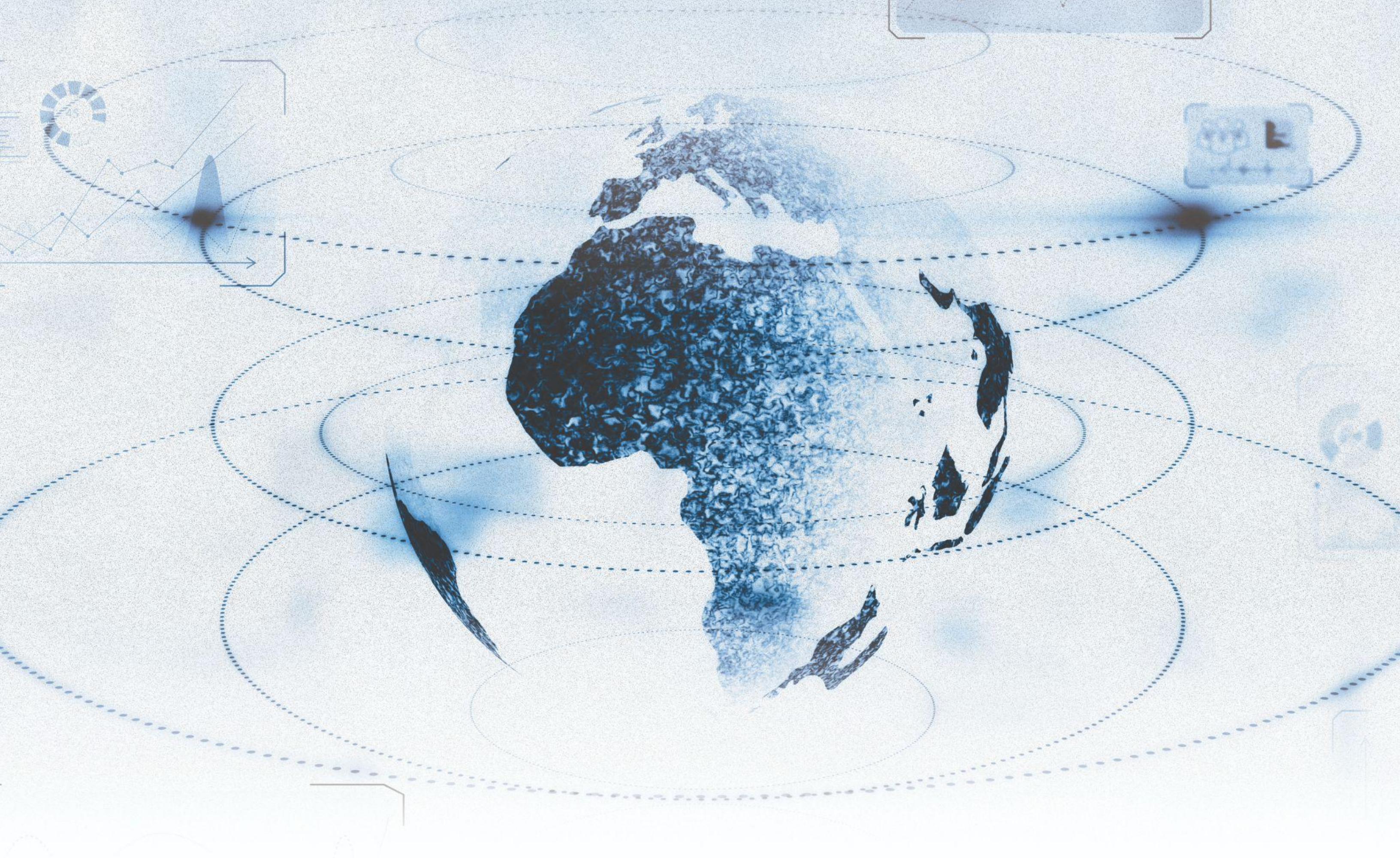
Recorded Future®

By Insikt Group®



Russia’s War Against Ukraine Disrupts the Cybercriminal Ecosystem

CTA-RU-2023-0223

Executive Summary

Russia's war against Ukraine has disrupted the cybercriminal ecosystem. On February 24, 2022, Russia launched a full-scale invasion against Ukraine. As outlined in the recent Recorded Future report "Themes and Failures of Russia's War Against Ukraine", Russia likely remains intent on seizing Kyiv, dismantling the government of Ukraine, and securing a decisive military victory despite "compounding strategic and tactical failures". Russia's offensive cyber operations have been "unable to substantively augment Russia's conventional military progress" and will likely shift to targeting civilian infrastructure in an attempt to "degrade Ukraine's morale ahead of an upcoming, renewed offensive". Russia's continued reliance on leveraging proxy groups to achieve its objectives in Ukraine while maintaining plausible deniability has further illuminated the links between Russian Intelligence Services (RIS) and non-state actors, evidenced by Russia's direct, indirect, and tacit relationships with cybercriminal and hacktivist groups as outlined in our report, "Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine".

The so-called "brotherhood" of Russian-speaking threat actors located in the Commonwealth of Independent States (CIS) has been damaged as a result of political disagreements among threat actors in the context of the war. This damage has established a new norm of internal instability, as evidenced by a continued wave of insider leaks. Additionally, as Russia experiences a "brain drain" of IT professionals, these now-fracturing organized cybercriminal cartels will likely become more geographically decentralized, in turn making their relationships more diffuse.

The resurgence of "crowdsourced hacktivism", an international phenomenon previously limited to the late 2000s, will likely create a new generation of non-state threat actors who are both politically and financially motivated. These so-called hacktivist groups, while their impact has been limited, have become symbolic in the public's perception of the "cyberwar" raging parallel to the war in Ukraine.

The economic consequences of the war in Ukraine are likely creating conditions conducive to an increase in the value of payment card fraud on the dark web, despite an overall slump in carding volume in 2022. Regardless of fraud's reputation as an unsophisticated form of cybercrime, it is likely becoming less a crime of opportunity than of survival. International arrests, seizures, and disruptive actions have destabilized the business model associated with commodified cybercrime, leading to wide-ranging and rippling effects on the malware- and ransomware-as-a-service (MaaS, RaaS) threat landscapes. These disruptions have also spread to the dark web shop and marketplace ecosystems, leading to price fluctuations and newfound competition among market administrators. Cybercrime, both based in the CIS and globally, is entering into a new era of volatility as a result of Russia's war against Ukraine.

