developed deployable #cyber toolkits

On the other hand, news outlets reported on 24 February that some Russian government entities' websites were not accessible. The official website of the Ministry of Defence of the Russian Federation was responding with "HTTP ERROR 418" by 7 PM on 24 February. We understand that Russia blocked access to this domain based on geography as a security mechanism.

## What are the Dark Web Activities Related to Russia-Ukraine War?

On the dark web, threat actors allegedly began to sell database data of citizens of Ukraine and data from several Government departments.

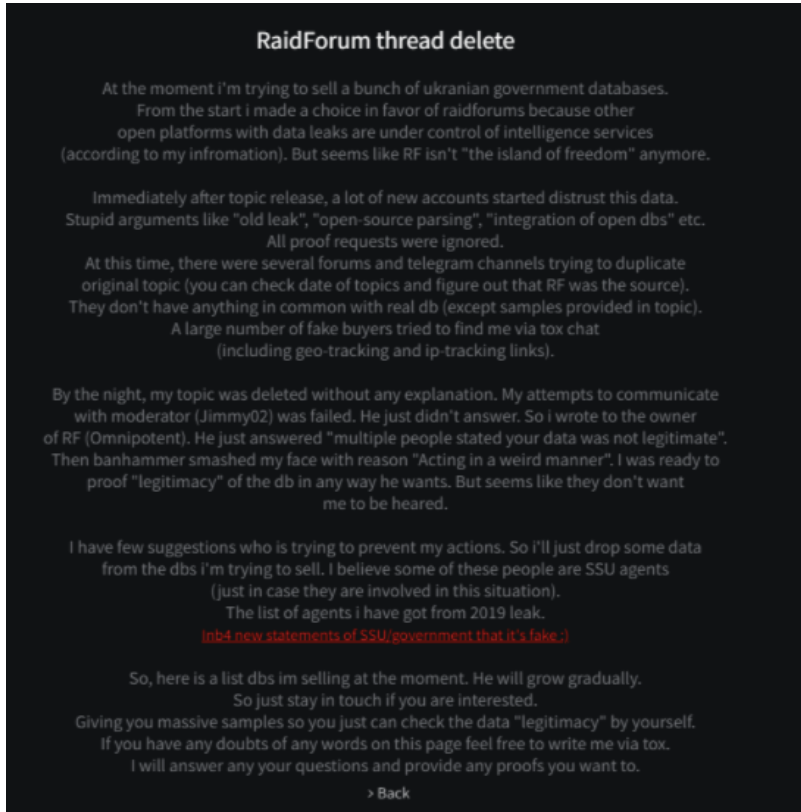


The screenshot shows a dark-themed forum post. On the left is a profile for 'Free Civilian' with a logo of two figures. The post content includes:

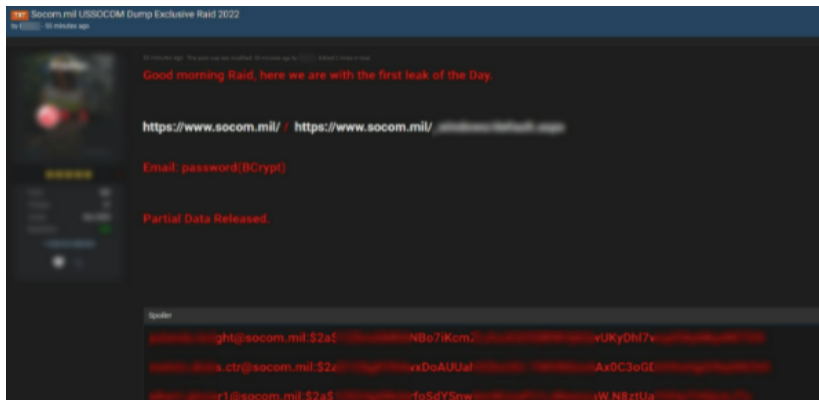
- About:** 'I sell a database of personal data of citizens of Ukraine. There is data from several government departments.'
- News:** '\*NEW\* New leaks', '\*NEW\* Database statement - diia.gov.ua', '> Deleting a post on RaidForum'
- Leaks:** '+ diia.gov.ua - 765 GB \*NEW\*', '+ e-driverchsc.gov.ua - 431 GB SOLD', '+ wanted.mvs.gov.ua - 3.29 GB', '+ minregion.gov.ua - 904 GB', '+ health.mia - 96,7 GB', '+ mtsbu.ua - OVER 3 TB', 'motorsich.com', '+ kyivcity.com', 'bdr.mvs.gov.ua', 'gkh.in.ua', 'kmu.gov.ua', 'mon.gov.ua', 'minagro.gov.ua', 'mfa.gov.ua', 'To be continued ...'
- Misc:** 'Contact me ONLY via Telegram ID: ...'

