

CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

January 31, 2023



Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine

This report examines the unspoken connections between the Russian Federation, cybercriminals, and self-described hacktivists in Russia and Eastern Europe in the context of the Russian war in Ukraine. It is a direct continuation of the findings presented in our 2021 report “Dark Covenant: Connections Between the Russian State and Criminal Actors”. This report will be of interest to threat researchers, as well as law enforcement, government, and defense organizations.


Executive Summary

Beginning on February 24, 2022, the Russian cybercriminal threat landscape underwent transformative changes in response to the Russian war in Ukraine. The war brought chaos to the cybercriminal underground, polarizing threat actors in Commonwealth of Independent States (CIS) nations. While some cybercriminal groups declared allegiance to the Russian government, others splintered over irreconcilable ideological differences or remained apolitical, opting to capitalize on geopolitical instability for financial gain. Some groups vanished entirely. Likely as indirect consequences of the war, there have been underground market disruptions, shifts in hacktivist and ransomware targeting, and a spike in financial fraud, among other phenomena affecting the Russian cybercriminal ecosystem.

Throughout these changes, one thing remained largely constant: cybercriminal threat groups continue to occupy important [roles](#) — in direct, indirect, and tacit capacities — with the Russian government. For cybercrime groups who have pledged their allegiance to the Kremlin, the unspoken connections have deepened. Russian cybercriminals and self-described hacktivists are actively involved in operations targeting Ukrainian entities and infrastructure, as well as entities located in states that have declared their support for Ukraine. Recorded Future has observed Russian and Russian-speaking threat actors targeting the United States, United Kingdom, the North Atlantic Treaty Organization (NATO), Japan, and others for financial gain and ego-driven publicity in support of Russia.

Cybercriminal organizations like Conti have overtly declared allegiance to the Russian government, and commodity malware like DarkCrystal RAT, Colibri Loader, and WarZoneRAT, which are available on top-tier Russian-language forums, are being used by advanced persistent threat (APT) groups to target entities in Ukraine. We have identified cybercriminal activities preceding the war, and immediately after it started, that we believe are the work of the Russian state. Russian-speaking, self-described “hacktivist” groups like Killnet and Xaknet are almost certainly actively engaging in information operations (IOs) against organizations and entities in the West, enabled by Russian state-sponsored media with the likely intended goal of stoking fear or decreasing support for Ukraine. We have also identified other phenomena, such as a rise in payment card fraud, database leaks, dark web marketplace closures, and more, that we believe are the consequences of economic, diplomatic, and law enforcement activities aimed at Russian entities due to their support for the war in Ukraine.

“WARNING”

 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

 2/25/2022

 39

 0 [0.00 B]

Figure 1: Conti Gang statement dated February 25, 2022, in which the group allies itself with the Russian government (Source: Conti.News)

Key Judgments

- It remains highly likely that Russian intelligence, military, and law enforcement services have a longstanding, tacit understanding with cybercriminal threat actors; in some cases, it is almost certain that these agencies maintain an established and systematic relationship with cybercriminal threat actors, either by indirect collaboration or via recruitment.
- Based on our understanding of cybercriminal and hacktivist activities related to the Russian war in Ukraine, it is likely that cybercriminal threat actors are working alongside the Russian state to coordinate or amplify Russian offensive cyber and information operations.
- Russian cybercriminal groups, tools, and tactics, techniques, and procedures (TTPs) likely serve to provide plausible deniability for state-sponsored threat actors involved in the Russian war in Ukraine. It is likely that financially motivated threat actors who are capitalizing on geopolitical instability are also aiding and abetting the interests of the Russian state, be it coincidentally or intentionally.
- Russian law enforcement seizures of dark web and special-access sources preceding the war appeared to be a show of good faith by the Russian state, signaling its willingness and ability to thwart cybercrime. However, we believe it is likely that these enforcement actions were intended to undermine allegations of cooperation between cybercriminals and the Russian state, providing further plausible deniability.
- Several cybercriminal industries have undergone transformational changes as a result of the Russian war in Ukraine. These include changes to the malware-as-a-service (MaaS) and ransomware-as-a-service (RaaS) threat landscapes, a rise in Russian payment card fraud, shifts in cybercriminal targeting, changes in infrastructure and hosting, and more.

Methodology

This report synthesizes information derived from open and human sources, including information gathered from monitoring of, and engagement on, dark web, special-access, and social media sources frequented by Russian-speaking cybercriminals. We looked at several English-language forums to cross-reference points of contact and link monikers suspected to be operated by Russian-speaking cybercriminals across the dark web. We also gathered intelligence from open and closed-source messaging platforms, such as Telegram, Tox, and Jabber (XMPP), as well as social media.

Our collections on ransomware extortion, chat, and payment websites helped us connect various ransomware groups with the Russian state. We used qualitative and quantitative methods to study ransomware victimology before and after the Russian invasion of Ukraine on February 24, 2022, to theorize about motives and ideology. This report relies heavily on the use of the Recorded Future Platform® to visualize its findings and draw connections between geopolitical events, cybercriminal threat actors and threat actor groups, advanced persistent threats (APTs), and the Russian state in the context of the Russian war in Ukraine.

We also rely heavily on other forms of OSINT research, such as academic publications, industry white papers, conference presentations, and more, to fill in gaps in our HUMINT collections process. This report uses previous open-source reporting, as well as the original 2021 [Dark Covenant](#) report, as the background and warrant for its research. This report was researched and written between February 24, 2022 and August 24, 2022.

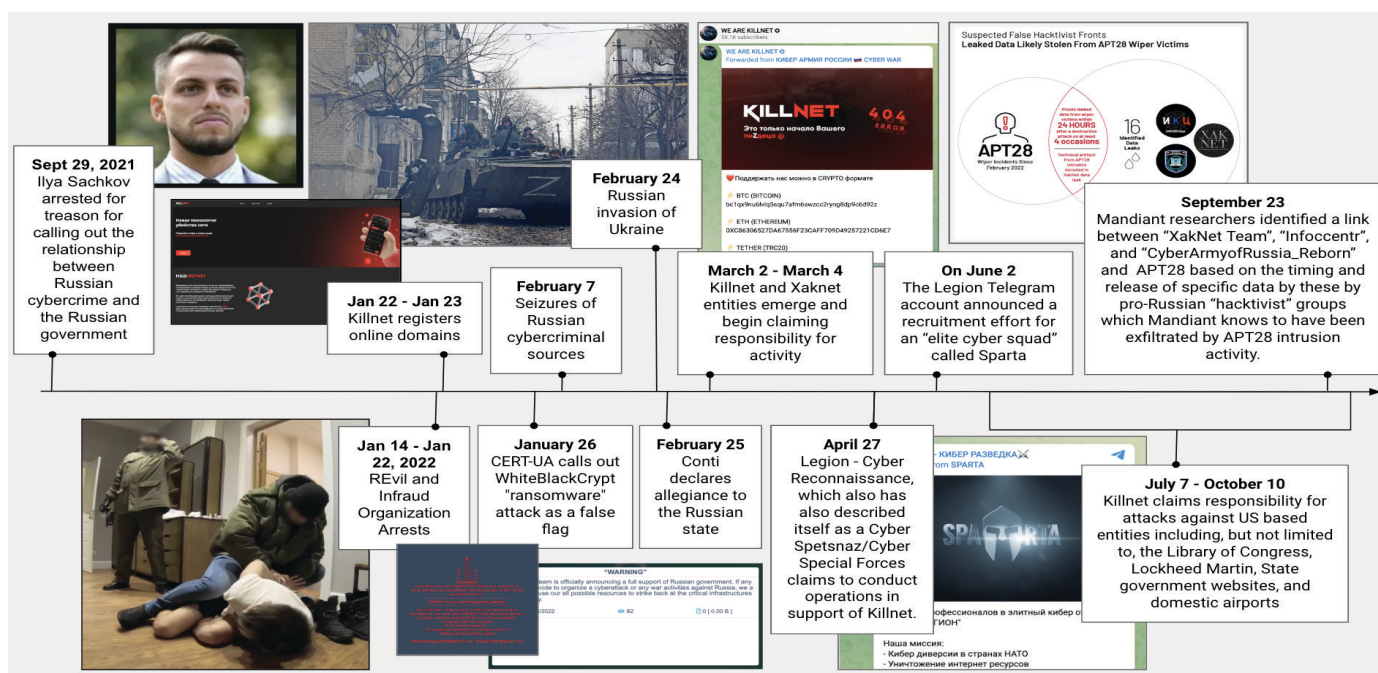


Figure 2: Timeline of events between the cybercriminal ecosystem, self-described hacktivist entities, and state-sponsored groups during the conflict in Ukraine (Source: Recorded Future)

Background

"Dark Covenant"

In 2021, we [detailed](#) how established, distributed networks of individuals in the Russian cybercriminal world and officials in Russian law enforcement or intelligence services — also known colloquially as *siloviki* — are connected. The report detailed how the relationships in this ecosystem are often premised on unspoken, yet understood, agreements that consist of malleable associations. This research was based on historical activity, public indictments, and ransomware attacks. Overall, the report broke down the associations between the Russian cybercriminal environment and the *siloviki* into 3 major categories: direct associations, indirect affiliations, and tacit agreements.

- Direct associations are identified by precise links between state institutions and criminal underground operators; an example of this is Dmitry Dokuchaev, a major in the Russian Federal Security Service (FSB) who was recruited after working as a cybercriminal.
- Indirect affiliations occur in cases where a direct link cannot be established but there are clear indications that the Russian government is using resources or personnel for its benefit; an example of this is the Russian government's likely use of the GameOver Zeus botnet for [espionage](#) or DDoS attacks by "patriotic hackers" during military conflicts.

- Tacit agreement is defined as overlaps in cybercriminal activity, including targeting and timing, that benefit Russian state interests or strategic goals; such activity is conducted without direct or indirect links to the state but is allowed by the Kremlin, which looks the other way when such activity is conducted.

In our 2021 report, we assessed that cybercriminal associations with the *siloviki* would almost certainly continue for the foreseeable future and these associations and activities would likely adapt to provide greater plausible deniability and fewer overt, direct links between both groups.

Since our first report, the Russian government has invaded Ukraine, an event that has illuminated our understanding of Russia's capabilities and shortcomings as they relate to military strength and cyber capacity. For example, a series of leaks about the cybercriminal groups Conti and Trickbot (Wizard Spider) provided an unprecedented look at the relationship between these groups and the state. The conflict has given rise to self-described hacktivists conducting pro-Russian attacks purportedly motivated by patriotic interest; in some cases, however, it is [likely](#) that such groups are providing the Russian government with plausible deniability.

The Russian Invasion of Ukraine

The February 2022 Russian invasion of Ukraine has resulted in a broader humanitarian crisis in Europe as well as heightened international tensions. A number of pro-Russian threat actor groups, as well as some previously unseen entities from within the cybercriminal ecosystem, have participated in the conflict, which Russia has conducted across the physical, information, and cyber domains. The war has already seen large-scale distributed denial-of-service attacks (DDoS), website defacements, phishing and spam campaigns, malware deployment, and wiper attacks against numerous Ukrainian entities in both the government and private sector.

Russian Cybercrime in Cyber Warfare

The Russian intelligence services' recruitment of highly skilled computer programmers, network specialists, and other technologically savvy personnel dates back to at least the 1990s, according to a [Meduza](#) report published on December 12, 2019. In this report, an FSB officer is quoted as suggesting that as soon as hackers achieve a certain level of success, they are targeted for recruitment: "In [the FSB officer's] words, as soon as 'the first technical college student from a humble background brought a Ferrari out onto the streets of Moscow', FSB agents started recruiting — both getting the cybercrime business under control and making it their own".

In his 2019 [book](#) "Intrusion: A Brief History of Russian Hackers", Daniil Turovsky quoted an unnamed Russian hacker who provided an account of the associations between the criminal underground and the Russian intelligence services. According¹ to the hacker, the Center for Information Security at the Russian Federal Security Service (CIB FSB) had limited technical staff, so it often brought in outside specialists, reportedly going so far as to hide some hackers in safe houses.