Key Takeaways

- We did not identify any direct links between credential leaks preceding Russia's war against Ukraine; however, we believe that these credential leaks could have been leveraged by threat actors seeking to exploit geopolitical tensions prior to the war. We also note that some of the database breaches we identified have since been attributed to nation-state actors.

- The so-called "brotherhood" of Russian-speaking threat actors located in the CIS has been damaged by insider leaks and group splintering, due to declarations of nation-state allegiance both in support of and opposed to Russia's war against Ukraine.
- Russia is experiencing a wave of IT "brain drain" that will likely decentralize the organized cybercriminal threat landscape. In addition to brain drain, waves of military mobilization of Russia's citizens are resulting in decreased activity on Russian-language dark web and special-access forums.
- The resurgence of "crowdsourced hacktivism" will likely create a new generation of non-state threat actors. The impact of hacktivism has been limited, but its role in enabling information operations (IOs) remains vital. Hacktivism has become symbolic in the public's perception of the "cyberwar" raging parallel to Russia's war against Ukraine.
- Russian law enforcement's seizure and closure of several top-tier carding shops in January and February 2022 severely disrupted the payment card fraud ecosystem until April 2022. Since May 2022, the emergence of new carding shops has driven a partial rebound in the volume of compromised card-not-present (CNP) data posted for sale on the dark web.
- International arrests, seizures, and disruptive actions have destabilized the business model associated with commodified cybercrime.
- Russia's war against Ukraine has disrupted the dark web shop and marketplace ecosystems. International supply-chain disruptions and border closures have made the shipping of "physical" contraband impractical for Russia-based threat actors.

Background

On February 24, 2022, Russia began a full-scale invasion of Ukraine that was supported by ground and aerial bombardment, surface-to-surface and surface-to-air missiles, cyberattacks, electronic warfare, information warfare, and more. Almost immediately, the Russian cybercriminal underground reacted with declarations of allegiance from forum administrators, threat actors, and threat actor organizations. Hacktivist campaigns, coordinated distributed denial-of-service (DDoS) attacks, "doxxing" activities, trolling, website defacement, ransomware infections, and more began within hours of the invasion.

While the vast majority of non-state cybercriminal and hacktivist activities in the early days of Russia's war against Ukraine targeted Russian and Belarusian entities in retaliation for the invasion, opportunistic threat actors sought to exploit the tensions by leveraging vulnerabilities in the cyber infrastructure of Russian, Belarusian, and Ukrainian entities and selling leaked information or unauthorized access for financial gain and publicity. Declarations of allegiance also prompted internal unrest within certain threat actor organizations, leading to hostile activities and schisms between threat actors.

Since February 24, 2022, we have been actively monitoring the daily activities of cybercriminal and non-state hacktivist entities that have been involved directly or indirectly in the Russian war against Ukraine.

Pre-invasion Dark Web Forum Activity

We believe that there are a number of key observations to be made related to phenomena on dark web and special-access forums immediately preceding Russia's war against Ukraine, which had long-term effects on the cybercriminal threat landscape following February 24, 2022. It is important to address these events in the context of Russia's war against Ukraine, as it shapes analysis about short-, medium-, and long-term trends related to the cybercriminal ecosystem. We concur with the findings of other security researchers, such as those at DarkOwl, who have theorized that the following trends and events preceding the war were part of a coordinated "psychological intimidation campaign against the people of Ukraine" and are potentially correlated to Russian nation-state hacker activity.

We must note that, in general, it is culturally taboo for threat actors to target entities located in the former Soviet Union on most dark web forums. While this prohibition was not explicitly codified in the rules of the now-defunct Raid Forums — unlike on Exploit, XSS, or RAMP — it still remained an unspoken rule due to the volume of Russian-speaking threat actors who maintained alternate monikers on Raid Forums. We argue that the first major disruption related to Russia's war against Ukraine is the breaking of this taboo, which has established a new precedent of targeting Ukraine and other "hostile nations" (such as Georgia, Estonia, or Latvia, among others) of the CIS on Russian-language dark web forums, as well as openly targeting Russia and Belarus on the mid-tier BreachForums.

Dark Web Forum Discussions

We identified more than 61,000 references to Ukraine on dark web, underground, and special-access cybercriminal forums between February 1, 2022 and February 24, 2022. The vast majority of this content was composed of misinformation, trolling, and benign political chatter. We did identify that on dark web and special-access forums, negative sentiment targeting Ukraine sharply increased in the days and weeks preceding the full-scale invasion. However, among the noise, we were able to identify several credible threats to Ukrainian, Russian, and Belarusian entities during the time preceding the February 24, 2022, invasion and immediately afterward.