The main title of the post is 'Database statement - diia.gov.ua'. The body text reads: 'The buyer of the database has been interested in absence of some data. I have deleted records about some people and in agreement with him I drop whole db for free. The motivation consist of two things. On the one hand I want to validate data I'm selling (A lot of UA mass media claimed leak as a fake) and earn some reputation as a data seller. On the other hand I want to request raidforums unban. Moderator banned me with reason "Acting in a weird manner". Further discussion with owner showed that some people vouched my data as fake. Feel free to check the whole db and data genuineness.' Below the text are links for 'Table "Users"', 'All data', 'Stay in touch...', and '> Back'.

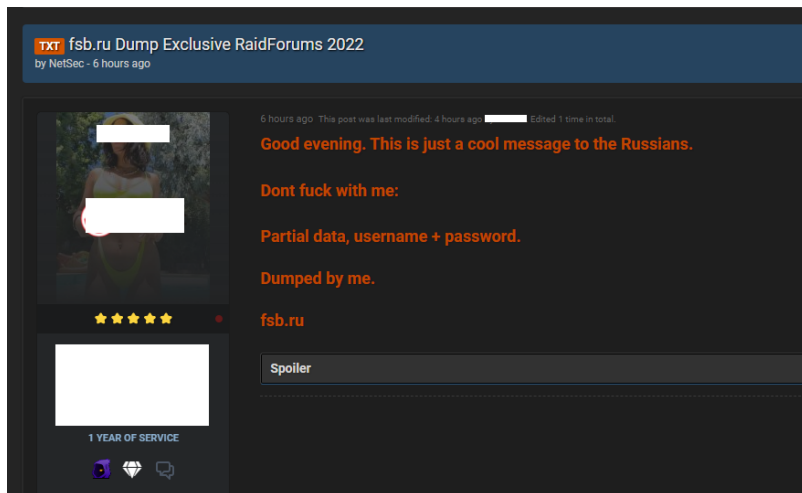
RaidForum deleted some posts related to the Ukraine Hack.



One of the posts allegedly shared a leak of US Special Operation Command.



Some of the information allegedly to be shared in the forums, on the other hand, claims that data sharing against Russia has started.



## How SOCRadar Can Help?

---

You can reach all these IoCs related to the Russia – Ukraine War and Russian Cyber Weapons from the [Intelligence Feed](#) on the SOCRadar Platform.

IOC list targeted Ukraine available in [SOCRadar Threat Feed Database](#).



If you are not a SOCRadar customer, you can register for the [Free Edition](#) to access this IoC and other feeds.

[Get Free Access Now](#)

You can reach all these IoCs related to the Russia – Ukraine War and Russian Cyber Weapons from the [Intelligence Feed](#) on the SOCRadar Platform.

IOC list targeted Ukraine available in [SOCRadar Threat Feed Database](#).

## List of IoC Sources Related to Russia-Ukraine War

---

Besides SOCRadar Intelligence Feeds and IoC details below of Russian Cyber Weapons, many organizations and cybersecurity companies also provide IoC lists of malware recently used by Russian hacker groups.

## Technical Analysis of Russian Cyber Weapons

---

### HermeticWiper: A Catastrophic Malware

---

ESET Research has found that a new data wiper malware dubbed HermeticWiper has been discovered on Ukrainian computers and machines in Latvia and Lithuania. ESET products first detected the malware as Win32/KillDisk.NCV around 3 p.m. UTC on Wednesday,

February 23rd, 2022.

The compilation timestamp shows December 28th, 2021, which suggests the attack was prepared for at least two months. The wiper attacks started after a series of DDoS attacks hit several important websites in the country and brought them down.

Since it is a developing story, some details might change, but HermeticWiper abuses some legitimate drivers from the EaseUS Partition Master software.

After the initial entry, attackers took control of the Active Directory (AD) server and pushed it using the default Group Policy Object (GPO). In the case of an attack against at least one organization in Ukraine, the attackers seemed to gain access to the network on December 23, 2021, via malicious SMB activity against a Microsoft Exchange Server, according to the Symantec Threat Hunter Team. It was immediately followed by credential theft.