Andrei Soldatov, a Russian investigative journalist and co-author of "The Red Web", a book about the Kremlin's online activities, [said](#) that while the Russian government's tactic of outsourcing cyber operations to various groups helps distance themselves (and ultimately provides deniability), it also left them vulnerable to hackers running amok.

1 [http://web.archive\[.\]org/web/20210720234233/https://www.rulit\[.\]me/books/vtorzhenie-kratkaya-istoriya-russkih-hakerov-read-586355-49.html](http://web.archive[.]org/web/20210720234233/https://www.rulit[.]me/books/vtorzhenie-kratkaya-istoriya-russkih-hakerov-read-586355-49.html)

Russian Cybercrime in Foreign Policy

In September 2021, around the time we released our initial *Dark Covenant* report, we identified a shift in calculus following recent high-profile ransomware attacks and subsequent intergovernmental consultations between the US and Russia. At the time, high-profile ransomware attacks against [Colonial Pipeline](#), [JBS](#), and [Kaseya](#) led the US to increase pressure on the Russian government to take action against the cybercriminal groups behind this activity. Around this time, the administrators of 2 major Russian-language forums, Exploit and XSS, quickly banned ransomware topics on their criminal underground platforms, likely as a result of the increased pressure. However, ransomware activities persist in the form of "initial access" and "data leak" brokerage services. Moreover, the DarkSide, REvil, and Avaddon ransomware families halted extortionist activities right before or days after the first [meeting](#) between US president Joe Biden and Russian president Vladimir Putin on June 16, 2021, in Geneva, Switzerland. This pause was only temporary, as ransomware attacks continued in 2022, including attacks affecting critical infrastructure targets in the energy sector and transportation entities in Europe ([1](#), [2](#), [3](#)).

Threat Analysis

Pre-Invasion Timeline of Major Events

Many of the events preceding the invasion of Ukraine demonstrate the unspoken connections between cybercrime and the Russian state. The research time frame for this section is September 29, 2021, to February 24, 2022.

Ilya Sachkov Arrested

On September 29, 2021, the FSB [detained](#) Ilya Sachkov, founder and CEO of Group-IB, on "high treason" charges, pursuant to Article 275 of Russia's Criminal Code. Sachkov, a critic of the Russian government's attitudes towards cybercrime and ransomware, as well as a critic of Maksim Yakubets and Evil Corp, was [reported](#) to have provided the US government with information on "Fancy Bear", a Russian APT group alleged to have interfered with the 2016 US presidential election.

[Statements](#) made by Sachkov in 2020, about Yakubets' [purported](#) leadership role within Evil Corp, [support](#) for the Russian government, and affiliations with the FSB — such as access to or engagement with classified materials and work on specific government projects — were marked by overt criticism including [speculation](#) that the FSB had been actively protecting Yakubets. As such it is believed that these statements, along with the negative implications they may have towards the Russian government, could potentially have contributed to his arrest.

According to Bloomberg, Sachkov had been involved in a number of “[transgressions](#)” over his career, primarily related to his outspoken perspective on the Russian government’s complicity in cybercrime. It is alleged that Sachkov’s disclosure of the Fancy Bear operations targeting the 2016 US presidential election provided the US Federal Bureau of Investigation (FBI) and US Department of Justice (DOJ) with the evidence required to identify, disrupt, and indict Russian Main Intelligence Directorate/Main Directorate (GRU/GU) Units 26165 and 74455 (Sandworm) personnel involved in the hacking. Given the timeline, if such allegations about Sachkov’s collaboration with US law enforcement are true, it is possible that the information Sachkov provided directly [resulted](#) in the July 13, 2018, indictment of 12 GRU/GU officers from the Special Counsel Investigation into Russian election interference. However, according to Bloomberg, sources indicated that the charges levied against Sachkov “relate to a separate incident from 2014”.

Group-IB told media organizations that “Sachkov worked in recent years to ingratiate himself with Western intelligence and law enforcement agencies” and that Sachkov “sought to reduce his dependence on Group-IB’s Russian state contracts”, which likely alarmed Russian government officials.

[According](#) to US cybersecurity executive Christopher Painter, Sachkov’s arrest “sends a bad signal about [cybercrime] cooperation with the US”. Sachkov’s arrest is widely considered by commentators, journalists, and human rights activists to be a case of political persecution intended to silence public-facing executives that point out the direct and indirect links between the Russian state and cybercrime. Sachkov’s arrest also marked the beginning of a series of high-profile arrests and seizures that took place over the next 6 months preceding the Russian war in Ukraine.

There is an understood agreement in Russia about the [relationship](#) between the oligarchy and the state. Generally, whether oligarchs are protected from or [subject to prosecution and state scrutiny](#) depends on how vocal they are about [opinions](#) in opposition to certain Kremlin policies. As long as public statements by oligarchs run parallel to the Russian state-sponsored media narrative, it is likely that no action will be taken against them. Ilya Sachkov appeared to have broken this rule by voicing concerns about Russia’s relationship with cybercrime. At the time of Sachkov’s arrest, some researchers speculated that this was a politically motivated move intended to silence any potential opposition to offensive Russian cyber operations.

REvil Affiliates Arrested

On January 14, 2022, Russian law enforcement [reported](#) that it apprehended 14 members of the REvil ransomware group. On January 15, 2022, the Tverskoi District Court of Moscow [released](#) the names of 8 individuals charged in the FSB’s investigation into REvil. Physical addresses belonging to another 6 individuals were also raided, but it is unclear if those raids resulted in the arrests of the individuals living at those addresses. Following the initial reports, the FSB released an official statement confirming that raids had taken place against “members of an organized criminal community”, indicating that the raids were prompted by an appeal from US authorities to target the leadership of a community responsible for introducing malware into foreign companies, encrypting information, and crimes involving extortion. FSB named REvil as the target of its investigation and alleged that criminal intent was established over the course of the investigation by tracking the development of malicious software, laundering of stolen funds, and purchase of luxury goods on the internet.

These 8 individuals were charged under Part 2 of Article 187 of the Criminal Code of the Russian Federation — a money-laundering charge that carries a maximum of a 7-year sentence. Typically, criminals charged for hacking and compromising computer infrastructure are charged under Articles 272 and 273 of the Russian Criminal Code. However, the burden of proof in Russia is much lower for charges under Article 187. It is possible that the charges will be updated later to include offenses found under Articles 272 and 273.

This wave of arrests was unprecedented at the time. This was the first time in the modern ransomware-as-a-service (RaaS) era in which the Russian state directly acknowledged a request by US law enforcement to arrest Russian nationals associated with a major cybercrime group. At the time, many researchers speculated that this was a sign of good faith by Vladimir Putin to demonstrate to the international community that Russian law enforcement was capable of, and willing to, crack down on cybercrime. However, this move was likely intended to provide plausible deniability to Russian intelligence and law enforcement services in any future cooperation with cybercriminal groups, by attempting to demonstrate that the Russian state and cybercrime are not connected. In fact, the arrests appear to be highly [publicized](#) by the Russian government, with some [speculation](#) from cybersecurity industry professionals like John Hultquist, that, though the arrests are ultimately beneficial overall they could be considered to have an element of “signaling”, to a skeptical viewer.

Infraud Organization Arrests

On January 22, 2022, the FSB detained Andrey Sergeevich Novak, a member of the Infraud Organization and administrator of UNICC Shop. UNICC Shop is one of the largest card-not-present (CNP) dark web shops, having grossed approximately \$358 million and sold 13 million compromised records since 2013.

On January 12, 2022, the shop's administrators announced that UNICC Shop would voluntarily cease operations on January 22, 2022. The announcement indicated that the shop's administrators intended to retire and advised users to withdraw their funds within 10 days. The post also indicated that LuxSocks, a proxy service used by cybercriminals, was also due to close.

Andrey Novak was reportedly known by the username "Unicccshop" on a variety of carding forums, as well as the usernames "Faaxxx" and "Faxtrod" on Verified Forum. The FSB also placed 3 other suspected members of the Infraud Organization under house arrest: Kirill Samokutyaev, Konstantin Vladimirovich Bergman, and Mark Avramovich Bergman. As of this writing, these individuals have not yet been connected to any known username on a shop or forum. The FSB is currently working on detecting other members of this cybercriminal organization.

Andrey Novak has been [sought](#) by the US DOJ since February 2018, following the arrests of 13 alleged members of the Infraud Organization. The US has alleged that Novak is part of a cybercriminal cartel that, as of 2018, was responsible for approximately \$580 million in damages. A Russian law enforcement source [told](#) TASS that Russia has no plans to extradite Novak to the US, as the extradition of Russian nationals to foreign countries is prohibited under Russian federal law.

Russian Cybercriminal Sources Seized

On or around February 7, 2022, Directorate "K" of the Russian Ministry of Internal Affairs seized the domains of at least 4 additional Russian-language dark web and special-access sources that facilitated cybercriminal activity. The seized websites are as follows:

- SkyFraud, a mid-tier Russian-language forum dedicated to payment card fraud, the sale of personally identifiable information (PII), counterfeiting, money laundering, scamming, and e-commerce fraud.
- Ferum Shop, a dark web shop specializing in the sale of fraudulent payment cards with card verification values (CVV), for the purpose of conducting fraudulent online transactions.
- Trump's Dumps, a dark web shop run by the threat actor "D. Trump" that specialized in the first-hand sale of compromised payment card information.
- UAS Shop, a dark web shop that specialized in the sale of remote desk protocols (RDPs), as well as compromised Social Security numbers (SSNs).

The Russian-language seizure banners indicated the websites were permanently closed during the course of a special operation by Russian law enforcement agencies. The announcement continues with a warning that the theft of monetary funds from stolen bank cards is illegal, citing Article 187 of the Criminal Code of the Russian Federation.

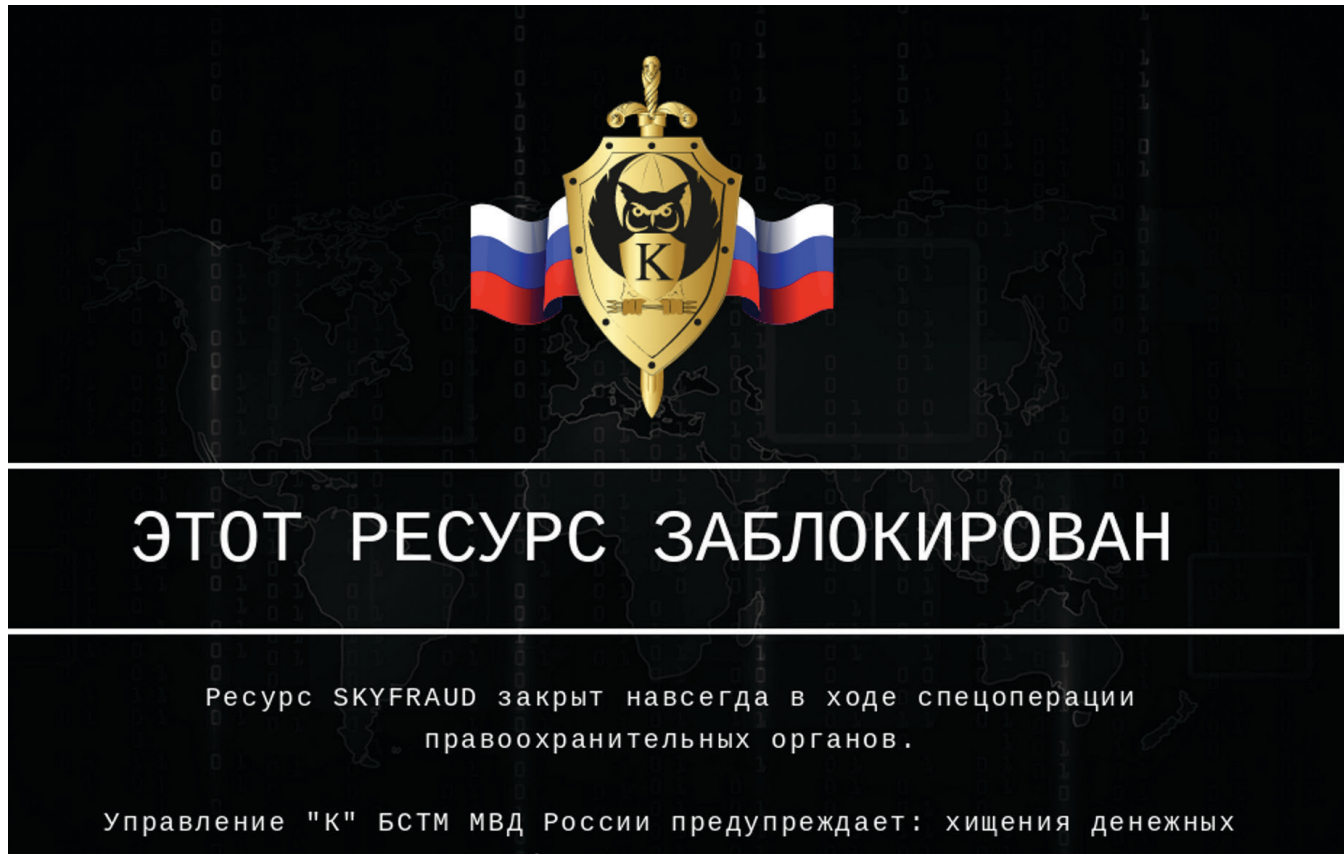


Figure 3: Seizure banner for SkyFraud, indicating that “Directorate K” of the Russian Ministry of Internal Affairs had closed the website. Directorate K is a division of the Ministry of Internal Affairs that investigates crimes in the field of information technology. (Source: Recorded Future)