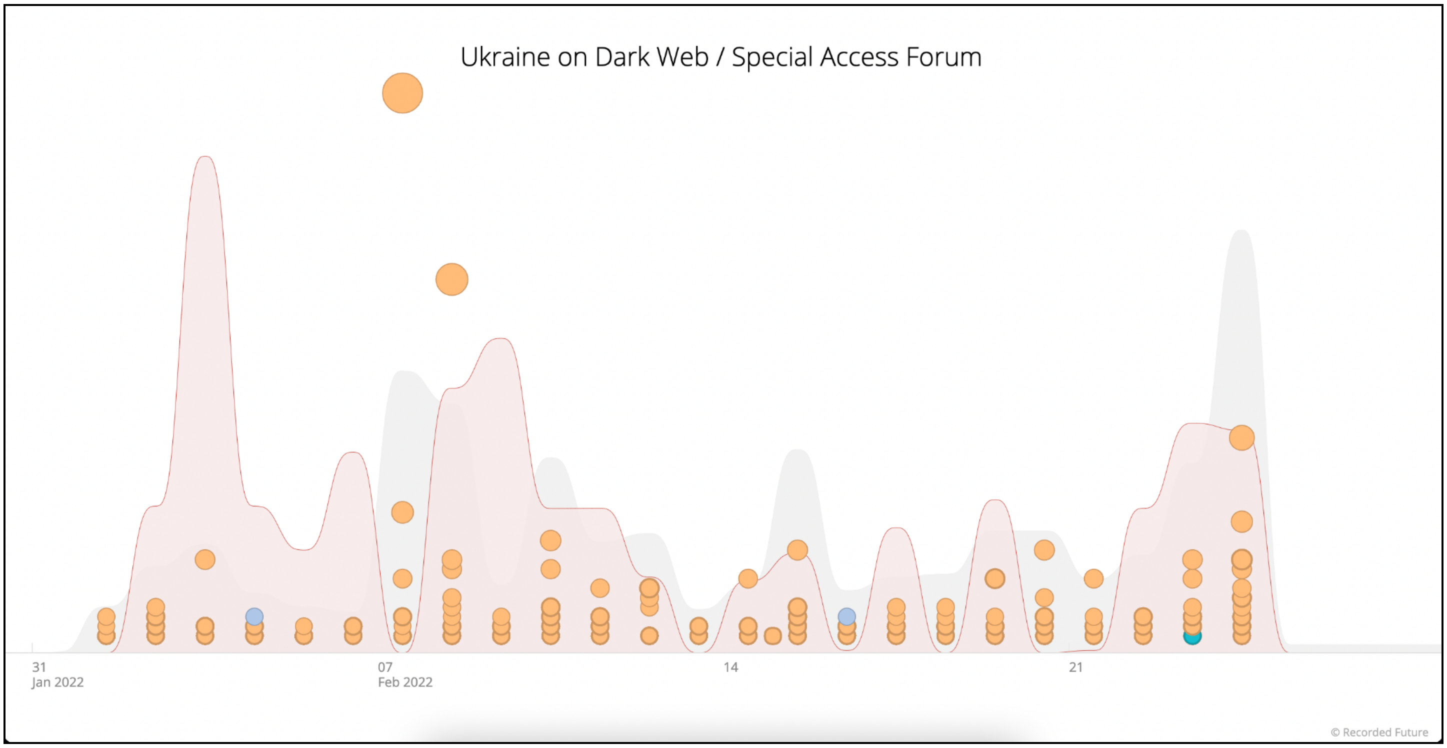


***Figure 1**: Negative sentiment involving "Ukraine" on dark web and special-access forums, preceding the February 2022 invasion (Source: Recorded Future)*

While the following list is not comprehensive, it includes some of the most noteworthy threats. Some of these events were also outlined in the our January 2023 report "Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine" and are still used as an important research guidepost for documenting historical activity on dark web and special-access forums prior to February 24, 2022.

DTEK Credentials for Sale on Exploit Forum

In late January 2022, "3ch0r00t", a member of the top-tier forum Exploit, attempted to sell 220 login credentials stolen from DTEK, the largest private Ukrainian investor in the Ukrainian energy industry, for $2,000. The stolen login credentials had emails ending with @dtek[.]com, and passwords were hashed in MD5. At the time, this advertisement was noteworthy because it was the first major advertisement we identified that broke the "unwritten rule" on Russian-language dark web forums, which says that targeting entities in the former Soviet Union is taboo. The thread received positive feedback and did not result in a ban for the threat actor, which was an unprecedented moment of inaction from forum administrators at the time.

"FreeCivilian" and EMBER BEAR

Beginning in January 2022, FreeCivilian, a former member of mid-tier Raid Forums, was identified as selling multiple databases from Ukraine on their personal website, hosted on the Tor network. The databases available for sale included the following:

- 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 listed 2 databases that we had identified as having been previously sold: 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 another diia[.]gov[.]ua database on Raid Forums. Raid Forums members commented that the database was not legitimate and that the passport data it contained was in an outdated format.

On the night of February 24, 2022, approximately 90 minutes before the Russian full-scale invasion of Ukraine began, we identified that FreeCivilian had updated their leak site with approximately 20 new Ukrainian databases. This action also coincided with a wave of DDoS attacks targeting Ukrainian government domains, beginning on February 23, 2022 — many of the victims of those attacks then appeared as “leaks” on the FreeCivilian dark web blog. At the time, we believed that FreeCivilian was possibly part of an active hybrid warfare campaign targeting Ukraine on behalf of Russia. However, we could not determine if FreeCivilian was a non-state threat actor serving in a proxy capacity or a unit of an unspecified Russian security service masquerading as a cybercriminal.

As outlined in our report “Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine”, this hybrid warfare strategy — known interchangeably as “next-generation warfare”, “new generation warfare”, or “information confrontation” — is a strategy by which the Kremlin directs, enables, and cooperates with cybercriminal groups in order to multiply its force in cyberspace. We believed that this could have been the situation we were observing with FreeCivilian.

According to CrowdStrike, FreeCivilian has since been attributed to the Russian state-sponsored advanced persistent threat (APT) group EMBER BEAR (UAC-0056), which was likely responsible for the January 2022 WhisperGate wiper attack on Ukraine and has ties to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and which was masquerading as a cybercriminal group on Raid Forums in order to provide the Kremlin with plausible deniability. This attribution is another major disruption to the cybercriminal ecosystem in the context of Russia’s war against Ukraine, because — much like Russian cyber operations targeting Estonia in 2007 or Georgia in 2008 — “cybercriminality” in the context of the war is now viewed as an extension of the Russian state.

This disruption extends to future analysis of "cybercriminal" and "ransomware" operations throughout 2022 that have since been attributed to Russian nation-state threat actors, including Prestige and RansomBoggs, both of which have been attributed to Sandworm by Microsoft and ESET, respectively.

Ukrainian Citizenship Data for Sale on Raid Forums

On February 12, 2022, "NetSec", who is also known as "Scarfac33" and is a member of the mid-tier Raid Forums, leaked 53 million records of Ukrainian citizenship data. The data set contained 53 million lines, had a compressed file size of 1 GB (the uncompressed file size was 7 GB), and included the following personally identifiable information (PII): date of birth, place of birth, place of residence, street name and zip code, phone number, physical address, and registration code. NetSec claims to be unaware of the source of the data set, and another forum user, "BullDozzer", speculated that this data set seems to be a recompiled database of the Ukrainian tax service from 2006.

In the days and weeks preceding February 24, 2022, we identified several instances of this 2006 tax service database appearing for sale on dark web and special-access sources, specifically Raid Forums and Exploit. Because this data set was so easily accessible at the time, we believe it was being leveraged by opportunistic and ego-driven threat actors that were capitalizing on geopolitical tensions by scamming parties interested in Ukrainian PII data. At this point, approximately 12 days before the war began, several countries had already suggested that a full-scale invasion by Russia was imminent. This trend of selling and reposting old Ukrainian databases is noteworthy because it begins a wave of "panic buying" and "panic selling" databases affecting entities and individuals located in Ukraine, Russia, and Belarus — which lasts until February 24, 2022.