A web shell was also installed on January 16, before the wiper was deployed on February 23. However, it is not obvious how the initial access to the Active Directory was gained.

The malware called HermeticWiper referenced the digital certificate used to sign the sample. Sentinel Labs' initial analysis shows that the digital certificate is issued under 'Hermetica Digital Ltd' and is valid as of April 2021. There are no known legitimate files signed with this certificate.

## How Does It Work?

---

According to Juan Andres Guerrero-Saade from Sentinel Labs, Hermetic Wiper uses a known and tested technique similar to the Lazarus Group (Destover) and APT33 (Shamoon) with Eldos Rawdisk. However, the Wiper abuses a different driver:

```
empntdrv[.]sys
```

to access the file system without calling Windows APIs. After that, the Hermetic Wiper focuses on corrupting the first 512 bytes, the Master Boot Record (MBR), for every physical drive to stop the booting process.

## Who Gets Affected by HermeticWiper?

---

The target seems to be the host computers in critical networks. The malware does not try to steal or exfiltrate data, but it just destroys it. In a time of crisis, the malware could create chaos by deleting importing data stored in the personal computers of the key personnel.

**Targeted Devices:** Windows device

**Targeted Countries:** Ukraine, Latvia, Czechia, Poland, and Lithuania

**Targeted Sectors:**

Financial, Defense, Aviation, and IT services sectors

**Malware Family:** NCV

**TTPs of HermeticWiper**

---

MITRE ATT&CK	T1059.003 Command and Scripting Interpreter: Windows Command Shell
MITRE ATT&CK	T1059.001 Command and Scripting Interpreter: PowerShell
MITRE ATT&CK	T1542.003 Pre-OS Boot: Bootkit
MITRE ATT&CK	T1561 Disk Wipe

**IoCs of HermeticWiper**

---

FileHash- SHA256	<u>1bc44eef75779e3ca1eebf8ff5a64807dbc942b1e4a2672d77b9f6928d292591</u>
FileHash- SHA1	<u>912342f1c840a42f6b74132f8a7c4ffe7d40fb77</u>
FileHash- SHA1	<u>61b25d11392172e587d8da3045812a66c3385451</u>
FileHash- MD5	<u>eb845b7a16ed82bd248e395d9852f467</u>
FileHash- MD5	<u>a952e288a1ead66490b3275a807f52e5</u>
FileHash- MD5	<u>231b3385ac17e41c5bb1b1fcb59599c4</u>
FileHash- MD5	<u>095a1678021b034903c85dd5acb447ad</u>
FileHash- SHA256	<u>ca3c4cd3c2edc816c1130e6cac9bdd08f83aef0b8e6f3d09c2172c854fab125f</u>

**Yara Rules for HermeticWiper:**

---

```

rule MAL_HERMETIC_WIPER {
  meta:
    desc = "HermeticWiper - broad hunting rule"
    author = "Friends @ SentinelLabs"
    version = "1.0"
    last_modified = "02.23.2022"
    hash = "1bc44eef75779e3caleefb8ff5a64807dbc942ble4a2672d77b9f6928d292591"
  strings:
    $string1 = "DRV_XP_X64" wide ascii nocase
    $string2 = "EPMNTDRV\\%u" wide ascii nocase
    $string3 = "PhysicalDrive%u" wide ascii nocase
    $cert1 = "Hermetica Digital Ltd" wide ascii nocase
  condition:
    uint16(0) == 0x5A4D and
    all of them
}

```

## Mitigation for HermeticWiper:

---

- Make sure you patched all the critical vulnerabilities and closed all the essential ports discovered SOCRadar Attackmapper module
- If you have anti-malware programs from vendors like SentinelOne or Symantec, their scanners can catch HermeticWiper. Make sure that your definitions are up-to-date.
- There are also YARA rules: <https://github.com/Cluster25/detection/tree/main/yara/hermeticwiper> out here if you would like to double-check your network.
- IOCs published by SOCRadar can be fed the security devices like Firewalls, IPSs, or SOAR solutions.
- Be extra careful against usual delivery methods of malware like phishing.
- Webshell detection plays a very critical role in hermetic wiper mitigation strategies. Please [see details here](#).

## Cyclops Blink: The New Weapon of Cyber-Warfare

---

U.S. and U.K. government agencies published a joint report on a new malware strain called Cyclops Blink.

