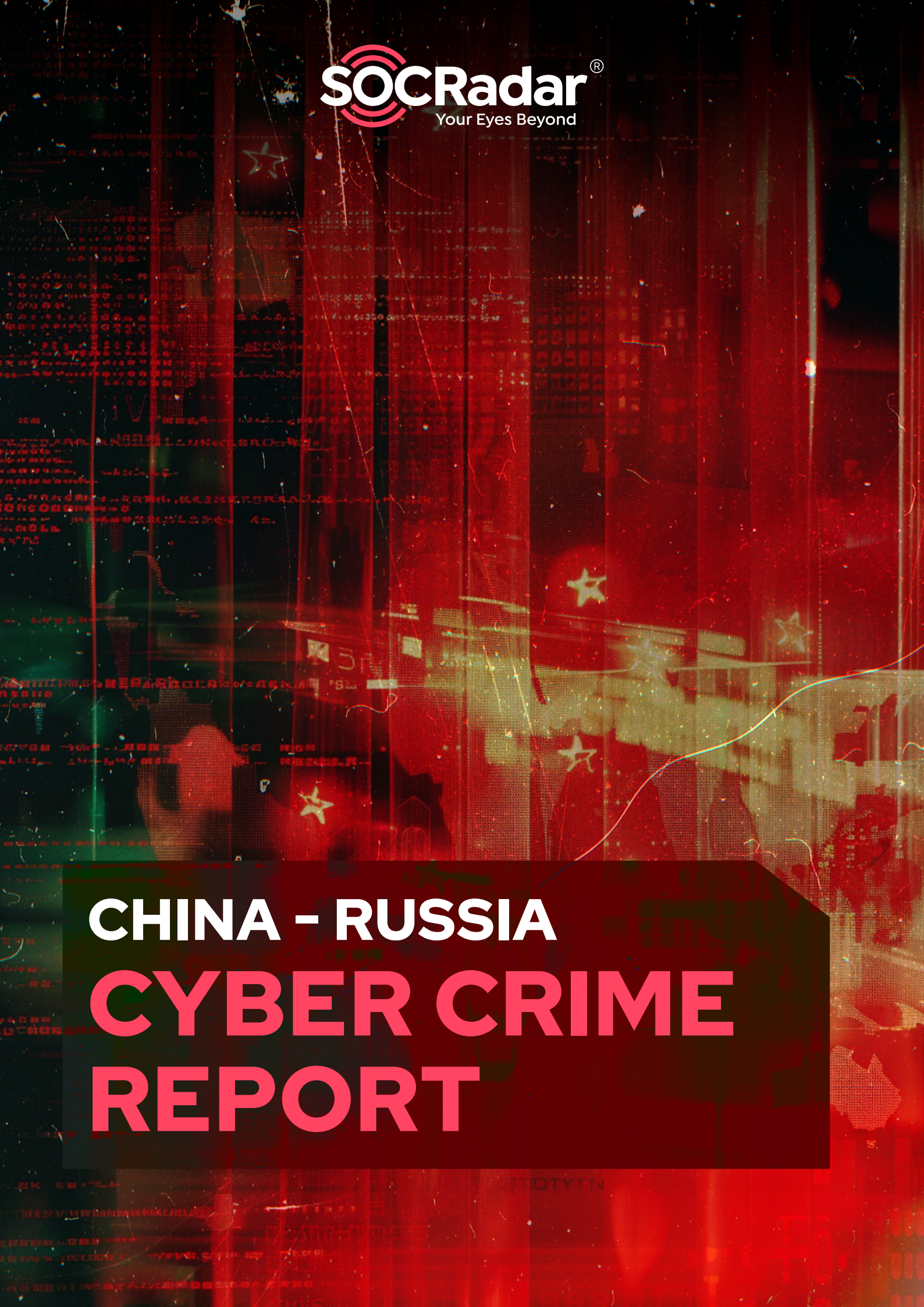

SOCRadar®
Your Eyes Beyond
CHINA - RUSSIA
CYBER CRIME
REPORT

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

In the rapidly evolving landscape of global cybersecurity, the actions of governments in China and Russia have significantly influenced the shape and trajectory of cybercrime within their borders. These actions, ranging from regulatory measures to tacit support of cyber operations, have cultivated environments where cybercrime platforms thrive. In both nations, these platforms are not merely facilitators of illicit activities but serve as sophisticated ecosystems where hackers exchange tools, strategies, and illicit goods. They underscore a burgeoning cybercrime economy, marked by the exchange of malware, hacking services, and stolen data, thereby fueling the proliferation of cyber threats.

At the forefront of these threats are the Advanced Persistent Threat (APT) groups, which, in both China and Russia, benefit from varying degrees of government backing. These entities specialize in conducting espionage, sabotage, and data theft, targeting global entities that range from governmental institutions to critical infrastructure, reflecting the strategic interests of their patrons. Their operations, characterized by complexity and stealth, exemplify the advanced capabilities within the cyber arsenals of these nations.

Parallel to the conventional cybercrime marketplaces, the rise of Telegram as a favored communication and coordination tool among cybercriminals stands out. Its encrypted messaging environment offers a secure channel for the dissemination of hacking tools, coordination of attacks, and the trade of stolen information, complicating efforts to track and counteract cybercriminal activities.

Moreover, the influence of global events, including geopolitical tensions and economic shifts, on the cybercrime rates in China and Russia cannot be overstated. These events often serve as catalysts for cyber operations, influencing their scale and sophistication. As such, the landscape of cyber threats emanating from China and Russia is a dynamic reflection of the interplay between state policies, global events, and the innovative adaptability of cybercriminals. Understanding this intricate web is crucial for crafting effective cybersecurity defenses and strategies in an age where cyber threats know no borders.

The Titans' Cyber Army

In the shadow of this sprawling conflict, where cyber operations continually redefine the boundaries of international engagement, we turn our gaze toward the intricate dynamics of the global cyber ecosystem. Within the digital realms navigated by the Titans' Cyber Army lies a complex web of actors and operations from China and Russia, shaping the future of global cyber interactions.

Spotlight On: Chinese Cybercrime Ecosystem

Over the years, cybersecurity research and reporting have primarily focused on cybercriminal activities in Western countries and Russia. However, there's a growing concern within the research community about the overlooked threat posed by the Chinese-language threat actor community.

China's unique model, blending state support with profit incentives, has fostered a vast network of actors driven by competition to exploit vulnerabilities and expand operations. Across platforms like Telegram, X (formerly known as Twitter), and various underground forums, Chinese hackers, data brokers, web crawlers, and vendors have established an expansive network dedicated to the illicit trade of personal identifiable information (PII), advertising substantial volumes of such data.

A Threat Actor's Profile on X

The illicit trade network impacts Chinese and global organizations, as Chinese-language cybercriminals increasingly target international individuals and businesses. Reports from early 2022 estimated the black data market value to range between 100 and 150 billion Yuan, based on insights from alleged industry experts. By January 2024, one Chinese news outlet claimed the figure surpassed 150 billion Yuan.

China enforces regulations restricting anonymous Internet usage, requiring service providers to collect users' real identities for Internet access, chat groups, online forums, and social media platforms. Operators face penalties for non-compliance. While users may utilize pseudonyms on forums or social media, their IDs must be stored and accessible to authorities as needed.

Due to these regulations, Chinese threat actors utilize their own language to describe and promote their illicitly acquired data. This language comprises Chinese colloquial terms and keywords that signify particular data types, targets, victims, and the roles of those engaged in illegal data trading.

Term	Chinese	Meaning
Take off pants data	脱裤数据	Hacked Database
Repository	數據庫 or 褲子	Database
Angels and Demons	天使与魔鬼	Chinese Police
Spinach	菠菜数据	Gambling Industry
Envelope	信封	Leaked Account Credentials

Chinese Threat Actor Terminology

Chinese Government-backed APT Groups

Western intelligence experts employ the APT naming convention to identify hacking groups associated with foreign governments. According to reports, there are over 40 APT groups, with over 20 of them suspected to be operated by China.

After establishing the prevalence of APT groups, particularly those with suspected ties to China, it's pertinent to highlight notable examples to provide insight into the broader threat landscape.

APT41 (Double Dragon or Barium):

> APT41, an alleged hacking group with purported connections to the Chinese Ministry of State Security (MSS), has been classified as an advanced persistent threat. Identified by the United States Department of Justice in September 2020, the group was implicated in charges against five Chinese and two Malaysian nationals for allegedly infiltrating over 100 companies worldwide.
>
> Sponsored by the Chinese Communist Party (CCP), APT41 is known for its dual nature of operations, engaging in both espionage and pursuing individual financial gains. Referred to as "Double Dragon," the group's tactics involve using devices typically associated with state-sponsored intelligence activities.