"danieltx51" Sells Ukrainian Ministry of Foreign Affairs Data on Raid Forums

On February 21, 2022, danieltx51, a member of the former Raid Forums, indicated that they had sold a database allegedly related to the Ukrainian Ministry of Foreign Affairs (MFA; mfa[.]gov[.]ua). The threat actor did not provide any sample data. Although this is not the first time the Ukrainian MFA appeared on Raid Forums, the timing of such an advertisement — especially by an unknown threat actor with no previous activities on the forum — relative to February 24, 2022, is suspicious enough to warrant mention.

In the days preceding the war, we identified multiple threat actors of "unknown" credibility registering accounts on dark web and special-access forums, briefly advertising databases or accesses affecting Russia, Ukraine, and Belarus, and then quickly deactivating their accounts. We cannot determine if these threat actors were advertising legitimate databases or if perhaps they were simply scammers capitalizing on tensions.

"CorelDraw" Selling Multiple Databases Related to Ukraine

On February 24, 2022, the day of the full-scale invasion of Ukraine, CorelDraw, a member of the mid-tier Raid Forums, posted an advertisement for multiple databases related to Ukraine:

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

CorelDraw has been a staple of the English-language cybercriminal threat landscape for several years, serving as one of the few vendors of Russian, Ukrainian, and Belarusian databases over the course of Raid Forums’s existence. CorelDraw now operates on the mid-tier BreachForums as “CorelDrawReal”.

We believe that this sale of Ukrainian databases from CorelDraw is the most noteworthy example of “panic selling” ahead of Russia’s war against Ukraine. At this moment, we do not believe that CorelDraw is affiliated or associated with any Russian nation-state hacker groups. CorelDraw has a long history of selling databases that disproportionately target Russian individuals and entities. We believe that CorelDraw was one of the first threat actors to “dump” their Ukrainian databases all at once, ahead of potential financial losses preceding the full-scale invasion. This dumping of Ukrainian databases in bulk inspired even more threat actors to dump Ukrainian data on February 24, 2022, in the hours before the war began.

“Psycho_Killer” Selling PII Database of 56 Million Ukrainian Citizens

Also 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. We determined that this data leak was different from the leak that NetSec had advertised, both in size and year of relevancy. As mentioned earlier, in the weeks preceding the full-scale invasion, a 2006 PII database related to 53 million Ukrainian citizens was observed on a number of mid-tier and top-tier forums. However, Psycho_Killer explicitly claimed that the database they posted for sale in February 2022 was current as of 2020 and was not related to the 53 million-record 2006 database. The threat actor did not specify the price openly and used Jabber (psycho_killer@jabberix[.]com) as a point of contact. The threat actor indicated that sample data could be acquired via Jabber engagement and that more databases related to Ukraine were available.

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

Also on February 24, 2022, Featherine, a member of the former 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 immediately clear if there is a difference between the DIIA leaks that were advertised by FreeCivilian and by Featherine. However, FreeCivilian has specified that its 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 have accused Featherine of re-selling old data, which Featherine has pushed back on. To date, we still cannot determine if there was a link between the databases sold by FreeCivilian and Featherine. However, we believe that it is certainly possible, if not likely, that FreeCivilian was operating under several monikers on Raid Forums that have still not been attributed to EMBER BEAR.

Dark Web Data Dumps Targeting Ukraine

In a search for references to Ukraine, Ukrainian entities, and domains related to Ukraine (.ua) in dark web data dumps, we identified 13,274 references between February 1, 2022, and February 24, 2022. As of February 10, 2023, we are still not able to identify any immediate connection between these database leaks and the Russian war against Ukraine. We believe that this observed spike in references is most likely coincidental in nature. We were also not able to identify any direct link between collected malware log data sets and any known malware signatures that have been used to target Ukrainian entities preceding the invasion. This does not mean that links do not exist, but rather that any direct connection between the events is not immediately clear, based on preliminary research using the Recorded Future® Intelligence Cloud. We urge caution when drawing conclusions about the connections between leaked credentials and geopolitical events.

Based on our research, there was a significant increase in references to Ukrainian entities in dark web data dumps in February 2022, relative to January 2022 and December 2021. For January 2022, we identified 7,323 references to Ukraine and Ukrainian entities in dark web data dumps. For December 2021, we identified 3,375 references to Ukraine and Ukrainian entities in dark web data dumps. It is important to note that credential data, especially combolists that may include recycled credentials, are often obtained and shared by opportunistic actors; as such, the increase in references may be coincidental. However, this increased volume of leaked credentials for Ukrainian organizations could have led to expanded opportunities for threat actors to exploit them in the days following the invasion.

While we did not identify any direct link between these data dumps and cybercriminal activities related to the Russian war against Ukraine, we must note that opportunistic threat actors who may target Ukraine or exploit tensions can use these leaked credentials in a number of ways. As a rule, these credential leaks provide the underground economy with an influx of new data, which can be subsequently used for credential stuffing, spamming, phishing, social engineering, SIM swapping, and business email compromise (BEC) attacks.

Key Pre-invasion Events

As with the dark web forum activities outlined above, there were a number of key events involving Russian law enforcement activity preceding the war which have since illuminated our understanding of the role that the Russian security services play in the cybercriminal ecosystem. Many of these events were explained in-depth in "Dark Covenant 2.0: Cybercrime, the Russian State, and War in Ukraine", but still warrant mention below due to their important role in shaping the narrative surrounding the war.

Arrests and Seizures

Ilya Sachkov Arrested

On September 29, 2021, the Federal Security Service of the Russian Federation (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 toward cybercrime and ransomware, and 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's 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 of the FSB, including speculation that the FSB had been actively protecting Yakubets. It is believed that these statements, along with the negative implications they may have for the Russian government, could potentially have contributed to his arrest.

There is a tacit 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 violated this agreement by voicing concerns about Russia's relationship with cybercrime. When Sachkov was arrested, some researchers speculated that his detainment was a politically motivated move intended to silence any potential opposition to offensive Russian cyber operations.