The report stated that Sandworm (aka Voodoo Bear or BlackEnergy) APT group developed a new malware to be used to remotely compromise network devices, primarily small office/home office (SOHO) routers and network-attached storage (NAS) devices. The group is a part of Russia's (foreign military intelligence agency) GRU's Main Centre for Special Technologies or GTsST.

The malicious cyber activities such as disruption of Ukrainian electricity in 2015, Industroyer in 2016, NotPetya in 2017, the Winter Olympics and Paralympics in 2018 cyberattacks, and attacks against Georgia in 2019 were all attributed to Sandworm. The new malware, Cyclops Blink, appears to replace the VPNFilter malware exposed in 2018.

According to the report, NCSC, CISA, FBI, NSA, and industry partners have identified a large-scale modular malware framework affecting network devices. This new malware strain is named Cyclops Blink. The report claims that the malware deployed at least June 2019, fourteen months after its successor VPNFilter was disrupted.

As with VPNFilter, Cyclops Blink deployment also seems indiscriminate and widespread. So far, Cyclops Blink has been only deployed to WatchGuard devices by Sandworm. (WatchGuard Technologies Inc. is a network security vendor that provides products designed to protect computer networks from outside threats.) However, Sandworm could likely use the malware to target other architectures and firmware.

The malware is highly sophisticated and modular, capable of sending device information back to a C2 server. Cyclops Blink could download and execute files. The modular nature of the **malware** also allows Sandworm to implement additional functionalities as needed.

After the exploitation, Cyclops Blink will generally arrive in a firmware update that achieves persistence once the target device is rebooted, making it very hard to remove. Then the malware organizes the victim's devices into clusters, and each deployment has a list of command and controls IP addresses and ports it uses.

The data transferred between Sandworm and compromised devices are protected with Transport Layer Security using individually generated keys and certificates. Sandworm manages compromised devices over the Tor network.

Another important note is that Cyclops Blink warn that Cyclops survives through a reboot and legitimate firmware updates. Therefore, the removing process is not easy and should be completed carefully using the directives from the WatchGuard.

**Targeted Countries:** Ukraine, United States of America, United Kingdom of Great Britain, and Northern Ireland

**Malware Families:** VPNFilter, Cyclops Blink

**TTPs of Cyclops Blink:**

---

MITRE ATT&CK T1140 Deobfuscate/Decode Files or Information

---

MITRE ATT&CK T1495 Firmware Corruption

---

MITRE ATT&CK T1547 Boot or Logon Autostart Execution

---

MITRE ATT&CK T1106 Native API

---

MITRE ATT&CK T1105 Ingress Tool Transfer

---

MITRE ATT&CK T1102 Web Service

---



MITRE ATT&CK	T1095	Non-Application Layer Protocol
MITRE ATT&CK	T1008	Fallback Channels
MITRE ATT&CK	T1036	Masquerading
MITRE ATT&CK	T1037	Boot or Logon Initialization Scripts
MITRE ATT&CK	T1041	Exfiltration Over C2 Channel
MITRE ATT&CK	T1059	Command and Scripting Interpreter
MITRE ATT&CK	T1071	Application Layer Protocol
MITRE ATT&CK	T1082	System Information Discovery
MITRE ATT&CK	T1090	Proxy
MITRE ATT&CK	T1132	Data Encoding
MITRE ATT&CK	T1133	External Remote Services
MITRE ATT&CK	T1542	Pre-OS Boot
MITRE ATT&CK	T1562	Impair Defenses
MITRE ATT&CK	T1571	Non-Standard Port
MITRE ATT&CK	T1571	Non-Standard Port

**IoCs of Cyclops Blink:**

IPv4	<u>185.82.169.99</u>
IPv4	<u>151.0.169.250</u>
IPv4	<u>109.192.30.125</u>
IPv4	<u>105.159.248.137</u>
IPv4	<u>100.43.220.234</u>
FileHash-SHA256	<u>ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6</u>
FileHash-SHA256	<u>c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862</u>
FileHash-SHA256	<u>50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a8</u>

---

FileHash- 4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1  
SHA256

---

FileHash- c59bc17659daca1b1ce65b6af077f86a648ad8a8  
SHA1

### Mitigation for Cyclops Blink:

---

- Make sure you patched all the critical vulnerabilities and closed all the critical ports discovered SOCRadar Attackmapper module
- If you have a WatchGuard Device, Follow the directions from WatchGuard Which can be found here:<https://detection.watchguard.com>
- The NCSC has also published its own analysis which can be found here:<https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf>
- There are IOCs published by SOCRadar that can be fed the security devices like Firewalls, IPSs or SOAR solutions.
- Be extra careful against usual delivery methods of malware like phishing.