Database Leaks Immediately Preceding Invasion

We identified more than 57,000 references to Ukraine on dark web, underground, and special-access forums between February 1, 2022 and February 24, 2022. The vast majority of this content is composed of misinformation, trolling, and benign political chatter. However, we were able to identify several credible threats to Ukrainian, Russian, Belarusian, and NATO entities during the time preceding the February 24 invasion and immediately afterward. It is possible that many of the seemingly benign and unrelated database leaks, initial access sales, and advertisements on dark web and special-access forums preceding the invasion were not the responsibility of non-state actors, but rather of state-sponsored threat actors and APTs in disguise, such as Ember Bear. The anonymity granted by these forums provides plausible deniability. The most noteworthy events we observed are listed below:

Ukrainian Citizenship Data for Sale on Raid Forums

On February 12, 2022, “NetSec”, also known as “Scarf33”, a member of the mid-tier and now-defunct Raid Forums, leaked 53 million records of Ukrainian citizenship data. The data set

contains 53 million lines, has a compressed file size of 1 GB (7 GB uncompressed), and contains the following PII: birth dates, places of birth, places of residence, geographic area codes, street names, phone numbers, physical addresses, and registration codes. NetSec claims to be unaware of the source of the data set, and another forum user, “BullDozzer”, speculated that it seems to be a recompiled database of the Ukrainian tax service from 2006.

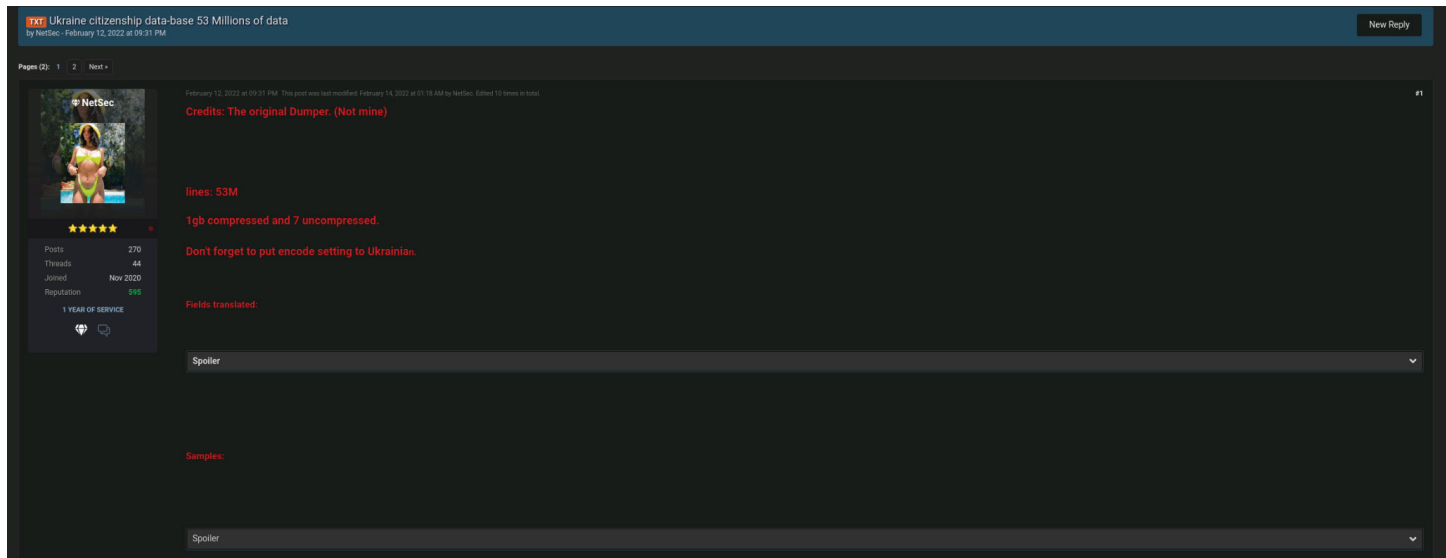


Figure 4: "NetSec" advertising Ukrainian citizenship database (Source: Raid Forums)

"FreeCivilian" Selling Multiple Ukraine Government Databases

Beginning in January 2022, "FreeCivilian", a former member of mid-tier Raid Forums, was selling multiple databases from Ukraine on their personal website, hosted on the Tor network:

- The "Wanted" Portal of the Ministry for Internal Affairs; wanted[.]mvs[.]gov[.]ua
- The Ministry for Communities and Territories Development of Ukraine; minregion[.]gov[.]ua
- The Motor (Transport) Insurance Bureau of Ukraine; mtsbu[.]ua
- Motor Sich Joint Stock Company; motorsich[.]com
- Kyiv City State Administration; kyivcity[.]com
- The Road Safety Service of the Ministry for Internal Affairs; bdr[.]mvs[.]gov[.]ua
- The Department of Housing and Communal Government Services; gkh[.]in[.]ua
- The Cabinet of Ministers of Ukraine; kmu[.]gov[.]ua
- The Ministry of Education and Science of Ukraine; mon[.]gov[.]ua
- The Ministry of Agrarian Policy and Food of Ukraine; minagro[.]gov[.]ua
- The Ministry of Foreign Affairs of Ukraine; mfa[.]gov[.]ua

Additionally, FreeCivilian's website lists 2 already-sold databases: Public Services Portal (DIIA; diia[.]gov[.]ua) and Driver's Office of the Ministry of Internal Affairs (e-driver[.]hsc[.]gov[.]ua). On January 20, 2022, the threat actor advertised the diia[.]gov[.]ua database on Raid Forums. Raid Forums members commented that the database was not legitimate and the passport data contained was in an outdated format, and thus could not have been in the DIIA. FreeCivilian can [likely be attributed](#) to the Russian APT group Ember Bear.

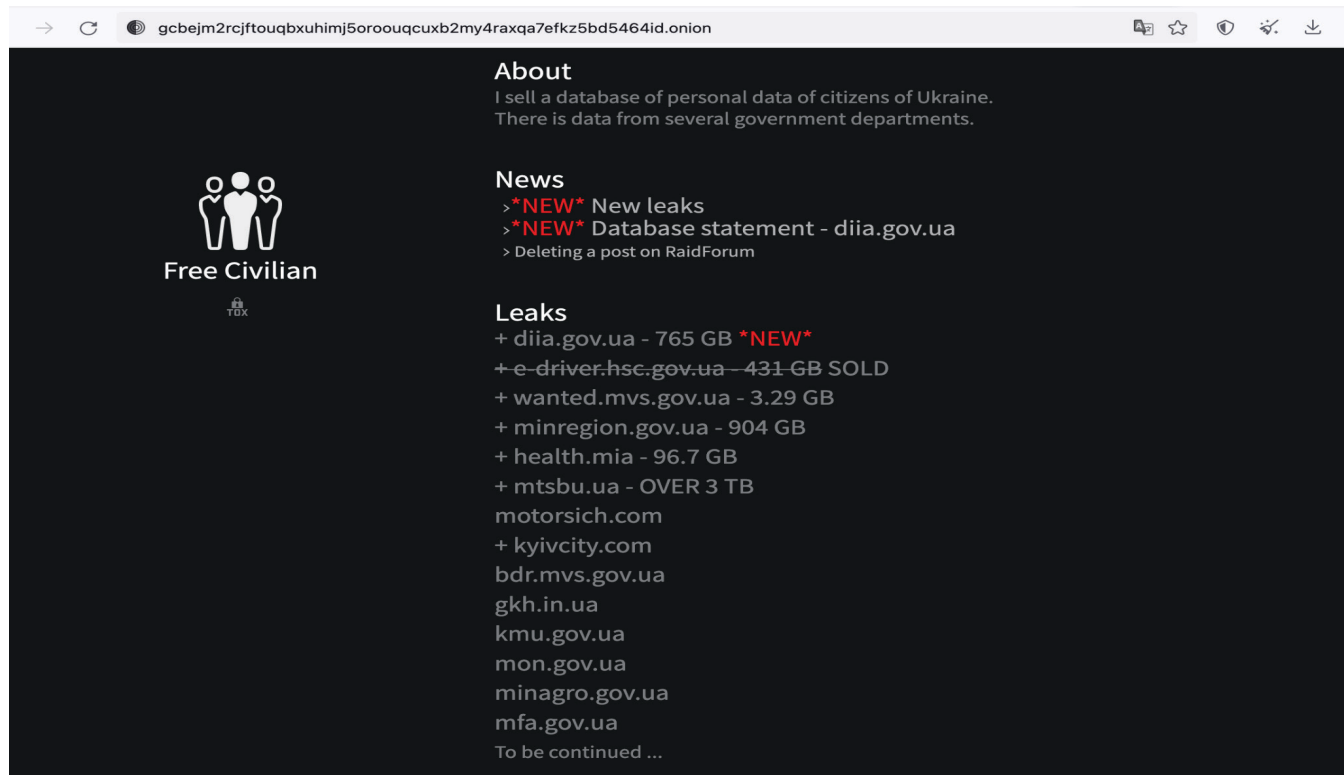


Figure 5: FreeCivilian. Screenshot from February 24, 2022. (Source: Recorded Future)