In September 2021, it was not immediately apparent that Russia would launch a full-scale invasion against Ukraine in February 2022. However, Sachkov's arrest remains important because, in retrospect, we believe it is likely a precedent set by the Russian security services to prosecute IT professionals who speak out against the state's relationship with cybercrime. As cybercrime and nation-state cyber operations become increasingly interconnected as the war progresses, silencing a critic like Sachkov could prove beneficial for the Russian state in its attempt to maintain deniability.

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.

This wave of arrests was unprecedented at the time and marked a major disruption to the cybercriminal status quo. Within hours of the news breaking, top-tier Russian-language forums like XSS and Exploit were filled with speculation from threat actors that their relative freedom to participate in cybercrime with impunity was over.

This was the first time in the modern 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, in hindsight, 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 although the arrests are ultimately beneficial overall, to a skeptical viewer they could be seen as falsely "signaling" Russian law enforcement's intention to limit cybercrime.

In addition to this speculation, the REvil arrests also came parallel to the deployment of WhisperGate and widespread defacement of Ukrainian government websites on January 14, 2022. We believe that the arrests were an attempt by Russia to control the media narrative and distract from ongoing cyberattacks on Ukraine — which have since been attributed to the Russian GRU.

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 was 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 due to close as well.

Andrey Novak was reportedly known by the username “Uniccshop” on a variety of carding forums, as well as by 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 Department of Justice (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 the Russian news agency 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 (MIA) seized the domains of at least 4 additional Russian-language dark web and special-access sources that facilitated cybercriminal activity. Directorate K is responsible for investigating crimes that involve authorized computer access. The seized websites are as follows:

- SkyFraud, a mid-tier Russian-language forum dedicated to payment card fraud, the sale of 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. This seizure is a noteworthy crackdown on the Russian carding threat landscape, with SkyFraud and Trump’s Dumps serving as staples of the payment card fraud ecosystem through early 2022. Similarly, Ferum Shop and UAS Shop were noteworthy competitors of other dark web shops like Russian Market, Genesis Store, and 2easy Shop. This seizure is significant for many reasons, as it could have led to an observed increase in both payment card and valid account listings on dark web shops following the full-scale invasion.

Key Trends in Cybercrime

Threat Group Disruption

Immediately following the Russian full-scale invasion of Ukraine, threat groups began to publicly declare allegiance. These declarations led to significant internal turmoil among threat groups. It is important to note that when researchers discuss the "Russian cybercriminal threat landscape", this term does not imply that all threat actors in this landscape are Russian nationals, ethnic Russians, or native Russian speakers. Many threat groups include a "brotherhood" of international threat actors from Ukraine, Belarus, the Baltics, the South Caucasus, Central Asia, and other parts of the Russian near-abroad such as Mongolia, Romania, Finland, and so on. Among these groups are individuals who have moral and political objections to Russia's war against Ukraine, including ethnic Ukrainians and Ukrainian nationals. When groups such as Conti Gang and CoomingProject — as referenced below — declare allegiance to the Russian government, this causes an in-group destabilizing effect for threat actors opposed to the war. Several likely Russia-based threat groups have had internal leaks since February 24, 2022, including but not limited to: Conti (Trickbot), LockBit, Yanluowang, Solaris, URSNIF, and more.

Conti Ransomware

On February 25, 2022, Conti, the threat group operating the Conti ransomware, posted a statement on its extortion blog 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".

Notably, some of Conti's current rivals — like ALPHV (BlackCat) and LockBit — refused to declare allegiance to the Russian government, indicating that their business is apolitical in nature and has nothing to do with Russia's war against Ukraine. We believe it is possible that ALPHV and LockBit both could have avoided initial insider leaks through their quickness to declare neutrality in the war.

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 their social media account. We indexed the leaked Jabber logs into the Recorded Future Intelligence Cloud under the source Conti Gang Leaked Chats.

The so-called "Conti Leaks" precipitated an event known as the "Trickbot Leaks". While the 2 leaks are derived from the same leaked data chat logs, the Trickbot leaks leverages information disclosed in the Conti leaks to "unmask" senior leadership of the Trickbot cybercriminal gang. In the months that followed the Conti and Trickbot leaks, Conti would eventually dissolve. We do not believe that Conti's dissolution was a direct result of the leaks, but rather that the leaks catalyzed the dissolution of an already fracturing threat group.

On February 9, 2023, approximately one year after Conti's declaration of allegiance to the Russian government, the US Department of the Treasury announced joint US and United Kingdom (UK) "cyber sanctions" targeting 7 members of the Trickbot cybercriminal gang. The announcement alleges that "current members of the Trickbot Group are associated with Russian Intelligence Services" and that "The Trickbot Group's preparations in 2020 aligned them to Russian state objectives and targeting previously conducted by Russian Intelligence Services".

The operators, developers, and supporting staff members of Trickbot — tracked as a nexus of threat activity as WIZARD SPIDER, UNC1878, FIN12, and GOLD BLACKBURN, among others — are likely also responsible for the development of the Ryuk, Diavol, Black Basta, BlackByte, Quantum, and Royal ransomware variants. Other malware families and cybercriminal groups affiliated with Trickbot include BazarLoader, Bumblebee Loader, and Karakurt, among others.

We also note that initial access brokers (IABs) associated with Conti have been observed collaborating with Russian nation-state actors in Ukraine. According to the Google Threat Analysis Group (TAG):

> UAC-0098 is a threat actor that historically delivered the IcedID banking trojan, leading to human-operated ransomware attacks. The attacker has recently shifted their focus to targeting Ukrainian organizations, the Ukrainian government, and European humanitarian and non-profit organizations. TAG assesses UAC-0098 acted as an initial access broker for various ransomware groups including Quantum and Conti, a Russian cybercrime gang known as FIN12 / WIZARD SPIDER.

We believe Conti's dissolution has resulted in Conti staff and affiliates collaborating with Russian nation-state attackers in Ukraine as a result of their newfound unemployment. We believe it is possible that the Russian government is purchasing access to tools developed and/or used by Conti staff, such as IcedID, in order to target Ukraine and provide plausible deniability. By working directly with cybercriminals, the Russian government can obscure its involvement in such attacks.

CoomingProject

On February 26, 2022, RaaS 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, the 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. CoomingProject's public downfall was likely the direct result of its declaration of allegiance to the Russian government.