### Katana: DDoS Attacks to Ukraine

---

One of the cyber-attack prongs which Russia used against Ukraine is DDoS attacks. Some Ukrainian websites were not accessible due to heavy DDoS attacks both on February 15 and 16. Banks, Government, and Military websites were impacted. Both UK and US officials have attributed these attacks to a known Russian GRU infrastructure stating The US has technical data to back it up.

Fortunately, the attacks` scale was only moderate. Therefore, the impacted sites recovered within hours. During attacks, it is reported that some customers could not access the banking websites and, in minimal cases, ATMs became unavailable too. In addition to these attacks, some fraudulent SMS messages were sent to Ukrainian phones, possibly creating panic.

The text messages said, “Due to technical circumstances, Privatbank ATMs do not work on February 15. We apologize”. These messages were sent from Polish, Austrian and Estonian numbers. Computer Emergency Response Team of **Ukraine** also reported a denial of service attack against the “.gov.ua” DNS servers; and a BGP hijacking attack against the Privatbank IP space causing difficulties routing traffic to their network.

According to the Ukrainian CERT, 360Netlab, and BadPackets, the source of these attacks was a Mirai botnet. Researchers matched the gathered IOCs to a botnet named Katana, which is, in fact, a variant of Mirai with improved DDoS capabilities. Katana source code is

available for purchase for less than a thousand dollars, and it is possibly shared for free on some deep and dark websites.

According to Malpedia, Mirai was one of the first significant botnets targeting exposed networking devices running Linux. Mirai was first discovered in August 2016 by MalwareMustDie.

It targeted various networked embedded devices such as IP cameras, home routers belonging to many different vendors, and other IoT devices. Since the source code was published on “Hack Forums,” many variants of the Mirai family appeared, infecting mostly home networks worldwide.

When an IoT device like network cameras are publicly accessible, they could be easily targeted and were exploited by the attacker to perform the DDoS. Due to how the exploit works, the records of their exploitation can be seen by anyone. It should also be noted that a file matching the attack IoCs was uploaded to the VirusTotal on February 13th.

Therefore, compromising the IoT devices had been started at least a couple of days before the DDoS attacks. Even though the impacted sites came back online relatively quickly, this does not dismiss the fact that this was a sophisticated and well-organized attack to create instability and chaos in Ukraine.

**Targeted Country:** Ukraine

**Target Sectors:** Banking, Military, Government

**Malware Family:** Mirai

**TTPs of Katana:**

---

MITRE ATT&CK T1583.005 Botnet

---

MITRE ATT&CK T1525 Implant Internal Image

---

MITRE ATT&CK T1499 Endpoint Denial of Service

**IoCs of Katana:**

---

URL <http://5.182.211.5/rip.sh>

---

Pv4 [5.182.211.5](http://5.182.211.5)

---

FileHash-SHA256 [978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed](https://www.virustotal.com/ui/978672b911f0b1e529c9cf0bca824d3d3908606d0545a5ebbeb6c4726489a2ed)

---

---

FileHash- 82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf  
SHA256

---

FileHash- 7504ac78e531762756e8ca8e94adc71fa2179104  
SHA1

---

FileHash- db8cc8adc726c3567b639c84ecf41aa5  
MD5

---

## Yara Rules for Katana:

---

```
rule Ddos_Linux_Katana {
  meta:
    description = "Detects Mirai variant named Katana"
    date = "2022-02-19"
    license = "Apache License 2.0"
    hash = "82c426d9b8843f279ab9d5d2613ae874d0c359c483658d01e92cc5ac68f6ebcf"
  strings:
    $ = "[http flood] fd%d started connect"
    $ = "Failed to set IP_HDRINCL. Aborting"
    $ = "[OVH] DDoS Started"
    $ = "[vega/table] tried to access table.%d but it is locked"
    $ = "Cannot send DNS flood without a domain"
  condition:
    all of them
}
```

---

## Mitigation for Katana:

---

- It is the ISP level filtering of all traffic that may come from abroad, except for the traffic that will come from abroad and which does not make sense to be blocked (Search engine traffic, etc.).
- Attacks from within the country are generally low. Potential amplifier IP addresses that can use for high-dimensional DDoS attacks should be uploaded to the security wall / IPS systems in a list and activated in monitoring mode.

