One Year After: The Cyber Implications of the Russo-Ukrainian War

By Livia Tibirna, Maxime A. and Sekoia TDR

Published: 2023-02-21 · Archived: 2026-04-05 16:57:11 UTC

As the ongoing Russo-Ukrainian conflict started on 24 February 2022 is about to mark its first year anniversary, Sekoia.io analysts share their analysis pertaining to the cyber picture. This report does not list all related cyber events related to the Russo-Ukrainian context, but rather aims at sharing Sekoia.io TDR takes on observed and assessed strategic, operational or tactical changes since the beginning of the conflict. This publication is mostly based on open source publications therefore incurs a lack of visibility due to the secrecy of military affairs, including the discreet implication from allies and foreign private companies.

This paper explores the Russian offensive cyber operations aimed at supporting the military invasion, whether it is to disrupt coordination, communication or narrative from Ukraine and supporting countries or entities. A second part analyses the rising role of cybercrime groups and hacktivist nationalist organisations in the cyber confrontation with a focus on the techniques used by non-state actors and the way the ongoing war shaped their activities.

Key Takeaways

- **The Russian invasion did not combine with a major destructive cyberattack causing significant disruption of military defence or governmental facilities.** However, Russian military intelligence GRU did employ multiple wipers targeting Ukraine and Western entities supporting Kiev.
- **Cyber operation objectives differ whether it is conducted by SVR- and FSB-operated intrusion sets or by GRU**. First ones aim at strategic intelligence and reconnaissance in support of the military operation, when military intelligence cyber operations seem to focus on immediate disruption.
- **A significant number of information operations were conducted by Russian and Belarusian intelligence services**, to relay anti-NATO and pro-Moscow narrative regarding the military invasion.
- **Non-state hacktivist groups increasingly demonstrated support in cyberspace to national efforts, on both sides, with mainly DDoS and hack-and-leaks operations**. Multiple pro-Russia collectives are suspected to cooperate with Russian intelligence services.
- **A limited number of financially motivated threat actors engaged in politically motivated attack campaigns**. They mainly conducted data breach and data exfiltration campaigns and contributed to the growth of the Cybercrime-as-a-Service market over 2022.