Hive

On January 26, 2023, the US DOJ announced that the Federal Bureau of Investigation (FBI) had disrupted the operations of the Hive ransomware group. Since late July 2022, the FBI had "penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in ransom demanded". The FBI provided over 300 decryption keys to Hive victims under attack and an additional 1,000 decryption keys to previous Hive victims in recovery. In coordination with law enforcement agencies located around the world, the FBI also seized the .onion services of the Hive extortion blog (HiveLeaks) and the victim chat portal. We can confirm that as of January 26, 2023, both of these services and all their related mirrors remain offline and display a law enforcement seizure banner. Hive leveraged an RaaS business model that relied on third-party affiliates to conduct its attacks and solicit ransom payments. Hive began its operations in October 2021 and targeted more than 1,500 victims in over 80 countries "including hospitals, school districts, financial firms, and critical infrastructure".

We do not believe that Hive's downfall is the direct result of any involvement Hive has had in Russia's war against Ukraine. However, this law enforcement action is a significant disruption, given the scope of Hive's victimology and the reputation of Hive as a key player in the ransomware threat landscape. Hive's exit from the market is a disruption that allows third parties to capitalize on lost market share and affiliates associated with Hive to migrate to other RaaS programs, such as LockBit. We believe that the core members of Hive will likely rebrand into a new threat group, much like when Conti splintered in mid-2022.

Hacktivism

Hacktivism involves a diverse range of tactics, techniques, and procedures (TTPs) used to disrupt the administration and operations of an adversarial entity for political or strategic gain. Hacktivism, by definition, is ideologically motivated in nature and involves the work of decentralized, non-state threat actors who adopt pseudonymic monikers and claim responsibility for attacks as part of a larger "collective" in order to avoid detection and arrest. Hacktivists often adopt trending geopolitical crises and events as their impetus for action, such as Russia's war against Ukraine, and may abandon operations in a specific campaign once the issue is not trending anymore. Due to hacktivism's fluid nature, hacktivists' areas of focus may vary widely in a short period of time. Much like cybercriminals, hacktivists are opportunistic threat actors. Hacktivist groups are often the subject of misinformation and coordinated disinformation campaigns alleging that they are APT groups masquerading as civilian activists. (In rare instances, some APT groups have indeed masqueraded as hacktivists for plausible deniability.)

We identified 8,799 references to hacktivism as an attack vector in the Recorded Future Intelligence Cloud from February 24, 2022, to February 10, 2023. The largest surge of references took place in March 2022, with approximately 3 times more references than the next-most active month, July 2022. This finding tracks with the overall frequency of hacktivist attacks observed by Recorded Future analysts following February 24, 2022 — as evidenced by the volume of victims identified by Insikt Group in its daily research.

When our search was expanded further to include references to discussions of hacktivism in general, not just as an attack vector, we identified approximately 1,000 named victims as targets of hacktivist activities. Victims include entities in Russia, Ukraine, Belarus, the US, Latvia, France, Poland, and others. This number is only an estimate, serving as an approximation of known targets that were publicly declared by hacktivist groups on their official messaging channels; the true number may be much higher. We identified approximately 2.5 million references to the word "hacktivism" and tracked approximately 100 hacktivist groups from February 24, 2022, to February 10, 2023. We note that references to "hacktivism" spike in discussion frequency in September 2022. It is important to note that this spike in references does not reflect the increased frequency in the number of targets claimed by hacktivist groups, but is rather a reflection of broader media coverage of major attacks — almost all of which have been attributed to Killnet.

We believe that Russia's war against Ukraine has caused a resurgence of "crowdsourced hacktivism", a phenomenon reminiscent of the late 2000s. Crowdsourced hacktivism occurs when a central hacktivist threat actor, such as the IT Army of Ukraine, publishes a "target list" to their devoted followers in an attempt to solicit the aid of third-party threat actors. Then, the central threat actor will claim responsibility for the crowdsourced attack and push the news to affiliated amplification channels and the media. Not only does this method of hacktivism allow for a more centralized narrative and focused effort, but it provides anonymous attackers with plausible deniability by attributing their actions to a larger group.

Pro-Ukrainian Hacktivism

On February 24, 2022, Reuters reported that the Ukrainian Defense Ministry asked hackers to volunteer their services in order to assist Ukrainian cyber efforts against Russia. Yegor Aushev, co-founder of a cybersecurity company in Kyiv, claimed that he was requested by Ukrainian officials to make posts on underground forums and Telegram to recruit volunteers. On February 26, 2022, the online Ukrainian newspaper Ukrainskaya Pravda reported that the "Minister for Digital Transformation of Ukraine Mykhaylo Fedorov announced the creation of an army of IT specialists to fight for Ukraine". The report indicated that all the operational posts would be shared via the Telegram channel "IT ARMY of Ukraine".

We use the terms "pro-Ukrainian", "pro-Western", and "anti-Russian" interchangeably when referring to broadly pro-Ukrainian hacktivist activities. In order to distinguish between clusters of threat activity, we track 2 separate lineages of hacktivism: activities attributed to the IT Army of Ukraine and activities attributed to Anonymous, the latter of which was popularized by the social media hashtag "#OpRussia". Pro-Ukrainian hacktivism is notably more diverse in its TTPs than pro-Russian hacktivism, including but not limited to: DDoS, website defacement, “hack-and-leak”, ransomware and data extortion, and more. The majority of high-profile verified leaks associated with pro-Ukrainian hacktivist groups have been published by Distributed Denial of Secrets (DDoSecrets), an online leak repository.

As of February 10, 2023, the IT Army of Ukraine has approximately 200,000 unique followers on their official Telegram channel. This follower count has plateaued since March 2022, when it totaled approximately 180,000 followers. This Telegram channel and the hacktivist activities associated with it are indexed in the Recorded Future Intelligence Cloud as the organization IT Army of Ukraine. The IT Army of Ukraine also maintains an official social media account (@ITarmyUA), but we have not observed any activity on this account since March 27, 2022. There is a separate social media account that shares IT Army of Ukraine news in Portuguese (@itarmyofukraine) for Brazilian followers, but there is no indication that this account is directly related to the IT Army of Ukraine.