APT41: Wanted by the FBI - Source: FBI

APT41 has exhibited a proactive approach in targeting organizations across at least 14 countries, with activities dating back to approximately 2012. The group's espionage campaigns have been particularly concentrated in vital sectors such as healthcare, telecommunications, and high-tech industries, often involving the theft of valuable intellectual property. Notably, they have also been implicated in cyber intrusions within the video game industry, engaging in activities such as the manipulation of virtual currencies and the attempted deployment of ransomware.

Methods: Spearphishing, Malware, Supply Chain Attacks

Toolset/Malware: Crackshot, Gearshift, Highnoon, Jumpall, Poisonplug, Hotchai, Latelunch, Lifeboat, Lowkey, NJRAT, Pacman, Photo, Potroast, Rockboot, Sagehire, Sweetcandle, SOGU, Tera, Tidyelf, Widetone, Winterlove, XDoor, Xmrig, ZxShell

Formation: 2012

Activities: 2021 APT41 Targeting U.S. State Governments
2022 APT41 Group Targets Materials Technology
2023 APT41 Actors Continue to Target Critical Infrastructure

MITRE ATT&CK: https://attack.mitre.org/groups/G0096/

APT40 (Leviathan):

> APT40, an advanced persistent threat in Haikou, Hainan Province, People's Republic of China (PRC), has maintained activity since at least 2009. Known for targeting governmental entities, corporations, and academic institutions spanning various sectors such as biomedical, robotics, and maritime research, APT40's operations extend across regions including the United States, Canada, Europe, the Middle East, the South China Sea area, as well as industries aligned with China's Belt and Road Initiative. APT40 is closely associated with Hafnium.

APT40: Wanted by the FBI - Source: FBI

APT40 also demonstrates a strategic focus on countries pivotal to the Belt and Road Initiative. While their scope extends to global organizations, particularly those involved in engineering and defense sectors, they have also historically launched campaigns targeting regional entities, notably in Southeast Asia.

Methods: Malware, Zero-days, Phishing, backdoor (computing), RAT, Keylogging

Toolset/Malware: Airbreak, Badflick, Photo, Homefry, Lunchmoney, Murkytop, China Chopper, Beacon, Blackcoffee, CVE-2017-11882, Derusbi, RoyalRoad RTF Weaponizer

Formation: 2009

Activities: 2021 Finland Parliament Breach
2021 New Zealand Parliament Attack

MITRE ATT&CK: https://attack.mitre.org/groups/G0125/

APT31 (Zirconium):

APT31, identified as a collective comprising Chinese state-sponsored intelligence officers, contract hackers, and supporting personnel, is involved in hacking activities and described as conducting "malicious cyber operations" by the U.S. Treasury Department.

Also recognized as Zirconium, the group allegedly operated under the guise of a front company, Wuhan Xiaoruizhi Science and Technology (Wuhan XRZ), from at least 2010 until January 2024, as indicated by a U.S. indictment filed in New York's eastern district court. It is purportedly linked to China's Ministry of State Security (MSS) in Hubei province.

APT31: Wanted by the FBI - Source: FBI

APT31 is known for targeting a wide range of sectors. These include government institutions, international financial organizations, aerospace and defense companies, high-tech firms, construction and engineering industries, telecommunications providers, media organizations, and insurance companies. The group's diverse targeting across these sectors highlights the potential threat posed by their cyber attacks and espionage activities, which aim to compromise strategic assets and critical infrastructure.

Methods: Spearphishing, Exploitation, Backdoor, RAT

Toolset/Malware: China Chopper Webshell, PlugX, Mimikatz, Sakula

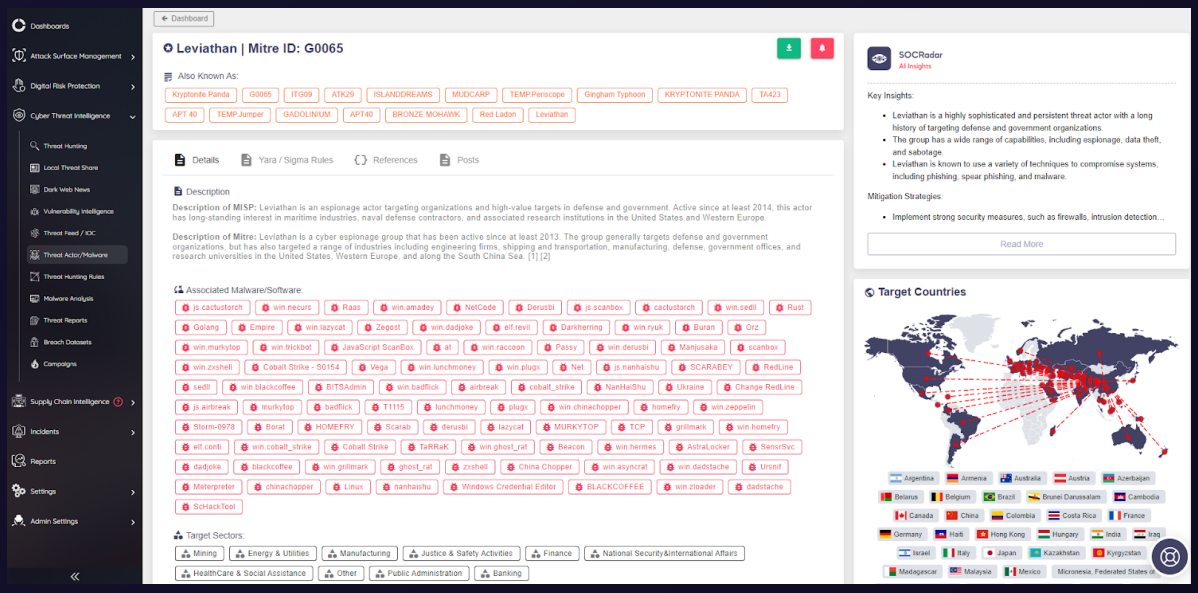
Formation: 2016

Activities: 2022 Eastern Europe Air-Gapped Devices Breach
2022 U.S. Government Phishing Campaign

MITRE ATT&CK: https://attack.mitre.org/groups/G0128/

> In light of the insights presented, remaining vigilant about threat actors' strategies and activities is essential in fortifying cybersecurity defenses. SOCRadar's Threat Actor Tracking module offers a robust solution, delivering real-time insights into known threat actors' behaviors and tactics.

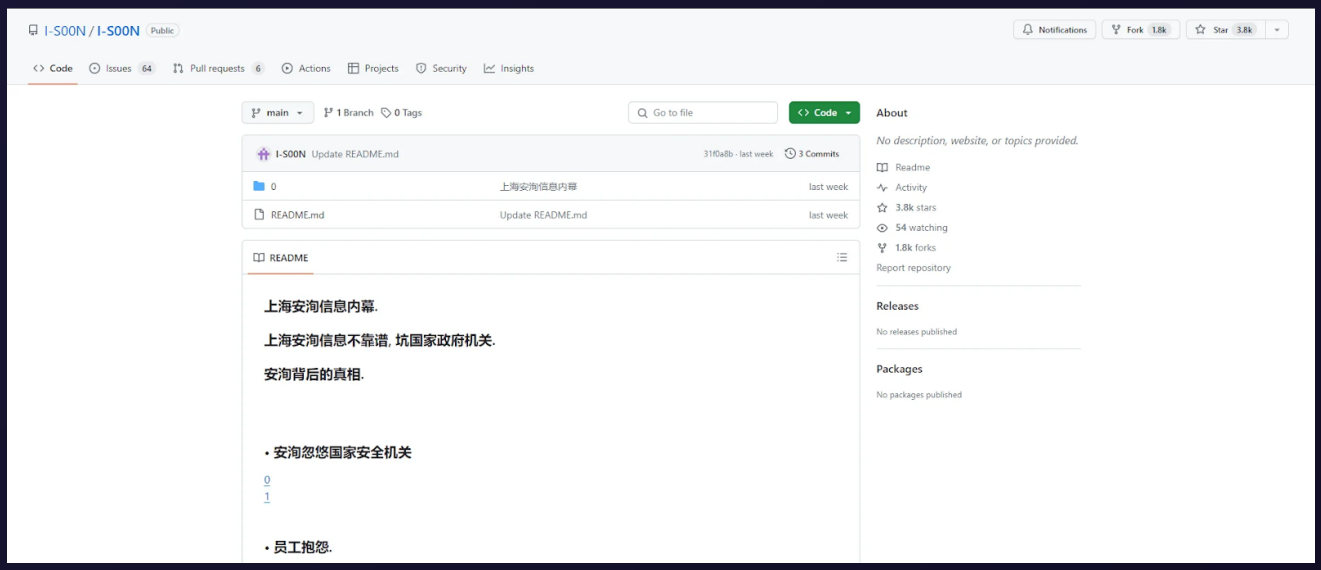
Request your demo now!