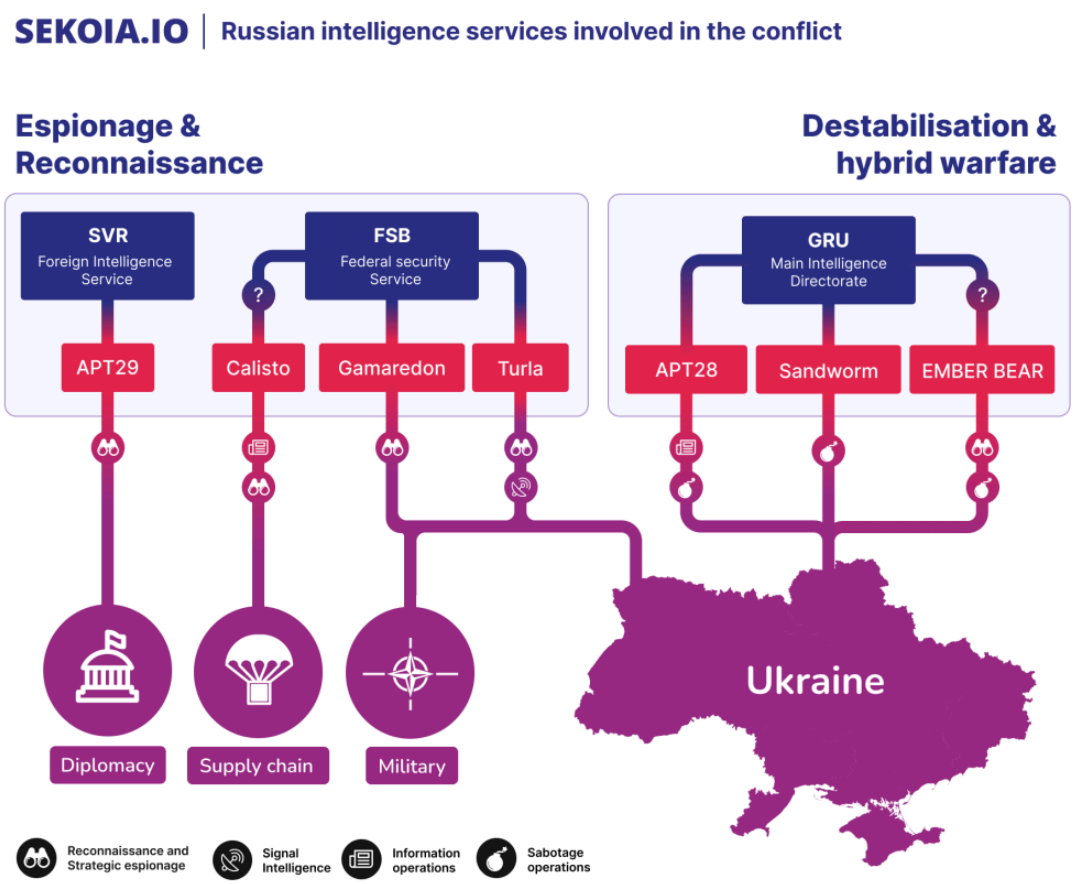
Russian-sponsored operations

While the expectation was a coordination between the military operation and a large-scale cyber operation disrupting Ukrainian defence, governmental or civil facilities, the Russo-Ukrainian conflict did not show, as far as we can observe in open source, corresponding events. However Sekoia.io observed a trend in open source documented **use of wipers malware** allegedly by Russian-nexus intrusion sets, especially – but not exclusively – ones known to be **operated** by **Russian military intelligence** Main Directorate of the General Staff (**GRU**).

The first destructive operations were observed before the beginning of the Russo-Ukrainian conflict, with a peak reported the days before 24 February 2022, aiming at strategic targets, such as the KA-SAT satellite communication modems, operated by VIA-SAT company, and allegedly used by the Ukrainian army. Sekoia.io technical investigation showed the operation used **AcidRain** wiper, an analysis shared by SentinelOne which associated the campaign to **Sandworm**, a Russia-nexus intrusion set attributed to the Russian GRU by the US Department of Justice in October 2020.

At least a dozen destructive malware originating from Russia-nexus intrusion sets, were observed in 2022**,** during the months following the beginning of the conflict**.** Based on open source publication, GRU-operated **APT28** leveraged CaddyWiper and AwfulShred, both wipers also reported being used by GRU's **Sandworm**, alongside to HermeticWiper, AcidRain, Industroyer2, ZeroWipe and SwiftSlicer.

Other destructive codes were leveraged by intrusion sets not yet associated with a specific Russian intelligence service, but reputedly aligned with Russian strategic objectives, namely **Ember Bear** (aka DEV-0586) and **UAC-088** which respectively used WhisperKill and DoubleZero. Based on Russian intelligence reputation, Sekoia.io assess, along with other cybersecurity vendors such as Microsoft, that it is **plausible** that **Ember Bear** and **UAC-088** are either subgroups or previously unassociated **intrusion sets operated by GRU**.



It should be noted that **no use of destructive malware** by identified intrusion sets operated by **Federal Security Service (FSB)** (Turla, Gamaredon, Calisto, DragonFly) **nor by the foreign Intelligence Service** (**SVR**) (APT29/Nobelium), were reported in open source. Sekoia.io notes that such observation is **coherent with the past observed activities** associated with these administrations**,** as well as the **alleged mandates** of the **three main Russian intelligence services**. Indeed, the FSB is known for its focus on targeted and strategic cyber espionage, internally and internationally, rather than destructive operations. The SVR is reputed to operate with a high degree of discretion, seeking to gain and gain pertinence and trying to avoid detection when GRU cyber operations aim at deception, manipulation and sabotage objectives.

Based on our technical investigations and open source publications, Sekoia.io analysts observe that most of the Russian destructive malware impacting Ukraine and supporting countries **differs from past Russia-nexus sabotage operations**.

Reported wipers are either **relatively simple** and **poorly developed wipers**, without automatic replication or lateral movement capability. As a reminder, after the first Russian military operation invading Crimea in 2014, Russian destructive operations impacted strategic entities of Ukraine, such as the **NotPetya** (2017) and **BadRabbit** (2017) **destructive worms**, originally sent to impact Ukrainian entities but counting an overly efficient automatic replication module leading to a worldwide compromission impacting as well multiple Russian companies. Sekoia.io TDR analysts observe that **destructive Sandworm operations** during the Russo-Ukrainian conflict did not leverage worms, **likely to prevent** past **side effects**.

> Sekoia.io observe that **destructive Sandworm operations** during the Russo-Ukrainian conflict did not leverage worms, **likely to prevent** past **side effects**.
>
> Tweet this!