After long bouts of inactivity, Anonymous has reformed and rebranded itself as a loose confederation of previously established threat actor organizations that are actively involved in the hybrid warfare resulting from the Russian war in Ukraine. The threat actor organizations that have formed the new “Anonymous” include Network Battalion 65, AgainstTheWest, v0g3lSec, DoomSec, SHDWSec, GhostSec, and many more that have openly pledged their allegiance to Anonymous. These organizations, along with thousands of Anonymous-affiliated social media accounts, form the core of Anonymous’s operations in 2022. Anonymous has worked closely with leak websites (DDoSecrets, WikiLeaks), hosting platforms (Anonfiles), and OSINT analysts (Bellingcat) to amplify the visibility of its work. Anonymous has openly expressed rivalries with Red Bandits, Killnet, and Xaknet. There are several accounts on social media that amplify the works of the Anonymous hacktivist collective, including @YourAnonOne, @YourAnonTV, @YourAnonNews, @PucksReturn, and @YourAnonCentral. While we do not believe that any of these accounts are directly involved in operations claimed by Anonymous, they do serve as the primary source of Anonymous-related news and propaganda. Among the most common hashtags on social media used by Anonymous-affiliated accounts are #OpRussia, #OpUkraine, and #CyberWar.

Pro-Russian Hacktivism

We identified so-called “pro-Russian” hacktivist activity on social media, Telegram, and dark web forums as early as February 25, 2022. The “first wave” of pro-Russian hacktivism was a hybrid movement including both pre-established threat groups, such as the Stormous ransomware gang, and new groups that were founded in response to the war, such as XakNet Team. We note that the first major pro-Russian hacktivist alliance founded in support of Russia’s war against Ukraine was called the “CYBER ARMY OF RUSSIA”, a now-defunct collaborative Telegram group launched by the leadership of XakNet Team and Killnet. Other now-defunct groups that were part of this first wave include Digital Cobra Gang, ZSecNet, and others.

This first wave of pro-Russian hacktivist activity began to transition to a second wave of “Killnet dominant” hacktivism on or around March 22, 2022, with Killnet’s first major targeted campaign on the government of Latvia following the arrest of Russian social media personality Kirill Fedorov. This campaign switched focus to Poland on March 25, 2022. We mark the definitive beginning of the second wave of pro-Russian hacktivism with the Killnet attack on Bradley International Airport in Windsor Locks, Connecticut, on March 29, 2022. This event marked the first time since the beginning of Russia's war against Ukraine that a pro-Russian hacktivist group publicly claimed responsibility for an attack on US critical infrastructure. At this point, Killnet begins to transition into its own brand and splinter from its alliance with XakNet Team, eventually overshadowing the latter.

By May 2022, Killnet had become the hegemonic pro-Russian hacktivist group and maintained dominance in both media attention and Telegram following. Killnet formed several subgroups that had distinct identities, such as Zarya, Mirai, Legion, and others, but these groups are all now defunct. Killnet's campaigns extended far beyond targets located in Europe, targeting entities located in North America, Asia, South America, and elsewhere.

According to security researchers like CyberKnow (@Cyberknow20), the total number of pro-Russian hacktivist groups active since February 24, 2022, exceeds 70 known groups. However, we assess that the majority of these groups are now defunct. As of February 10, 2023, we believe that the majority of public-facing pro-Russian hacktivist activity falls under the umbrella of "Killnet nexus" activity — meaning that Killnet and its allies, such as Anonymous Russia, Anonymous Sudan, INFINITY Hackers, and others, claim responsibility for more than 50% of all pro-Russian hacktivist activity tracked by Recorded Future analysts. We identified approximately 100 so-called pro-Russian hacktivist groups and individual threat actors active between February 24, 2022, to February 10, 2023. As of February 10, 2023, only 5 major groups remain.

According to a September 2022 Mandiant report, groups that fall under the so-called "XakNet nexus" — such as XakNet Team, Infoccentr, CYBER ARMY OF RUSSIA REBORN, and others — were "coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored cyber threat actors". The assessment was "based in part on the deployment of GRU-sponsored APT28 tools on the networks of Ukrainian victims, whose data was subsequently leaked on Telegram within 24 hours of wiping activity by APT28, as well as other indicators of inauthentic activity by the moderators and similarities to previous GRU information operations".

We have assessed that the majority of claims made by pro-Russian hacktivists since February 24, 2022, are false, misleading, or exaggerated in impact. The overwhelming majority of attacks claimed by pro-Russian hacktivists constitute relatively unsophisticated distributed denial-of-service (DDoS) for which little publicly available forensic evidence exists. We believe that the national security threat posed by pro-Russian hacktivists is not their attacks, but rather their ability to sow panic and enable the spread of Russian propaganda and disinformation; the impact of pro-Russian hacktivists on both Russia's war against Ukraine and foreign support for Ukraine has been negligible at most.

Dark Web Economy Disruptions

Malware-as-a-Service (MaaS)

On March 25, 2022, the operators of Raccoon Stealer announced on the Russian-language forums XSS and Exploit that they were suspending operations due to Russia's war against Ukraine. In reality, Mark Sokolovsky, one of the key developers of Raccoon Stealer, was arrested in the Netherlands after fleeing Russia's war against Ukraine. Raccoon Stealer's exit from the market caused a widespread disruption to the MaaS threat landscape, as third-party infostealers advertised on dark web forums began to fight for Raccoon's former share of the market. New competition included Mars Stealer, Meta Stealer, Phoenix, Titan, and more.

In the time since Raccoon Stealer's exit from the market, we have observed a rise in cracked malware variants appearing on cybercriminal forums. It is also noteworthy that many of these cracked variants have patched out the "anti-CIS" strings commonly associated with MaaS, by which the malware self-destructs if it detects that Russian — or any other major language in the CIS — is installed on the victim's keyboard.

Payment Card Fraud

Russian law enforcement's closure of several top-tier carding shops in January and February 2022 severely disrupted the card fraud ecosystem, severing links between buyers and sellers. This caused the average daily volume of card-not-present (CNP) records posted for sale from February 2022 through April 2022 to equal only 44% of the 2021 average daily volume.

Since May 2022, new carding shops have emerged and existing carding shops have expanded their presence to assume the lost market share, enabling the average daily CNP volume to rebound to 88% of the 2021 average daily volume. As described in our "Annual Payment Fraud Intelligence Report: 2022", it is highly likely that factors stemming from Russia's war against Ukraine — most prominently, mobilization and "brain drain" — have prevented compromised card volumes from fully rebounding to 2021 levels.