“danieltx51” Sells Ukrainian Ministry of Foreign Affairs Data on Raid Forums

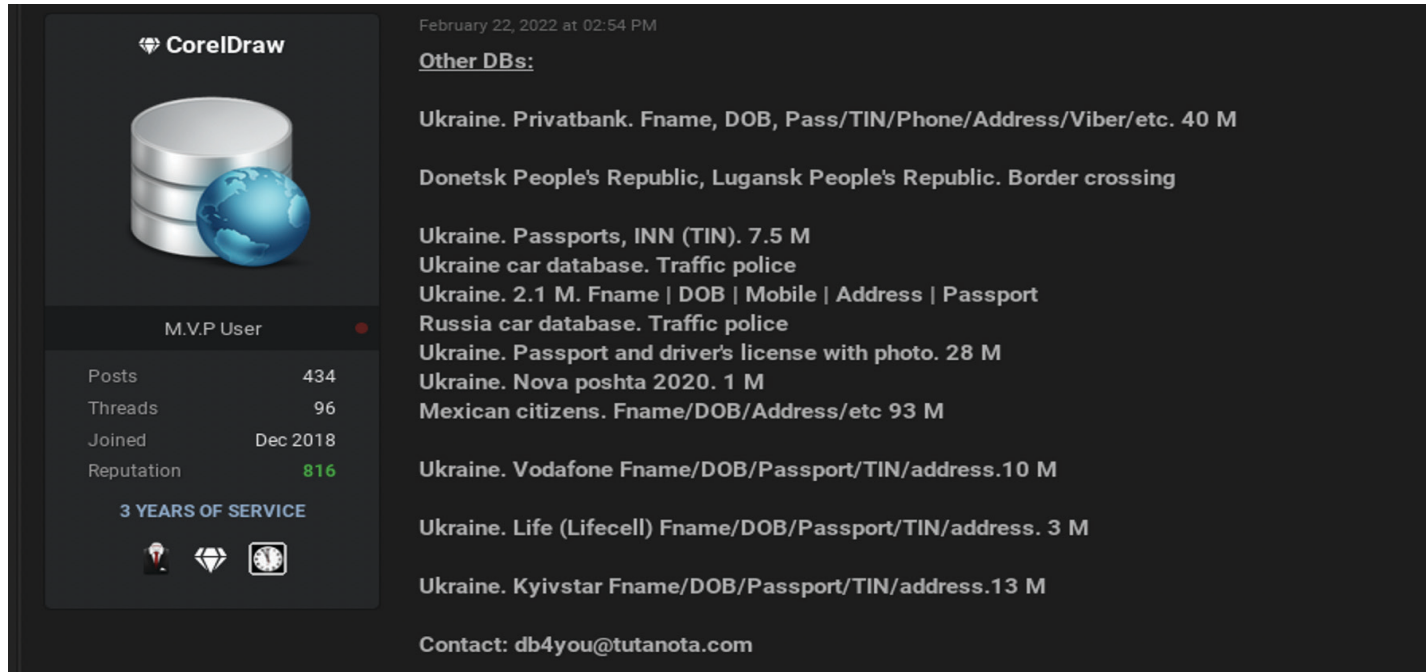
On February 21, 2022, “danieltx51”, a member of the mid-tier Raid Forums, sold an alleged data leak related to the Ukrainian Ministry of Foreign Affairs (MFA; mfa[.]gov[.]ua). The threat actor did not provide any sample data, and the database was likely a repost of the FreeCivilian leaks. At least 7 other unidentified threat actors purchased the compromised information.

“CoreIDraw” Selling Multiple Databases Related to Ukraine

From February 22, 2022 to February 24, 2022, the morning after the Russian invasion of Ukraine, “CoreIDraw”, a member of the mid-tier Raid Forums, posted advertisements for multiple databases related to Ukraine:

- 40 million-record database of PII related to the customers of PrivatBank; privatbank[.]ua
- Databases of unspecified types and sizes related to “border crossings” in the Donetsk People’s Republic (DPR) and Luhansk People’s Republic (LPR)
- 7.5 million-record database of Ukrainian passports
- A database of unspecified type and size related to Ukrainian car registrations, license plates, and records related to Ukrainian traffic police

- 2.1 million-record database of PII related to the citizens of Ukraine
- 28 million-record database related to passports and driver’s licenses, with full scans and photographs, related to Ukrainian citizens
- 1 million-record database related to Nova Poshta (novaposhta[.]ua), a private postal and courier service in Ukraine
- 10 million-record database related to the Ukrainian customers of Vodafone Ukraine (vodafone[.]ua)
- 3 million-record database related to the customers of lifecell (lifecell[.]ua), a Ukrainian telecommunications company
- 13 million-record database related to Kyivstar (kyivstar[.]ua), a Ukrainian telecommunications company



February 22, 2022 at 02:54 PM

CoreIDraw

M.V.P User

Posts 434
Threads 96
Joined Dec 2018
Reputation 816

3 YEARS OF SERVICE

Other DBs:

Ukraine. Privatbank. Fname, DOB, Pass/TIN/Phone/Address/Viber/etc. 40 M

Donetsk People's Republic, Lugansk People's Republic. Border crossing

Ukraine. Passports, INN (TIN). 7.5 M

Ukraine car database. Traffic police

Ukraine. 2.1 M. Fname | DOB | Mobile | Address | Passport

Russia car database. Traffic police

Ukraine. Passport and driver's license with photo. 28 M

Ukraine. Nova poshta 2020. 1 M

Mexican citizens. Fname/DOB/Address/etc 93 M

Ukraine. Vodafone Fname/DOB/Passport/TIN/address.10 M

Ukraine. Life (Lifecell) Fname/DOB/Passport/TIN/address. 3 M

Ukraine. Kyivstar Fname/DOB/Passport/TIN/address.13 M

Contact: db4you@tutanota.com

Figure 6: CoreIDraw advertising several databases related to Ukrainian government entities (Source: Raid Forums)

This was the first major leak and sale of compromised Ukrainian data following the Russian invasion of Ukraine. The threat actor CoreIDraw, while potentially related to Russian state operations, was likely a financially motivated threat actor who attempted to capitalize on geopolitical instability. It is possible that CoreIDraw took advantage of Ukraine's focus on Russian kinetic and APT operations by running SQL injections and database exfiltration attacks on vulnerable Ukrainian websites. Since the compromised data affects the administration and operations of the Ukrainian government, CoreIDraw might have sold the databases to Russian state-sponsored or state-nexus threat actors, who could use the compromised information to enable long-term information operations or espionage campaigns targeting Ukrainian citizens and government officials.

"Psycho_Killer" Selling PII Database of 56 Million Ukrainian Citizens

On February 24, 2022, "Psycho_Killer", a member of the top-tier forum Exploit, posted an advertisement for a PII database related to 56 million Ukrainian citizens, which differed from the leak that NetSec had advertised. In the weeks preceding the Russian war in Ukraine, a 2006 PII database related to 53 million Ukrainian citizens appeared on a number of mid- and top-tier forums. The threat actor claimed that this database is current as of 2020 and is not related to the 53 million-record 2006 database. The threat actor did not specify the price openly and uses Jabber psycho_killer@jabberix[.]com as a point of contact. The threat actor indicated that sample data can be acquired via Jabber engagement and that more databases related to Ukraine are available.

"Featherine" Selling Database Leak Related to Ukrainian "Diia" E-Governance Portal

On February 24, 2022, "Featherine", a member of the mid-tier Raid Forums, posted an advertisement for a 1.35 GB SQL database related to Diia (diia[.]gov[.]ua), the e-governance and public services portal of the Ministry of Digital Transformation of Ukraine. It is not clear whether there is a difference between the Diia leaks advertised by FreeCivilian and by Featherine. However, FreeCivilian has specified that their leaks contain access to the web server in addition to exfiltrated data. Based on sample data and threat actor indications, the Diia leak from Featherine is data only. Some threat actors accused Featherine of re-selling old data, which Featherine denied.

Cybercriminal Threat Actor Analysis

ALPHV/BlackCat Ransomware

On February 28, 2022, ransomware group ALPHV (BlackCat) — part of the larger CARBON SPIDER (FIN7, Carabanak) nexus — announced that it will be taking an apolitical stance regarding the Russian invasion of Ukraine, condemning Conti Gang's pro-Russian stance. In its statement, the group writes that “we are incredibly saddened by what is happening ... in our business, there are no nationalities, fictional borders, or any other reason why people can kill people”. ALPHV states that it does not believe the internet, including its “dark side”, is any place for politics.



Support ALPHV

348845



Support AL...

Мы крайне огорчены
происходящим. В нашем бизнесе
нет национальностей,
вымышленных границ или
какой-либо иной причины по
которой люди могут убивать

14:00:00

Figure 7: Partial statement by ALPHV in response to the Russian invasion of Ukraine (Source: [ALPHV](#))

Conti Ransomware

On February 25, 2022, Conti Gang, the threat group operating the Conti ransomware, posted a statement on its website announcing “full support of the Russian government” and stating that it will use “all possible resources to strike back at the critical infrastructures of an enemy”. However, the threat group later amended the statement to add that it does not “ally with any government” and that it “condemn[s] the ongoing war” between Ukraine and Russia. The amended version declared that the group will use its “full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia and Russian-speaking region of the world”.

“WARNING”

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022

39

0 [0.00 B]

Figure 8 The original Conti Gang statement dated February 25, 2022, in which the group allies itself with the Russian government (Source: Conti.News)

“WARNING”

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

2/25/2022

905

0 [0.00 B]

Figure 9: Amended statement from Conti Gang saying the threat group will use its capacity to retaliate against Western forces targeting Russia (Source: Conti.News)

On February 27, 2022, a Ukrainian security researcher shared internal files related to the Conti Gang, including Jabber chat logs, on social media. The leaked files contained approximately 600 JSON files with internal Jabber chat logs and source code for various tools used by Conti Gang including Conti Locker v2, an older version of the Conti decrypter, Conti admin panel, Trickbot Command Dispatcher, and Trickbot Data Collector. The researcher has posted multiple pro-Ukrainian statements and appears to have leaked the files following the pro-Russian government statements Conti Gang posted on its website. The security researcher maintains their anonymity and as of this writing continues to post intermittently on its social media account. We indexed the leaked Jabber logs into the Recorded Future Platform under the source Conti Gang Leaked Chats.

Leaked Item Description (# of Files)	Date
Conti Jabber logs (1)	15:22 ET, February 27, 2022
2020 Conti Jabber logs (11)	17:22-17:24, 17:25 ET, February 28, 2022
2020 Conti Jabber logs, dump #2 (16)	15:52-18:05 ET, February 28, 2022
Screenshots of Conti root server	23:32-23:34 ET, February 28, 2022
Conti root server passwords	01:17, 1:19 ET, March 1, 2022
Conti RocketChat leak	01:49 ET, March 1, 2022
Conti - Trickbot Jabber leak	03:40 ET, March 1, 2022
Conti document repository	05:57 ET, March 1, 2022
Misc. Conti Jabber logs (2)	07:16 ET, March 1, 2022
Doxxing "begemot"	07:17 ET, March 1, 2022
Conti ransomware source code	10:17 ET, March 1, 2022
Misc. "fresh" Conti Jabber logs	14:07 ET, March 2, 2022
Conti ransomware source code v3	02:38 ET, March 20, 2022
Interview w/CNN	09:23 ET, March 30, 2022

Table 1: Leaked item description with time stamps (Source: Conti Gang Leaked Chats)

CoomingProject

On February 26, 2022, ransomware-as-a-service threat group CoomingProject announced on its Telegram channel that it would be supporting the Russian government in the event of cyberattacks targeting Russia. On February 27, 2022, threat group "AgainstTheWest" posted information on its social media page implying that it had passed information about the identities of CoomingProject operators to French law enforcement. AgainstTheWest alleged that CoomingProject is operated by 6 "teenagers and young adults" in France. We have not verified the legitimacy of AgainstTheWest's claims. At the time of this writing, CoomingProject's Telegram channel is no longer active.

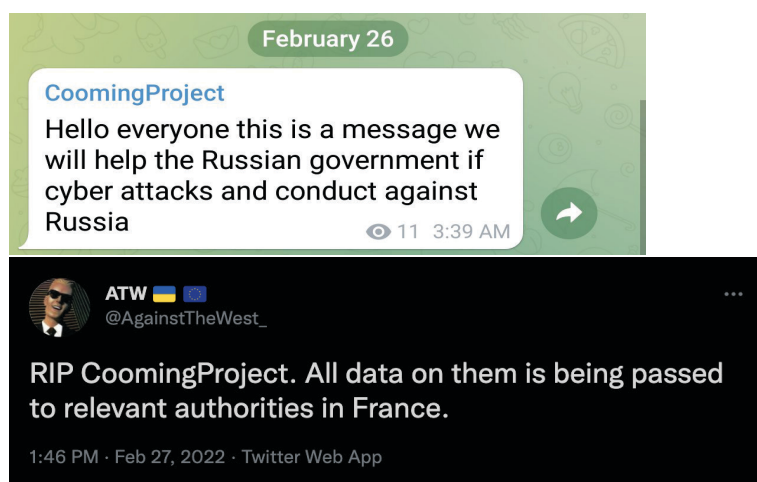


Figure 10: Left: Statement by CoomingProject on its Telegram channel siding with the Russian government. Right: AgainstTheWest implies that law enforcement has been notified of CoomingProject operators' identities. (Source: AgainstTheWest and CoomingProject)

LockBit 2.0 (3.0)

On February 26, 2022, the ransomware-as-a-service threat group LockBit 2.0 posted a statement on its extortion website, LockBit Blog, about its stance on the conflict between Russia and Ukraine. In the statement, which is available in languages including Russian, English, French and Spanish, the threat group proclaimed that its members are "all apolitical" and for them "it is just business", noting that the group "will never, under any circumstances, take part in cyberattacks on critical infrastructure of any country in the world or engage in any international conflicts".