SOCRadar Threat Actor Tracking Module

The i-SOON Leak:

> Many institutions and researchers are investigating a substantial leak of cybersecurity documents from a private security firm associated with the Chinese government, which has been published on GitHub. This leak, believed to have been orchestrated by a disgruntled employee, exposes various cyberattack tools and services provided by i-Soon (or Anxun in Mandarin), a contractor operating on behalf of the Chinese government.



i-SOON Leaks On Github

The leaked documents contain evidence of espionage activities targeting both Chinese citizens and foreigners, shedding light on i-Soon's involvement in monitoring ethnic groups and dissidents, particularly in regions like Hong Kong and Xinjiang. Additionally, a legal dispute between Chengdu 404 and i-SOON has garnered attention due to its connection with alleged Chinese state hacking activities, notably involving APT41. Despite US indictments implicating key Chengdu 404 personnel as APT41 members, the company has continued its operations and sought municipal support for expansion efforts.

This significant security breach, confirmed by two i-SOON employees, exposed a collection of detailed information despite not unveiling particularly new or advanced espionage methods. The leaked documents encompass hundreds of pages detailing contracts, marketing strategies, product guides, and lists of clients and staff linked to the Ministry of Public Security, but not limited to it. Additionally, the breach allegedly involved the theft of terabytes of data from various countries, allegedly including Afghanistan, Cambodia, Egypt, Hong Kong, India, Indonesia, Kazakhstan, Kyrgyzstan, Malaysia, Mongolia, Myanmar, NATO, NATO member countries, Nepal, Nigeria, Pakistan, Rwanda, South Korea, Taiwan, Thailand, Turkiye, Vietnam, Philippines, and more.

> The leaked data encompasses personal information such as names, email addresses, physical addresses, and phone numbers, therefore showcasing how further Chinese espionage activities are reaching.

国家区域	目标类型	目标名称	域名	样本数据量	数据类型	样本日期	
巴基斯坦	运营商	Zong					权
哈萨克斯坦	运营商	Kcell通讯公司		820GB	话单、用户表	2019 - 2021	内
吉尔吉斯斯坦	运营商	megacom					在
马来西亚	政府	工程部		288MB	邮件	2021.12.20	权
马来西亚	政府	内政部		6.85GB	邮件	2021.04 - 2021.12	邮
马来西亚	政府	外交部		6.59GB	PC文件、邮件	2021.01 - 2021.12	邮
蒙古	政府	警察局		539MB	PC文件	2021.04	邮
蒙古	政府	外交部		2.37GB	邮件	2021.12	邮
尼泊尔	政府						在
台湾	医疗	台大医院					病
泰国	运营商	CAT					权
土耳其	科技	科学技术研究理事会		421KB	数据表	2020	邮
印度	医疗	阿波罗医院					在
印度	政府	印度出入境		95.2GB	数据表	2020	查
巴基斯坦	政府	旁遮普省反恐中心邮服数据		1.43GB	邮件	2021.05 - 2022.01	邮
哈萨克斯坦	运营商	Beeline通讯公司		637GB	话单、用户表	2019 - 2020	内
哈萨克斯坦	运营商	Tele2通讯公司		1.09TB	话单、用户表	2019 - 2020	内
哈萨克斯坦	运营商	Telecom固话运营商		257GB	话单、用户表	2021.05	内
哈萨克斯坦	政府	养老金		1.92GB	用户表	2019.12	内
马来西亚	运营商	DIGI通讯公司		89.5GB	话单、基站表	2021.05	内
台湾	教育	圆桌教育基金会		1.23GB	用户表	2020.06	内
泰国	运营商	Ais通讯公司		17.7GB	数据表	2020.06	内
泰国	政府	外交部		3.33GB	邮件	2021.05 - 2021.09	邮
泰国	政府	国家情报局		326MB	邮件	2022.01	邮
埃及	政府	政府网		286MB	文件、邮件	2021.04	部
法国	教育	巴黎政治学院		723MB	文件、邮箱	2011.01 - 2021.04	具
柬埔寨	政府	经济部					域
卢旺达	政府	调查局					域
卢旺达	政府	卫生部					内
马来西亚	政府	军网					邮
蒙古	运营商	skytel天空通讯					办
蒙古	运营商	蒙古电信					办
蒙古	政府	公安部					办
尼泊尔	运营商	尼泊尔电信		2.26GB	数据表	2021.05	办
尼日利亚	政府	政府网		1.3GB	邮件	2021.05	全
台湾	教育	台湾大学应用力学研究所					内
台湾	教育	淡江大学		6.9GB	邮件	2022.01	邮
泰国	政府	财政部					办
泰国	政府	参议院		144MB	邮件	2021.12.31	邮
泰国	政府	国内贸易部					主
泰国	政府	国务委员会办公室					域
泰国	政府	内政部					部
泰国	政府	商务部					主
香港	教育	香港东华学院					主
香港	教育	香港教育大学		3.23GB	数据表		主
香港	教育	香港科技大学		2.48GB	文件、邮件	2021	部
香港	教育	香港树仁大学		643MB	数据表、邮件	2019.10 - 2021.03	主
香港	教育	香港中文大学		2.95MB	数据表	2019.12	部
香港	教育	职工盟		972KB	数据表、文件	2020 - 2021	法

Many websites mentioned in the leak have domains of foreign countries

You can visit our blog post for more information about the i-SOON Leak.

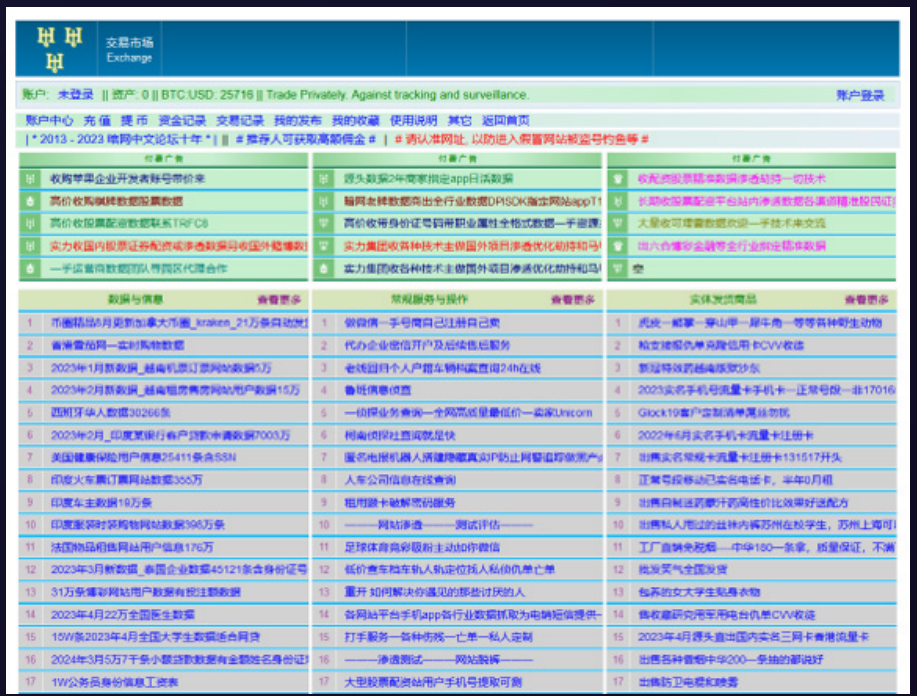
Top 5 Chinese-Speaking Hacking Platforms

Over the past few years, China has experienced a notable upsurge in activity on the deep and dark web, despite its stringent internet regulations and extensive digital surveillance infrastructure.

Despite the obstacles presented by the Chinese Great Firewall, an increasing number of Chinese users have found methods to access and engage with the deep and dark web. Their motivations span a wide spectrum, encompassing activities such as hacking, cybercrime, and participation in illicit trade, including drugs, weapons, and counterfeit goods.

Exchange Market (交易市场)

> Originally established in 2013 as the "Chinese Darknet Forum," Exchange Market (**交易市场**), underwent a significant evolution by 2015, transitioning into a fully-fledged marketplace. With a core emphasis on preserving user anonymity, the platform has emerged as a prominent hub for a diverse array of illicit goods and services, tailored primarily to the Chinese demographic. Despite encountering persistent challenges such as DDoS attacks and the complexities of rebranding, it has managed to maintain its stature as a key player within the Chinese darknet ecosystem.