Dark Web Shops

From February 24, 2022, to February 10, 2023, we identified approximately 155 million references to new and updated listings on the dark web shops Russian Market, Genesis Store, and 2easy Shop. We noticed 2 major spikes in activity on these shops: in August 2022 and in January 2023. While we have not identified any direct links, we believe it is possible that threat actors based in Russia were liquidating their supply of infostealer logs in these months — ahead of rumors that Russia would enact partial mobilization in order to conscript personnel for its war against Ukraine.

We have not identified any significant fluctuations in the price of infostealer logs on major dark web shops, but only in the volume. We believe that this increase in volume may potentially lead to price destabilization, as the demand for infostealer logs will either plateau or decrease.

Dark Web Marketplaces

From February 24, 2022, to February 10, 2023, we identified approximately 434 million references to new and updated listings on dark web marketplaces, including those that sell physical goods such as narcotics, weapons, and other products. We note several interesting periods of activity; specifically, we identify an overall decrease in the total number of listings between May 2022 and July 2022, as well as a spike in activity beginning in January 2023.

We believe that this collapse of dark web marketplace listings in May 2022 is likely the result of the German Federal Criminal Police (BKA's) seizure of Hydra, a notorious Russia-based dark web marketplace. The US DOJ indicated that "in 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace has received approximately $5.2 billion in cryptocurrency". The BKA's seizure of Hydra runs parallel to border closures, international sanctions, disruptions to the Russian and international supply chain, disruptions to the Russian logistics and transportation industries, and more.

Beginning in January 2023, several Russian dark web marketplaces have attempted to fill the void left by Hydra. Among these marketplaces are Mega, OMG!OMG!, and BlackSprut — the last of which has been openly advertised on physical billboards in Moscow. We believe that this newfound market competition is re-igniting competition among both pre-existing markets and new markets, leading to an overall spike in the number of active listings collected in the Recorded Future Intelligence Cloud.

Dark Web Forum Activity

From February 24, 2022, to February 10, 2023, we identified approximately 126 million references to new threads and posts on dark web forums. Dark web forum activity has remained overall relatively stable since Russia's war against Ukraine began, but had a significant decrease in the volume of new references in September 2022 — likely as a result of the first partial mobilization order in Russia.

Anecdotally, we have observed significant decreases in the number of new threads and posts — as well as the total number of all Insikt Group threat leads — related to content on Russian-language dark web forums since September 2022. We believe that the partial mobilization orders issued by Russia may have conscripted several threat actors. We also believe it is possible that Russian-speaking threat actors have been part of the "brain drain" of Russian IT and cybersecurity professionals to Georgia, Estonia, Finland, and Kazakhstan. We believe that this could explain the decrease in activity on Russian-language sources, beginning in September 2022.

In order to make up for this decrease in references, English-language forums such as BreachForums have become far more active and publicly accessible. BreachForums has experienced significant increases in activity since its launch in March 2022.

Outlook: An Unpredictable Future

In the coming months, we expect many of the trends identified above to continue. We believe that, as Russia will likely initiate a renewed offensive ahead of February 24, 2023, we may see an increase in database breaches affecting Russia and Belarus on dark web forums compared to the disproportionate amount of Ukrainian databases that were published prior to February 24, 2022. We also believe that, with an increase in Russian and Belarusian leaked databases, we will see a correlation in the increase of credential leaks on dark web forums targeting .ru and .by domains. We believe this will happen because of the overwhelming amount of Russian databases that have been leaked since the beginning of #OpRussia, and which have yet to enter into public circulation. Some of the Ukrainian databases leaked prior to the invasion have been attributed to Russian nation-state threat actors, which we believe are now occupied in supporting Russia's war effort. We also believe that insider leaks targeting Russia-based threat groups will continue in 2023. We believe that the Conti and Trickbot leaks have set a precedent that has been made standard by insider leaks related to LockBit, Yanluowang, URSNIF, and others.

We expect to continue to see pro-Russian hacktivism monopolize media attention and dominate the discourse surrounding the "cyberwar" taking place parallel to Russia's war against Ukraine. As Killnet continues to cement itself as the hegemonic pro-Russian hacktivist group, it will further amplify the work of its official allies and therefore solidify its position as the dominant voice controlling the pro-Russian hacktivist narrative.

With regard to the dark web economy, we believe that this period of volatility and instability will continue into 2023. We believe that the MaaS threat landscape will be in flux, as it is still attempting to recover from the destabilization of Raccoon Stealer's exit from the market. As third-party MaaS offerings attempt to supplant Redline and Vidar, threat actors will continue to turn to open-source and cracked tools — as well as bespoke, fully undetectable malware — instead of a major MaaS program. We expect to see a continued disruption in the dark web shop and marketplace ecosystems, with the latter turning increasingly inward on the marketplaces located physically in the CIS. Finally, we believe that English-language forums such as BreachForums will supplant the dominance of Russian-language forums in terms of sheer volume of activities and public reputation, as Russian nationals flee the country or are mobilized to take part in Russia's war against Ukraine.

We believe that 2023 could bring several paradigmatic changes to the cybercriminal threat landscape — including the absolution of crimes committed by pro-Russian cybercriminals. On February 10, 2023, Russian State Duma deputy Alexander Khinshtein suggested to reporters that Russia release pro-Russian "white [hat] hackers" from administrative and criminal liability, given that they operate in the interests of the Russian state. Per the Russian news agencies Interfax, TASS, and RIA Novosti, Khinshtein told reporters that members of the State Duma are "talking about, in general, working on an exemption from [criminal] liability for persons who act in the interest of the Russian Federation in the field of computer information both on the territory [of Russia] and abroad". Khinshtein referenced a hypothetical wartime scenario in which offensive cybersecurity countermeasures ("destroying the enemy’s firing positions”) could be beneficial for the attacker’s defensive posture, but are currently “highly likely to be considered offenses under Russian administrative or criminal law because this [destruction] can be qualified as a crime in the field of computer information”. Khinshtein suggested that “we adjust this norm”.

We believe that Khinshtein’s proposal to release pro-Russian cybercriminals from administrative and criminal liability is a policy pivot intended to further provide plausible deniability to the Russian state in its offensive cyber operations. As detailed in the reports “Dark Covenant: Connections Between the Russian State and Criminal Actors” and “Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine”, we have identified several direct, indirect, and tacit relationships between cybercriminals and the Russian state. Russian intelligence services often recruit cybercriminals into public service, collaborate with cybercriminal groups in their attacks, or masquerade as cybercriminals to provide plausible deniability.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

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.