Многие спрашивают нас, будет ли наше международное сообщество пентестеров с пост оплатой, угрожать западу на критически важные инфраструктуры в ответ на кибер агрессию к России? Наше сообщество состоит из многих национальностей мира, большая часть наших пентестеров — это жители СНГ в том числе русские и украинцы, но также в нашей команде есть американцы, англичане, китайцы, французы, арабы, евреи и многие другие. Наши программисты разработчики проживают на постоянной основе в разных странах мира в Китае, США, Канаде, России и Швейцарии. Наши сервера находятся в Нидерландах и Сейшельлах, все мы простые и миролюбивые люди, все мы Земляне. Для нас это просто бизнес и все мы аполитичны. Нас интересуют только деньги за нашу безобидную и полезную работу. Мы всего лишь проводим платное обучение системных администраторов всего мира, как правильно настроить корпоративную сеть. Мы никогда и ни при каких обстоятельствах не будем принимать участие в кибератаках на критические инфраструктуры любой страны мира и вступать в какие-то международные конфликты.

Many people ask us, will our international community of post-paid pentesters, threaten the west on critical infrastructure in response to cyber aggression against Russia? Our community consists of many nationalities of the world, most of our pentesters are from the CIS including Russians and Ukrainians, but we also have Americans, Englishmen, Chinese, French, Arabs, Jews, and many others in our team. Our programmers developers live permanently around the world in China, the United States, Canada, Russia and Switzerland. Our servers are located in the Netherlands and the Seychelles, we are all simple and peaceful people, we are all Earthlings. For us it is just business and we are all apolitical. We are only interested in money for our harmless and useful work. All we do is provide paid training to system administrators around the world on how to properly set up a corporate network. We will never, under any circumstances, take part in cyber-attacks on critical infrastructures of any country in the world or engage in any international conflicts.

Figure 11: LockBit statement proclaiming neutrality in international conflicts (Source: LockBit 2.0 Blog)

Advanced Persistent Threat Activity

Russian advanced persistent threat (APT) groups like UAC-0113 have been using commodity malware available on top-tier Russian-language forums as well as deploying attacks that employ overt hallmarks of ransomware to mask their use of custom, destructive tooling. The use of commodity tooling appears to have increased in comparison to past years, during which custom malware was primarily used in operations. In some cases, commodity malware is likely being adopted to complicate attribution efforts or provide plausible deniability for Russian state-sponsored threats. In other cases, commodity tools are likely used for expediency and to reduce the costs of espionage campaigns.

Misdirection: Use of WhiteBlackCrypt in Wiper Attacks

On January 26, 2022, CERT-UA [published](#) a comparative analysis of WhisperGate and the Encrpt3d (also known as WhiteBlackCrypt) wiper malware disguised as ransomware, identifying an 80% code overlap. CERT-UA assessed that WhisperGate was deliberately designed to mimic WhiteBlackCrypt as part of a false-flag operation attempting to blame the attack on a pro-Ukrainian hacking group:

- WhiteBlackCrypt is known to use an ASCII depiction of a trident, Ukraine's official coat of arms, in the ransom note it shows to users.
- WhiteBlackCrypt reused the same Bitcoin address, 19B5Bt11oUqYnwSXfBgRpwwDGg5Ajirbjn, to solicit ransom payments as an address that was previously reportedly used in email bomb threats sent to Russian organizations in 2019. Some of the funds gathered through this campaign [were allegedly sent](#) to a group associated with the Ukrainian special services.

- [According](#) to the State Service of Special Communications and Information Protection of Ukraine, a Russian Telegram channel used the aforementioned 2 incidents — involving the historic use of the Bitcoin address and the inclusion of the same address in the Encrpt3d tooling — to incorrectly link the WhiteBlackCrypt ransomware to Ukraine's Special Services and Armed Forces.
- An individual who posed as the same person who blackmailed Russian organizations in 2019 reemerged in January 2022 when they mass-messed and urged Ukrainian organizations to mount attacks against Russia.

The WhisperGate activity was almost certainly [conducted](#) by operators tied to the Russian government but has not been attributed to existing groups and instead to newly designated entities. The group is referred to as DEV-0586 by Microsoft, [UAC-0056](#) by CERT-UA, [Ember Bear](#) by CrowdStrike, [Bleeding Bear](#) by Elastic, and [Lorec53](#) by NSFOCUS Security Labs.

It is highly likely that the WhisperGate attack was conducted by a Russian state-sponsored or state-nexus threat actor, based on:

- The coordination with UNC1151's website defacements
- The similarities to past Russian state-sponsored destructive malware attacks, particularly with regards to how this attack was initially staged as a ransomware attack in order to cover for an actual destructive intrusion, much like NotPetya and BadRabbit
- The attack being destructive instead of financially motivated

- The shared victimology with other cyberattacks conducted by Russian state-sponsored and state-nexus threat actors before and during Russia's war against Ukraine
- The false-flag attempt to pin the attack on a pro-Ukrainian hacker group that had allegedly targeted Russia in the past

UAC-0113 Commodity Malware Use

UAC-0113, a group that CERT-UA has indicated with moderate confidence is likely linked to Sandworm, has been employing a number of different commodity malware families that have been in use since at least 2018, including DarkCrystal RAT, CrescentImp, Colibri Loader, as well as Warzone RAT. CERT-UA initially [reported](#) on June 10, 2022, about UAC-0113's use of CrescentImp malware to target Ukrainian domestic media entities such as radio stations, newspapers, and news agencies. On June 24, 2022, CERT-UA indicated that UAC-0113 had used DarkCrystal RAT, delivered via a malicious lure document likely targeting individuals or entities in Ukraine with the goal of gaining access to information about Ukrainian military service personnel in relation to matters of legal assistance. Although the theme of this lure document was focused on legal matters pertaining to military service personnel, CERT-UA noted that the attack was also likely targeting telecommunications providers of Ukraine.

Insikt Group used intelligence provided by CERT-UA to discover additional command and control (C2) infrastructure linked to UAC-0113; the information uncovered shows the continuing use of commodity malware use, with shifts away from CrescentImp and DarkCrystal RAT to Colibri Loader and Warzone RAT, as well as overlaps in previously described TTPs employed by the threat actor, such as ongoing efforts to masquerade as telecommunication providers operating within Ukraine.

Hacktivist Threat Actor Analysis

Cyber Army of Russia

Since the start of the war, at least 2 self-proclaimed patriotic, pro-Russian hacktivist groups, Killnet and Xaknet, under the auspices of the Cyber Army of Russia, emerged as noticeably vocal and active supporters of the Kremlin. The Cyber Army of Russia is a Russian troll farm and source of pro-Russian disinformation, as well as the most popular source of Killnet and Xaknet propaganda.

These groups have dedicated themselves to operating against perceived enemies of Russia by coordinating attacks against entities inside and outside of Ukraine deemed a threat to Russia. Their coordination largely came in the form of publicly announced target lists for DDoS attacks and claimed hack-and-leak operations.

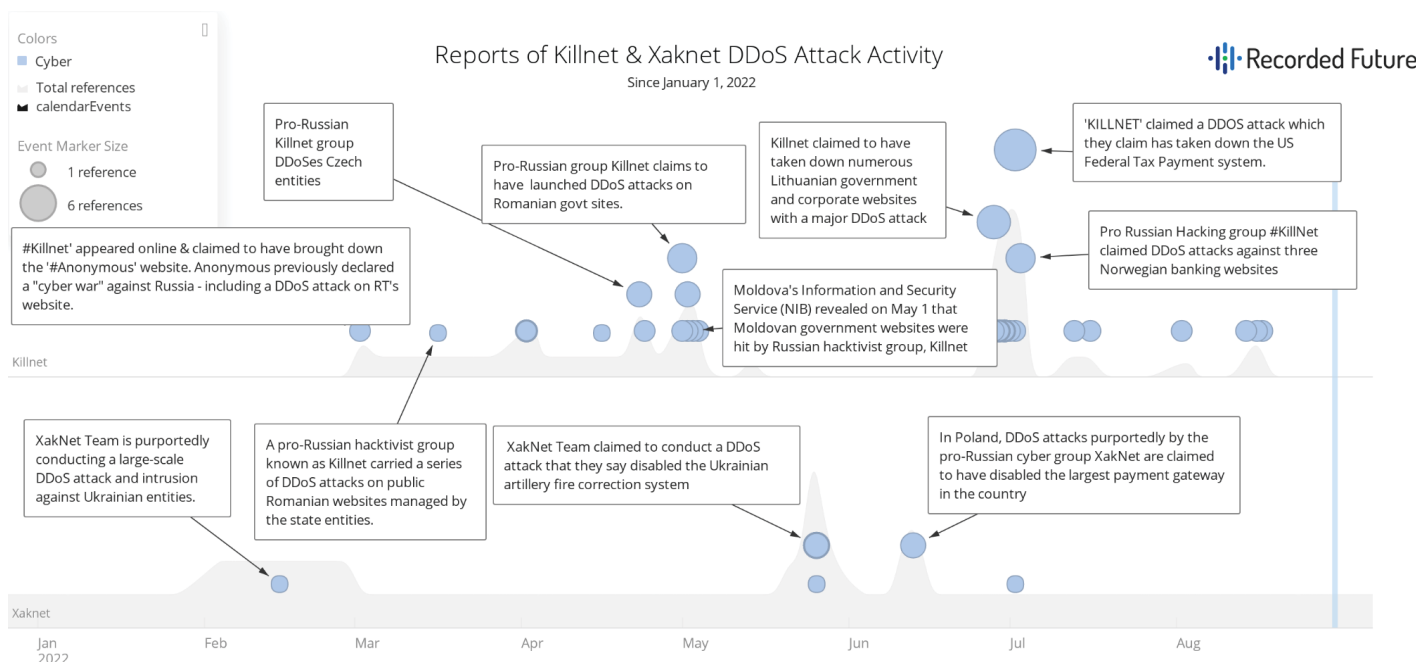


Figure 12: Timeline of DDoS activity claimed by Killnet (top) and Xaknet (bottom) since January 1, 2022 (Source: Recorded Future)

Killnet engaged in a much more public campaign in which it claimed attacks and promoted its activity in a manner that surpassed Xaknet. Not all of the purported attacks claimed by Killnet could be independently verified.

Killnet

Killnet is a self-described pro-Russian hacktivist group [widely considered](#) to be among the most disruptive hacktivist sources of cyberattacks targeting Ukrainian and NATO entities. The group has reportedly engaged in, or claimed responsibility for, DDoS attacks, hack-and-leak activity, and website defacements since the start of Russia's war against Ukraine. Killnet also reportedly [established](#) a number of entities, such as:

- Легион - Кибер Разведка or Legion - Cyber Reconnaissance² on April 27, 2022, which also has described itself as a КиберСпецназ or Cyber Spetsnaz/ Cyber Special Forces, who claim to conduct operations in support of Killnet. Legion communicates via the Telegram account @Legion_Russia³ and, like Killnet, claim to be a group of self-proclaimed pro-Russian patriotic hackers operating in squads that work together to conduct activity against set target lists.
- On June 2, 2022, the Legion Telegram account [announced](#) a recruitment effort for an “elite cyber squad” called Sparta; the announcement links to “https://t.me/sparta_channel”, a private Telegram account. Sparta’s mission is listed as follows: “cyber sabotage’ in NATO countries, destruction of Internet resources, cyber reconnaissance, financial activity, theft of private information”.