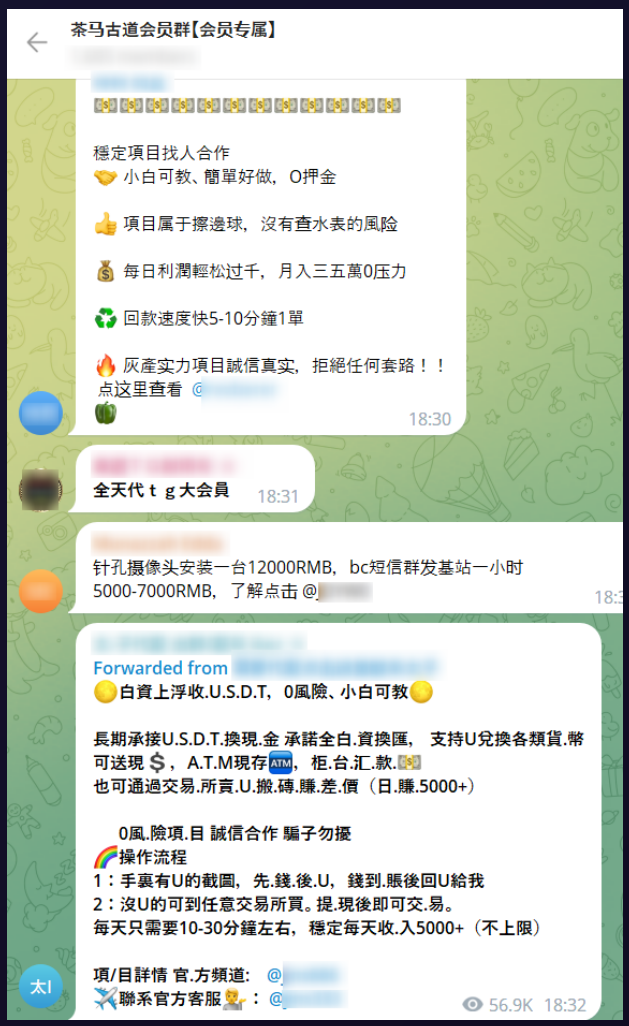


Screenshot of Exchange Market Homepage

Tea Horse Road Market (Telegram Channel)

Launched in April 2020, Tea Horse Road emerged as a prominent Chinese dark web marketplace, carving a niche for itself within the digital underground. Its operations, however, came to an abrupt halt in November 2021, marking the end of its approximately 19-month tenure. Following its sudden shutdown, remnants of its main page resurfaced in cybercrime combat reports, serving as a reminder of its once-active presence.

In the aftermath of Tea Horse Road Market's web platform closure, dedicated vendors of the platform have taken to alternative channels to sustain the community they once thrived in. Notably, these vendors have established Telegram channels directly linked to the market, utilizing them as virtual hubs to perpetuate their trade in various illicit goods and services. Through these Telegram channels, they maintain connections with fellow vendors and clientele, ensuring the continuation of their operations within the clandestine realm of the dark web.



Tea Horse Road Market Telegram Channel - Source: Webz

I love cracking (52pojie)

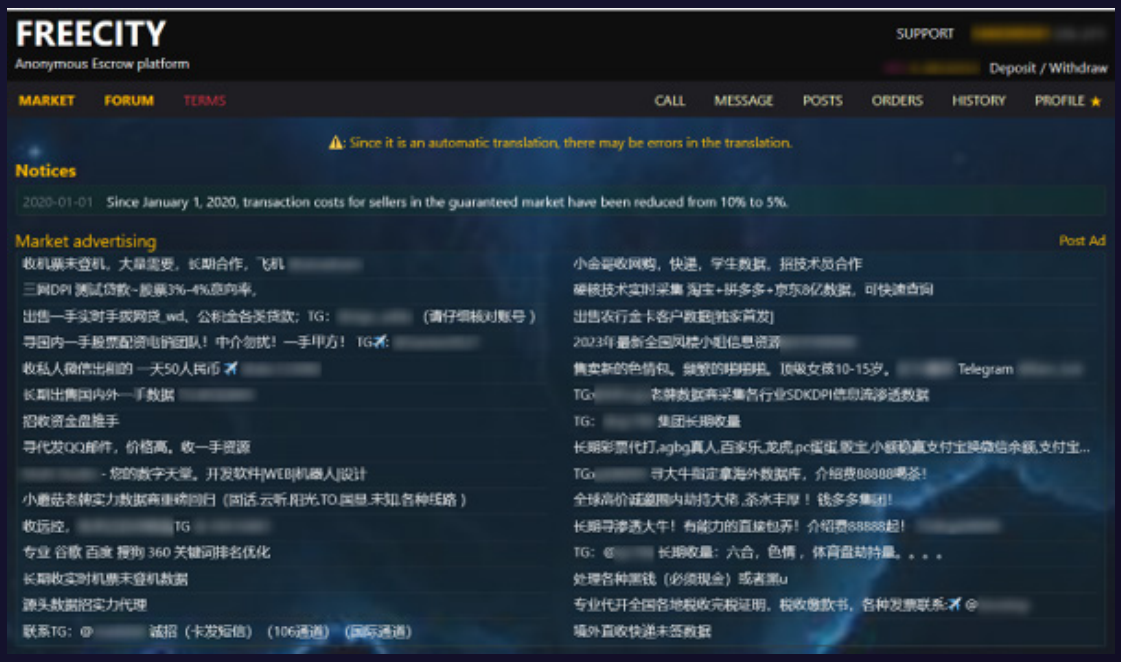
Dedicated to software security, particularly in the realm of hacking-related subjects like software encryption and decryption, I love cracking (52pojie) has cemented its status as a leading forum in its niche. Boasting a vibrant community and a wealth of insightful discussions, the forum has garnered acclaim for the exceptional quality of its content. Despite the inherently controversial nature of software cracking, the forum has flourished for over a decade, a testament to the proactive management of its admin team.

Throughout its tenure, I love cracking (52pojie) has remained steadfast in its mission, cultivating a dedicated following of users who appreciate its unwavering commitment to its core offerings. As a result, it has emerged as a key player in the Chinese cyber landscape, serving as a go-to platform for enthusiasts and professionals alike to engage in discussions on hacking-related topics.

Screenshot from "I love cracking (52pojie)" Homepage

FreeCity

> Operating in multiple languages including English, Chinese, and Korean, FreeCity is a versatile platform that caters to a diverse global audience. With its dual focus on forum discussions and marketplace transactions, the platform provides users with access to an extensive array of offerings, spanning from compromised accounts to tangible products. Despite the anonymity of its operators, FreeCity maintains an active presence on Telegram, serving as a hub for communication and coordination within its community.



Screenshot from FREECITY Homepage

Chang'An Sleepless Night

> Chang'An Sleepless Night has emerged as a prominent player in the dark web marketplace arena, garnering attention for its extensive range of offerings, which span from stolen data to specialized hacking services. What sets this platform apart is its user-friendly interface, coupled with the provision of escrow services and support for various cryptocurrencies, catering to the diverse needs of its user base.
>
> In addition to its marketplace operations, Chang'An Sleepless Night maintains an official Telegram channel, serving as a hub for user engagement and dissemination of updates. Through this channel, the platform has swiftly solidified its position as a trusted entity within the dark web community, fostering a sense of reliability and transparency among its users.

Screenshot from Chang'An Sleepless Night Homepage

SOCRadar's Dark Web Monitoring acts as a digital watchdog, scanning the hidden depths of the internet to detect threats and exposures. It keeps an eye on discussions and activities related to your organization among threat actors, tracking the unauthorized distribution of sensitive data. With real-time alerts and a comprehensive overview of potential risks, organizations can act swiftly to mitigate threats, guarding their data and reputation.

Spotlight On: Russian Cybercrime Ecosystem

With the Russian government reportedly exploring potential cyberattack options, it's evident that the landscape of Russian cybercrime is undergoing significant shifts. Past state-sponsored cyber activities from Russia have included DDoS attacks and the use of destructive malware against Ukrainian targets. Some cybercrime factions openly support the Russian government, threatening cyber operations in response to perceived aggression against Russia. Others have targeted nations aiding Ukraine. Meanwhile, other factions have attacked Ukrainian websites, likely in support of Russia's military campaign.

The Russian cybercrime landscape poses a complex challenge, from ransomware schemes to state-backed cyber espionage. Effective strategies to combat these threats require a thorough understanding of the ecosystem and its motivations in our interconnected world.