---

## How the Cyber-war Escalating Between Russia and Ukraine as Conflict Became Brutal?

---

In addition to recent interventions, Russia's cyberattacks against Ukraine date back to earlier times.

The cyber warfare between Russia and Ukraine is a part of the confrontation which goes back to the collapse of the Soviet Union in 1991. Russian cyberwar capabilities had been available since 2005 with Uroburos. The first recorded Russian cyberattacks against Ukraine happened during the mass protests in 2013.

In an operation called Armageddon, a Russian campaign of systematic cyber espionage on the information systems of law enforcement and defense agencies started to help Russia on the battlefield.

In 2014, DDoS attacks and cyber espionage were common during the Crimea Crisis. On December 23, 2015, a cyber-attack on Ukraine's power grid resulted in power outages for roughly 230,000 consumers in the country for 1-6 hours. The attack is attributed to a Russian APT (Advanced Persistent Threat) group known as "Sandworm." The mass supply-chain attack 2017 using Petya was the most potent known hacker attack according to the US Presidential Administration.

Therefore, cyber warfare was always part of the contemporary Russia-Ukraine conflict. As a result, it was not a surprise that the special cyber activity reports came just hours before Russian forces began the invasion of neighboring Ukraine.

---

### What to Do to Mitigate Potential Impacts of the Russian-Ukrainian Cyber Crisis?

Since there is no single attack vector or a new type of malware used in the **Russian – Ukrainian cyberattacks**, there is no single way of protecting your organization against critical cyber threats in the escalating cyber crisis.

Countries that make quick statements about their side in the conflict are the first to be targeted in global political crises. It can be predicted that cyberattacks from **Russia** will increase in the coming days. Against potential attacks, SOCRadar's recommendations are as follows:

Cyberattacks could come in various forms and have disastrous effects on your organization. To minimize risk and protect your organization, analysts at SOCRadar suggest you to:

**Accelerate Incident Response:** Reducing incident response time is crucial for organizations to mitigate the potential consequences. Alert your SOC team, implement a mitigation action plan in case of a cyber-attack, and test your communication and backup protocols.

**Update and Patch Software in Endpoints:** Unpatched vulnerabilities could be exploited to gain access and damage your organization in any way possible, so it is crucial to update and patch critical software in your organization's endpoints. It is suggested that all software be updated to the latest release.

**Backup Your Data in case of a Ransomware Attack or Data-wiping:** The new HermeticWiper malware has targeted organizations in **Ukraine** and destroyed organizations' data without leaving any chance of recovery. It is strongly suggested that all sensitive and important data is backed up, and recovery and backup protocols are thoroughly tested to quickly recover from data-wiping and ransomware attacks.

The vast majority of ransomware attacks that have affected almost every country in the last two years are originated in **Russia**. To be protected from these attacks, it is essential to regularly check the attack surface that is open to the internet and regularly scan it for critical vulnerabilities.

One of the main ways to protect from malware and ransomware attacks is using EDR/EPP software. We recommend that you monitor your infrastructure against cyber operations carried out by integrating IOCs shared by SOCRadar into SIEM, XDR, and EDR systems.

**Scan your Endpoints to Detect Anomalies:** Any unclosed RDP (Remote Desktop Protocol) ports along with compromised credentials could seriously damage your organization's infrastructure and result in an unrecoverable cyberattack. It is strongly suggested that security scans and tests are carried out to detect anomalies in your endpoints and prevent potential cyberattacks.

**Be aware of DDoS attacks:** As the conflict continues and more countries declare their side in this conjuncture, it will be inevitable for DDoS attacks to head towards other countries and their critical infrastructures. In such cases, we recommend preparing a "Plan B" for companies/institutions in regions where the attack is likely to escalate to be activated at the time of the attack.

The first item of your "Plan B" should be filtering at the ISP level of all traffic, except for the traffic that will come from abroad and does not make sense to be blocked (Traffic that comes from search engine traffic, etc.).

The attacks that may come from within your country are generally low-level. The potential "amplifier IP addresses" that can be used for high-dimensional DDoS attacks should be uploaded to the firewall/IPS systems in a list. These should be activated in monitoring mode.

SOCRadar observes that many social media accounts and domain purchases are made for phishing and disinformation purposes. In this context, if SOC teams are using it, we recommend DNS monitoring solutions or following such newly acquired domains in monitoring mode via SIEM. Finally, we also recommend following the CERTs and newsletters issued by CISA.