Known Infrastructure

Killnet maintains a number of social media accounts and websites. The websites associated with Killnet are listed in [Appendix B](#) and social media accounts in [Appendix C](#).

The majority of these sites and accounts were created beginning in late January, dating almost one month before the beginning of the invasion in Ukraine, and continuing through June 2022. Material initially displayed on early versions ([1](#), [2](#)) of the “killnet[.]io” website promoted “network killing technology” — a botnet that reportedly employs Blockchain for security and anonymity. The contact information originally listed on the “killnet[.]io” website links to “https://t.me/killnet_support”, a private Telegram channel still linked to Killnet that no longer offers help with the botnet but promotes itself as being linked to the “@killnet_reserves” Telegram.

2 https://t.me/s/Legion_Russia

3 The username Legion uses on Telegram matches another social media account, @Legion_Russia, which uses the name “Anonymous Russia”. It is unclear whether there is a direct link between these entities.

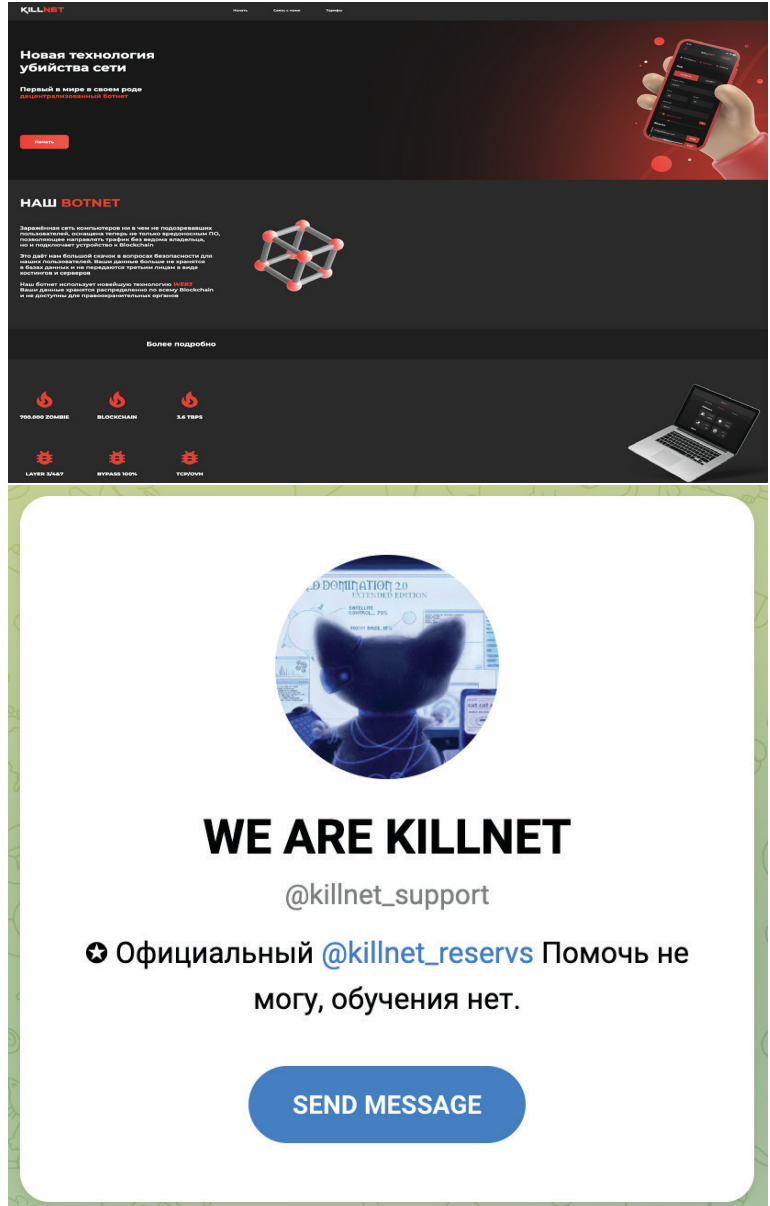


Figure 13: Screenshots of the Killnet[.]io website as of February 26, 2022 (top), and screenshot of the private @killnet_support Telegram landing page (bottom) (Sources: [Internet Archive](#) and [Telegram](#))

The “killnet[.]io” website [no longer promotes content](#) about the botnet but appears to be a parked page.

Although the “killnet[.]io” page no longer promotes the botnet, the YouTube account⁴ associated with Killnet contained only one video which does so; the video advertises “network killing technology”, individualized for each user with “no analog in the world of DDoS” and contains the same imagery as the early versions of the killnet[.]io website as well as the domain name, linking the two. The killnet[.]io domain is also shown in the YouTube video, linking the material and account with the website.

4 <https://youtu.be/qA9jCO4UNXs>

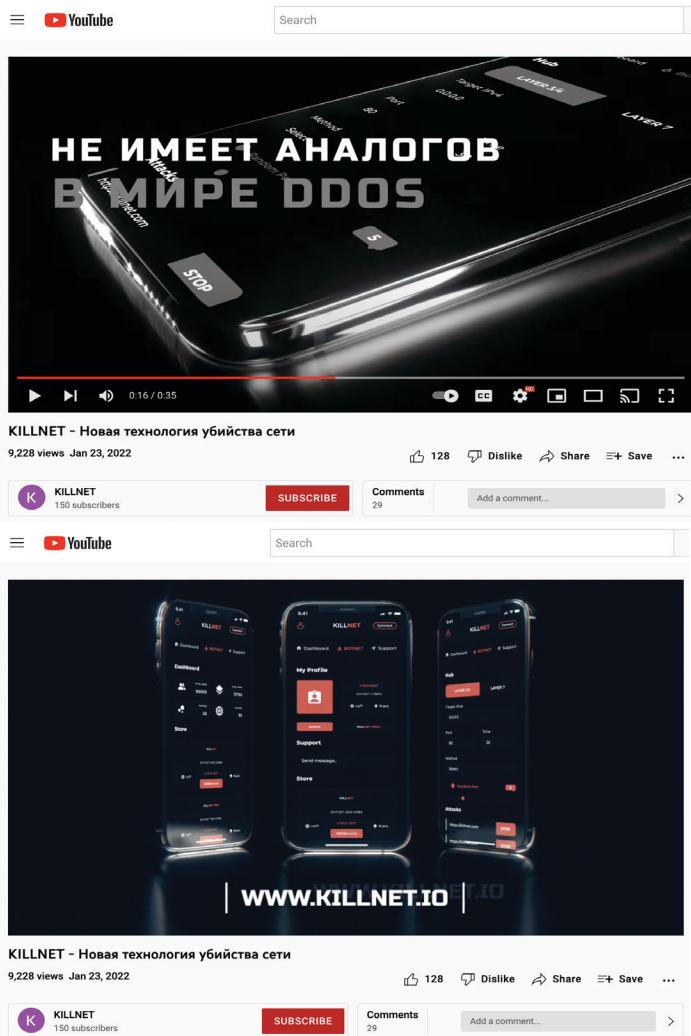


Figure 14: Screenshots from the video posted to a YouTube account linked to Killnet (Source: YouTube⁵)

Many of the domains were registered between January 22 and 23, 2022 using the same registrant organization, Tester Inc., and the name “Alex Cambirgen” appears at least 2 times in association with the domain “killnet[.]net” in the contact information and registrant fields.

⁵ <https://youtu.be/qA9jCO4UNXs>

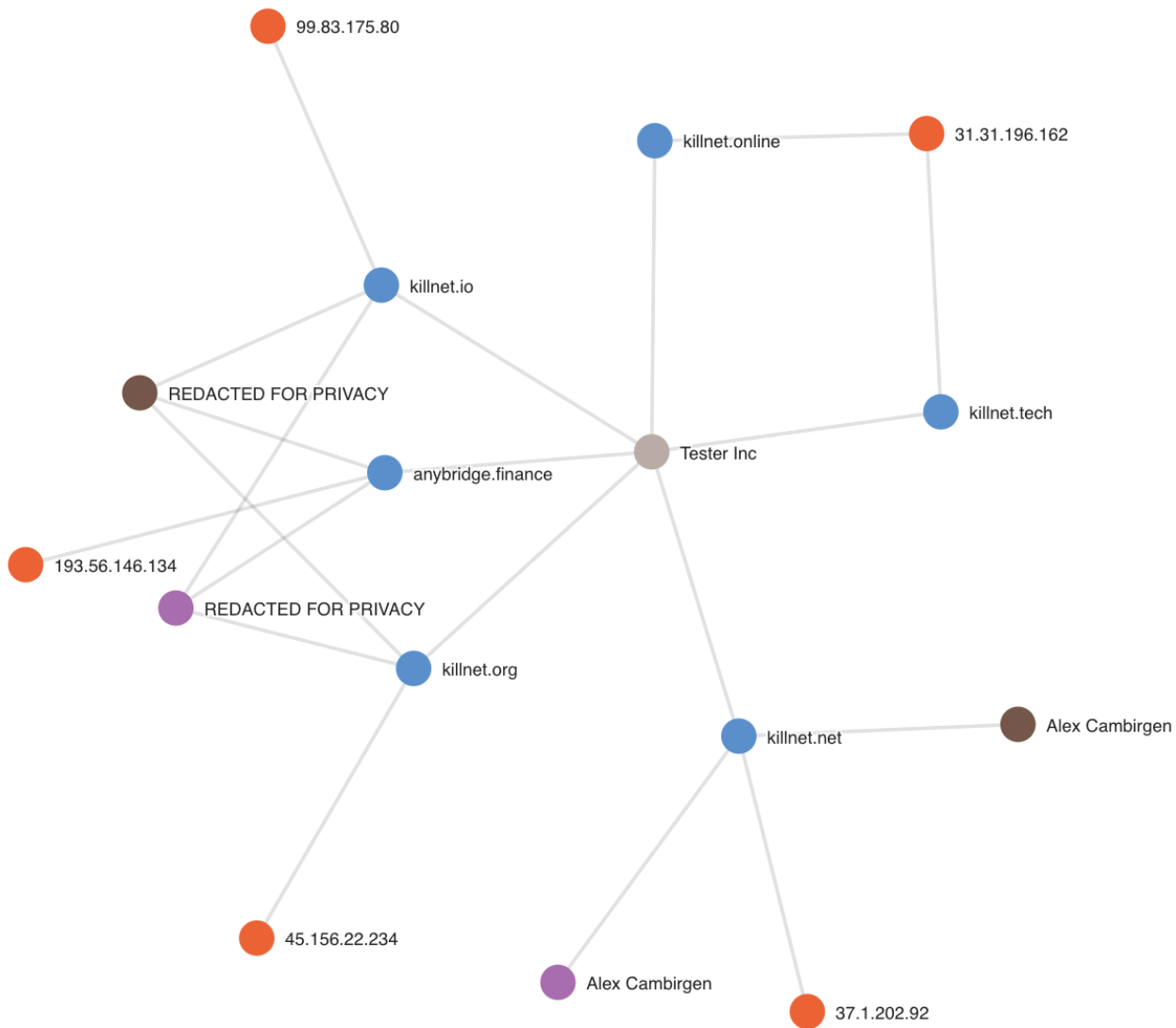


Figure 15: DomainTools graph of Killnet domain registration information and associated IP data
(Source: DomainTools IRIS)

One of the domains, killnet[.]io, was previously hosted on the IP address 92.255.106[.]148, part of Autonomous System Number 9123 (AS9123), [assigned](#) to Russian telecommunications provider TimeWeb. TimeWeb is also a favored web hosting provider of Gamaredon, which has used TimeWeb for C2 infrastructure according to [reporting](#) from the Security Service of Ukraine (SBU) as well as cybersecurity industry research ([1](#), [2](#)). Although this information is valuable data to individuals researching Killnet, it is not sufficient information to make a direct attribution to this particular threat actor.