Influence of Russia - Ukraine War

> Since February 24, 2022, the Russian cybercriminal scene has seen significant changes due to the war in Ukraine. This conflict polarized threat actors in CIS (Commonwealth of Independent States) nations, with some aligning with the Russian government while others splintered over ideological differences or pursued financial gain amid geopolitical instability. This upheaval led to disruptions in underground markets, shifts in hacktivist and ransomware activities, and a rise in financial fraud within the Russian cybercriminal ecosystem.

"Cyber War: Russia - Ukraine" Source: Securin

Before the outbreak of the conflict, Russian-speaking threat actors generally avoided activities that would adversely affect or target former Soviet Union countries. However, this stance shifted with the onset of the war, notably exemplified by Conti Group's unequivocal declaration of allegiance to Russia.

Amidst these shifts, one constant factor has persisted: cybercriminal threat groups maintain significant direct, indirect, or implicit ties with the Russian government. These connections have deepened for cybercrime factions aligned with the Kremlin, often without explicit acknowledgment. Russian cybercriminals and self-professed hacktivists are actively engaged in operations aimed at Ukrainian entities and infrastructure, as well as targets in nations expressing solidarity with Ukraine. Recorded Future has observed Russian and Russian-speaking threat actors targeting various countries, including the United States, United Kingdom, North Atlantic Treaty Organization (NATO) members, Japan, and others, driven by financial motives and a quest for recognition supportive of Russia's interests.

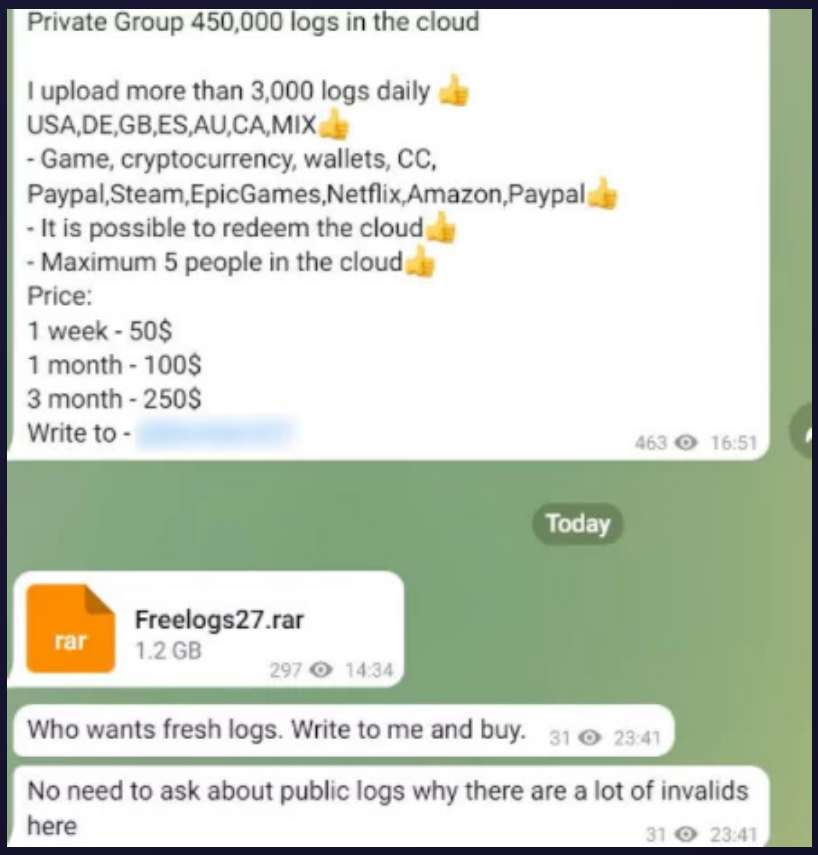
Dark Side of Telegram: The Hidden Hub of Cyber Threat Actors

> After the controversy surrounding WhatsApp's privacy policy in January 2021, resulting in a hefty fine of 225 million euros ($266 million) due to its lack of transparency regarding personal data handling under the reinforced European Union data protection law, Telegram, a widely used messaging platform, witnessed a significant increase in its user base. The disclosure of WhatsApp sharing confidential user data with Facebook prompted users to explore alternative messaging platforms, resulting in a migration towards apps like Telegram.
>
> Despite default encryption limited to communication between devices and Telegram servers (end-to-end encryption can be manually enabled), Telegram is renowned for its safety and encryption protocols. With estimated 1.562 billion total users and 800 million monthly active users in 2024, the app's appeal has skyrocketed.

Telegram: Cyber Crime's Channel of Choice - Generated by DALL-E

However, Telegram's widespread popularity has also made it a prime target for hackers, serving as a central hub for threat actors. Exploiting its legitimacy and large user base, threat actors have found ample opportunity to conceal their activities and carry out malicious deeds.

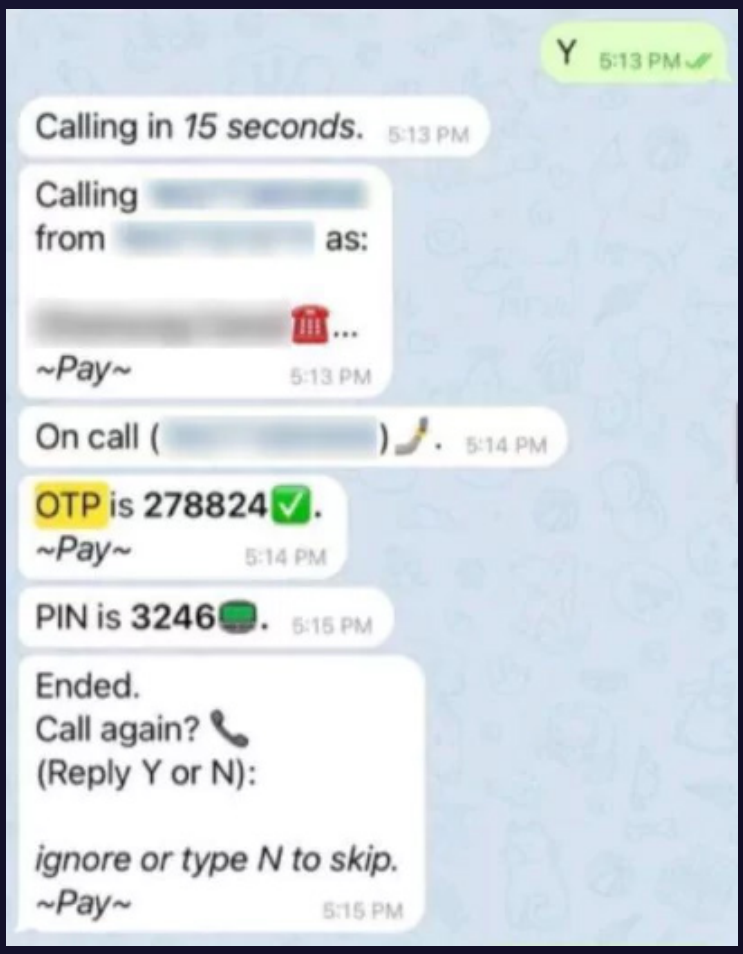
Cybercriminals leverage Telegram for a range of illicit activities, such as selling data dumps on Dark Web forums. These databases are often auctioned to the highest bidder for profit maximization. When faced with difficulties in selling the data, they resort to openly sharing it on platforms like hacker forums, Pastebin, and Telegram.



Private Data Leak Channel Advertisement in another Telegram Channel

In addition to data sales, Telegram serves as a hub for discussions on cyber attack tactics, emerging vulnerabilities, zero-days, cybersecurity events, and news. Threat actors utilize the platform to communicate with potential buyers of databases posted on Dark Web forums. This demonstrates Telegram's significance as a primary communication platform for cybercriminals.

> Telegram bots present cybercriminals with a versatile toolkit for automating malicious activities. For instance, leveraging Artificial Intelligence capabilities, certain bots execute sophisticated social engineering schemes, masquerading as reputable banks and businesses to pilfer OTP and SMS codes from unsuspecting users. Notably, OTP-Bot, a notorious Telegram bot, boasts a staggering 98% success rate in its OTP capture endeavors, indicative of its alarming efficacy. Below, you'll find an illustrative screenshot showcasing successful OTP-Bot attacks.



Successful OTP Bot Attack

Moreover, Telegram serves as an infection vector for malware deployment, facilitated by automated bots. These malware enable threat actors to infiltrate victim systems by establishing a connection to Command and Control (C2) servers.

Telegram Windows app Zero-day:

After the first week of April, there has been speculation within online communities, including X (Formerly, Twitter) and hacking forums, regarding a potential vulnerability affecting Telegram for Windows, allegedly enabling remote code execution. Contrary to initial claims suggesting a zero-click flaw, videos illustrating the purported security warning bypass and RCE vulnerability reveal user interaction through clicking on shared media to activate the Windows calculator.