Another possible explanation of this **operational change** is the **alleged impreparation** from Russian intelligence, which possibly did not properly assess the need of cyber offensive preparation to support the military operation. As a parallel to the failure of its military operation to conquer Kiev and the full Ukrainian territory, **cyber operations may have been poorly prepared** (insufficient malware development or prepositioning).

Still in comparison to military operations, Sekoia.io TDR analysts assess it is plausible that Russian intelligence had to **work faster to catch up**, looking for **more immediate effects** by building **straightforward** and **ready-to-use wipers** rather than complex and long-term planned destructive worms.

Additionally, a significant number of destructive operations were conducted as **pseudo-ransomware used as wipers**. The example of **Prestige ransomware**, identified by Microsoft and leveraged by **Sandworm** to impact Ukraine and Poland, illustrates a possible scheme of **plausible deniability** behind the **false-flag** of cybercrime-related operations. However, as Prestige ransomware and other documented pseudo-ransomware were signature codes, and not picked up from cybercrime malware, the false-flag operation seems easily uncovered. It remains unclear for Sekoia.io analysts why Russian destructive campaigns would try to operate undercover in the context of an open cyber and military confrontation with Ukraine.

Sekoia.io assess it is possible that, **given the limits** of **straightforward wipers** and **pseudo-ransomware** codes, these operations had the **objective** to **cause confusion, disrupting** Kiev's ability to **coordinate its defence**, rather than looking for a game changing impact.

SEKOIA.IO investigation on KA-SAT incident

Following the KA-SAT incident, SEKOIA.IO analysts investigated the SurfBeam2 modems to understand the impact and the context of the attack. Our analysis showed that the firmware was entirely wiped by the same algorithm as the one present inside the AcidRain wiper (cf. FLINT 2022-015). Moreover, by diffing two firmware versions (pre- and post-attack) our analysis showed that the vector of this compromise was likely SSH as every SurfBeam2 modems has SSH enabled on SDWAN network, and the new firmware versions has almost no changes, except for the SSH public key of the root user.

As KA-SAT was allegedly used by the Ukrainian government as a backup link, it is worth noting that this attack had almost no impact on its communications because it was launched too early. However the compromission had consequences on the KA-SAT commercial offer, impacting European companies and individuals through compromised modems. **A private presentation of this investigation is now available for download here**.

While a significant number of destruction-motivated cyber campaigns were reported over the Russia-Ukraine conflict, most of them associated by cybersecurity researchers to GRU, multiple Russia-nexus cyber operations also aimed at gathering **strategic intelligence** related to **the conflict.**

Such operations were notably conducted by **FSB-operated** (Gamaredon, Calisto and Turla) or **SVR intrusion sets** (APT29/Nobelium), targeting multiple sectors as diplomacy, logistics, NGOs, NATO-related entities, or strategic research.

Sekoia.io published about a **Calisto** operation (aka **Cold River**), an intrusion set we associate with moderate confiance to the **FSB**, observed carrying out phishing campaigns aiming at credential theft in November 2022. Impacted organisations were notably involved in military logistics and war crime investigation. Sekoia.io analysts assess Calisto collection activities probably contribute to Russian efforts to disrupt Kiev supply-chain for military reinforcements. Moreover, Russian intelligence collection about identified war crime-related evidence is likely conducted to anticipate and build counter narrative on future accusations.

Throughout the war, SVR-operated **APT29** (aka Nobelium) **continued its strategic espionage** activities focused on the diplomatic entities from Western countries, carrying out long-term and covert operations in Embassies network. Despite the lack of open source information about the aim of those operations, we assess it is likely **APT29 supplies Russian executives with intelligence related to Western diplomatic and logistics support to Ukraine**. Sekoia.io actively follow APT29 threat and published reports about the group TTPs, such as the EnvyScout infection chain and Slack Downloader (FLINT 2022-038), its Trello command and control infrastructure to target European embassies in April 2022 (FLINT 2022-009) or its HTML Smuggling technique (FLINT 2021-098).

These operations illustrate the **continuation** of **strategic cyber espionage operations** conducted **by FSB** and **SVR.** Sekoia.io assess the mandate of Russian intelligence services conducting cyber operations did not change despite the Russia-Ukraine conflict and is likely to be pursued over the future.

> Sekoia.io assess Calisto collection activities probably contribute to Russian efforts to disrupt Kiev supply-chain for military reinforcements.
>
> Tweet this!

Cyber operations during the Russo-Ukrainian conflict were also conducted for **information warfare** (or **info ops**), in order to gather or **relay narratives**. A significant number of information operations were reported in open source publications, Sekoia.io chose to focus on a few examples.