Known Activity

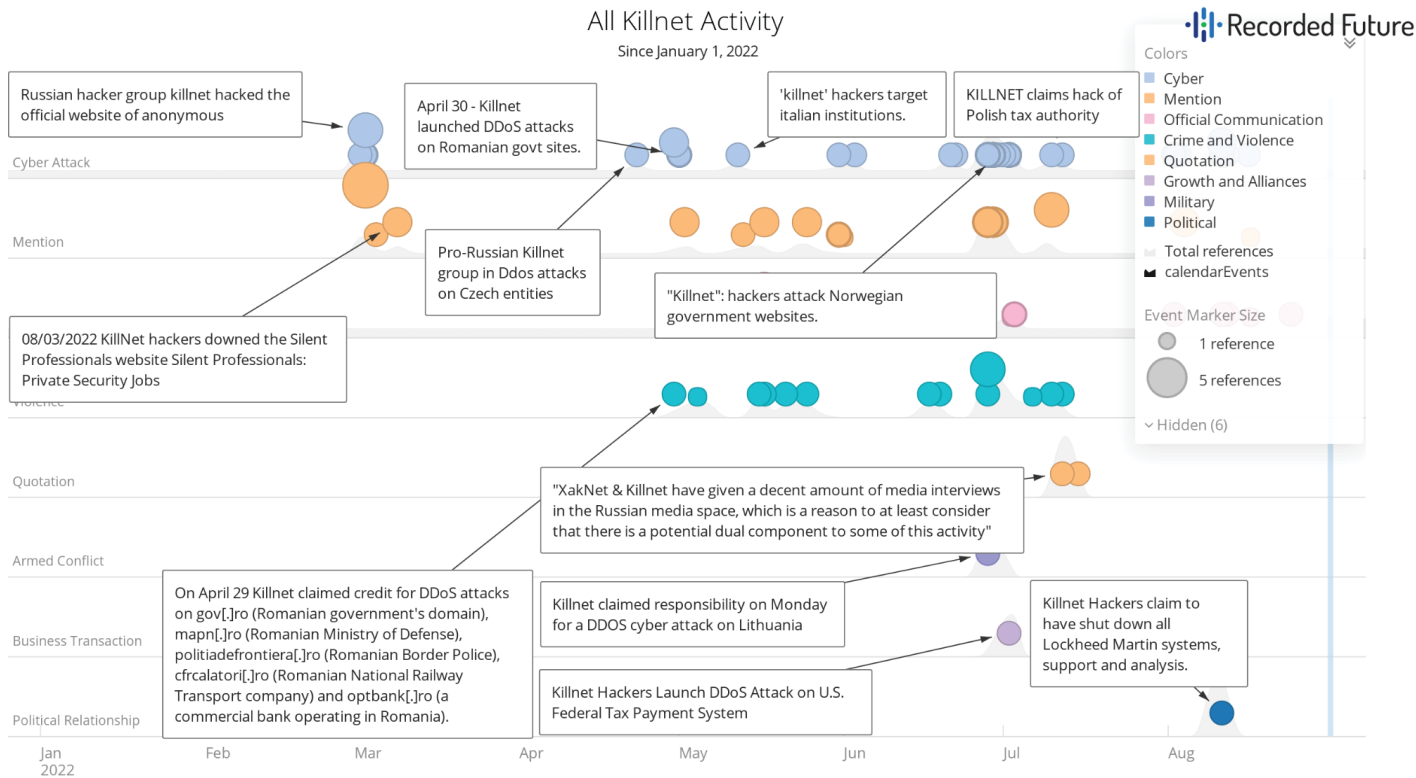


Figure 16: Annotated timeline of all references to reports and claims of Killnet activity (Source: Recorded Future)

The Killnet hacktivist group began its activities on or about March 4, 2022, and originally announced attacks through the Cyber Army of Russia troll farm and disinformation channel on Telegram. At the outset of its activity, there have been questions relating to the veracity of the claimed attacks. In early March 2022, The Record [reported](#) that a social media account using the name “Zatoichi”, which supported Russia through the spread of disinformation, claimed Killnet had “put down the Anonymous website, which announced the start of a cyber war with the Russian government, the Right Sector website, and the website of the President of Ukraine”.

On March 17, 2022, Insikt Group reported that the Cyber Army of Russia had already claimed to have leaked PII and sensitive documents related to 7 Russian celebrities and media personalities, who it claimed to be “traitors to Russia” for declaring their opposition to the Russian war in Ukraine. Additionally, the group revealed the identity of an anonymous Ukrainian blogger as well as leaked PII related to a field commander of the 8th Volunteer Battalion of the Ukrainian Ground Forces in Donbas.

On March 22, 2022, Killnet conducted DDoS attacks on the Ministry of Internal Affairs of Latvia (mvd[.]riga[.]lv) in retaliation

for the arrest of Russian social media personality Kirill Fedorov. Then, beginning on March 24, 2022, Killnet began to claim responsibility for attacks on government entities in Poland in retaliation for Polish military and humanitarian aid to Ukraine.

Killnet expanded its operations sometime between March 28 and March 30, 2022, when it claimed to have conducted a DDoS attack against Bradley International Airport in Connecticut. In advance of reporting on the incident, Killnet posted the following statement to its social media:

It is temporarily impossible to purchase a ticket, we apologize to Joe Biden. This action is not terror, but a hint that the United States government is not the master of millions of lives in Europe. When the supply of weapons to Ukraine stops, attacks on the information infrastructure of your country will stop! America, no one is afraid of you.

On July 7, 2022, we identified a post on the “@killnet_reservs” Telegram channel that claimed responsibility for a DDoS attack on congress[.]gov, leaving it inaccessible for approximately 90 minutes, returning HTTP errors 503 (Service Temporarily Unavailable), 522 (Connection Timed Out), 524 (Time Out), and 525 (SSL Handshake Failed). Maintained by the Library of Congress, congress[.]gov is the official online repository and archive of US federal legislation information pertaining to the US Senate and House of Representatives. The attack was likely an HTTP DDoS attack conducted through the use of an open-source (“cracked”) variant of the Mirai botnet. Because we did not observe any Killnet affiliates or splinter groups such as Legion, Rayd, or Mirai crowdsourcing DDoS traffic or claiming responsibility for the attack on congress[.]gov, we attribute this attack to Killnet and its affiliates.

The attack marks the first time in which Killnet has claimed responsibility for a verified DDoS attack on a website related to a US federal government entity. Other self-described pro-Russian hacktivist groups such as ZSecNet, Digital Cobra Gang, the Information Coordination Center (ICC), and the Cyber Army of Russia have claimed DDoS and defacement attacks on US federal government entities, but these claims have been determined by Recorded Future to be disinformation. Notably, Killnet was also the first self-proclaimed, pro-Russian hacktivist group to conduct attacks on NATO entities, NATO member states, and US critical infrastructure (Bradley International Airport) in support of the Russian war in Ukraine.

Since that initial incident against the Library of Congress, we have observed at least 3 more, separate instances in which Killnet has claimed to have targeted entities in the United States. While these claims consisted of purported DDoS attacks against the identified entities, there were some instances in which Killnet purports to have conducted targeted intrusions as well. The organizations that Killnet has claimed to target are included below together with dates and platform references to reports associated with the claims:

- August 3, 2022: Lockheed Martin
- October 5, 2022: State government websites in Colorado, Kentucky, and Mississippi, and others
- October 10, 2022: Websites for US airports including Los Angeles International, Chicago O’Hare, and Hartsfield-Jackson International in Atlanta

We cannot verify whether any of the aforementioned instances transpired or had any lasting or detrimental effect to the purported targets. In each of these instances, we have assessed that Killnet’s main goal has been to gain notoriety through the promotion of the purported incidents in social media, cause entities observing these claims to react or panic, and engage in diversionary tactics or foment fear and doubt.

Xaknet

Xaknet is a pro-Russian hacktivist group that was briefly active immediately following the Russian invasion of Ukraine. Xaknet conducted DDoS attacks against several Ukrainian government entities — attacks which were [rated](#) as “credible” by the Cybersecurity and Infrastructure Security Agency (CISA). Xaknet began its activities with an initial wave of DDoS attacks on or about March 2, 2022, that took a number of local Ukrainian government websites offline for several days.

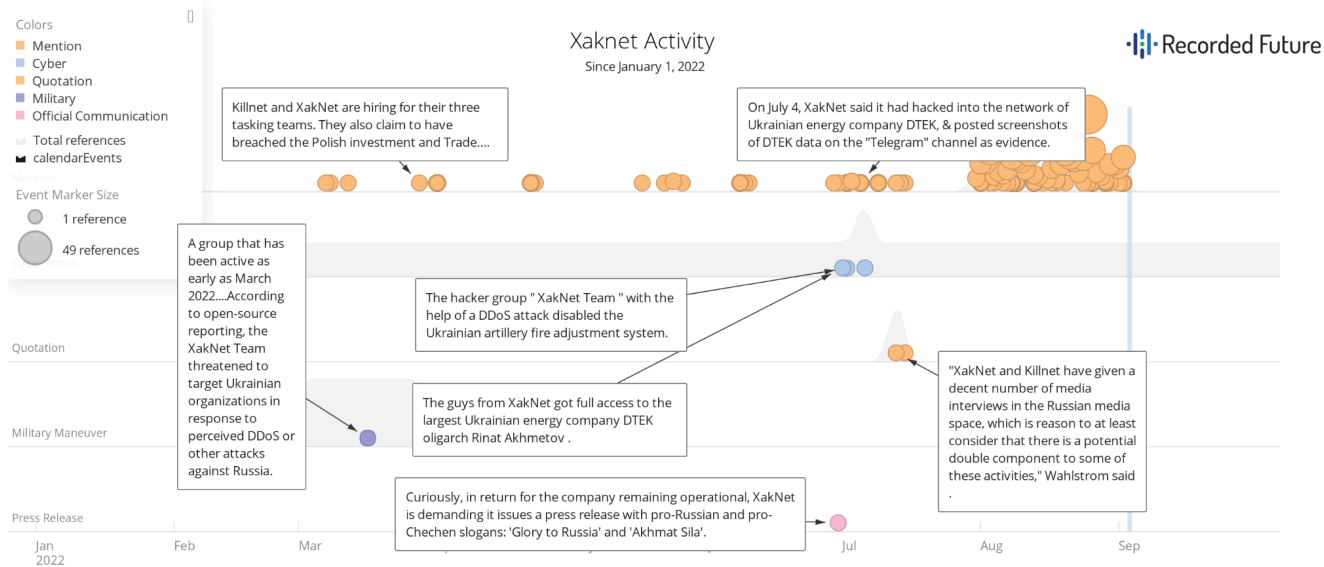


Figure 17: Annotated timeline of all references to reports and claims of Xaknet activity (Source: Recorded Future)

Mandiant researchers [identified](#) a link between Xaknet, along with several other pro-Russian hacktivist online personas, and the Russian Main Intelligence Directorate Unit 26165-aligned threat actor APT28. The link is [based](#) on the timing and release of specific data, believed to have been exfiltrated by APT28 intrusion activity, by pro-Russian "hacktivist" groups, namely the accounts "XakNet Team", "Infocentr", and "CyberArmyofRussia_Reborn". Mandiant's analysis notes that their assessment links the timing of the data releases and the material disclosed by XakNet, and the other previously identified groups, to APT28. Mandiant's attribution of this activity to APT28 is specific to its attribution of Caddywiper, the destructive malware first [discovered](#) by ESET in mid-March 2022. Mandiant notes that other security vendors have attributed Caddywiper to Sandworm, as opposed to APT28. Therefore, based on this conflict, we abstract the associations between Xaknet, Infocentr, and CyberArmyofRussia_Reborn to the known parent organization of both APT28 and Sandworm — the Main Intelligence Directorate.