Telegram swiftly addressed these assertions, asserting an inability to confirm the existence of such a vulnerability and suggesting the possibility of the video being a fabrication.

Telegram Messenger's claim on X (Formerly, Twitter) about the vulnerability

Subsequently, a proof of concept exploit surfaced on the XSS hacking forum the following day, elaborating on a coding error within the Telegram for Windows source code. This flaw purportedly allows the transmission of Python .pyzw files, circumventing security prompts upon clicking.

As a result, these files are executed automatically by Python without triggering Telegram's typical warning mechanisms, which would have occurred had it not been for the coding error.

SOCRadar actively monitors Telegram groups frequented by hackers and detects instances of data leaks affecting your organization. You can also visit our blog post for more information about Telegram, being used by threat actors.

Russian Government-backed APT Groups:

> Over time, Russia has been associated with numerous hacking groups, with notable names like "Fancy Bear" and "Cozy Bear," alongside alternative designations such as APT28 and APT29, frequently used by intelligence analysts. It's apparent that Russia maintains highly skilled groups engaged in offensive operations, some of which are linked to entities like the General Staff of the Armed Forces (GRU's 6th Directorate/Military Intelligence), the Foreign Intelligence Service (SVR), and the Federal Security Service (FSB).

Representative Image - Source: Business Insider

UAC-0056 (TA471, SaintBear, Lorec53):

> The UAC-0056 threat group, active since at least March 2021, has targeted government and critical infrastructure organizations in Georgia and Ukraine. While their interests align with the Russian government's, their state sponsorship remains unknown. Using spear phishing emails containing malicious Word documents or PDF files with links to ZIP archives embedded with malicious LNK files, UAC-0056 gains initial access. These files install first-stage malware loaders like the OutSteel document stealer and SaintBot loader, which fetch further payloads. Hosting their malicious payloads on Discord's content delivery network (CDN), UAC-0056 employs obfuscation and anti-analysis mechanisms. Amid heightened tensions between Russia and Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA) attributed UAC-0056 to an attack on a Ukrainian energy organization in February 2022. This attack, part of a larger campaign initiated in 2021, used spear phishing emails impersonating the National Police of Ukraine. UAC-0056's use of spoofing phishing techniques indicates a potential threat to European or United States companies.

UAC-0056's activities are notably focused on Ukraine, employing spoofing phishing tactics in their cyber offensives. This strategy holds the potential to extend beyond Ukrainian targets, posing risks to companies across Europe and the United States. The sectors and industries under UAC-0056's radar encompass government entities and the energy sector.

Methods: Spear Phishing Attacks Target Organizations in Ukraine. Payloads Include the Document Stealer OutSteel and the Downloader SaintBot

Toolset/Malware: WhisperGate wiper, Elephant Framework, Graphiron

Formation: 2021

Activities: 2022 Graphiron: Information Stealer Malware Deployed Against Ukraine
2022 UAC-0056 continues to target Ukraine in its latest campaign
2022 Spear Phishing Attacks Target Organizations in Ukraine

MITRE ATT&CK: https://attack.mitre.org/groups/G1003/

Sandworm Group (Electrum, Black Energy):

Sandworm, also known as ELECTRUM, Black Energy, and VOODOO BEAR, is a highly sophisticated APT group believed to be affiliated with Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455, according to the US. Since at least 2009, Sandworm has been actively involved in cyber operations aimed at advancing Russia's strategic interests.

Their tactics typically involve spear phishing to deliver malware and exploiting zero-day vulnerabilities. Sandworm's malicious activities have been observed across Europe, North America, and Asia, with a primary focus on targeting Industrial Control Systems (ICS) in critical sectors such as energy, utilities, national security, international affairs, and telecommunications globally. Despite their broad targeting, Ukraine appears to be their main objective, with multiple high-impact attacks on critical infrastructures occurring over the past decade.

You can visit our blog post for more information about the Sandworm Group.

Sandworm Group: Wanted by the FBI - Source: FBI

Methods: Spear Phishing Attacks Target Organizations in Ukraine. Payloads Include the Document Stealer OutSteel and the Downloader SaintBot

Toolset/Malware: ArguePatch, AWFULSHRED, BlackEnergy, CaddyWiper, Colibri Loader, Cyclops Blink, DarkCrystal RAT, Gcat, Industroyer2, ORCSHRED, P.A.S., PassKillDisk, PsList, RansomBoggs, SOLOSHRED, SwiftSlicer, VPNFilter, Warzone RAT, Living off the Land

Formation: 2009

Activities: 2023 Kyivstar Attack
2023 Russian Sandworm hackers breached 11 Ukrainian telcos
2023 The attack against Danish critical infrastructure

MITRE ATT&CK: https://attack.mitre.org/groups/G0034/

Venomous Bear (Snake, UNC4210, Turla):

> Venomous Bear, also referred to as Snake, UNC4210, Turla, Waterbug, or Uroburos, is a highly advanced APT group driven by espionage and intelligence-gathering objectives. Operating since the late 1990s, this group is considered one of the earliest pioneers of cyber espionage, focusing primarily on government entities, military organizations, and embassies.
>
> Attributed to the Russian Federal Security Service (FSB) on numerous occasions, Turla has established a formidable reputation for conducting cyber espionage campaigns across diverse sectors including high-tech, pharmaceuticals, and retail trade. Renowned for its stealth and adaptability, the group frequently modifies its tactics, techniques, and procedures (TTPs) to evade detection and maintain long-term access to targeted networks.

Turla Threat Actor Card - Source: SOCRadar

You can visit our blog post for more information about the Venomous Bear, aka Turla.

Methods: Spear Phishing Attacks, Watering Hole Attacks

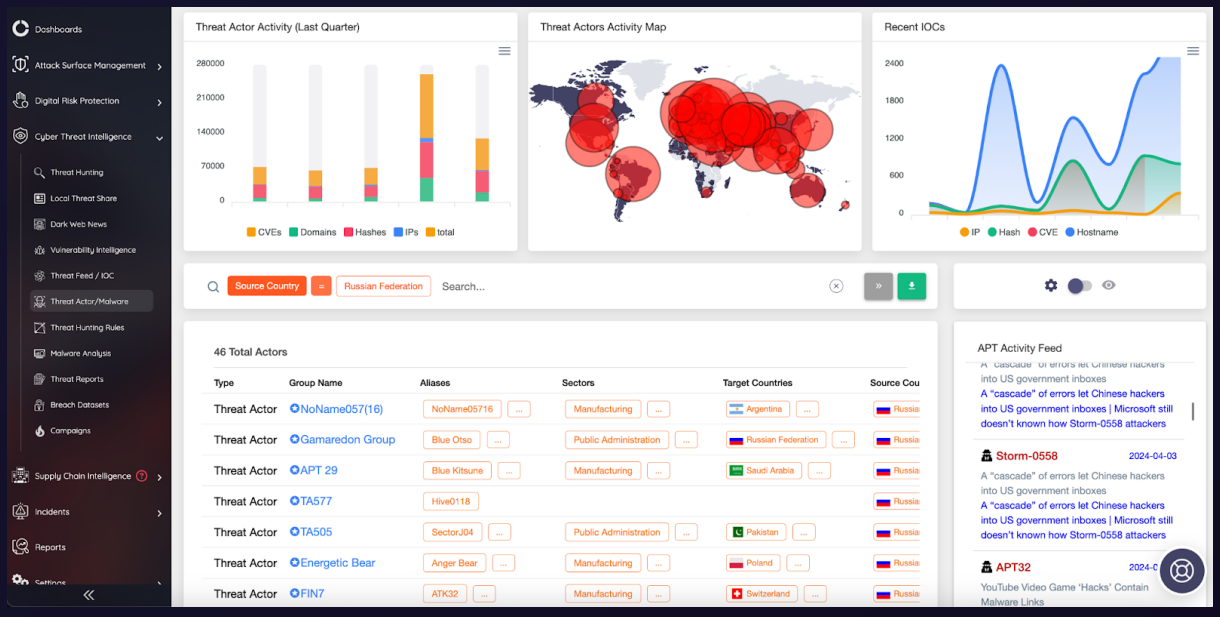
Toolset/Malware: systeminfo, net, tasklist, gpresult, wce, pwdump, Uroburos, Turla, Agent.BTZ, Tavdig, Wipbot, Agent.dne, AdobeARM, ATI-Agent, MiniDionis, WhiteBear, Gazer, Neuron, Nautilus

Formation: Late 1990s

Activities: 2023 Microsoft Exchange Servers Targeted by Turla
2023 Kazuar Backdoor used by Pensive Ursa (aka Turla)
2023 Turla APT spies on Polish NGOs

MITRE ATT&CK: https://attack.mitre.org/groups/G0010/

As we conclude, it's evident that staying informed about the strategies and activities of threat actors is paramount in safeguarding against cyber threats. SOCRadar's Threat Actor Tracking module offers a comprehensive solution to this challenge, providing real-time insights into the behaviors and tactics of known threat actors.