Starting in January 2022, multiple operations from **GhostWriter** (aka UNC1151) were observed by cybersecurity vendors and the Ukrainian government. GhostWriter, whose narratives are consistent with **Belarusian government interests** – a country aligned on Russian narrative toward Ukraine, conducted info ops mostly aimed at Eastern European countries (Ukraine, Poland, Lithuania and Latvia) with **anti NATO narratives**. For instance, in July 2022, Poland Prime minister Mateusz Morawiecki accused Russian and Belarusian secret services of “hacking into government systems” and leaking emails aimed to show political discord in Poland regarding Warsaw’s support for Ukraine.

Another example of information operation was described by Mandiant in September 2022. The cybersecurity vendor showed that **self-proclaimed hacktivist groups** working in support of Russian interests, namely Xaknet, Infoccentr and CyberArmy of Russia Reborn, were **cooperating with- or** were **strait fronts** used by **GRU**-operated intrusion sets. **Sekoia.io concurs** with Mandiant assessment based on **our knowledge** of **APT28 use for**

fronts, such as Cyber Berkut (2014), Yemeni Cyber Army (2015), CyberCaliphate (2015) or Guccifer 2.0 and DCLeaks (2016) all leveraged to conduct false flag hack and leak operations posing as hacktivist.

Non-state threat groups

Another evolution that Sekoia.io observed is the importance of the role played by allegedly **non-state collectives**, either belonging to the **cybercrime ecosystem**, or structured as **cyber hacktivist groups taking part** in the **conflict**.

Among the non-state cyber threat groups involved in the confrontation, **hacktivist groups** were one of the most active actors of the cyber landscape since February 2022. **Organised hacktivist** collectives **declaring support** to Russia or to Ukraine were existing structures progressively joining the war effort in the cyberspace (Belarusian Cyber Partisans, Killnet) or newly created groups in the wake of 24 February (NoName057, XakNet, People's Cyber army of Russia, 2402team, IT Army of Ukraine, Squad303).

Killnet is a prominent Pro-Russian hacktivist collective and **one of the most active** in recent months. The group's activity on Telegram goes back to January 2022 and started with offering DDoS-for-hire services. Killnet joined the Russo-Ukrainian war in cyberspace later in February and positioned itself as a counter-offensive to an Anonymous-nebula initiative, which declared its support for Ukraine. **Killnet** is currently **a highly structured** hacktivist group, operating with a galaxy of "special forces squads" notably via social media accounts and websites. While it mainly engages **DDoS attacks with minor damage**, the critical nature of its documented targets (e.g. **healthcare organisations, national governments and international organisations**) and its continuous alignment with Russian strategic interests in the context of the conflict turn this group into a **top tier hacktivist threat for Ukraine and NATO countries**.

> Killnet is a highly structured collective which represents a top tier hacktivist threat for Ukraine and NATO countries.
>
> Tweet this!

Another emblematic example is the **IT Army of Ukraine**, created to conduct cyber operations notably against Russia and Belarus on 26 February 2022. This volunteer organisation announced by Ukraine's Minister for Digital Transformation is allegedly coordinated by Ukrainian state representatives. Based on open sources, the IT Army is composed of both amateurs (civilians) and dedicated professionals (civilian, military, intelligence representatives) **from all over the world**. The IT Army of Ukraine **provides its members the attack infrastructure** as well as targeting indications likely to support and reinforce **Ukraine's offensive efforts** in cyberspace.

Hacktivist groups also **emerged in other countries**, including Poland, from where **Squad303** would be coordinated. Based on Sekoia.io observations, Squad303 hacktivists allegedly developed a tool allowing anyone to send text messages to verified Russian mobile numbers and email addresses to spread anti-war messages and share them on a dedicated website.

Sekoia.io also observed a number of existing hacktivist **groups from around the world** that progressively joined the Russian or Ukrainian side starting from February 2022. **Belarusian Cyber Partisans** (allegedly a group of Belarusian politically motivated hackers) and **AgainstTheWest** (allegedly operating out of western Europe) both show support to Ukraine.

Social media platforms and **messaging apps** such as Twitter and Telegram played a significant role in the hacktivists' implications in the ongoing confrontation in cyberspace. Telegram in particular became a hub for hacktivists groups' organisation. From Sekoia.io observations, they use Telegram for sharing hacking guidelines, pointing targets, publicly claiming past or ongoing attacks and recruiting adherents to their cause.