Suspected False Hactivist Fronts Leaked Data Likely Stolen From APT28 Wiper Victims

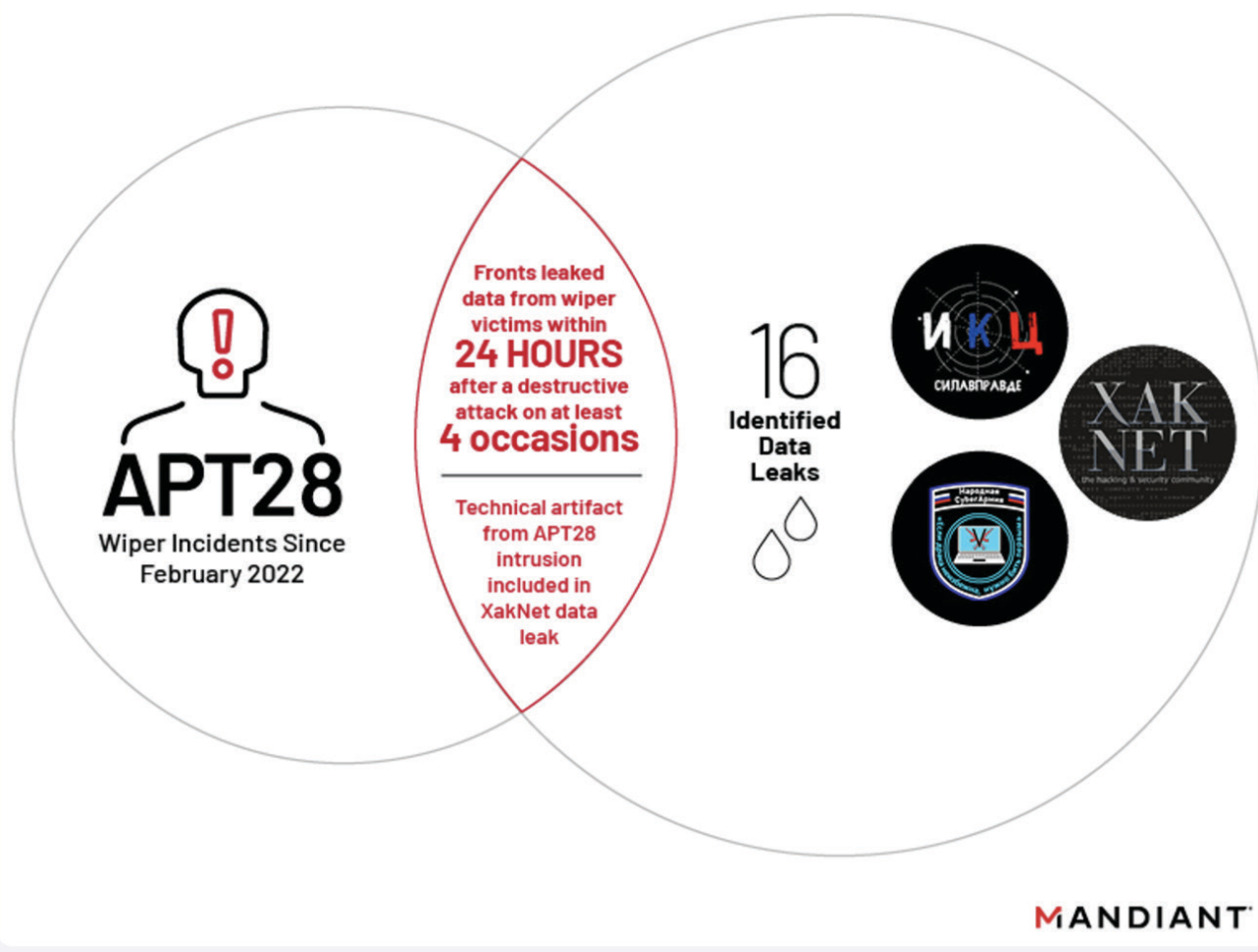


Figure 18: Assessed association between APT28, XakNet, and other self described “hactivist” groups supportive of Russia (Source: [Mandiant](#))

In addition to Mandiant’s [reporting](#), which aligns the provenance of the data and timing with “hactivist” data leaks, we note that the use of fake hactivist fronts and proxies has been an established TTP consistently observed by Russia’s Main Intelligence Directorate entities, as previously seen with the [Guccifer 2.0 persona](#).

Outlook

Russian intelligence services have historically relied upon their relationship with the cybercriminal ecosystem to facilitate reconnaissance operations or support efforts meant to destabilize their targets. The Russian government's war against Ukraine has made this long-standing relationship even more vital, especially as the conflict becomes protracted and the Russian military forces falter.

Entities operating on Russian cybercriminal forums, such as hacktivists or ransomware threat actors, can provide plausible deniability, tooling, or access for state sponsored threat actors. They also can engage in activity that could be diversionary, as many of their actions are often overt, highly publicized, and challenging to validate. The services, accesses, and tooling these entities provides very likely privileges them with a favorable relationship with the Russian security services in return, in which they are protected from prosecution unless they run afoul of the agreement or become engaged with political opinions counter to the goals of the Russian government. This apparent symbiotic relationship will almost certainly persist for the foreseeable future.

One development we have observed has been the increase in self-described pro-Russian "hactivist" entities in relation to the conflict in Ukraine, which somewhat mirrors the emergence of Russian state-sponsored APT "hactivist" proxies like Cyberberkut at the outset of their efforts against Ukraine in 2014. It is likely that the current iterations of these false hactivist organizations — Killnet, Xaknet, and others — are likely to continue to play a role in conducting operations against entities in NATO and the west, as this provides a veneer of plausible deniability for Russia in these operations, enabling the Russian government to subvert claims of state-sponsored attacks against Western entities.

Appendix A: Update on Individuals Referenced in the “Dark Covenant” 2021 report

Dark Covenant Threat Actor Update		
Name	Likely Affiliation(s)	Update
Dmitri Dokuchaev	FSB	According to Interfax , Moscow’s Lefortovo Court granted an early release from prison to Dokuchaev on May 13, 2021. On September 30, 2021, Russian state-owned TASS reported that the arrest of Group-IB head Ilya Sachkov was related to Dokuchaev’s criminal case.
Konstantin Kozlovsky	FSB	On January 26, 2022, Yekaterinburg media outlet 66[.]ru provided details of Kozlovsky’s case, which was ongoing at the Kirov Court of Yekaterinburg. According to the report, Kozlovsky claimed that his case was “connected with the FSB, and he only carried out the instructions of his handler from the special services”. On February 14, 2022, Kozlovsky was sentenced to 14 years in prison.
Pavel Sitnikov	GRU	On November 12, 2021, Kommersant reported that Moscow’s Main Directorate of the Ministry of Internal Affairs had opened a case against Pavel Sitnikov in relation to a major leak of Moscow citizens’ personal and medical data. The outlet noted that there were discrepancies in relation to the case, particularly that the charges were made four months before the incident occurred.
Maksim Yakubets and Evil Corp	FSB	Before his arrest by the Russian government, Group-IB head Ilya Sachkov was critical of Maksim Yakubets in comments issued in 2020, saying, “When the whole world says that the hacker Maxim Yakubets, who drives a Lamborghini in Moscow with [highly identifiable license plates that mark him as a “thief”], is a computer criminal, the creator of viruses, every engineer in the world knows about it, but not a single Russian state body, not the police nor the FSB and the Foreign Ministry simply don’t respond to this in any way ... it affects the image of Russian companies that sell information security abroad”. Evil Corp is still active according to one report, which noted that “A newly discovered cyberattack panel dubbed TeslaGun has been discovered, used by Evil Corp to run ServHelper backdoor campaigns”. The report additionally stated that, “Evil Corp has been one of the most prolific groups of the last five years ... It continues to hone a raft of weapons for its arsenal as well; last week, it came to light that it’s associated with Raspberry Robin infections”.
Pavel Vrublevsky	MVD/FSB	On March 10, 2022, Pavel Vreublevsky was detained in Moscow as part of an investigation connected to an economic criminal case initiated by the Ministry of Internal Affairs (MVD) according to a report by independent Russian-language media outlet Meduza.
Roman Seleznev	FSB	The Russian Embassy has claimed, via its Telegram channel , that American authorities were denying Roman Seleznev necessary medical care while jailed in the US on cybercrime charges. There has also been an effort by the Russian government to have Seleznev extradited to Russia in a potential prisoner swap for Women’s National Basketball Association (WNBA) player Brittney Griner.
Alexey Stroganov	FSB	There have been several references, in both open sources and Telegram channels , to Alexey Stroganov’s involvement in business ventures, such as construction efforts to build a bridge to the island of Sakhalin in Russia’s far east via the company Rusdor-Finance. The company also supported infrastructure projects in the Moscow region, per a Kommersant report . These reports suggest that Stroganov may have used his political connections to develop “legitimate” business interests in Russia.
Evgeny Nikulin	FSB	According to the Eurasia Daily media outlet, Nikulin filed a lawsuit against the Czech Republic seeking financial restitution in relation to their role in his extradition to the US. Nikulin, who has been serving time in prison in the US on charges that he gained unauthorized access to accounts on LinkedIn, Dropbox, and Formspring, remains in prison.

Dark Covenant Threat Actor Update

Pyotr Levashov	FSB	The US DOJ District of Connecticut's Attorneys office reported , "On July 20, 2021, Levashov was sentenced to time served. In addition, he was ordered to serve a three-year period of supervised release." In December 2021, Levashov conducted an interview with Time in which he indicated that he "has been working on a new venture, which he calls SeveraDAO. Its goal, he says, is to crack one of the most elusive puzzles of the information age: teaching machines how to pick stocks".
Evgeniy Bogachev	FSB	There has been limited open source reporting on Bogachev's whereabouts since the Dark Covenant report was published. The US DOJ has issued a \$3 million USD reward for his arrest. Since that time, however, other reporting has substantiated findings in our report that indicate that Bogachev, and the GameOver Zeus botnet he created, is linked to Russian intelligence services.
Alexander Vinnik	GRU	<p>On August 5, 2022, the US DoJ indicated that Alexander Vinnik would be extradited from Greece in order to face charges in the US for his role in managing a criminal cryptocurrency exchange.</p> <p>On August 5, 2022, the US Department of Justice (DOJ) announced the extradition of Russian national Alexander Vinnik to the US. Vinnik is accused of operating the BTC-e cryptocurrency firm, which has links to the hack of Mt. Gox in 2014. At the time, Mt. Gox was handling 70% of the world's BTC transactions. During this hack the operators of Mt. Gox lost over 700,000 BTC that were never recovered. Vinnik was originally charged by the DOJ in 2017. Outside of its links to Mt. Gox, BTC-e allegedly facilitated the laundering of more than \$4 billion worth of illicit cryptocurrency during its operations.</p>

Appendix B: Killnet-Associated Internet Infrastructure

Date of Registration	Registrant Org	Domain	Security Certificate	Active Website?
January 23, 2022	Tester Inc	KILLNET[.]IO	Let's Encrypt	Not currently active, archived site link
January 23, 2022	Tester Inc	KILLNET[.]ORG	N/A	Not currently active, archived site link
January 22, 2022	Tester Inc	KILLNET[.]NET	N/A	Not currently active, site not archived
January 22, 2022	Private	KILLNET[.]PRO	N/A	Not active; previously redirected to killnet[.]io
February 28, 2022	Private	KILLNET[.]RU	N/A	Parked domain
January 22, 2022	Private	KILLNET[.]UNO	N/A	Not active; previously redirected to killnet[.]io
January 23, 2022	Tester Inc	KILLNET[.]ONLINE	N/A	Not currently active, site not archived
January 23, 2022	Tester Inc	KILLNET[.]TECH	N/A	Not currently active, site not archived

Appendix C: Killnet-Associated Social Media Accounts

Date of Account Creation	Social media Platform	Account Name/Information
January 20, 2022	YouTube	https://www.youtube[.]com/channel/UCEmwPk59wPRmlzWETHWD-vw
January 23, 2022	Telegram	@killnet_channel
February 26, 2022	Telegram	@killnet_mirror
February 26, 2022	Telegram	@killnet_reservs
March 27, 2022	Telegram	@killnet_hacking
June 29, 2022	Telegram	@killnet_info
Unknown	Telegram	@killnet_support private channel, likely created sometime in January due to its links with the KILLNET[.]IO website

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.