Request your demo now!

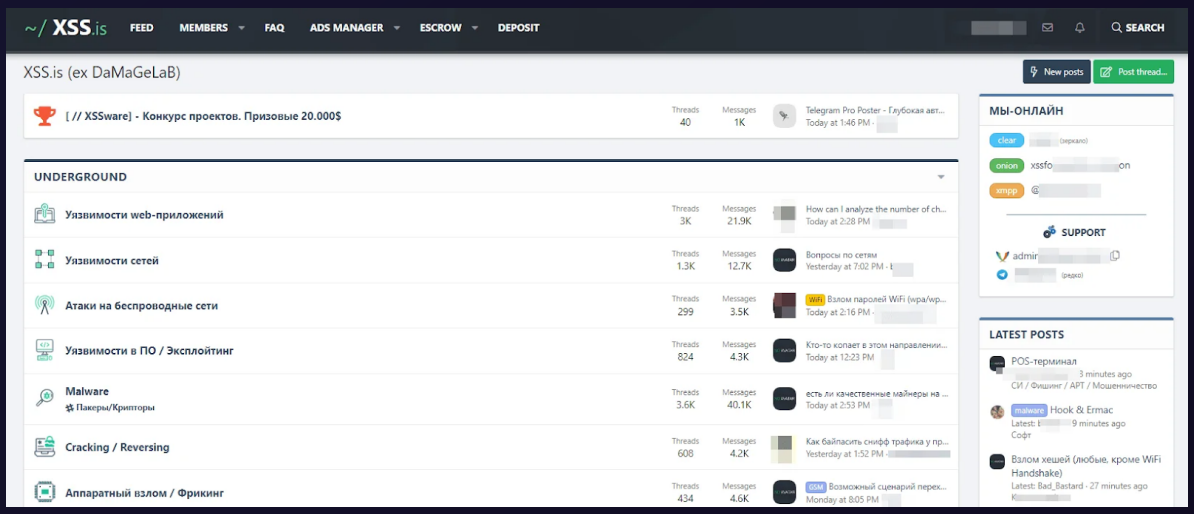
Top 5 Russian-Speaking Hacking Platforms

XSS.is

Since its inception in 2013, XSS.is has risen to prominence as a key player within the cybercriminal sphere. This Russian-speaking dark web forum, operating across both surface and dark web domains, serves as a secluded haven for threat actors and initial access brokers seeking anonymity and security. Renowned for its stringent measures against scammers and spammers, XSS.is has earned the trust of its users, establishing itself as a reliable hub for cybercriminal activities.

Setting itself apart with a plethora of security features, XSS.is prioritizes user anonymity by disabling IP address logs and encrypting private messages. Members of the forum benefit from access to valuable insights on credential access, exploits, and coveted zero-day vulnerabilities.

Moreover, XSS.is boasts exclusive private sections that require payment for entry, adding an air of exclusivity to its offerings. Notably, a significant development unfolded in 2021 when XSS.is took a bold stance against ransomware, prohibiting discussions on the topic despite its previous association as a hotspot for Ransomware-as-a-Service (RaaS) recruitment.



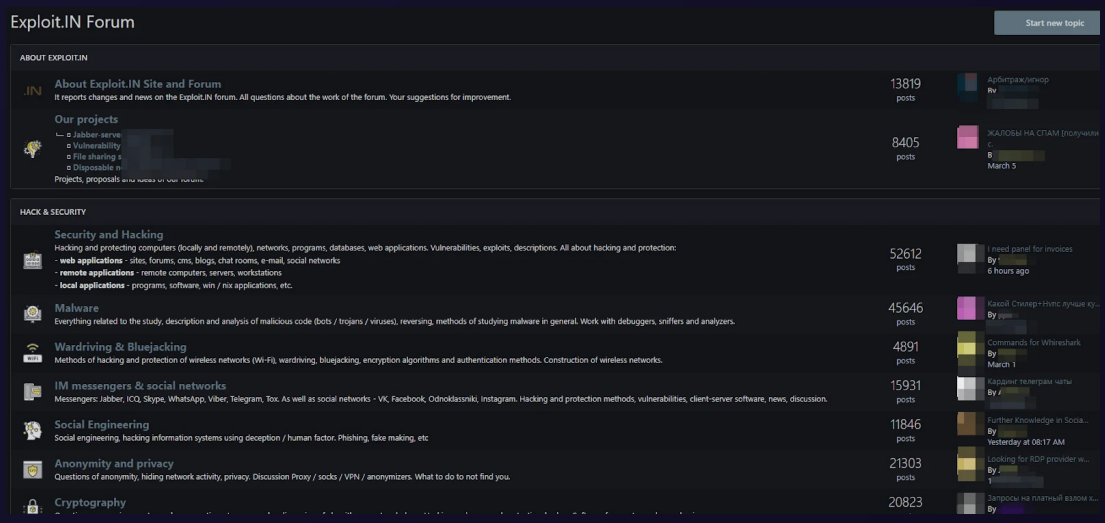
Screenshot from XSS.is Homepage

Exploit.in

Established back in 2005, Exploit.in has entrenched itself as a pivotal entity within the cybercriminal landscape, garnering widespread recognition among dark web forums. Renowned for its structured organization and rigorous membership protocols, this Russian-speaking dark web forum exudes professionalism and exclusivity, placing it in league with esteemed platforms like XSS.is.

Serving as a bustling hub of cybercriminal activity, Exploit.in offers an extensive range of services, ranging from auctions for initial access brokers to dedicated hacking forums and a marketplace teeming with illicit cybercrime tools and pilfered data. Notably, this marketplace has earned notoriety for facilitating the trade of stolen credit card information, malware strains, and sought-after zero-day exploits.

Moreover, Exploit.in serves as a vibrant knowledge-sharing platform for hacking and cyber activities, fostering an environment where users can exchange experiences and glean insights from one another. Operating predominantly in Russian, the forum accommodates access through standard internet browsers as well as the Tor browser for those delving into the depths of the dark web.



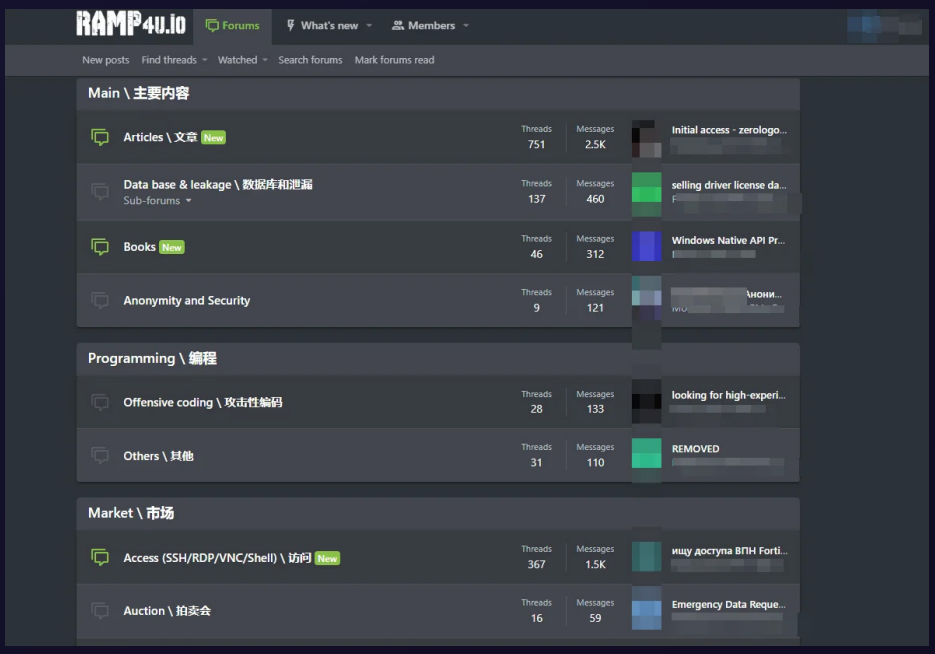
Screenshot from Exploit.in Homepage

RAMP

Emerging from the shadows of the cyber underworld, RAMP (Russian Anonymous Marketplace) has solidified its position as a notable player within the Russian-speaking dark web forum arena. Exclusive to the dark web, RAMP has garnered recognition for its distinctive approach to serving a predominantly Russian and Chinese clientele.