Based on a CheckPoint report, **the number of Telegram groups increased** sixfold between February 24 and early March 2022. However, most of them (71%) were dedicated to news around the ongoing war, according to the same source. This is likely due to the **great visibility** social networks can provide, the **ease of use**, the **extended functionalities** and the fact that **moderation measures** of messaging apps are hard to implement.

DDoS attacks became one of the most widely used techniques by hacktivist groups. Sekoia.io analysts observed **both pro-Russian and pro-Ukrainian groups** mainly targeting entities of interest with Distributed Denial-of-Service (DDoS) and website defacement attacks over the last year, likely due to 1) the relative ease of carrying out such attacks and 2) their immediate impact and the potential victim's reputational damage it can involve.

In some cases, hacktivists claimed cyber **attacks that were not confirmed** afterwards, highly likely to generate publicity around their actions, to improve their public image and to demoralise the opposing side.

While we believe hacktivist groups are not the most impactful in terms of cyber operations so far, they still conducted successful attacks with significant **operational consequences**, mainly by deploying **ransomware**. For example, one month before the beginning of the Russo-Ukrainian conflict , Belarusian Cyber-Partisans encrypted the servers of Belarus's national state-owned railway company and claimed it as an act of protest against the deployment of the Russian military troops near Ukraine using the Belarusian Railways' system. The hacktivist collective Network Battalion '65 also claimed ransomware attacks against Russian targets without demanding a ransom (or declaring donating it to Ukraine). Therefore, Sekoia.io assess **these ransomware attacks should be considered as disruptive** and not lucrative.

An additional technique widely used by hacktivists since February 2022 is **hack and leak operations**. The **RaHDIt** group (for "Russian Angry Hackers Did It") notably obtained and leaked personal **information about military intelligence representatives** in Ukraine and NATO countries. From their words, the RaHDIt threat actors **cooperate** with the Russian army by providing actionable intelligence about the Ukrainian army.

We assess hack-and-leak campaigns conducted by hacktivist groups directly contributed to the proliferation of stolen data released in the Deep and Dark Web last year. Sekoia.io assess that hack-and-leak operations can possibly be **storefront events** of **future cyber operations**.

At this stage, it is almost certain that the hack-and-leak campaigns involving sensitive data since February 2022 significantly **broadened the attack surface** of affected entities. Apart from compromising the victims' security and reputation, this data can now be used by threat actors as a pivot for **further malicious campaigns**.

The most visible impact of hacktivism during the first year following the Russian invasion of Ukraine was the **reduced availability** of targeted public-facing websites and **disrupted services** due to DDoS attacks and ransomware operations, along with the associated **reputational damage**.

> The proliferation of hacktivist groups joining different sides in the conflict served the purpose of influencing the war narrative.
>
> Tweet this!

Finally, the proliferation of hacktivist groups joining different sides in the conflict served the purpose of **showing suppor**t (or opposition) to ongoing military and political actions and **influencing the war narrative**. Evidence of hacktivist groups influence on war narrative can be illustrated with the **CyberAzov** campaign associated with **FSB-operated Turla**, a reconnaissance operation collecting data related to anti-Russia hacktivists. Sekoia.io assess that the fact this advanced intrusion set was activated to **counter pro-Ukraine hacktivism initiative** shows the **importance** Russian intelligence gives to such cyber threats (cf. FLINT 2022-043).

Cybercrime communities implications

Sekoia.io noted that **cybercrime groups**, assessed to be opportunistic by nature, **did not significantly change their modus operandi** after the beginning of the Russo-Ukrainian conflict.

The first major cybercrime group reported to share their reaction about the conflict was the **now-disbanded Conti syndicate**. The day after the launch of the invasion of Ukraine, Sekoia.io analysts noticed a declaration on Conti's Dark Web site expressing **Conti's support** for the **Russian authorities** in their operations in Ukraine: "The Conti team officially announces its full support for the Russian government".

Even though the initial statement was changed the same day ("We are not associated with any government and we denounce the ongoing war"), it allegedly prompted a group member to leak internal compromising data in a series of posts on social media. While it is uncertain whether this was the reason, **the group decided to disband** later and its members are believed to be now involved in other cybercrime organisations. This is an example of how the war impacted on the structure and functioning of a cybercrime group.

We also observed the **BlackCat** ransomware group claiming an increasing number of **ransomware attacks targeting western energy infrastructures** during last year. Although this happened at a time when Russian attacks on the Ukrainian energetic infrastructure were on the rise, in absence of any evidence of a link between those ransomware attacks and the war, the connection is to be considered as circumstantial.