Setting itself apart from its counterparts, RAMP implements a unique membership system that requires more than just a straightforward application process. Prospective users must either possess active memberships on other dark web forums with a commendable reputation or be prepared to pay a fee for entry. This aura of exclusivity has cultivated an environment of trust and heightened engagement among its discerning user base.

Interestingly, despite its closure in 2017, RAMP experienced a resurgence in July 2021, marking its return to the forefront of the dark web landscape. Analysts attribute this revival and the subsequent surge in membership to the heightened scrutiny of ransomware groups following diplomatic discussions between Presidents Putin and Biden.



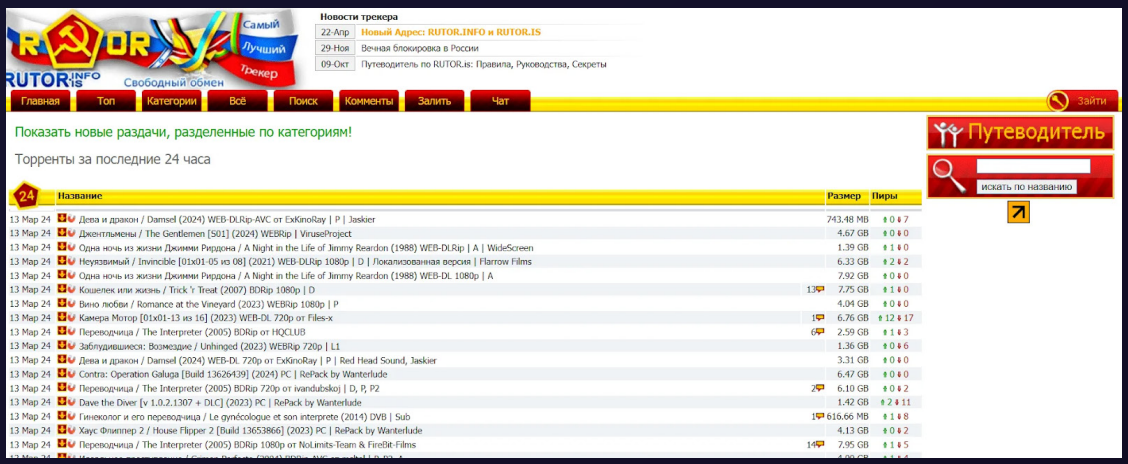
Screenshot from RAMP Homepage

RuTor

Since its establishment in 2015, RuTor, a Russian-speaking dark web forum, has emerged as a prominent player in the realm of cybercrime. Drawing inspiration from the layout of the now-defunct RAMP marketplace, RuTor provides users with a familiar interface featuring distinct sections dedicated to Vendor Shop Fronts, Security, and News.

Notably, RuTor's cryptomarket segment, overseen with strict control by the site administrator, has evolved into a trusted repository of cybersecurity news, corporate data breaches, and invaluable technical insights.

Following the takedown of the Hydra Market, RuTor experienced a surge in activity, swiftly transitioning from a forum to a bustling marketplace. The seamless integration of the OMGOMG marketplace into RuTor's platform underscores its adaptability in navigating the dynamic landscape of the dark web.



Screenshot from RuTor Homepage

CrdClub

Experiencing a significant breach in security on March 3, 2021, CrdClub, a prominent Russian-speaking dark web forum, fell victim to a scam that defrauded its users. However, in a display of their unwavering dedication to upholding user trust, the forum administrators promptly took action by offering reimbursement to those affected by the incident.

CrdClub serves as a central hub for a multitude of illicit activities, ranging from carding and real shopping with dumps to hacking ATMs and distributing trojans. Its content is meticulously organized into various sections, including Verified Services, International Forum, Forum for Russians, and a Freebie Section, catering to the diverse needs of its user base.

One notable aspect of CrdClub is its bilingual platform, accommodating users fluent in both Russian and English languages. This bilingual support enhances the forum's appeal and accessibility, drawing in a global audience of cybercriminals seeking to engage in nefarious activities. Established on July 8, 2016, CrdClub operates through an onion address, ensuring user anonymity, while surface web mirrors provide additional accessibility through standard web browsers.

Screenshot from CrdClub Homepage

Conclusion

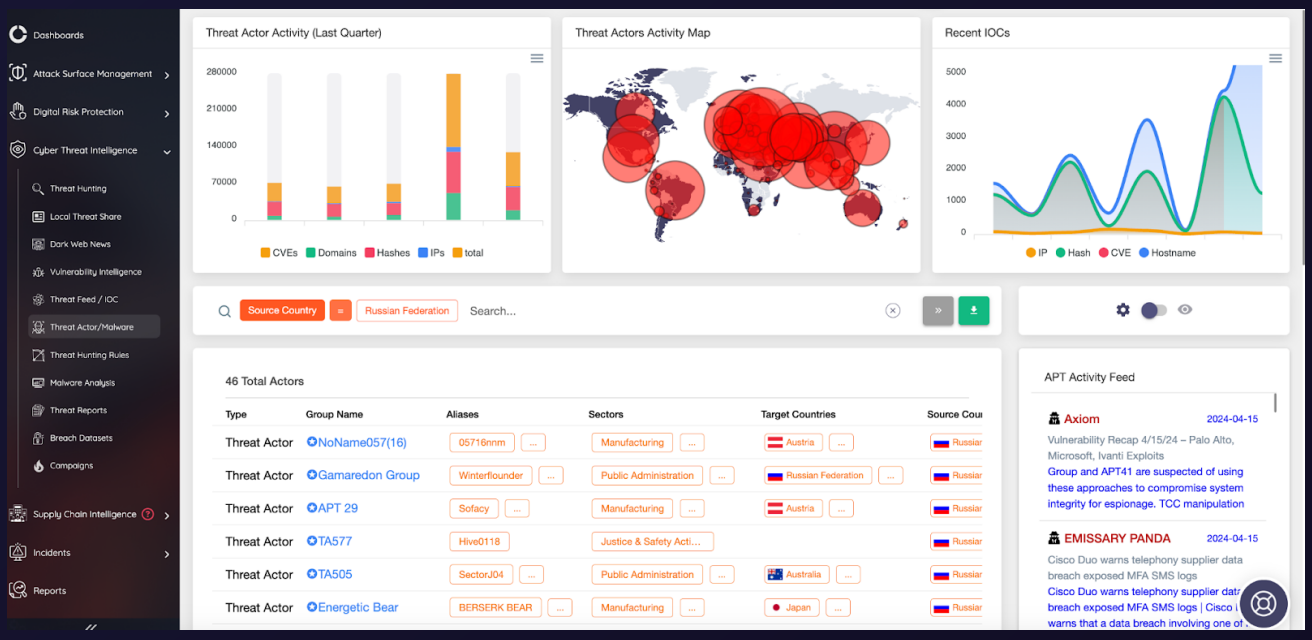
Based on our thorough analysis of the cybercrime landscapes in China and Russia presented in this report, it is evident that these nations play pivotal roles in the global cybersecurity arena, each posing distinct challenges and complexities.

China's cyber environment, characterized by government-backed APT groups and recent incidents like the i-SOON leak, highlights the intricate interplay between state-sponsored cyber activities and illicit cyber operations. The emergence of prominent Chinese-speaking hacking platforms underscores the increasing sophistication and organization of cybercrime within the country.

Similarly, Russia's cyber landscape is shaped by geopolitical tensions, as evidenced by the influence of the Russia-Ukraine war and the clandestine role of Telegram as a hub for cyber threat actors. The presence of government-backed APT groups and the proliferation of Russian-speaking hacking platforms further underscore the multifaceted nature of cyber threats originating from Russia.

In conclusion, our examination of the cybercrime ecosystems in China and Russia underscores the critical importance of international collaboration and robust cybersecurity measures in mitigating the evolving threats posed by state-sponsored actors and underground cybercriminal networks. As cyber threats continue to evolve and proliferate, a proactive and collaborative approach is imperative to safeguarding global digital infrastructure and protecting sensitive data against malicious actors.

As SOCRadar, we are committed to empowering our customers with preemptive strike capabilities through our comprehensive threat intelligence modules. By providing actionable insights and early warning indicators, we enable organizations to proactively identify and neutralize emerging threats before they manifest into full-scale attacks. Our innovative solutions equip businesses with the agility and resilience needed to stay ahead of adversaries in today's dynamic cyber landscape, ensuring the security and integrity of their digital assets.



Request your demo now!

Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

21.000+
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play

socradar.io

Gartner Peer Insights™ 4.8/5