Additionally, other threat actors are assessed to be **part of the conflict in an indirect way**, notably supplying the underground community with commodity toolkits. Of note, threat actors traditionally offer DDoS tools and services and other cybercrime frameworks on the Deep and Dark Web for sale. Yet this practice changed from Q1 2022 onwards. Not only the frequency of messages related to DDoS increased significantly, but also the ratio of threat actors **offering attack tools for free** to the community soared on Telegram. Sekoia.io asses that the almost unrestricted access to these tools (*e.g.* the "DDoS_RU_Bot" provided by the IT Army of Ukraine) and the target-

oriented communication from leading hacktivist and cybercrime groups will keep driving up the number of DDoS attacks in 2023.

> Sekoia.io assess implications of cybercrime and Dark Web-related threat actors in the conflict were mostly isolated cases.
>
> Tweet this!

One recent example of such a commodity toolkit is the **Passion DDoS-as-a-Service** (DDoSaaS) platform, reportedly attributed to a group affiliated with **Killnet** and already leveraged in attacks against medical institutions across Europe and the United States in early 2023.

Other groups decided **to remain neutral**. For instance, the **LockBit** ransomware group underlined the **apolitical** nature of its activities. Based on a notice published on the group's Dark Web dedicated site, it would be motivated by the fact that LockBit members originate **from both CIS countries** (including Russia and Ukraine) and **countries from all over the world**. It is likely that LockBit adopted this position to **avoid any political-based internal conflict** and to prevent Law Enforcement Agencies' scrutiny.

Overall, we assess that the cybercrime community operating on the Dark Web **did not experience major cleavages** following the war in Ukraine that would clearly divide it into multiple sub-communities, or at least into some distinct pro-Ukrainian and pro-Russian underground bodies. While it remained unitary and the top-tier Russian-speaking cybercrime forums and marketplaces harbour threat actors **regardless of their position** in the conflict**,** we observed several **isolated exceptions**.

For example, in mid-2022 the pro-Ukrainian hacking group **Cyber.Anarchy.Squad** (CAS) created **Dump Forums** – a new cybercrime forum specialised on **exposing** and **selling Russian-related data**. Later in 2022, Cyber.Anarchy.Squad also claimed responsibility for attacks on Russian administration and critical infrastructure and auctioned the **exfiltrated data** to **fund the Ukrainian army**. Another such example is the Infinity forum launched by the **Killmilk** group (part of the Killnet galaxy) in 2023 to reunite the pro-Russian threat actors.

We also monitor dedicated platforms hosting repositories of hacked data, mainly from Russian government agencies and private companies (such as DDoSecrets platform), or else from Ukrainian targets (such as FreeCivilian).

Final words

After a year of confrontation Sekoia.io observes the Russia-Ukraine conflict had different impacts on the cyber threat ecosystem.

Despite tactical evolutions on GRU destructive cyber operations, the mandate of Russian intelligence services conducting cyber operations did not significantly change: the **FSB and SVR** conducting **strategic intelligence-oriented campaigns** in order to **disrupt Kiev's ability to gain support and coordinate its defence**. Sekoia.io assess **GRU**-operated will likely **continue** to **target Ukraine** and **supply chain** in allied Western countries, **with destructive malware** when FSB and SVR will pursue intelligence gathering operations for strategic purposes.

An evolution is still discernible in the ecosystem of non-state cyber threats. Among non-state actors joining the conflict in cyberspace, hacktivist groups were the most involved. Part of hacktivist collectives aligned with Russian or Ukrainian strategic interests are **presumed to cooperate with national intelligence services**.

From Sekoia.io observations, **implications of cybercrime and Dark Web-related threat actors** in the conflict were **mostly isolated cases**. We assess that financially motivated actors taking positions regarding the war partially did it by conviction, but rather by opportunism to benefit from the ongoing targeting trends, and as a precaution with regard to the authorities of their respective countries.

Sekoia.io reminds that the **blurred nature of war** and military secrecy makes it **difficult to get an exhaustive view** of cyber events based on open source. The real impact of destructive operations or the strategic benefits from cyber espionage can not be properly assessed due to the implication of allies, such as the USCyberCom Hunt Forward Operations or the role played by private firms like Microsoft and Amazon in securing Ukraine government data in the cloud.

Thank you for reading this blogpost. You can also consult other blogposts on the same topic:

Featured image done with Midjourney

APT calisto russia turla ukraine

Share this post:
